HEALTH CARE AUTHORITY OF THE CITY OF ANNISTON

HIPAA COMPLIANCE PLAN

ADOPTED: APRIL_14, 2003

AMENDED: FEBRUARY 2011

AMENDED SEPTEMBER 1, 2012

AMENDED FEBRUARY 20, 2013

AMENDED MAY 30, 2013

AMENDED OCTOBER 26, 2016

AMENDED MARCH 20, 2017

AMENDED MAY 1, 2017

AMENDED AUGUST 20, 2018

AMENDED JUNE 1, 2021

AMENDED OCTOBER 1, 2021

AMENDED JUNE 1, 2022

AMENDED JUNE 1, 2024

AMENDED FEBRUARY 2, 2026

Any questions regarding this HIPAA Compliance Plan should be directed to either the Privacy Officer at (256) 235-5373 or the HIPAA Security Officer at (256) 235-5862

TABLE OF CONTENTS

RMC HEALTH SYSTE
HIPAA COMPLIANCE PLAN

ADOPTION OF THE REVISED COMPLIANCE PLAN

This Revised HIPAA Compliance Plan ("Compliance Plan") has been implemented to safeguard the confidentiality, security, and privacy of Protected Health Information ("PHI") as required by the Health Insurance Portability and Accountability Act of 1996, and its implementing regulations, as may be amended from time to time ("HIPAA"), and applicable state privacy laws.

The Regional Medical Center Board, a not-for-profit corporation, owns and operates Northeast Alabama Regional Medical Center, RMC Neurology, RMC Urology, Dr. Nwgo Cardiology, RMC Cardiology, physician clinics of Northeast Alabama Regional Medical Center, and (collectively referred to herein as "RMC" or "RMC Health System"). The Board has designated itself as a "hybrid" entity under HIPAA, with RMC as a health care component subject to the requirements of HIPAA and the RMC Foundation and the Wellness Connection excluded from HIPAA compliance. As a result, this Compliance Plan does not apply to the RMC Foundation or the Wellness Connection. Further, this Compliance Plan does not cover the activities of Regional Health Services, Inc., the Regional Health Management Corporation, or The Surgery Center, LLP.

All RMC employees, volunteers, trainees, independent contractors, and other persons whose conduct, in the performance of work for RMC, is under RMC's direct control (collectively, the "Workforce") will perform their duties and responsibilities with an uncompromising commitment to the policies, procedures, and guidelines set forth in this Compliance Plan. This "team approach" to HIPAA compliance will establish a culture at RMC that enhances the prevention, detection, and resolution of instances of conduct and behavior that do not conform to HIPAA and state privacy laws.

This Compliance Plan will be directed and implemented by a Privacy Officer and Security Officer, who are charged with reviewing the compliance policies and procedures, as well as addressing specific compliance issues that may arise at RMC.

Although implementation and enforcement of this Compliance Plan will be the direct responsibility of the Privacy Officer and Security Officer, ultimately compliance is the responsibility of all Workforce members of RMC. By virtue of implementing and enforcing this Compliance Plan, RMC is committed to ensuring that PHI is collected, handled, transmitted and stored in a manner which preserves its confidentiality and privacy in accordance with HIPAA and state privacy laws.

Keith Parrott
President and CEO

8-19-25
Date of Revision

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

DESIGNATION AS AN ORGANIZED HEALTH CARE ARRANGEMENT

The Health Care Authority of the City of Anniston, owns and operates ("we" or, "us"), hospitals and clinics. Hospitals and clinics Northeast Alabama Regional Medical Center, RMC Cardiology, RMC Neurology, RMC Urology, RMC Cardiology Dr. Nwogu and Stringfellow Campus of Northeast Alabama Regional Medical Center , d/b/a Northeast Alabama Regional Medical Center along with the Regional Health Management Corporation clinics and RMC Oxford Mediplex ,(collectively referred to herein ("The Health Care Authority"). is designated as an organized health care arrangement and as such will pursue compliance with HIPAA in accordance with that designation. As an organized health care arrangement, this Compliance Plan will cover The Health Care Authority, all of its employed health care providers and Workforce members, including, but not limited to, the following classes of persons to the extent they provide services at The Health Care Authority: Physicians; Dentists; Podiatrists; Optometrists; Physical, Occupational, Respiratory and Speech Therapists and Assistants; Rehabilitation Attendants; Dietary Consultants; Nurses; Psychologists and Social Workers/Consultants; Hospice Workers; Pharmacists; Medical Equipment Suppliers; Diagnostic Providers; Physician Assistants; Lab Technicians; Allied Health Professionals, Students, Volunteers and other health care providers. (These individuals may or may not be employees of The Health Care Authority)

All non-employee and non-Workforce members who provide treatment services at The Health Care Authority will be included in The Health Care Authority's organized health care arrangement and shall receive an *Acknowledgment of Participation in an Organized Health Care Arrangement* form. If such individual decides to opt-out of participation in the organized health care arrangement the Privacy Officer will take the necessary steps to ensure HIPAA compliance by that individual at The Health Care Authority ➢ **Form: Acknowledgment of Participation in an Organized Health Care Arrangement**

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PURPOSE OF THE HIPAA COMPLIANCE PLAN

Our Compliance Plan is reasonably designed, implemented and enforced so that it is effective in preventing, detecting, and remedying the improper use and disclosure of PHI. The specific purposes of our Compliance Plan are:

- To assist us in identifying PHI, and the manner in which it is to be used and disclosed;
- To assist us in avoiding improper uses and disclosures of PHI;
- To establish compliance standards and procedures for members of our Workforce that are reasonably capable of reducing the prospect of violating HIPAA;
- To appoint a Privacy Officer who is a high-level and trustworthy employee, with responsibility to implement and oversee our compliance with the standards and procedures set forth in this Compliance Plan and as required by the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, as may be amended, modified, or superseded, from time to time ("Privacy Rules");
- To appoint a Security Officer who is a high-level and trustworthy employee, with responsibility to implement and oversee our compliance with the standards and procedures set forth in this Compliance Plan and as required by the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160, 162, and 164, as may be amended, modified, or superseded from time to time ("Security Rules");
- To effectively communicate the compliance standards, policies and procedures set forth in this Compliance Plan to all members of our Workforce by, for example, conducting training and disseminating publications and other materials that explain in a practical manner the HIPAA standards and procedures to be followed;
- To take reasonable steps to achieve compliance with the standards, policies and procedures set forth in this Compliance Plan by, for example, implementing, monitoring, and auditing systems reasonably designed to detect the improper use and disclosure of PHI;
- To establish and publicize a reporting system so that members of our Workforce can report perceived wrongful uses and disclosures of PHI by others without fear of retribution; and
- To respond appropriately to non-compliance after detection and to prevent recurrence, which may require modifications to this Compliance Plan.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

ADHERENCE TO AND SAFEGUARDING THE HIPAA COMPLIANCE PLAN

All members of our Workforce must carry out their duties and responsibilities in accordance with this Compliance Plan. Strict compliance with the Compliance Plan is a condition of employment or otherwise providing services for The Health Care Authority. We will take disciplinary action up to, and including, termination for violation of our HIPAA policies and procedures.

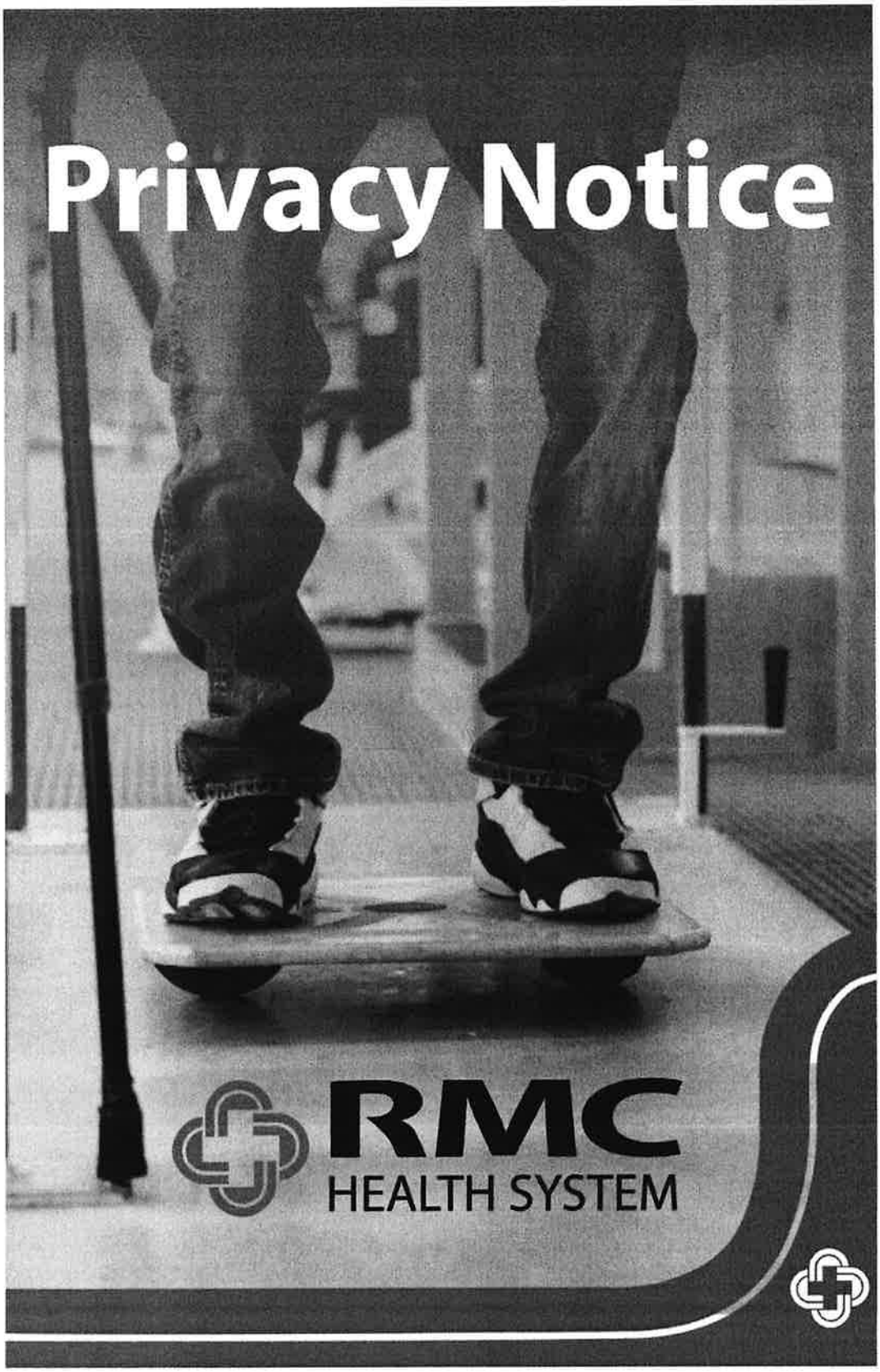
> *The promotion of and adherence to the regulatory laws and standards of conduct set forth in this Compliance Plan will be an element in the job evaluation of all members of our Workforce.*

All members of our Workforce must sign an *Acknowledgment of a HIPAA Compliance Plan* acknowledging their obligation to protect and safeguard health information in accordance with the terms of this Compliance Plan and applicable law.

All members of our Workforce will be instructed to address with their supervisor, the Privacy Officer, or the Security Officer any questions regarding the information provided in this Compliance Plan, or the scope or application of HIPAA. All compliance concerns from individuals will be investigated and documented by the Privacy Officer, Security Officer, or his/her designee. Our Privacy Officer will maintain the records of all HIPAA-related investigations.

This Compliance Plan is specifically tailored to the needs and processes of The Health Care Authority and contains sensitive and confidential information, which if disclosed to outside third parties, could harm our organization. Therefore, members of our Workforce must not disclose this Compliance Plan, or any of its terms or conditions, to any third-party without the express, written consent of the President and CEO.

- **Form: Acknowledgment of HIPAA Compliance Plan**


Privacy Notice
RMC
HEALTH SYSTEM

The Health Care Authority of the City of Anniston
400 East Tenth Street
Anniston, Alabama 36207
WWW.RMCCARES.ORG

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED; HOW YOU CAN ACCESS YOUR INFORMATION; YOUR RIGHTS WITH RESPECT TO YOUR HEALTH INFORMATION; AND HOW TO FILE A COMPLAINT CONCERNING A VIOLATION OF THE PRIVACY OR SERCURITY OF YOUR HEALTH INFORMATION OR OF THE RIGHTS CONCERNING YOUR HEALTH INFORMATION. PLEASE REVIEW IT CAREFULLY. YOU HAVE THE RIGHT TO OBTAIN A COPY OF THIS NOTICE AND TO DISCUSS IT WITH OUR PRIVACY OFFICER AT (256) 235-5373 OR PRIVACY@RMCCARES.ORG IF YOU HAVE ANY QUESTIONS.

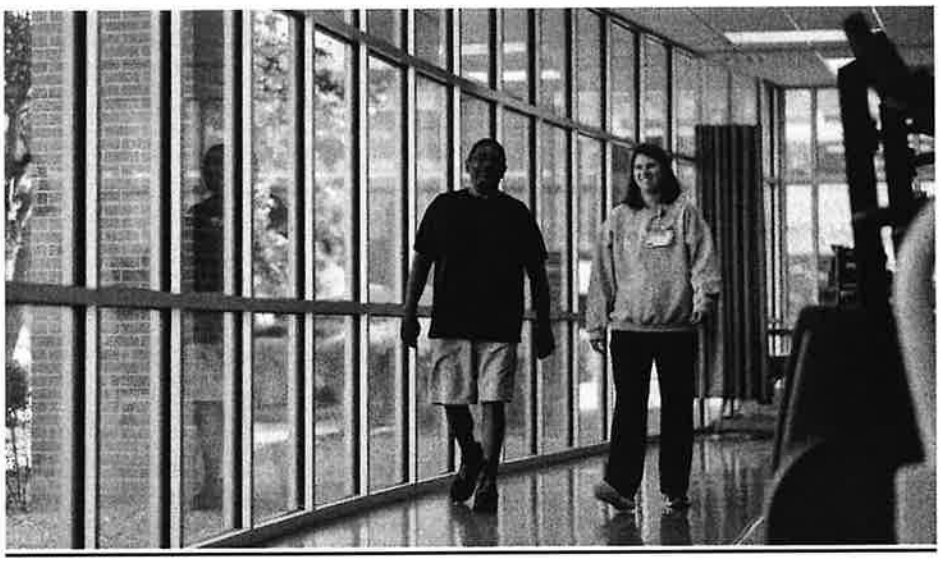
THE EFFECTIVE DATE OF THIS PRIVACY NOTICE IS APRIL 14, 2003, AS AMENDED ON FEBRUARY 2011, SEPTEMBER 1, 2012, FEBRUARY 20, 2013, MAY 30, 2013, OCTOBER 2016, MARCH 20, 2017, MAY 1, 2017, AUGUST 20, 2018, JUNE 1, 2021, OCTOBER 1, 2021, JUNE 1, 2022, AND FEBRUARY 16, 2026.

PRIVACY NOTICE

The Health Care Authority of the City of Anniston owns and operates ("we" or "us") hospitals and physician practices and clinics. This notice covers the hospitals, physician offices or clinics and the health care providers listed on the last page that may provide services to you at the hospitals, physician offices or clinics. We are part of an organized health care arrangement ("OHCA"). This Privacy Notice is a joint notice that covers the functions of the OHCA and any health care professional working within the hospitals, physician offices or clinics.

We are required under the Health Insurance Portability and Accountability Act of 1996, the Health Information Technology for Economic and Clinical Health Act, and their implementing regulations, as may be amended from time to time (collectively, "HIPAA"), to protect the privacy of your health information, which includes information about your health history, symptoms, test results, diagnoses, treatment, and claims and payments history (collectively, "Health Information"). We are also required under 42 C.F.R. Part 2 to protect the privacy of Health Information found in substance use disorder ("SUD") records created or maintained by us. We are required to provide you with this Privacy Notice regarding our legal duties, policies and procedures to protect and maintain the privacy of your Health Information. This Privacy Notice will be posted in prominent locations and will be posted on our website.

We are required to follow the terms of this Privacy Notice unless (and until) it is revised. We reserve the right to change the terms of this Privacy Notice and to make the new notice provisions effective for all Health Information that we maintain and use, as well as for any Health Information that we may receive in the future. Should the terms of the Privacy Notice materially change, we will make a revised copy of the Privacy Notice available to you. Revised Privacy Notices will be available for individuals to take with them, and we will post a copy of the revised Privacy Notice in a prominent location. Revised Privacy Notices will also be posted and made available electronically on our website.



PERMITTED USES AND DISCLOSURES OF YOUR HEALTH INFORMATION.

1. **General Uses and Disclosures.** Under applicable law, we are permitted to use and disclose your Health Information for the following purposes and in support of the following, without obtaining your permission or Authorization, unless more stringent state or federal laws, including 42 C.F.R. Part 2, apply:

- **Treatment.** We are permitted to use and disclose your Health Information in the provision and coordination of your health care. For example, we may disclose your Health Information to your physician and to other health care providers who have a need for such information for your care and treatment.

- **Payment.** We are permitted to use and disclose your Health Information for the purpose of determining coverage, billing, and reimbursement. This information may be released to Medicare, an insurance company, a third party payer, or other authorized entity or person involved in the payment of your medical bills and may include copies or portions of your medical record which are necessary for payment of your bill. For example, a bill sent to your insurance company may include information that identifies you, your diagnosis, and the procedures and supplies used in your treatment. We may also disclose medical information about you to the responsible party of your account. If you are listed as a dependent on another person's insurance policy or if another person is financially responsible for your account, financial information regarding medical care provided to you may be disclosed to the responsible party.

- **Health Care Operations.** We are permitted to use and disclose your Health Information for certain administrative, legal and quality improvement activities that are necessary to run our facilities and to support our functions of treatment and payment, including, but not limited to: quality assurance, auditing activity, credentialing activity, licensing activity, and for educational purposes. For example, we can use your Health Information to internally assess the quality of care we provide.

- **Health Care Providers Working in the OHCA.** The hospitals and physician clinics listed on the last page and the various health care providers who render services to you are part of an "organized health care arrangement." These providers have agreed, as permitted by applicable law, to share your Health Information among themselves as necessary to carry out treatment, payment and/or health care operations. This enables us to better address your health care needs.

- **Uses and Disclosures Required by Law; Judicial and Administrative Proceedings; Law Enforcement Purposes.** We may use and disclose your Health Information when required to do so by law, including disclosure to the Department of Health and Human Services. We may also disclose your Health Information in judicial and administrative proceedings, as well as in response to an order of a court, administrative tribunal, or in response to a subpoena, summons, warrant, discovery request, or similar legal request. We may disclose your Health Information to law enforcement officials when required to do so by law, including, but not limited to reporting abuse, neglect and domestic violence or to alert law enforcement to criminal conduct on our premises or of a death that may be the result of criminal conduct.

- **Public Health Activities.** We may disclose your Health Information for public health reporting, including, but not limited to: reporting child abuse and neglect; reporting communicable diseases and vital statistics; reporting product recalls and adverse events; or notifying person(s) who may have been exposed to a disease or are at risk of contracting or spreading a disease or condition.

- **Abuse, Neglect, or Domestic Violence.** We may disclose your Health Information to a local, state, or federal government authority if we have a reasonable belief that abuse, neglect or domestic violence has occurred.

- **Regulatory Agencies.** We may disclose your Health Information to a health care oversight agency for activities authorized by law, including, but not limited to, licensure, investigations and inspections. These activities are necessary for the government and certain private health oversight agencies to monitor the health care system, government programs, and compliance with civil rights. We may be required to disclose protected patient health information to the Secretary of the Department of Health and Human Services.

- **Coroners, Medical Examiners, Funeral Directors.** We may disclose your Health Information to a coroner or medical examiner. This may be necessary, for example, to determine a cause of death. We may also disclose your health information to funeral directors, as necessary, to carry out their duties.

- **Organ or Tissue Donations.** We may disclose your Health Information to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue.

- **Research.** Under certain circumstances, we may disclose your Health Information to researchers when their clinical research study has been approved and where certain safeguards are in place to ensure the privacy and protection of your Health Information.

- **Avert Threats to Health and Safety.** We may use or disclose your Health Information if we believe, in good faith, that the use or disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public or is necessary for law enforcement to identify or apprehend an individual.

- **Specialized Government Functions.** We may disclose your Health Information to authorize federal officials for national security reasons and the Department of State for medical suitability determinations. We may also disclose your Health Information to authorized federal officials for the provision of protective services to the President of the United States or to foreign heads of state or to conduct related investigations. If you are a member of the U.S. Armed Forces, we may disclose your Health Information as required by military command authorities.

- **Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release your Health Information to the correctional institution or law enforcement official, where such information is necessary for the institution to provide you with health care; to protect your health or safety, or the health or safety of others; or for the safety and security of the correctional institution.

- **Workers' Compensation.** We may disclose your Health Information as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs that provide benefits for work-related injuries or illnesses without regard to fault.

Marketing. We may use or disclose your Health Information to make a marketing communication that occurs in a face-to-face encounter with us, or which concerns a promotional gift of nominal value provided by us.

- **Fundraising.** We may use or disclose your Health Information to make a fundraising communication to you for the purpose of raising funds for our own benefit. With each fundraising communication, we will provide you with an opportunity to elect not to receive any further fundraising communication. We will also make reasonable efforts to ensure that if you opt out of such communications you are not sent future fundraising communications. We may also use, or disclose to a business associate or to an institutionally related foundation, the following Health Information for the purpose of raising funds for our own benefit: (a) demographic information relating to you, including your name, address, other contact information, age, gender, and date of birth; (b) the dates of health care provided to you; (c) the department or area of service that provided you treatment; (d) your treating physician; (e) outcome information; and (f) your health insurance status.

- **Refill Reminders, Care Coordination, Alternative Therapies.** We may provide you with refill reminders about a drug or biologic that is currently being prescribed for you, but only if any financial remuneration received by us in exchange for making the communication is reasonably related to our cost of making the communication. Except where we receive financial remuneration in exchange for making the communication, we may communicate with you for the following treatment and health care operations purposes: (a) for your treatment including case management or care coordination, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care; (b) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits, including communications about a health care provider network or health plan network; replacement of or enhancements to, a health plan; and or (c) for case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities are not considered treatment.

- **Business Associates.** Other individuals and companies provide management assistance and other services to us. Under HIPAA, these individuals and companies are called Business Associates. We may disclose your Health Information to Business Associates who provide services to us. Our Business Associates are required to protect the confidentiality of your Health Information.

- **Other Uses and Disclosures**. In addition to the items outlined above, we may use and disclose your Health Information (without your written permission) for other purposes permitted by applicable state and federal law.

- **We can with your consent and phone number**-Text you results of your tests.

2. **Uses and Disclosures Which Require an Opportunity to Verbally Agree or Object.** Under HIPAA, we are permitted to use and disclose your Health Information: (i) for the creation of facility directories, (ii) to disaster relief agencies, and (iii) to family members, close personal friends or any other person identified by you, if the information is directly relevant to that person's involvement in your care or treatment. Except in emergency situations, you will be notified in advance and have the opportunity to verbally agree or object to this use and disclosure of your Health Information.

3. **Uses and Disclosures Which Require Written Authorization.** As required by applicable law, all other uses and disclosures of your Health Information (not described above) will be made only with your written permission, which is called an Authorization. For example:

   - **Psychotherapy Notes.** If we maintain psychotherapy notes, we must obtain your Authorization for any use or disclosure of such psychotherapy notes, except: to carry out the following treatment, payment, or health care operations: (a) use by the originator of the psychotherapy notes for treatment; (b) use or disclosure by us for our own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or (c) use or disclosure by us to defend ourselves in a legal action or other proceeding brought by you.
   - **Certain Marketing Purposes.** If we receive financial remuneration in exchange for making a marketing communication, we must obtain your Authorization for any use or disclosure of protected health information other than a face-to-face communication made by us to you, or for a promotional gift of nominal value provided by us.
   - **Sale of Health Inform.** We must obtain your Authorization for any sale of your Health Information and such Authorization will state that the disclosure will result in our receiving remuneration.

4. **Uses and Disclosures Under Other Applicable Laws.** To the extent other applicable state or federal laws, such as 42 C.F.R. Part 2, provide more stringent requirements regarding the protection of your Health Information, we will also abide by those requirements.

5. **Revoking Your Authorization.** You may revoke your Authorization in writing at any time. The revocation of your Authorization will be effective immediately, except to the extent that: we have relied upon it previously for the use and disclosure of your Health Information; if the Authorization was obtained as a condition of obtaining insurance coverage where applicable law provides the insurer with the right to contest a claim under the policy or the policy itself; or where your Health Information was obtained as part of a research study and is necessary to maintain the integrity of the study.

   Potential for Redisclosure. Please note that information disclosed as described herein may be subject to redisclosure by the recipient without your consent and may no longer be protected by state or federal law.

PATIENT RIGHTS.

You have the following rights concerning your Health Information:

1. **Right to Receive Written Notification of a Breach of Your Unsecured Health Information.** You have the right to receive written notification of a breach of your unsecured Health Information if it has been accessed, used, acquired, or disclosed in a manner not permitted by applicable law, which compromises the security or privacy of your Health Information. We will provide this notification by first-class mail or, if necessary, by such other substituted forms of communication allowable by law or you may request in writing to receive a notification of a breach by electronic mail.

2. **Right to Inspect and Copy Your Health Information.** Upon written request, you have the right to inspect and copy your own Health Information contained in a designated record set maintained by or for us. A "designated record set" contains medical and billing records and any other records that we use for making decisions about you. You may also request that we transmit a copy of such Health Information to a designated third-party, provided the designation is clear, specific, and contained in a writing signed by you. Under most circumstances, a request will be responded to within 30 days. However, we are not required to provide you access to all the Health Information that we maintain. For example, this right of access does not extend to psychotherapy notes, or information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative proceeding. Instead of copies, we can provide you with a summary of your Health Information if you agree to the form and cost of such summary. We may charge you a reasonable cost-based fee for your copies, which may include copying costs, supplies, postage, and other costs associated with preparing a summary or explanation. We may, in some cases, deny your request to inspect and copy your Health Information and will notify you in writing of the reasons for our denial and provide you with information regarding your rights to have our denial reviewed. Where permitted by HIPAA, you may request that we review certain denials to inspect and copy your Health Information.

3. **Right to Request Restrictions on the Use and Disclosure of Your Health Information.** You have the right to request restrictions on the use and disclosure of your Health Information for treatment, payment and health care operations. We will consider, but do not have to agree to, such requests in all circumstances. However, we must agree to restrict a disclosure of Health Information about you to a health plan if: (a) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law; and (b) the Health Information pertains solely to a health care item or service for which you, or someone other than the health plan on your behalf, has paid in full.

4. **Right to Request an Amendment of Your Health Information.** You have the right to request an amendment of your Health Information. We may deny your request if we determine that you have asked us to amend information that: was not created by us, unless the person or entity that created the information is no longer available; is not Health Information maintained by or for us in a designated record set; is Health Information that you are not permitted to inspect or copy; or we determine that the information is accurate and complete. If we disagree with your requested amendment, we will provide you with a written explanation of the reasons for the denial, an opportunity to submit a statement of disagreement, and a description of how you may file a complaint.

5. **Right to an Accounting of Disclosures of Your Health Information.** You have the right to receive an accounting of disclosures of your Health Information made by us. With respect to Health Information contained in paper form, our accounting will not include: disclosures related to treatment, payment or health care operations; disclosures to you; disclosures based upon your Authorization; disclosures to individuals involved in your care; incidental disclosures; disclosures to correctional institutions or law enforcement officials; disclosures for facility directories; disclosures that are part of a Limited Data Set; or disclosures that occurred prior to April 14, 2003 or as otherwise allowed by HIPAA. With respect to Health Information contained in an electronic health record, unless otherwise specified by law, the accounting will not contain disclosures made to you upon your request; based upon your Authorization; to individuals involved in your care; or as allowed by law. You may request an accounting of applicable disclosures made by us within six (6) years prior to the date of your request for Health Information stored in paper form and made within three (3) years prior to the date of your request (but not for any disclosures made prior to implementation of our electronic health records system) for Health Information stored in an electronic health record. If you request an accounting more than once in a 12-month period, we may charge you the reasonable cost-based expenses incurred to comply with your additional request.

6. **Right to Alternative Communications.** You have the right to receive confidential communications of your Health Information by a different means or at a different location than currently provided. For example, you may request that we only contact you at home or by mail. Such requests should be made in writing.

7. **Right to Receive a Paper Copy of this Privacy Notice.** You have the right to receive a paper copy of this Privacy Notice upon request, even if you have agreed to receive this Privacy Notice electronically.

NOTICE OF MORE STRINGENT RIGHTS CONCERNING SUBSTANCE USE DISORDER RECORDS.

1. **42 C.F.R. Part 2.** The aforementioned provisions regarding the use and disclosure of your Health Information and patient rights apply unless more stringent state or federal laws apply. In certain circumstances, 42 C.F.R. Part 2 applies more stringent requirements than HIPAA with regard to the use and disclosure of Health Information contained in SUD records created or maintained by us. With regard to SUD records, the following additional rights and obligations apply:

- We must obtain your written consent to use or disclose: (a) your SUD treatment records received from a Part 2 program, or (b) testimony relaying the content of your SUD treatment records, in either case when the use or disclosure is in the context of a civil, criminal, administrative or legislative proceeding against you. Alternatively, we may use and disclose such SUD treatment records with a court order accompanied by a subpoena or other legal requirement compelling disclosure, provided that you have first been provided notice and an opportunity to be heard as required by 42 C.F.R. Part 2.

- Except in the case of a medical emergency, we must obtain your written consent for uses and disclosures of SUD records for purposes of treatment, payment, and health care operations. Such consent may be obtained through a single consent for all future uses that remains in effect until revoked in writing.

- We must obtain your written consent before using or disclosing SUD counseling notes, which are notes recorded (in any medium) by a SUD or mental health professional documenting or analyzing the contents of conversations during a counseling session and that are separated from the rest of the medical record.

- Before we use your SUD records for fundraising purposes, we will provide you with the opportunity in advance to opt-out of receiving any fundraising communications by submitting an opt-out request to the Privacy Officer as indicated below.

CONTACT INFORMATION AND HOW TO REPORT A PRIVACY RIGHT VIOLATION.

If you want to exercise any of these rights, have any questions, or feel that your privacy rights have been violated, please contact us. All requests must be submitted to us in writing and returned to the address below.

The Health Care Authority of the City of Anniston
400 East Tenth Street
P.O. Box 2208
Anniston, Alabama 36202
Attn: Privacy Officer
Telephone: (256) 235-5373
E-mail: Privacy@rmccares.org

If you believe that your privacy rights have been violated or that we have violated our own privacy practices, you may file a complaint with us. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services. Our Privacy Officer can provide you with the address. Complaints filed directly with the Secretary must be made in writing, name us, describe the acts or omissions in violation of applicable law or our privacy practices, and must be filed within 180 days of the time you knew or should have known of the violation. Complaints submitted directly to us must be in writing and sent to the attention of our Privacy Officer. There will be no retaliation for filing a complaint.

The following health care providers may provide services to you as part of our organized health care arrangement and are covered by this Privacy Notice: Physicians; Dentists; Podiatrists; Optometrists; Physical, Occupational, Respiratory and Speech Therapists and Assistants; Rehabilitation Attendants; Dietary Consultants; Nurses; Psychologists and Social Workers; Hospice Workers; Pharmacists; Medical Equipment Suppliers; Diagnostic Providers; Lab Technicians and Providers; Physician Assistants; Allied Health Professionals; Students; Volunteers and other health care providers. These individuals may not all be employees.

The Healthcare Authority of the City of Anniston is comprised of the following hospital and physician clinics: Northeast Alabama Regional Medical Center, Stringfellow Campus of Northeast Alabama Regional Medical Center, RMC Neurology, RMC Urology, RMC Cardiology, RMC Cardiology II Dr. Nwogu, the Oxford Mediplex Oxford Family Practice, Anniston Family Practice, Dr. Shubair, Dr. Hixon, Surgery Group and Jacksonville Family Medicine and includes physician offices that are operated by Regional Medical Center and Regional Health Management Corporation.

BY SIGNING BELOW, I HEREBY ACKNOWLEDGE RECEIPT OF THIS NOTICE OF PRIVACY PRACTICES.

_____ _____

Printed Name of Patient Date

_____

Signature of Patient

_____

Printed Name of Parent/Patient's Representative (If Applicable)

_____

Signature of Parent/Patient's Representative (If Applicable)

_____

Representative's Relationship to Patient (If Applicable)

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PRIVACY OFFICER JOB DESCRIPTION

Job Class: PRIVACY OFFICER

Appointment: The Privacy Officer is a high-level and trustworthy employee. Reasonable inquiries into the prior conduct and background of the appointed individual should be made and it should be determined that the appointed individual is qualified to serve as The Health Care Authority's Privacy Officer.

Position Summary:

The Privacy Officer is responsible for the overall implementation and operation of the privacy of PHI, and shall have authority to review all documents and other information relevant to privacy activities, including, but not limited to, patient records, billing records, and records concerning arrangements with other parties, including employees, independent contractors, physicians, agents, suppliers, business associates, etc.

Privacy activities are a significant component of the Privacy Officer's job description, and therefore his/her performance will be judged, in part, on privacy compliance activity and the effectiveness of such activity.

Essential Job Functions:

- To assist us with the development of our Compliance Plan, which sets forth the legal and ethical standards, policies and procedures to be followed by members of our Workforce;
- To implement and enforce the standards, policies and procedures set forth in our Compliance Plan to ensure our compliance with the Privacy Rules, state privacy laws, and applicable business and professional ethical policies;
- To keep apprised of changes to the Privacy Rules and state privacy laws. As part of this responsibility, the Privacy Officer will keep track of new regulatory developments, including new HIPAA bulletins and initiatives, much of which can be found at: http://www.hhs.gov/ocr/hipaa;
- To communicate the contents of this Compliance Plan, new legal developments, and new policies and procedures to members of our Workforce through training programs, memoranda, and other appropriate means;
- To establish and coordinate regular training programs designed to ensure compliance with the standards and procedures set forth in this Compliance Plan and to document the regularity and consistency of such training programs, as well as attendance;
- To assist with the development and communication of a system for members of our Workforce to seek guidance on privacy issues and to report suspected violations of the Privacy Rules or our Compliance Plan;

- To investigate alleged violations of our Compliance Plan and the Privacy Rules, and work with appropriate parties to handle violations promptly, properly and consistently;

- To establish a record-keeping system designed to document the ongoing operation of our Compliance Plan, including documentation of certification of compliance by all members of our Workforce;

- To review and revise (as necessary) our Compliance Plan on at least an annual basis in order to enhance our privacy efforts;

- To receive and investigate all complaints relating to possible Privacy Rules violations and/or violations of our Compliance Plan, and record/document the result of any such complaint; and

- To report to our Governing Body on the operation and implementation of this Compliance Plan.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

MINIMUM NECESSARY REQUIREMENTS

When PHI is used or disclosed or when we request PHI from another covered entity or business associate, reasonable efforts will be made to limit such use, disclosure, or request to the "minimum necessary" to accomplish the intended purpose of the use, disclosure or request. The minimum necessary standard is intended for covered entities to evaluate their privacy practices and to enhance protections as needed to limit unnecessary or inappropriate access to, disclosure of and the request of PHI.

Importantly, however, there are a number of general exceptions to the "minimum necessary" requirement:

- Disclosures to or requests by a health care provider for treatment.
- Disclosures made to the individual, including a request by the individual for access to or an accounting of disclosures of his/her PHI.
- Uses and/or disclosures made pursuant to an authorization (See Policy: *Use and Disclosure of PHI for Which an Authorization is required*).
- Uses and/or disclosures required by law (See Policy: *Use and Disclosure of PHI Without Authorization or Opportunity to Verbally Agree or Object).*
- Disclosures made to the Secretary of the U.S. Department of Health and Human Services ("HHS") that are related to the compliance and enforcement of HIPAA.
- Uses and/or disclosures required for compliance with HIPAA.

1. Use of PHI.

(a) **General Standards for Use of PHI.**

For uses of PHI by our Workforce we will:

- Identify the persons or groups of persons who need access to PHI to carry out their job function;
- Identify the type of PHI to which each person or group needs access, as well as the conditions under which they need access, and
- Make reasonable efforts to limit the access to only the information appropriate to the job requirements. (See *Workforce Minimum Necessary Matrix*).

(b) **Workforce Member Access.**

(i) *Unrestricted Access to PHI.* The following persons or group of persons have been identified as needing access to the entire medical record of patients in order to carry out their job functions:

- Nurses, doctors and other members of our Workforce involved in the care or treatment of patients. However, this access is limited to an "as needed" basis and these Workforce members should only access those medical records or portions necessary to properly treat our patients.

- Workforce members involved in claims processing, billing or payment processing. However, this access is limited to an "as needed" basis and these Workforce members should only access those medical records or portions necessary to properly bill for or code procedures or services, or process payment for patients.

- Workforce members involved in the registration of the patient, creation, processing and storage of the medical record. However, this access is limited to an "as needed" basis and these Workforce members should only access that PHI or portions of the medical record necessary to provide required services for our patients.

(ii) *Restricted Access to PHI.* We have determined that the following persons or group of persons are not otherwise involved in treatment, or claims, coding, billing or payment processes and therefore only need access to the PHI necessary to carry out their job functions and may only access that minimum amount of PHI necessary to perform their job functions:

- Workforce members involved in information systems or information technology may only access that PHI which is necessary to perform their job.

- Workforce members involved in providing meals to our patients may only access that PHI which is necessary to perform their jobs.

(iii) *No Access to PHI.* We have determined that the following persons or group of persons may NOT access PHI.

- Workforce members involved in cleaning and general maintenance of our facility.

- Workforce members involved in providing the laundry services of our facility.

- Workforce members involved in non-healthcare components of our hybrid entity.

2. Disclosure of PHI.

(a) **General Standards for PHI Disclosures.** We may reasonably rely on a request for disclosure as being for the "minimum necessary" amount of information if:

(i) The disclosure is to a public official for Public Health Activities and the public official represents that the request is for the minimum necessary information (See Policy: *Use and Disclosure of PHI Without Authorization or Opportunity to Verbally Agree or Object).*

(ii) The disclosure is in response to a request from another covered entity.

(iii) The disclosure is in response to a request from a professional of our Workforce or from a Business Associate in order to provide a professional service to us and the professional or Business Associate represents that the request is for the "minimum necessary" information.

(iv) The disclosure is in response to a request for information and the requestor provides documentation or representations from an Institutional Review Board ("IRB") or Privacy Board that meet the requirements for disclosure of PHI for Research Purposes (See Policy: *Use and Disclosure of PHI Without Authorization or Opportunity to Verbally Agree or Object).*

(b) **Routine Disclosures.** For routine or recurring disclosures, we will identify: (i) the type of PHI to be disclosed; (ii) the type of person(s) who receive the PHI; and (iii) the conditions that would apply to such disclosure.

(v) *Routinely Hired Business Associates.* We will limit the disclosure of PHI to Business Associates to the information necessary for the Business Associate to perform its services for us. Each contract with a Business Associate should contain sufficient terms and provisions to identify the type of information necessary for the arrangement. (See Policy: *Obtaining Business Associate Agreements*).

(vi) *Judicial and Administrative Proceedings*. We will limit the disclosure of PHI in judicial and administrative proceedings to that expressly authorized and sought in connection with the proceeding. (See Policy: *Use and Disclosure of PHI Without Authorization or Opportunity to Verbally Agree or Object).*

(vii) *Life Insurance Requests.* Requests for information relative to applying for life insurance shall be completed in accordance with the specific authorization, and shall include information dating back five (5) years, unless otherwise specified in the authorization. As a general rule, the information provided shall include discharge summary, face sheet, history and physical examination, unless specific information is set forth in the authorization.

(viii) *Disability Insurance Requests*. Requests for information relative to establishing a disability shall be completed in accordance with the specific authorization, and shall include information dating back five (5) years, unless otherwise specified in the authorization. As a general rule, the information provided shall include discharge summary, face sheet, history and physical examination, unless specific information is set forth in the authorization.

(ix) *Workers' Compensation Requests.* We will limit the disclosure of PHI pursuant to workers' compensation requests to that information necessary to respond to the request.

c. **Non-Routine Disclosures.** For non-routine or non-recurring disclosures, we will (i) develop reasonable criteria to limit the amount of PHI disclosed to the "minimum necessary" to accomplish the purpose of the disclosure; and (ii) use the criteria to review these disclosures

on a case-by-case basis. All non-routine disclosures should be handled by the Privacy Officer.

3. Requests for PHI.

PHI will be limited on any request from another health care provider, health plan or health care clearinghouse to that which is reasonably necessary to accomplish the purpose for which the request is made. However, requests made for treatment purposes are not subject to the minimum necessary standard.

(a) **Routine Requests.** For routine or recurring requests, we will: (i) describe what information is reasonably necessary for the purpose of the request; and (ii) limit the request for PHI to that information.

(b) **Non-Routine Requests**. For non-routine or non-recurring requests, we will: (i) develop reasonable criteria to limit the amount of PHI requested to the minimum necessary to accomplish the purpose of the request; and (ii) use the criteria to review these requests on a case-by-case basis. All non-routine requests should be handled by the Privacy Officer.

4. Special Rule – Entire Medical Record.

For all uses, disclosures or requests for the entire medical record of a patient, we will not use, disclose or request an entire medical record, except in those instances where the entire medical record is specifically justified as reasonably necessary given the reason for the request. However, disclosures to health care providers are not subject to this requirement, provided that the disclosure is for treatment purposes.

5. Special Rule – Physician Office Electronic Access to One Content/Patient Folder.[1]

Physicians who are credentialed by The Health Care Authority, and their staff members, may be granted electronic access to PHI stored in the Health Care Authority One Content. Prior to receiving such electronic access, the physician and his/her staff members using One Content system must execute the *Electronic Health Record User and Confidentiality Access Agreement*, and the physician and his/her staff members using the One Content system must execute the *Confidentiality and Security Agreement* and *Information Systems Access Form*. All access through the One Content /Patient Folder system shall be solely for job-related purposes, shall be limited to that minimally necessary to carry out such job-related purposes, and shall be in accordance with the provisions of the *Electronic Health Record User and Confidentiality Access Agreement* (if applicable), *Confidentiality and Security Agreement* (if applicable), *Information Systems Access Form* (if applicable), and this Compliance Plan. All persons accessing PHI through One Content/Patient Folder shall immediately notify the Privacy Officer in the event they are terminated or otherwise no longer require access to the One Content/Patient Folder system.

➢ **Form: Workforce Minimum Necessary Matrix**

10

[1] One Content is used by Northeast Regional Medical Center and Stringfellow Campus of Northeast Alabama Regional Medical Center.. Physician offices use a variety of programs for their EMR.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

DISCLOSURE OF DE-IDENTIFIED INFORMATION

PHI can be disclosed by The Health Care Authority if it does not contain "individually identifiable information." PHI is not individually identifiable if the patient (*i.e.*, the individual) is not identified, directly or indirectly, and we have no reasonable basis to believe that the information can be used to identify the patient. In order to de-identify PHI, one of the two procedures will be followed:

1. **Use of a Statistician.**

   - Obtain the services of a person with appropriate experience and knowledge applying generally acceptable statistical and scientific principles and methods for determining that information is not individually identifiable;

   - Who makes a determination that there is a very small risk that the information could be used by itself or in combination with other available information by the anticipated recipient(s) to identify the subject of the information; and

   - Who documents the methods and results in making such determination.

2. **Removal of All Identifiers.** Either directly or through one of our Business Associates, all of the following list of identifiers will be removed (including those of the patient, and his/her relatives, employers or household members) and we shall have no actual knowledge that the information remaining could be used alone or in combination with other information to identify the patient who is the subject of the information. The identifiers which will be removed for PHI to be considered "de-identified" are:

   - Names;

   - All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip codes and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of Census;

     - The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; or

     - The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

   - All elements of date (except year) for dates directly related to a patient, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

   - Telephone numbers;

   - Fax numbers;

   - Electronic mail addresses;

- Social security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable image; and
- Any other unique identifying number, characteristic or code.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

DISCLOSURE OF LIMITED DATA SETS

We may use or disclose a "limited data set" of PHI for the purposes of research, public health or health care operations when the following requirements are met:

(a) A limited data set is PHI that excludes the following information regarding the patient and his/her relatives, employers or household members:

- Names;
- Postal address information, other than town, city, state and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

(b) We may use or disclose a limited data set only if we obtain assurances, in the form of a Limited Data Use Agreement compliant with the requirements of HIPAA, that the limited data set recipient will only use or disclose the limited data set for limited purposes.

(c) We may use PHI to create a limited data set that meets the requirements of HIPAA, or disclose PHI only to a Business Associate for such purpose, whether or not the limited data set is to be used by us.

(d) Contents of Limited Data Use Agreement. A Limited Data Use Agreement must:

(i) Establish the permitted uses and disclosures of such information by the limited data set recipient. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of HIPAA;

(ii) Establish who is permitted to use or receive the limited data set; and

(iii) Provide that the limited data set recipient will:

a) Not use or further disclose the information other than as permitted by the Limited Data Use Agreement or as otherwise required by law;

b) Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for by the Limited Data Use Agreement;

c) Report to us any use or disclosure of information not provided for by the Limited Data Use Agreement of which it becomes aware;

d) Ensure that any agents to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

e) Not identify the information or contact the individuals.

(e) Obligation to Address Material Breaches/Violations.

(i) Where we know of a pattern of activity or practice of a limited data set recipient that constitutes a material breach or violation of the Limited Data Use Agreement, we shall take reasonable steps to cure the breach or end the violation, as applicable.

(ii) In the event steps to cure the breach or end the violation are unsuccessful, we shall either:

a) Terminate the Limited Data Use Agreement and discontinue disclosure of PHI to the recipient; or

b) Report the problem to the Secretary of HHS.

➢ **Form: Limited Data Use Agreement**

LIMITED DATA USE AGREEMENT

THIS LIMITED DATA USE AGREEMENT ("LDU Agreement") is made and entered into as of _____, 2003 (the "Effective Date") by and between Northeast Alabama Regional Medical Center (hereinafter referred to as the "Covered Entity") and _____(hereinafter referred to as the "Recipient").

WHEREAS, Recipient desires to obtain certain information from Covered Entity for the limited purposes of performing Recipient: (i) Research, (ii) Public Health Activities, or (iii) Health Care Operations and, in connection with those purposes, Recipient will receive from Covered Entity certain Protected Health Information in the form of a Limited Data Set ("LDS") that is subject to protection under the Privacy Rules of the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA");

WHEREAS, Covered Entity and Recipient intend to protect the privacy and provide for the security of the LDS in compliance with the Privacy Rules; and

WHEREAS, the Privacy Rules require Recipient to enter into a contract containing specific requirements that it must meet in order to receive the LDS from or on behalf of Covered Entity.

NOW, THEREFORE, in consideration of the foregoing and of the covenants and agreements set forth herein, the parties, intending to be legally bound, agree as follows:

Section 1. Definitions. The terms used, but otherwise not defined, in this LDU Agreement shall have the same meaning as those terms in the Privacy Rules.

(a) "Recipient" shall mean the person or entity designated as such above, as well as his/her/its officers, directors, employees, agents and representatives.

(b) "Health Care Operations" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, the following activities of Recipient: quality assessment and improvement activities, credentialing, accreditation, conducting medical reviews, legal services, business planning and development, business management, and general administrative activities.

(c) "Individual(s)" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, a person who is the subject of the LDS, and shall include an individual or entity who qualifies as a personal, legal representative of the person, as the context requires.

(d) "Limited Data Set" ("LDS") shall mean Protected Health Information that Recipient receives from, or on behalf of, Covered Entity and that excludes the following direct identifiers of the Individual and of relatives, employers or household members of the Individual pursuant to 45 CFR 164.514(e): names; postal address information (other than town or city, state and zip code); telephone and fax numbers; e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers (including license plate); device identifiers and serial numbers; web universal resource locators ("URLs"); internal protocol ("IP") address numbers; biometric identifiers; including finger and voice prints and full face photographic images and any comparable images.

(e) "Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, Subparts A and E, as may be amended, modified or superceded, from time to time.

(f) "Protected Health Information" ("PHI") shall have the meaning set forth in 45 CFR 164.501, including, without limitation, any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; or (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual; and (iv) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(g) "Required by Law" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, a mandate contained in law that compels a covered entity to make a use or disclosure of PHI and that is enforceable in a court of law.

(h) "Public Health Activities" shall have the meaning set forth in 45 CFR 164.512(b), including, without limitation: (i) a public health authority that is authorized by law to collect or receive Protected Health Information for the purpose of preventing or controlling disease, injury, or disability, including but not limited to, the reporting of disease, injury, vital events such as birth and death, and the conduct of public surveillance or public health investigations; (ii) a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect; (iii) a person subject to the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for which that person has responsibility; or (iv) a public health authority that is authorized by law to notify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition.

(i) "Research" shall have the meaning set forth in 45 CFR 164.501, including, without limitation, a systematic investigation, including research development, testing, and evaluation, designated to develop or contribute to generalizable knowledge.

(j) "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

Section 2. Obligations of Recipient.

(a) Limited Data Set. Recipient shall have access only to the following specific LDS information, as set forth in Section 1(d): _____. Recipient hereby affirms and acknowledges that his/her/its request for LDS information is the minimum necessary to accomplish his/her/its purpose as set forth in Section 2(b) below.

(b) Permitted Uses. Recipient shall not use LDS except for the express purpose of performing Recipient's (describe the particular Research, Public Health Activity, or Health Care Operation purpose): _____
Recipient shall not use the LDS in any manner that would constitute a violation of the Privacy Rules.

(c) Permitted Disclosures. Recipient shall not disclose LDS except as may be related to the specific purpose(s) as set forth in Section 2(b) and shall not disclose LDS in any manner that would constitute a violation of the Privacy Rules.

(d) Appropriate Safeguards. Recipient shall implement appropriate administrative, technical, and physical safeguards in compliance with the Privacy Rules as are necessary to prevent the use and/or disclosure of LDS other than as permitted by the terms of this LDU Agreement. Recipient shall maintain a comprehensive written information privacy program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Recipient's operations and the nature and scope of his/her/its activities in order to safeguard the LDS.

(e) Recipient's Agents and/or Subcontractors. To the extent Recipient retains any agents or subcontractors that will use or have access to the LDS for the purposes of performing Recipient's: (i) Research, (ii) Public Health Activities, or (iii) Health Care Operations in accordance with Section 2(b) above, Recipient shall require that each agent or subcontractor agree, in writing, to be bound by the terms of this LDU Agreement to the same extent as Recipient. Recipient shall implement and maintain sanctions against agents and subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

(f) Re-Identify or Contact Individuals. The Recipient agrees not to re-identify or contact the Individual(s) who is/are the subject(s) of the LDS.

(g) Governmental Access to Records. Recipient shall make his/her/its internal practices, books and records relating to the use and disclosure of LDS available to Secretary in a time and manner designated by the Covered Entity or the Secretary, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rules. Recipient shall provide Covered Entity access to or a copy of any LDS or other information that Recipient makes available to the Secretary concurrently with providing such LDS to the Secretary.

(h) Covered Entity Access to Records. Within five (5) days of a written request by Covered Entity, Recipient shall allow Covered Entity to conduct a reasonable inspection of Recipient's facilities, systems, books, records, agreements, policies and procedures relating to the use and/or disclosure of LDS for the purpose of determining whether Recipient has complied with this LDU Agreement; provided, however, that: (i) Recipient and Covered Entity shall mutually agree in advance upon the scope, timing and location of such an inspection; (ii) Covered Entity shall protect the confidentiality of all confidential and proprietary information of Recipient to which Covered Entity has access during the course of such inspection; and (iii) Covered Entity shall execute a non-disclosure agreement, upon terms mutually agreed upon by the parties, if requested by Recipient. The fact that Covered Entity inspects, or fails to inspect, or has the right to inspect, Recipient's facilities, systems, books, records, agreements, policies, and procedures does not relieve Recipient of his/her/its responsibility to comply with this LDU Agreement. Moreover, Covered Entity's failure to detect or, in the alternative, detection, but failure to notify or require Recipient to remediate any unsatisfactory practices, does not constitute acceptance of such practice or a waiver of Covered Entity's enforcement rights under this LDU Agreement.

(i) Minimum Necessary Use and Disclosure Requirement. Recipient shall only request, use and disclose the minimum amount of LDS necessary to reasonably accomplish the purpose of the request, use or disclosure in accordance with 45 CFR 164.502(b). Further, Recipient will restrict access to LDS to those employees of Recipient or other workforce members under control of Recipient who are actively and directly participating in the request, use or disclosure of LDS in accordance with the purposes set forth in Section 2(b) above and who need to know such information in order to fulfill such responsibilities.

(j) LDS Ownership. Recipient acknowledges that it has no ownership rights with respect to LDS received by Recipient pursuant to this LDU Agreement.

(k) Notification of Breach; Mitigation. During the term of this LDU Agreement, Recipient shall notify Covered Entity within twenty-four (24) hours of any actual or suspected use and/or disclosure of LDS in violation of the Privacy Rules or this LDU Agreement. Recipient shall take prompt corrective action to mitigate and cure any harmful effect that is known to Recipient of an improper use and/or disclosure of LDS.

Section 3. Term and Termination.

(a) Term. This LDU Agreement shall commence on the Effective Date and will remain effective for the entire time Recipient maintains the LDS, unless earlier terminated in accordance with the terms herein.

(b) For Cause Termination Due to Material Breach. In the event of a material breach by Recipient of any of his/her/its obligations hereunder, Covered Entity shall have the right, as specifically recognized by Recipient, to terminate this LDU Agreement at any time by providing Recipient written notice of termination setting forth a description of the breach and the effective date of termination.

(c) Reasonable Steps to Cure Material Breach. If Covered Entity knows of a pattern of activity or practice of Recipient that constitutes a material breach of Recipient's obligations under the provisions of this LDU Agreement and does not terminate this LDU Agreement pursuant to Section 3(b) above, then Recipient shall take reasonable steps to cure such breach. If Recipient's efforts to cure such breach are unsuccessful within thirty (30) days following a written request to cure provided by Covered Entity, Covered Entity shall either: (i) terminate this LDU Agreement, if feasible; or (ii) if termination of this LDU Agreement is not feasible, Covered Entity shall report Recipient's breach to the Secretary.

(d) Judicial or Administrative Proceedings. Either party may terminate this LDU Agreement, effective immediately, if: (i) the other party is named as a defendant in a criminal proceeding for a violation of the Privacy Rules; or (ii) there is a finding or stipulation that the other party has violated any standard or requirement of the Privacy Rules in any administrative or civil proceeding.

(e) Effect of Termination. As of the effective date of termination of this LDU Agreement, neither party shall have any further rights or obligations hereunder except: (a) as otherwise provided herein; (b) for continuing rights and obligations accruing under the Privacy Rules; or (c) arising as a result of any breach of this LDU Agreement, including, but not limited to, any rights and remedies available at law or equity. Upon termination of this LDU Agreement for any reason, Recipient shall return or destroy all LDS (regardless of form or medium), including all copies thereof. The obligation to return or destroy all LDS shall also apply to LDS that is in the possession of agents or subcontractors of Recipient. If the return or destruction of LDS is not feasible, Recipient shall provide Covered Entity written notification of the conditions that make return or destruction not feasible. Upon mutual agreement of the parties that the return or destruction of LDS is not feasible, Recipient shall continue to extend the protections of this LDU Agreement to such information, and limit further uses or disclosures of such LDS to those purposes that make the return or destruction of such LDS not feasible, for as long as Recipient maintains such LDS. If Recipient elects to destroy the LDS, Recipient shall notify Covered Entity in writing that such LDS has been destroyed.

Section 4. Indemnification. Recipient shall indemnify and hold the Covered Entity, and its employees, officers, directors and independent contractors, harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards or other expenses, of any kind or nature whatsoever, including, without limitation, attorneys' fees, expert witness fees, and costs of investigation, litigation or dispute resolution, relating to or arising out of any breach or alleged breach of this LDU Agreement by Recipient. The obligations set forth in this Section 4 shall survive termination of this LDU Agreement, regardless of the reasons for termination.

Section 5. Disclaimer. Covered Entity makes no warranty or representation that compliance by Recipient with this LDU Agreement or the Privacy Rules will be adequate or satisfactory for Recipient's own purposes. Recipient is solely responsible for all decisions made by Recipient regarding the safeguarding of its confidential information.

Section 6. **Assistance in Litigation or Administrative Proceedings.** Recipient shall be available to Covered Entity, at no cost to Covered Entity, to testify as a witness, or otherwise provide reasonable assistance, in the event of litigation or administrative proceedings being commenced against Covered Entity, his/her/its directors, officers or employees based upon a claimed violation of HIPAA, the Privacy Rules or other laws relating to LDS security or privacy, except where Recipient is named as an adverse party.

Section 7. **Injunctive Relief.** In the event of a breach by Recipient of any of his/her/its obligations hereunder, Covered Entity shall have, in addition to any other rights and remedies available at law or in equity, the right to obtain injunctive relief without the necessity of proving actual damages or that any irreparable harm would or might result from a failure to obtain injunctive relief, it being acknowledged and agreed to by all parties hereto that any such breach will cause irreparable harm to Covered Entity and that monetary damages alone will not provide an adequate remedy.

Section 8. **Construction.** This LDU Agreement shall be construed as broadly as necessary to implement and comply with the Privacy Rules. The parties agree that any ambiguity in this LDU Agreement shall be resolved in favor of a meaning that complies and is consistent with the Privacy Rules.

Section 9. **Captions.** The captions contained in this LDU Agreement are included only for convenience of reference and do not define, limit, explain or modify this LDU Agreement or its interpretation, construction or meaning and are in no way to be construed as part of this LDU Agreement.

Section 10. **Notice.** All notices and other communications required or permitted pursuant to this LDU Agreement shall be in writing, addressed to the party at the address set forth at the end of this LDU Agreement, or to such other address as either party may designate from time to time in writing in accordance with this Section. All notices and other communications shall be mailed by registered or certified mail, return receipt requested, postage pre-paid; by facsimile with a copy sent by First Class Mail, postage prepaid; or transmitted by hand delivery. All notices shall be effective as of the date of delivery by hand delivery, two (2) days following the date of facsimile, or for certified mail on the date of receipt, whichever is applicable.

Section 11. **Assignment.** This LDU Agreement and the rights and obligations hereunder shall not be assigned, delegated, or otherwise transferred without the prior written consent of the other party and any attempted assignment or transfer without proper consent shall be null and void.

Section 12. **Governing Law and Venue.** This LDU Agreement shall be governed by, and interpreted in accordance with, the Privacy Rules and the internal laws of the State of Alabama, without giving effect to any conflict of laws provisions. Any action at law, suit in equity, or other judicial proceeding for the enforcement of this LDU Agreement, or any provision hereof, shall take place in the State of Alabama in the County in which Covered Entity has his/her/its place of business. Recipient hereby consents to the personal jurisdiction of the state and federal courts in such County, in any dispute arising from or related to this LDU Agreement.

Section 13. **Binding Effect; Modification.** This LDU Agreement shall be binding upon, and shall enure to the benefit of, the parties hereto and their respective permitted successors and assigns. This LDU Agreement may only be amended or modified by mutual written agreement of the parties; provided, however, that in the event provisions of this LDU Agreement shall conflict with the requirements of the Privacy Rules, this LDU Agreement shall automatically be deemed amended as necessary to comply with such legal requirements.

Section 14. **Waiver.** The failure of either party at any time to enforce any right or remedy available hereunder with respect to any breach or failure shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

Section 15. **Severability.** In the event that any provision or part of this LDU Agreement is found to be totally or partially invalid, illegal, or unenforceable, then the provision will be deemed to be modified or restricted to the extent and in the manner necessary to make it valid, legal, or enforceable, or it will be excised without affecting any other provision of this LDU Agreement with the parties agreeing that the remaining provisions are to be deemed to be in full force and effect as if they had been executed by both parties subsequent to the expungement of the invalid provision.

Section 16. **No Third-Party Beneficiaries.** Nothing express or implied in this LDU Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Recipient and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

Section 17. **Entire Agreement.** This LDU Agreement constitutes the entire agreement between the parties with respect to the matters contemplated herein and supersedes all previous and contemporaneous oral and written negotiations, commitments, and understandings relating thereto.

[Signatures on the following page]

IN WITNESS WHEREOF, Covered Entity and Recipient have each caused this LDU Agreement to be executed in their respective names by their duly authorized representatives, as of the day and year first above written.

"COVERED ENTITY"	**"RECIPIENT"**
Northeast Alabama Regional Medical Center	**[Insert Name]**
Signature:_____	Signature:_____
Print Name: _____	Print Name: _____
Title: _____	Title: _____
Date: _____	Date: _____
Address: NEARMC	Address: _____
P.O. Box 2208	_____
Anniston, Alabama 36202	_____
Facsimile: _____	Facsimile:_____

Title: Photography/Videoing/Recording Policy

Effective Date: _01/01/2020__

Purpose:

1. To facilitate compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), the Heath Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations, and any and all other applicable Federal or state law, regulations and interpretive guidelines.

2. To establish guidelines for situations where patients, visitors, and/or workforce members may or may not be photographed, recorded, or otherwise imaged while on or within the premises of the RMC Health System

Definitions:

1. Recording: Recording an individuals' voice using video recording (*e.g.*, video cameras, cellular telephones), tape recorders, or other technologies capable of capturing audio or transmitting sound.

2. Authorization: The patient's or patient's legal representative's written authorization for the use and/or disclosure of protected health information. The authorization is only good for the type of protected health information indicated and the timeframe listed in the authorization. Otherwise, a new authorization form must be obtained. The appropriate authorization form is the Patient Authorization for Use/Disclosure of Protected Health Information or the Patient Authorization for Use/Disclosure of Protected Health Information for Marketing/Educational Purposes.

3. Consent: The patient's or patient's legal representative's written consent to being photographed or recorded. The consent is only good for the type of photographs, videos, or recordings indicated and the timeframe listed in the consent. Otherwise, a new consent form must be obtained. The appropriate consent form is the Consent for Capturing Images, Recordings, or Videos Form or the Conditions of Admission or Consent for Treatment Form (if capturing for security or general healthcare operations purposes).

4. Photography: Recording an individual's likeness (*e.g.*, image, picture) using photography (*e.g.*, cameras, cellular telephones), video recording (*e.g.*, video cameras, cellular telephones), digital imaging (*e.g.*, digital cameras, web cameras) or other technologies capable of capturing an image and/or video (*e.g.*, Skype).

5. Workforce Member: Employees, volunteers, and other persons whose conduct, in performance of work for RMC Health System, is under direct control of RMC Health System, whether or not they are paid by RMC Health System or the Health Care Authority of the City of Anniston. As used herein, providers are considered workforce members.

iv. If the photograph or recording is being used for any purpose other than a clinical/treatment purpose, unless stated otherwise herein, RMC Health System will not retain a copy of the photograph or recording in the hospital medical record or in the patient's designated record set, as defined by HIPAA. A copy of the photograph or recording may be retained by the treating provider as appropriate under applicable law and in accordance with RMC Health System's policies and procedures.

v. Photographing and/or recording should cease immediately at the request of the patient and/or treating provider. The patient has the right to refuse to being photographed or recorded, and may withdraw his/her consent and/or authorization at any time in writing.

e. With regard to the disclosure of photographs or recordings, the following shall apply:

i. Photographs or recordings shall not be released without specific written authorization from the patient, unless the disclosure is for treatment, payment or health care operations purposes or is otherwise permitted under applicable law without patient authorization.

ii. Unless prohibited by law, photographs and recordings contained in the patient's designated record set, as defined by HIPAA, may be released to the patient in accordance with the Patients' Right to Access Policy. See Patient's Right to Access Policy.

iii. RMC Health System will retain all originals when photographs or recordings retained by RMC Health System are disclosed by RMC Health System.

iv. Photographs or recordings may not be disclosed to any production company, media developer, broadcast media producer or similar entity or person without RMC Health System's prior review and written approval.

v. With regard to the intellectual property rights, RMC Health System is the copyright holder and has the sole ability to license the photographs and recordings.

2. Photographing/Recording Patients in the Routine Course of Treatment Using RMC Health System-Owned Device or Equipment:

a. Written patient informed consent is required before workforce members may photograph or record a patient for treatment purposes. See Consent Policy and Procedure. Endoscopy or laparoscopy will require the Photography Consent NS 042 to be signed by the patient.

b. If written consent is obtained, workforce members may photograph and/or record patients in the routine course of treatment using an RMC Health System-owned device or equipment. This includes diagnostic imaging, endoscopy, laparoscopy, telemedicine, or images of specimens.

c. Photographs or records may be used and/or disclosed for treatment purposes without patient authorization.

a. The Conditions of Admission or Consent for Treatment form advises patients that photographs or recordings may be taken for security or general health care operations purposes (*e.g.*, quality assurance).

b. Photographs or records may be used and/or disclosed for the general health care operations of RMC Health Systemwithout patient authorization.

c. Photographs or records may be used and/or disclosed for security purposes without patient authorization as long as such uses and/or disclosures are allowed by applicable state and federal law.

d. This policy does not apply to general security surveillance of public areas, which is permitted without patient consent. However, the use and/or disclosure of such surveillance videos and/or images must comply with applicable state and federal law.

6. Photographing/Recording Patients by Workforce Members to Document Abuse or Neglect:

a. Patient consent or authorization is generally not required to document and report abuse or neglect; however, the photographs or recordings may not be used and/or disclosed for any other purpose beyond submission to the appropriate reporting agency unless otherwise permitted by federal or state law (*e.g.*, for treatment purposes). See Sanie Policy

b. Documentation of the need/benefit to take photographs or recordings to document abuse or neglect should be retained in the medical record. A copy of the photograph or recording shall be included in the hospital medical record.

7. Photographing/Recording Patients by Workforce Members for Research:

a. Written patient informed consent is required before workforce members may photograph or record a patient for research purposes.

b. Any use and/or disclosure of photographs or recordings for research purposes will be in compliance with state and federal regulations concerning privacy and research.

c. If a photograph or recording is determined to be identifiable, the Institutional Review Board overseeing the specific research project will determine if additional patient authorization is required.

d. A copy of the photograph or recording shall be included in the hospital medical record.

8. Photographing/Recording Patients by Workforce Members for Educational, Publicity, or Marketing Purposes:

a. RMC Health System must obtain written consent from the patient prior to photographing or recording a patient for educational, publicity, or marketing purposes.

RMC
Regional Medical Center

HIPAA AUTHORIZATION FOR USE/DISCLOSURE OF INFORMATION AND CONSENT/USE OF PHOTOGRAPHS AND AUDIO/VIDEO IMAGES ON SOCIAL MEDIA

Consent To: _____ Audio Recordings
(Please check as many as apply) _____ Motion Pictures
_____ Photographs
_____ Electronic Images

Patient:_____ **Date:**_____

Summary: ***This form says that you, the patient, give your permission to be interviewed, photographed, filmed or taped for medical education and/or promoting the activities of the hospital or your Provider, and that you give the permission for free.***

In the interest of promoting the hospital *and or Provider* and/or informing the public concerning activities at the hospital or for medical, educational or scientific purposes, I consent to audio recordings, the taking of motion pictures, videotape recording, or photographs, as indicated above, of the treatment or operation which is scheduled to be performed on me or in connection with medical services I am receiving from the Provider/Surgeon who is responsible for my care, on or about _____, 20___. I authorize this under the following conditions:

(1) You give permission for RMC and your surgeon to share details of you treatment and experience as a patient in communication produced by or on behalf of RMC/Provider, and consent to take and make use of you audio/video/photographic images in publications, produced by or on behalf of RMC/Provider. This permission extends both to electronic versions on the RMC websites or your Providers' internet/electronic applications as well as to printed, filmed and taped versions.

(2) If I sign this form, I have the right to request that audio/video recording, filming, or photographing ceases at any time. I am aware of the information will be posted on the internet is public.

(3) I am aware that my protected health information will exist forever in either a recoded, printed and/or electronic version or other version as many develop over time and that once it is published or disclosed in any form it will continue to be used. I understand that information about me used or disclosed pursuant to this authorization may be subject to re-disclosure by the recipient and will no longer be protected by the federal regulations protecting privacy and an individual's health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and other applicable federal and state law.

(4) Such recordings, motion pictures, live broadcast, electronic images, text interviews or photographs may be taken only with the consent of RMC and or my Provider responsible for my care.

(5) Only an individual approved by the RMC or my Provider shall produce the photographs, motion pictures or recordings.

(6) The photographs, electronic images, motion pictures, interview/text or recordings shall be used for publicity, education or science; such photographs and information relating to my case may be published and republished, exhibited either separately or in connection with each other, in a professional journals, *YouTube, LinkedIn, Twitter Instagram, Snapchat* or any other social media types or medical book, or used for any other purpose deemed proper in the interest of medical education, knowledge, research or to promote activities at RMC and or my Provider in the news media provided, however, that it is specifically understood that in any such publication or use, I shall not be identified by name without my consent below. I grant this consent as a voluntary contribution in the interest of medical education and knowledge, or to promote RMC and or my Provider.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

USE AND DISCLOSURE OF PHI TO CARRY OUT TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

PHI can be used or disclosed (except for psychotherapy notes), without any written permission/authorization from the patient as follows:

(a) PHI may be used or disclosed for our treatment, payment or health care operations.

(b) PHI may be disclosed for the treatment activities of any health care provider.

(c) PHI may be disclosed to another covered entity or any health care provider for the payment activities of that other entity or provider.

(d) PHI may be disclosed to another covered entity for the health care operations of the covered entity, if each of us has or had a relationship with the patient who is the subject of the PHI (we will communicate with the other entity as necessary to determine if this condition is met), the PHI pertains to such relationship, and the disclosure is for one or more of the following purposes:

- Conducting quality assessment and improvement activities -- including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; and/or

- Fraud and abuse detection and compliance.

Since we are a part of an organized health care arrangement ("OHCA"), PHI may be disclosed about an individual to another covered entity that participates in the OHCA for any health care operations of the OHCA.

In making any use or disclosure of PHI, we will follow the minimum necessary standards as described in our Compliance Plan. (See Policy: *Minimum Necessary Requirements*). If permitted to disclose PHI to a covered entity, PHI may also be disclosed to a Business Associate acting on behalf of that covered entity.

(e) ADT – Healthcare providers are required to use a new standartd for electronic ADT Patient Event Notificaitoons. Hospitals are required to send electronic notifications to all applicale post –acute care service porovders and sppliers, including a patient's primary care practitioner or group, and any other

practioner or group primarily responsible for the patient's care. The notifications must includes at a minium the patient name, the treating practitioner. Name and sending institution name. Notifications must be sent upone the pateint's registration in the hospital Emergency Room or admission to inpatient and discharge or transfer from the Emergency Room or inpatient services.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

USE AND DISCLOSURE OF PHI FOR WHICH AN AUTHORIZATION IS REQUIRED

Valid authorization from a patient, or his/her representative, must be received before PHI may be used and/or disclosed (or requested) for purposes other than treatment, payment or health care operations and when such use or disclosure is not otherwise permitted by HIPAA. (See Policies: *Use and Disclosure of PHI that Requires an Opportunity to Verbally Agree or Object and Use and Disclosure of PHI Without Authorization or Opportunity to Verbally Agree or Object*).

As necessary, the patient, or his/her representative, will sign and complete a *Patient Authorization for Use and/or Disclosure of PHI* form. This authorization details the PHI to be used and/or disclosed (or requested) and the purposes for which it may be transmitted. The authorization also advises the patient, or his/her representative of, among other things, his/her right to refuse to sign the form, his/her right to revoke the authorization in writing at any time, and the expiration date/event. The use of standardized authorization forms ensures that we receive all the necessary information to process the request. Prior to disclosing PHI pursuant to an authorization, verify that the authorization is valid and not otherwise defective. (See Policy: *Defective Authorizations*). Copies of signed authorizations are to be placed in the patient's file, as well as provided to the patients themselves.

Treatment is not conditioned on the execution of an authorization, except that the provision of research-related treatment may be conditioned on the execution of an authorization for the use or disclosure of PHI for such research and the provision of treatment performed for a third-party may be conditioned on execution of an authorization for disclosure to the third-party. We will not combine an authorization with any other type of document, such as our Privacy Notice.

Psychotherapy Notes.

(a) Psychotherapy notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the patient's medical record. Psychotherapy notes excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

(b) We must obtain a patient authorization for any use or disclosure of psychotherapy notes except:

(i) To carry out the following treatment, payment, or health care operations:

a) Use by the originator of the psychotherapy notes for treatment;

b) For our use or disclosure for our own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

c) Our use or disclosure to defend The Health Care Authority in a legal action or other proceeding brought by the individual; and

(ii) A use or disclosure that is otherwise required or permitted by the HIPAA Privacy Rules with respect to the oversight of the originator of the psychotherapy notes.

(See Policy: *Use and Disclosure of PHI Containing Psychiatric/Mental Information*)

Marketing.

(a) We must obtain an authorization for any use or disclosure of PHI for marketing, except if the communication is in the form of:

(iii) A face-to-face communication made by a covered entity to an individual; or

(iv) A promotional gift of nominal value provided by the covered entity.

(b) If we receive direct or indirect remuneration, as defined in the HIPAA Privacy Rules, from a third party the patient authorization must state that such remuneration is involved.

(See Policy: *Use and Disclosure of PHI for Marketing Policy*)

Sale of PHI.

We must obtain a patient authorization for any disclosure of PHI which is considered a sale of PHI, as defined in the HIPAA Privacy Rules, and such authorization must state that the disclosure of PHI will result in our receiving remuneration.

(See Policy: *Prohibition On Sale of PHI Policy*)

All appropriate members of our Workforce will familiarize themselves with the content of a patient authorization, as well as with the circumstances and events which trigger the form's utilization. Questions and/or concerns regarding whether an authorization form is required for the use and/or disclosure (or request) of PHI should be directed to the Privacy Officer.

➢ **Form: Patient Authorization for Use and/or Disclosure of PHI**

Patient Authorization for Use and/or Disclosure of PHI for Marketing Purposes

RMC HEALTH SYSTEM

RMC Anniston RMC Stringfellow Campus
Anniston, Alabama 36207

RELEASE FOR PROTECTED HEALTH INFORMATION

Place label here

Patient Authorization for Use and/or Disclosure of Protected Health Information

Patient Name:	Date of Birth:
Address:	Account Number:

I hereby authorize ("RMC Health System") to use, disclose and/or obtain the above-named patient's health information as follows (*check all that apply*):

☐ **use the following health information maintained by RMC Health System until:** _____ **Expiration Date/ will expire one year from signed date unless otherwise specified above.**	☐ **disclose the following health information to:** _____ **Address:** _____ **City, State, Zip:** _____ **Phone:** _____	☐ **obtain the following health information from:** RMC Health System **Address:** Post Office Box 2208 **City/State/Zip:** Anniston, AL 36202 **Phone:** _____ **Fax** _____

Specific description of the health information to be used/disclosed/obtained (*include dates of service, i.e., appointment date, type of service, etc*): _____

_____

This health information is used/disclosed/obtained for the following purpose (*if Authorization requested by the patient put: "At the request of the individual"*): _____

_____

Specific health information to be disclosed (*check all that apply*):

☐ Complete Medical Record	☐ Discharge Summary	☐ History & Physical
☐ Emergency Room Records	☐ Labs	☐ Pathology
☐ Radiology Reports	☐ Specific Dates of Service (*please specify*): _____	

The health information is being disclosed for the following purpose (*please check one*):

☐ Judicial/Administrative Proceedings	☐ Law Enforcement	☐ Investigation
☐ Health Oversight	☐ Coroner/Medical Examiner	☐ Other: _____

By providing this Authorization, I understand as follows:

1. I understand that RMC Health System may receive financial or in-kind compensation or remuneration in exchange for the use and/or disclosure of the above-named patient's protected health information.

2. I understand that this Authorization is continuous in nature and is to be given full force and effect, including disclosing and/or utilizing any and all of the foregoing information learned or determined after the date hereof but prior to the expiration date noticed below.

3. **I understand that this Authorization may result in the sending of clinical information and x-rays with reference to the above-named patient's diagnosis and/or any alcohol, drug or child abuse problems, behavioral or mental health services, reproductive health and/or information concerning sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency syndrome (HIV). I understand that these records are strictly confidential and are solely for the information of the person to whom addressed.**

Place label here

RELEASE FOR PROTECTED HEALTH INFORMATION

4. I understand that this Authorization is voluntary. I may refuse to sign this Authorization and the above-named patient's treatment and/or payment obligations will not be affected unless either of the following applies:

   - The treatment is related to research and the use and/or disclosure is related to such research; or
   - The treatment is solely for the purpose of creating protected health information for disclosure to a third-party.

5. I understand that the health information to be released may be subject to redisclosure by the recipient of the health information and no longer protected by federal or state law.

6. I understand that I may revoke this Authorization at any time by notifying RMC Health System in writing, but if I do, it will not have any effect on uses or disclosures prior to the receipt of the revocation. Unless otherwise revoked, this Authorization will expire on _____ (date, event, or condition). If I fail to specify a date, event, or condition, this Authorization will expire in one (1) year.

7. I understand that, upon request, I may receive a copy of this Authorization form after I sign it.

8. I understand that a photocopy or facsimile of this Authorization shall be valid and effective, just as the original.

_____ _____

Signature of Patient or Patient's Representative Date

_____

Printed Name of Patient's Representative (*if applicable*)

_____

Representative's Relationship to Patient (*if applicable*)

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

DEFECTIVE AUTHORIZATIONS

Authorizations are valid only for the conditions outlined in the document and may not be used for any purpose or purposes not specifically stated and agreed to. The Privacy Rules provide that when an authorization is defective, PHI cannot be used or disclosed pursuant to that authorization without subjecting us to possible civil and criminal penalties. Accordingly, prior to using or disclosing a patient's PHI (where an authorization is required), we shall confirm that a valid authorization is on file.

The Privacy Rules provide that an authorization is defective where:

(a) The expiration date has passed or the expiration event is known by us to have occurred;

(b) The authorization has not been filled out completely;

(c) The authorization is known by us to have been revoked;

(d) The authorization lacks a required element specified in the Privacy Rules;

(e) The authorization is a prohibited compound authorization, *i.e.,* it has been combined with other documents as prohibited by the Privacy Rules;

(f) The authorization is a prohibited authorization in that it conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits as prohibited by the Privacy Rules ;or

(g) Any material information contained in the authorization is known by us to be false.

- Where it appears that an authorization may be defective, Workforce members shall report such findings immediately to the Privacy Officer and wait for further instructions before using or disclosing the patient's PHI. At no time should PHI be utilized or released where the authorization governing such activity is determined to be defective, unless otherwise permitted by the Privacy Rules.

- Any questions and/or concerns about the validity of authorizations are to be directed to the Privacy Officer for guidance and instruction.

3. An authorization for use or disclosure of PHI may not be combined with any othr document to create a compound auhtorization, except as follows: (i) an authorization for the use or disclosure of PHI for a reaserch study may be combined with any other type of written permission for the same or another research study. This includes combining an authorization for the use or disclosure of PHI for a research study. This includes combing an authorization for the use or disclosure o PHI for a research study with another authorization for the same research study, with an authoritization for the creation or maintenance of a research database or repository, or with a consent to participate in reaserch. Where we have conditioned the provision of reaserch related treatment on the provision of on the authorizations, any compoundd authorization must clearly differentiate between the conditioned an unconditioned components and provide the patient with an opportunity to opt in to the research activities described in the unconditioned authorization: (ii) an authorization for a use or disclosure of psychotherapy notes may only

be combined with another authorization for use or disclosure of psyhtotherpay notes, or (iii) a patient authorization (other than an authorization for a use of disclosure of psychotherapy notes) may be combined with any other patient authorization, except when we have conditioned the provision of treatment, payment, enrollment in the health plan, or eligibility for benefits on the provision of one of the patient authorizations.

4. We may not condition the provision of treatment, payment , enrollment in the health plan, or eilgibility for benefits to an individual on the provision of an authorization, except (i) we may condition the provision of research-related treatment on the provsion of any authorization for use or disclosure of PHI for such research (ii) our health plan many condition enrollment in the health plan or eligilbity of benefits on the privions of an authorization reuested by the health plan prior to an individuals'enrollment in the health plan, if (a) the authorization sought is for the health plan's elgibility or enrollment determinations relating to the individual or for its underwriting or risk rating deteriminaitons; and (b) the authorization is not for a use or psychotherapy notes: and (iii) we may condition the provision of health care that is solely for the purpose of creating PHI for disclosure to a third party on provision of an authorization for the disclosure of the PHI to such third party.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

RESOLVING CONFLICTS BETWEEN AUTHORIZATIONS AND OTHER WRITTEN RELEASES

In the event we obtain an authorization and receive any other legal permission from a patient for the disclosure of PHI and those documents conflict, we may disclose such PHI only in accordance with the authorization. If we receive two authorizations for the same use or disclosure of PHI, we will follow the more restrictive authorization. We will attempt to determine the true intentions of the patient and resolve the conflicting authorizations prior to releasing any PHI if possible.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PATIENT'S RIGHT TO REVOKE AN AUTHORIZATION

A patient authorization is required where we seek to use, obtain, or release PHI for purposes other than treatment, payment or health care operations or for situations not addressed by an exception under HIPAA. In such instances, patients will generally be required to read and sign an authorization form prior to the use, release or request of their PHI. (See Policy: *Use and Disclosure of PHI for Which an Authorization is required*).

A patient may revoke previously granted authorizations at any time, provided that revocation is in writing. The revocation of an authorization will be effective immediately, except to the extent that we have taken action in reliance on the authorization or if the authorization was obtained as a condition of obtaining insurance coverage where other law provides the insurer with the right to contest a claim under the policy.

When a patient seeks to revoke an authorization, such revocation must be made in writing to us on the *Revocation of Authorization for Use and/or Disclosure of PHI* form. Revocations submitted on a form or in a format other than that prescribed above will not be accepted. Rather, patients who submit non-compliant revocation requests will be advised of this policy and will be provided the necessary form to complete and sign. The use of a standardized form for revoking authorizations is meant to ensure that we receive all the necessary information from a patient, in order that we may process and document revocations in a timely and thorough manner. Copies of authorization revocations will be included in the patient's file.

- **Form: Revocation of Authorization for Use and/or Disclosure of PHI**

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

USE AND DISCLOSURE OF PHI THAT REQUIRES AN OPPORTUNITY TO VERBALLY AGREE OR OBJECT

This policy outlines certain uses and disclosures of PHI that are allowed without the written consent or authorization of the patient as long as the patient is informed in advance of the use and/or disclosure and has the opportunity to verbally agree or object to the use and/or disclosure.

All questions and concerns regarding whether a use or disclosure of PHI falls within one of the categories outlined below should be directed to the Privacy Officer.

1. **Creation of Facility Directory.**

We may maintain a Directory of patients in our facility. However, the Directory will contain only the following information:

(a) The patient's name;

(b) The patient's location in the facility;

(c) The patient's condition described in general terms that does not communicate specific medical information about the patient; and

(d) The patient's religious affiliation.

This information may be disclosed to members of the clergy or, with the exception of information regarding the patient's religious affiliation, to persons who ask for the patient by name.

Prior to including a patient's information in our Directory, registration staff will inform the patient, or his/her representative, of the information to be included and the persons to whom it may be disclosed. The patient, or his/her representative, may agree or object to the inclusion of some or all of the information in the Directory.

If the patient, or his/her representative, objects to the inclusion of some or all of the information in the Directory, registration staff at Northeast Regional Medical Center facilities will make that patient a **"CONFIDENTIAL"** patient type and/or enter a **"No Press" [@]** publicity code during the registration process. Registration staff will explain to the patient that should individuals, including family and friends, inquire about them, those individuals will be informed "we have no information on the patient" or "due to confidentiality reasons, I have no information to provide on this patient". Entry of the patient's response into the automated registration system will populate reports that are accessed throughout the facility by appropriate members of the Workforce. Stringfellow private patients do not show up on the census for employees to see.

In the event that a patient cannot agree or object due to incapacity or emergency treatment circumstances, we may include some or all of the information in our Directory if use of the information is consistent with any prior preferences of the patient recorded in the hospital information system, and we believe in good faith that we are acting in the best interest of the patient. However, once the patient is able to make a

decision regarding the inclusion of information in our Directory, the patient has an opportunity to agree or object.

2. Disclosures to Family and Friends.

We may disclose a patient's PHI to a family member, relative, close personal friend, or any other person identified by the patient where such use and disclosure is directly relevant to such person's involvement with the patient's care or payment for health care services. Further, we may use or disclose PHI to notify or assist in notifying a family member, personal representative of the patient, or other person responsible for the patient's care regarding the patient's location, general condition, or death.

(a) Patient is Available. Where the patient is available, disclosure of PHI to family members or others may only be made if:

- The patient agrees;
- After an opportunity to object to the disclosure, the patient does not object; or
- The patient's consent can be reasonably inferred from the surrounding circumstances, based on the exercise of professional judgment.

The following mechanism has been developed to provide the patient with the right to control their PHI to individuals such as family and friends who may be involved with the patient's care and for notification purposes.

At the time of admission, registration and/or nursing staff will inform patients that they are being provided with a Patient Identification Number ("PIN") that is located on their armband. It is a 3-digit number enclosed in asterisks.

Registration and nursing staff will communicate to the patients or his/her representative that it is their responsibility to provide their PIN to only those individuals that they want to have involved in their care, informed about their medical condition, and/or notified.

Hospital operators, information desk volunteers may receive phone inquiries regarding a patient's condition/health status. These members of the Workforce will transfer only those phone calls to nursing care areas where the caller has provided a PIN number. Any inquiries received by staff at other points of entry to the facility, i.e., emergency department, will be forwarded to either the switchboard operators or the information desk volunteers to handle according to procedure. Emergent inquiries should be automatically forwarded to the nursing care areas.

Nursing personnel and other healthcare staff who receive phone inquiries must verify that the caller has the full name of the patient and the PIN before responding to inquiries.

When communicating PHI to individuals authorized by the patient, nursing staff should communicate only the minimum necessary information so that the individual is informed in order to be involved in the patient's care.

Individuals may be referred to the patient's physician when inquiring about specific health information related to the patient's condition or plan of care.

(b) Patient is not available. Where the patient is not available or cannot object to the disclosure due to incapacity or emergency circumstances, we will exercise our professional judgment to determine whether the disclosure is in the best interest of the patient. If such a disclosure is warranted, only the PHI that is directly relevant to the family member's or personal representative's involvement with the patient may be disclosed.

With regard to family members or personal representatives acting on behalf of a patient in picking up prescriptions, medical supplies, X-rays, or other similar forms of PHI, we shall use professional judgment, experience, and common practice to determine if such use and disclosure of PHI are in a patient's best interest.

3. Uses and Disclosures to Disaster Relief Agencies.

We may disclose PHI to public or private disaster relief agencies to coordinate the notification of family and friends regarding a patient's location, general condition, or death. Where the patient is available and has the capacity to make health care decisions, we will obtain the patient's agreement prior to such use or disclosure, to the extent it does not interfere with the ability to respond to emergency circumstances. Where the patient is not available or cannot object to the use or disclosure due to incapacity or emergency treatment circumstances, a patient's agreement may be reasonably inferred from the circumstances, based on the professional judgment of his/her treating physician.

4. Uses and Disclosures When Patient is Deceased.

If a patient is deceased, we may disclose to a family member, relative, close personal friend, or any other person who was involved in the patient's care or payment for health care prior to the patient's death, PHI of the patient that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the patient that is known to us.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

USE AND DISCLOSURE OF PHI WITHOUT AUTHORIZATION OR OPPORTUNITY TO VERBALLY AGREE OR OBJECT

Under HIPAA, certain uses and disclosures of PHI do not require authorization or opportunity for a patient to verbally agree or object. Therefore, it is not necessary to obtain patient authorization, or verbal agreement or objection for the following:

- Use and disclosure Required by Law;
- Disclosure for Public Health Activities;
- Disclosure about Victims of Abuse, Neglect, or Domestic Violence;
- Disclosure for Health Oversight Activities;
- Disclosure for Judicial and Administrative Proceedings;
- Disclosure for Law Enforcement Purposes;
- Use and disclosure about Decedents;
- Use and disclosure for Organ or Tissue Donation;
- Use and disclosure for Research Purposes;
- Use and disclosure to Avert Serious Threats to Health or Safety;
- Use and disclosure for Specialized Government Functions; and
- Disclosure for Workers' Compensation.

All questions and concerns regarding whether a use or disclosure of PHI falls within one of the above categories should be directed to the Privacy Officer.

1. Required by Law.

PHI may be used or disclosed when required by law, provided the use or disclosure complies with and is limited to the relevant requirements of such law. Special considerations are given for PHI disclosures related to victims of abuse, neglect or domestic violence, judicial and administrative proceedings, and law enforcement purposes.

2. Public Health Activities.

PHI may be disclosed to the following persons/entities for public health activities and purposes:

(a) To a public health authority that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or

disability, including, but not limited to, the reporting of disease, injury, vital events such as birth or death, and the conduct of public health surveillance, investigations, and interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority;

(a) To a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

(b) To persons working for or under the jurisdiction of the Food and Drug Administration ("FDA") with respect to an FDA-regulated product or activity for the purpose of monitoring quality, safety or effectiveness of such FDA-regulated product or activity. Such purposes include:

- Collecting or reporting adverse events (or similar activities with respect to food or dietary supplements) product defects or problems (including problems with the use or labeling of a product), or biological product deviations;
- Tracking FDA-regulated products;
- Enabling product recalls, repairs, or replacement or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn or are the subject of lookback); or
- Conducting post-marketing surveillance.

(c) To a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, if we or a public health authority is authorized by law to notify the person as necessary in the conduct of a public health intervention or investigation; or

(d) To a school, about a patient who is a student or prospective student of the school, if:

(i) The PHI that is disclosed is limited to proof of immunization;

(ii) The school is required by State or other law to have such proof of immunization prior to admitting the patient; and

(iii) We obtain and document the agreement to the disclosure from either:

a) A parent, guardian, or other person acting in loco parentis of the patient, if the patient is an unemancipated minor; or

b) The patient, if the patient is an adult or emancipated minor;

(e) To an employer about a patient who is a member of the employer's workforce if:

- We are a member of the workforce of the employer or we provide health care to the patient at the request of the employer in order to: (i) conduct an evaluation relating to medical surveillance of the workplace, or (ii) evaluate patients for work-related illness or injury;

- The PHI that is disclosed consists of findings concerning work-related illness or injury or workplace related medical surveillance;

- The employer needs such findings in order to comply with its obligations under the Occupational Safety and Health Administration Act ("OSHA") or the Mine Safety and Health Administration Rule or similar state law, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

- Patients are to be notified when disclosures of PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer: (i) by giving a copy of the notice to the patient at the time health care is provided, or (ii) if health care is provided at the work-site of the employer, by posting the notice prominently where the health care is provided.

3. Victims of Abuse, Neglect, or Domestic Violence.

Except for reports of child abuse or neglect permitted for disclosure according to paragraph 2(b) above, disclosure of PHI on a patient whom we reasonably believe to be a victim of abuse, neglect, or domestic violence to a government authority, including social services or a protective services agency, i.e., DHR, authorized by law to receive such reports. Disclosures are subject to the following:

(a) The disclosure is required by law and complies with and is limited to the relevant requirements of such law;

(b) The patient agrees to the disclosure; or

(c) The disclosure is expressly authorized by statute or regulation and:

- According to professional judgment, the disclosure of PHI is necessary to prevent serious harm to the patient or other potential victims; or

- The patient is unable to agree because of incapacity and a law enforcement or other public official authorized to receive the PHI documents represents that the PHI is not intended to be used against the patient and delays in receipt of the PHI would materially and adversely affect the patient.

When we make a disclosure as permitted above, we will promptly inform the patient of such report, except if: (i) we believe, in the exercise of professional judgment, that informing the patient would place him/her at risk of serious harm; or (ii) we would be informing a personal representative of the patient whom we reasonably believe may be responsible for the abuse, neglect, or other injury, and informing such a person would not be in the best interest of the patient.

4. Health Oversight Activities.

PHI may be disclosed to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative or criminal investigations, proceedings, or actions; inspections; licensure or disciplinary actions. In addition, PHI may be disclosed for other activities necessary for appropriate oversight of the health care system; government benefit programs for which health information is relevant to beneficiary eligibility; entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or entities subject to civil rights laws for which health information is necessary for determining compliance.

PHI cannot be disclosed for health oversight activities if an investigation or other activity relates to a patient but does not arise out of and is not directly related to the receipt of health care; a claim for public benefits related to health; or qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services. However, if the health oversight activity or investigation is conducted in conjunction with an activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation should be considered a health oversight activity for the purposes of this section.

5. Regulatory Agencies we may disclose your Health Information to a health care oversight agency for activities authorized by law. These activities are necessary for the government and certain private health oversight agencies to monitor the health care system, government programs and compliance with civil rights. We are required to disclose as needed protected health information to the Secretary of HHS.

6. Judicial and Administrative Proceedings.

PHI may be disclosed in the course of any judicial or administrative proceeding in accordance with the following:

(a) In response to an order of a court or administrative tribunal, provided that only the PHI expressly authorized by such order is disclosed; or

(b) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if satisfactory assurances are obtained from the requestor seeking the information that reasonable efforts have been made to: (i) "notify the patient" who is the subject of the PHI, or (ii) secure a "qualified protective order".

(i) *To Notify the Patient*. Satisfactory assurances must be received from a requestor seeking PHI that reasonable efforts have been made to notify the patient. This is done through a written statement and accompanying documentation demonstrating that:

- The party requesting such information has made a good faith attempt to provide written notice to the patient or, if the patient's location is unknown, to mail a notice to the patient's last known address;
- The notice includes sufficient information about the litigation or proceeding in which the PHI is requested to permit the patient to raise an objection to the court or administrative tribunal; and
- The time for the patient to raise objections to the court or administrative tribunal has lapsed, and no objections were filed, or all objections filed by the patient have been resolved by the court or the administrative tribunal and the disclosures being sought are consistent with such resolution.

(ii) *Qualified Protective Order*. Satisfactory assurances are received from a requestor seeking PHI that reasonable efforts have been made to secure a protective order, if from such requestor a written statement and accompanying documentation demonstrates that:

- The parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or administrative tribunal with jurisdiction over the dispute; or

- The party seeking the PHI has requested a qualified protective order from such court or administrative tribunal.

For the purposes of this section, a "qualified protective order" means an order of a court or an administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that: (i) prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and (ii) requires the return or destruction of the PHI (including all copies made) at the end of the litigation or proceeding.

(iii) Notwithstanding section 5(b) above, we may disclose PHI in response to lawful process without receiving satisfactory assurances under section 5(b) above, if we make reasonable efforts to provide notice to the patient sufficient to meet the requirements of section 5(b)(i) above or to seek a qualified protective order sufficient to meet the requirements of section 5(b)(ii) above.

(iv) *Alabama Law.* According to the Alabama Rules of Civil Procedure, a subpoena can be served on a non-party (also called a third-party) to a lawsuit, if that non-party has relevant information or documents needed in the lawsuit. Generally, a non-party will receive a notice of the intent to serve a subpoena from a party to the lawsuit. This notice is not an actual subpoena and a patient's PHI should not be released at this time. Once the subpoena is received, The Health Care Authority must seek satisfactory assurances from the party requesting the information that the patient has been notified or a qualified protective order has been sought by the party seeking the PHI.

6. Law Enforcement Purposes.

PHI for law enforcement purposes to a law enforcement official may be disclosed under the following circumstances:

(a) Pursuant to Process and Otherwise Required by Law.

- As required by law, including laws that require the reporting of certain types of wounds or other physical injuries, except for reports of Victims of Abuse, Neglect, or Domestic Violence (Paragraph 3 above);

- Pursuant to court orders, court ordered warrants, summons or subpoenas issued by a judicial officer, or a grand jury subpoena;

- Pursuant to an administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that:

  (i) The information sought is relevant and material to a legitimate law enforcement inquiry;

(ii) The request is specific and limited in scope to the extent of the purpose for which the information is sought; and

(iii) De-identified information could not reasonably be used.

(b) Limited Information for Identification and Location Purposes. Except for disclosures required by law as permitted by Paragraph 6(a) above, PHI may be disclosed in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that we disclose only the following information:

- Name and address;
- Date and place of birth;
- Social security number;
- ABO blood type and Rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

PHI may not be disclosed for the purpose of identification or location that is related to the patient's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

(c) Victims of Crime. Except for disclosures Required by Law, PHI may be disclosed in response to a law enforcement official's request for such information about a patient who is or is suspected to be a victim of a crime, other than disclosures that are subject to the requirements for reporting Public Health Activities (Paragraph 2 above) and Abuse, Neglect and Domestic Violence (Paragraph 3 above), if:

- The patient agrees to the disclosure; or
- Patient's agreement cannot be obtained because of incapacity or other emergency circumstance, provided that:

(i) The law enforcement official represents that such information is needed to determine whether a violation of law by a person other than the patient-victim has occurred, and such information is not intended to be used against the patient-victim;

(ii) The law enforcement official represents that immediate law enforcement activity that depends upon the disclosure would be materially and

adversely affected by waiting until the patient is able to agree to the disclosure; and

(iii) The disclosure is in the best interest of the patient-victim as determined by professional judgment.

(d) Decedents. PHI may be disclosed about a patient who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the patient if we have a suspicion that such death may have resulted from criminal conduct.

(e) Crime on Premises. PHI may be disclosed to law enforcement officials when in good faith the PHI is believed to constitute evidence of criminal conduct that occurred on our premises.

(f) Reporting Crime in Emergencies. If health care is provided in response to a medical emergency, other than in an emergency on our premises, PHI may be disclosed to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

- The commission and nature of a crime;
- The location of such crime or of the victim(s) of such crime; and
- The identity, description, and location of the perpetrator of such crime.

If it is believed that the medical emergency is the result of abuse, neglect, or domestic violence of the patient, this section does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to the reporting requirements for Abuse, Neglect and Domestic Violence (Paragraph 3 above).

7. Decedents.

(a) Coroners and Medical Examiners. PHI may be disclosed to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or for other official duties of the coroner or medical examiner as authorized by law.

(b) Funeral Directors. PHI may be disclosed to funeral directors, as necessary to carry out their duties with respect to a decedent. Where it is necessary for funeral directors to carry out their duties, PHI may be disclosed prior to, in anticipation of, a patient's death.

8. Organ and Tissue Donation.

PHI may be disclosed to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purposes or facilitating organ, eye, or tissue donation and transplantation.

9. Research Purposes.

If an appropriate authorization has not been received from the patient, PHI may be used or disclosed for research, regardless of the source of funding of the research, provided that we meet any of the three criteria below (a, b, or c):

(a) Approval of a Waiver of Authorization. A statement must be obtained that an alteration to or waiver of the Privacy Rules' patient authorization has been approved by the IRB or Privacy Board established in accordance with the Privacy Rules. The statement provided by the IRB or Privacy Board must satisfy the following criteria:

- Must include a statement identifying the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
- Must state that the use or disclosure of PHI involves no more than a minimal risk to the privacy of the patient, based on, at least, the presence of the following elements:
  - (i) an adequate plan to protect the identifiers from improper use and disclosure;
  - (ii) an adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
  - (iii) adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of protected health information would be permitted;
- Must state that the research could not practicably be conducted without the waiver or alteration;
- Must state that the research could not practicably be conducted without access to and use of the PHI;
- Must describe the PHI for which use or access has been determined to be necessary;
- Must state that alteration or waiver has been reviewed and approved under acceptable normal or expedited review procedures; and
- Must be signed by the chair or other member, as designated by the chair of the IRB or Privacy Board.

(b) Reviews Preparatory to Research. Researcher representations reflect that:

- The use or disclosure is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;
- No PHI is to be removed from our premises by the researcher in the course of the review; and
- The PHI for which use or access is sought is necessary for the research purposes.

(c) Research on Decedent's Information. If the research is related to decedents, obtain:

- Representation that the use or disclosure sought is solely for research on PHI of decedents;
- Documentation, at our request, of the death of such patients; and
- Representation that the PHI for which use or disclosure is sought is necessary for research purposes.

10. Threats to Health and Safety.

PHI may be used if it is believed in good faith that use or disclosure:

(a) Is necessary to prevent or lessen a serious or imminent threat to the health or safety of a person or the public and is disclosed to a person(s) reasonably able to prevent or lessen the threat;

(b) Is necessary for law enforcement authorities to identify or apprehend a patient because of a statement by a patient admitting participation in a violent crime that may have caused serious harm to the victim. However, where it is learned about a patient's participation in a violent crime during the course of treatment, counseling, or therapy to address the patient's propensity to commit crimes, or through a request for such services, then no use or disclosure of such information may be made; or

(c) Is necessary for law enforcement authorities to identify or apprehend a patient where it appears that the patient has escaped from a correctional institution or from lawful custody.

Acts of good faith will be presumed with regard to reporting threats to health and safety if our belief is based on actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

11. Specialized Governmental Functions.

PHI may be used and disclosed in situations involving government agencies and functions, as follows:

(a) Armed Forces Personnel. Use and disclose PHI of patients who are U. S. Armed Forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission.

(b) Foreign Military Personnel. Disclose PHI of patients who are foreign military personnel to their appropriate military authority for the same purposes for which disclosures are permitted for armed forces personnel.

(c) National Security and Intelligence Activities. Disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act.

(d) Protective Services for the President and Others. Disclose PHI to authorized federal officials for the provision of protective services to the President or other designated persons.

(e) Correctional Institutions and Other Law Enforcement Custodial Situations. Disclose PHI to correctional institutions or law enforcement officials having lawful custody of an inmate or other patient, if they represent that such information is necessary for:

- The provision of health care to the patient;
- The health and safety of the patient or other inmate;
- The health and safety of the officers or employees of or others at the correctional institution;
- The health and safety of the patients and the officers or other persons responsible for the transportation or transfer of inmates from one institution, facility, or setting to another;
- Law enforcement on the premises of the correctional institution; or
- The administration and maintenance of the safety, security, and good order of the correctional institution.

For the purposes of this provision, a patient is no longer an inmate when released on parole, probation, supervised release, or other lawful custody.

12. Workers' Compensation.

PHI may be disclosed as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

➢ **Form: Reference List for Authorizations/Disclosures of PHI**

Employee Authorization for Use and/or Disclosure of Protected Health Information
COVID-19 Testing

Employee Name:	Employee Date of Birth:
Employer:	

I hereby authorize The Health Care Authority of the City of Anniston d/b/a RMC Occupational Health and Wellness Department and/or its affiliated entities, employees and contractors (collectively, "RMC") to disclose the above-named employee's Health Information, as described below, to the employer identified above ("Employer") for report to work and workplace surveillance purposes. The Health Information is being disclosed at my request.

The health information that may be disclosed pursuant to this Authorization includes the above-named employee's name, date of birth, COVID-19 screening date and results, and COVID-19 testing date and results (collectively, the "Health Information").

By providing this Authorization, I understand as follows:

1. I understand that this Authorization may result in the use and/or disclosure of the Health Information specified above without further approval by or notification to me.

2. I understand that the COVID-19 screening and COVID-19 testing is being conducted by RMC at the request of the Employer and is for the purpose of creating protected health information for disclosure to the Employer. Thus, I understand that if I refuse to sign this Authorization allowing disclosure to the Employer, the COVID-19 screening and COVID-19 testing will not be rendered to the above-named employee.

3. I understand that RMC may receive financial or in-kind compensation or remuneration in exchange for the use and/or disclosure of the Health Information.

4. I understand that the Health Information to be released may be subject to redisclosure by the recipient of the Health Information and no longer protected by federal or state law.

5. I understand that this Authorization is continuous in nature and is to be given full force and effect, including disclosing and/or utilizing any and all of the foregoing Health Information learned or determined after the date hereof but prior to the expiration date noticed below.

6. I understand that I may revoke this Authorization at any time by notifying RMC in writing, but if I do, it will not have any effect on uses or disclosures prior to the receipt of the revocation. Unless otherwise revoked by the Employee or Employee's Representative, this Authorization will expire within one (1) year.

7. I understand that, upon request, I may receive a copy of this Authorization form after I sign it.

8. I understand that a photocopy or facsimile of this Authorization shall be valid and effective, just as the original.

_____ _____

Signature of Employee or Employee's Representative Date

_____

Printed Name of Employee's Representative (*if applicable*)

_____

Representative's Relationship to Employee (*if applicable*)

RMC HEALTH SYSTEM

Patient Authorization for Use and/or Disclosure of Protected Health Information

Patient Name:	Date of Birth:

Address: _____ Phone Number _____

Email Address: _____

I hereby authorize the disclosure of the above-named patient's health information as follows:

□ **use the following health information maintained by RMC Health System until:** _____ **Expiration Date/ will expire one year from signed date unless otherwise specified above.**	□ **disclose the following health information to:** _____ **Address:** _____ **City, State, Zip:** _____ **Phone:** _____	□ **obtain the following health information from:** _____ **Address:** _____ City, State, Zip _____ Phone: _____

Specific description of the health information to be used/disclosed/obtained (*include dates of service, i.e., appointment date, type of service, etc):* _____

This health information is used/disclosed/obtained for the following purpose (*if Authorization requested by the patient put: "At the request of the individual"*): _____

Please print the email address if requesting medical records to be sent by email: _____

Specific health information to be disclosed (*check all that apply*): RMC Health System ☐ RMC Health Clinic ☐

□ Complete Medical Record	□ Discharge Summary	□ History & Physical
□ Emergency Room Records	□ Labs	□ Pathology
□ Radiology Reports	□ Specific Dates of Service (*please specify*): _____	

The health information is being disclosed for the following purpose (*please check one*):

□ Judicial/Administrative Proceedings	□ Law Enforcement	□ Investigation
□ Health Oversight	□ Coroner/Medical Examiner	□ Personal
□ Other: _____		

By providing this Authorization, I understand as follows:

By providing this Authorization, I understand as follows:

1. I understand that RMC Health System may receive financial or in-kind compensation or remuneration in exchange for the use and/or disclosure of the above-named patient's protected health information.

2. I understand that this Authorization is continuous in nature and is to be given full force and effect, including disclosing and/or utilizing any and all of the foregoing information learned or determined after the date hereof but prior to the expiration date noticed below.

3. **I understand that this Authorization may result in the sending of clinical information and x-rays with reference to the above-named patient's diagnosis and/or any alcohol, drug or child abuse problems, behavioral or mental health services, reproductive health and/or information concerning sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency**

syndrome (HIV). I understand that these records are strictly confidential and are solely for the information of the person to whom addressed.

4. I understand that this Authorization is voluntary. I may refuse to sign this Authorization and the above-named patient's treatment and/or payment obligations will not be affected unless either of the following applies:

   - The treatment is related to research and the use and/or disclosure is related to such research; or
   - The treatment is solely for the purpose of creating protected health information for disclosure to a third-party.

5. I understand that the health information to be released may be subject to redisclosure by the recipient of the health information and no longer protected by federal or state law.

6. I understand that I may revoke this Authorization at any time by notifying RMC Health System in writing, but if I do, it will not have any effect on uses or disclosures prior to the receipt of the revocation. Unless otherwise revoked, this Authorization will expire on _____ (date, event, or condition). If I fail to specify a date, event, or condition, this Authorization will expire in one (1) year.

7. I understand that, upon request, I may receive a copy of this Authorization form after I sign it.

8. I understand that a photocopy or facsimile of this Authorization shall be valid and effective, just as the original.

_____	_____
Signature of Patient or Patient's Representative	Date
_____	_____
Printed Name of Patient's Representative (*if applicable*)	Representative's Relationship to Patient (*if applicable*)

If you are signing as the personal representative, you may be asked by the Releasing Entity to submit proof of your authority to act as the personal representative of the patient.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

USE AND DISCLOSURE OF PHI FOR MARKETING

1. General Definitions.

(a) Financial Remuneration - "Financial remuneration" means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

2. Marketing Activities.

(a) What Constitutes a "Marketing" Communication? A communication concerning a product or service that encourages recipients of the communication to purchase or use the product or service. However, marketing does not include a communication made:

(i) To provide refill reminders or otherwise communicate about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by us in exchange for making the communication is reasonably related to our cost of making the communication.

(ii) For the following treatment and health care operations purposes, except where we receive financial remuneration in exchange for making the communication:

a) For treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual;

b) To describe a health-related product or service (or payment for such product or service) that is provided by us, or included in a plan of benefits of ours, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; or

c) For case management or care coordination, contacting of individuals with information about treatment alternatives, and related functions to the extent these activities do not fall within the definition of treatment.

(b) General Rule.

(i) Authorization Required. If we use or disclosure PHI for marketing purposes, we shall obtain a patient authorization. If the marketing communication involves financial remuneration from a third party the patient authorization shall contain a statement which notifies the individual that such remuneration is involved.

(ii) Exception - If the communication is in the form of a face-to-face communication made by us to an individual; or is a promotional gift of nominal value provided by us a patient authorization is not required.

(c) Oversight.

(i) Our HIPAA Privacy Officer shall be responsible for reviewing and assessing all potential marketing arrangements to determine if a communication constitutes "marketing" as defined herein.

(ii) If a workforce member is unsure as to whether a patient authorization is needed in order to make a marketing communication, the workforce member shall seek guidance from the Privacy Officer prior to using or disclosing PHI for such communication.

➢ **Form: Patient Authorization for Use and/or Disclosure of PHI for Marketing Purposes**

RMC HEALTH SYSTEM

Patient Authorization for Use/ Disclosure of Protected Health Information for Marketing/Educational Purposes

Patient Name:	Date of Birth:
Address:	Account Number:

By signing below, I hereby authorize RMC Health System and/or its healthcare providers, employees, contractors, and medical staff members collectively, to use and/or to disclose, through any form or medium, the above-named patient's protected health information, written and video images, audio and video recordings, testimonials, photographs, and any other images or recordings (collectively referred to herein as the "Information") for marketing, advertising, educational, and/or promotional purposes. I further hereby authorize RMC Healthy System to disclose, through any form or medium, the above-named patient's Information for use in broadcast media.

Specific description of the Information to be used and/or disclosed pursuant to this Authorization (*e.g., patient's name and/or contact information, dates of service, type of service, etc.):* _____

_____

_____

By providing this Authorization, I understand as follows:

1. I understand that this Authorization may result in the use and/or disclosure, through any form or medium, of the Information referencing the above-named patient's treatment. I understand that such Information may be used and/or disclosed without further approval by or notification to me. **I understand that such Information may be unflattering, embarrassing, or portray the above-named patient in a negative manner.**
2. I understand that this Authorization is voluntary. I may refuse to sign this Authorization and the above-named patient's treatment and/or payment obligations will not be affected.
3. I understand that RMC Health System may receive financial remuneration in exchange for making the communication from or on behalf of a third party
4. I understand that any Information consisting of written and video images, audio and video recordings, testimonials, photographs, and any other images or recordings shall become the property of RMC Health System. I understand that, by signing this Authorization, I release to RMC Health System any rights, title and/or interest of any kind that I may have in such types of Information.
5. I understand that the Information used and disclosed may be seen by members of the general public.
6. I understand that the Information to be disclosed may be subject to redisclosure by the recipient and may no longer be protected by federal or state law.
7. I understand that if the Information is protected by any applicable legal privilege, I hereby waive such privilege with respect to the Information disclosed.
8. I understand that this Authorization is continuous in nature and is to be given full force and effect, including disclosing and/or utilizing any and all of the foregoing Information learned or determined after the date hereof but prior to the expiration date noticed below.
9. I understand that I may revoke this Authorization at any time by notification to RMC Health System in writing, but if I do, it will not have any effect on uses or disclosures of Information occurring prior to the receipt of the revocation. Unless otherwise revoked, this Authorization will expire five (5) years after the date below or sooner by my choice (in which case this Authorization will expire on _____).
10. I understand that, upon request, I may receive a copy of this Authorization form after I sign it.
11. I understand that a photocopy or facsimile of this Authorization shall be valid and effective, just as the original.

_____ _____

Signature of Patient or Patient's Representative Date

_____ _____

Printed Name of Patient's Representative (*if applicable*) Representative's Relationship to Patient (*if applicable*)

RMC HEALTH SYSTEM

RMC Anniston RMC Stringfellow Campus
Anniston, Alabama 36207

RELEASE FOR PROTECTED HEALTH INFORMATION

Place label here

Patient Authorization for Use and/or Disclosure of Protected Health Information

Patient Name:	Date of Birth:
Address:	Account Number:

I hereby authorize ("RMC Health System") to use, disclose and/or obtain the above-named patient's health information as follows (*check all that apply*):

□ **use the following health information maintained by RMC Health System until:**
_____
Expiration Date/ will expire one year from signed date unless otherwise specified above.

□ **disclose the following health information to:**
_____
Address:_____
City, State, Zip:_____
Phone:_____

□ **obtain the following health information from:**
RMC Health System
Address: Post Office Box 2208
City/State/Zip: Anniston, AL 36202
Phone: _____ **Fax** _____

Specific description of the health information to be used/disclosed/obtained (*include dates of service, i.e., appointment date, type of service, etc):*_____
_____

This health information is used/disclosed/obtained for the following purpose (*if Authorization requested by the patient put: "At the request of the individual"*): _____
_____

Specific health information to be disclosed (*check all that apply*):

□ Complete Medical Record □ Discharge Summary □ History & Physical
□ Emergency Room Records □ Labs □ Pathology
□ Radiology Reports □ Specific Dates of Service (*please specify*): _____

The health information is being disclosed for the following purpose (*please check one*):

□ Judicial/Administrative Proceedings □ Law Enforcement □ Investigation
□ Health Oversight □ Coroner/Medical Examiner □ Other: _____

By providing this Authorization, I understand as follows:

1. I understand that RMC Health System may receive financial or in-kind compensation or remuneration in exchange for the use and/or disclosure of the above-named patient's protected health information.

2. I understand that this Authorization is continuous in nature and is to be given full force and effect, including disclosing and/or utilizing any and all of the foregoing information learned or determined after the date hereof but prior to the expiration date noticed below.

3. **I understand that this Authorization may result in the sending of clinical information and x-rays with reference to the above-named patient's diagnosis and/or any alcohol, drug or child abuse problems, behavioral or mental health services, reproductive health and/or information concerning sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency syndrome (HIV). I understand that these records are strictly confidential and are solely for the information of the person to whom addressed.**

Place label here

RELEASE FOR PROTECTED HEALTH INFORMATION

4. I understand that this Authorization is voluntary. I may refuse to sign this Authorization and the above-named patient's treatment and/or payment obligations will not be affected unless either of the following applies:

   - The treatment is related to research and the use and/or disclosure is related to such research; or
   - The treatment is solely for the purpose of creating protected health information for disclosure to a third-party.

5. I understand that the health information to be released may be subject to redisclosure by the recipient of the health information and no longer protected by federal or state law.

6. I understand that I may revoke this Authorization at any time by notifying RMC Health System in writing, but if I do, it will not have any effect on uses or disclosures prior to the receipt of the revocation. Unless otherwise revoked, this Authorization will expire on _____ (date, event, or condition). If I fail to specify a date, event, or condition, this Authorization will expire in one (1) year.

7. I understand that, upon request, I may receive a copy of this Authorization form after I sign it.

8. I understand that a photocopy or facsimile of this Authorization shall be valid and effective, just as the original.

_____ _____

Signature of Patient or Patient's Representative Date

_____

Printed Name of Patient's Representative (*if applicable*)

_____

Representative's Relationship to Patient (*if applicable*)

RMC HEALTH SYSTEM

RMC Anniston RMC Stringfellow Campus
Anniston, Alabama 36207

Place label here

CONSENT FOR CAPTURING IMAGES, RECORDINGS, OR VIDEOS

Consent To Capture:
(Please check as many as apply)

_____ Audio Recordings
_____ Video Recordings
_____ Photographs
_____ Other (*please specify*: _____)

Purpose:
(Please check as many as apply)

_____ Treatment
_____ Educational
_____ Marketing
_____ Research
_____ Broadcast Media/Entertainment
_____ Law Enforcement
_____ Commemorative
_____ Other (*please specify*: _____)

Patient Name:_____ **Date of Birth:**_____

By signing this form, you give your permission for the above-named patient to be photographed, videoed, or recorded (as indicated above) for the purposes indicated above. You give this permission freely and voluntarily.

I consent to the taking of audio recordings, video recordings, photographs, or other images, as indicated above, by RMC Health System and/or its healthcare providers, employees, contractors, and medical staff members (collectively,) of the treatment and medical services the above-named patient is or will be receiving. I hereby consent under the following conditions:

(1) I give permission for RMC Health System to take, make use of, and disclose audio or video recordings, photographs, or images for the purposes indicated above. This consent extends to, but is not limited to, disclosures by RMC Health System and the patient's treating provider on websites and social media platforms, for broadcast media, in medical journals or marketing publications/materials, as well as in any printed, audio, video or other format for the purposes specified in this consent. **I understand that such audio or video recordings, photographs, or images taken, used and/or disclosed may be unflattering, embarrassing, or portray the above-named patient in a negative manner.**

(2) I have the right to request that the recording or photographing cease at any time.

(3) I am aware that information that is disclosed pursuant to this consent is public and subject to redisclosure. I am aware that the recordings and images captured will exist forever in either a recorded, printed and/or electronic version and that it may continue to be accessed, viewed, and/or used and no longer protected by applicable federal and state law.

(4) I understand that such audio or video recordings, photographs, or images shall become the property of RMC, and by signing this Consent, I release to RMC Health System any rights, title and/or interest of any kind that I may have in such items.

(5) I waive all rights I may have to any claims for payments, royalties, or any other type of remuneration or compensation in connection with the audio or video recordings, images, or photographs captured by RMC Health System and any disclosures and/or publications related thereto.

(6) I understand that photographs, videos, recordings, or images may be edited, modified, or retouched for artistic purposes or for other graphic production reasons which may or may not be within the control of RMC Health System.

(7) I understand that I may revoke or withdraw this consent at any time by notification in writing to RMC Health System. I understand that any revocation of this consent will only extend to the version of the information within RMC Health System and/or my treating provider's control that has not been previously disclosed. If not revoked or withdrawn by me, this consent will expire five (5) years from the date that I sign it.

(8) I understand that, upon request, I may receive a copy of this consent form after I sign it.

(9) I understand that a photocopy or facsimile of this consent form shall be valid and effective, just as the original.

Patient or Personal Representative Signature _____ Date: _____ Time: _____

Relationship to Patient (*if applicable*) _____

Printed Name of Personal Representative (*if applicable*) _____

MEDICAL STAFF PHOTOGRAPHING/RECORDING/FILMING PERMISSION AGREEMENT

This Medical Staff Photographing/Recording/Filming Permission Agreement ("Agreement") must be completed and signed by each medical staff member requesting permission to personally photograph/film/record treatment rendered to patients on the premises of RMC Health Care System

Name of Medical Staff Member Requesting Permission (please print): _____

Individual's Clinic Name and Address ("**Clinic**"): _____

_____

_____

Request Type *(please check all that apply)*: ☐ Photograph ☐ Film (Video) ☐ Record (Audio)

Use for the Images: _____

Intended Licensee for Images *(if applicable)*: _____

I, the undersigned, am requesting permission to personally photograph/film/record treatment rendered to patients on the premises of RMC Health System. The photographs, videos, and recordings captured (collectively, referred to herein as "**Images**") will be created, maintained, retained, used, and disclosed solely in accordance with the terms of this Agreement. By signing below, I agree to the following terms and conditions:

1. I agree to photograph/film/record solely my rendering of health care services to consenting patients for whom I am the treating physician.

2. I agree that only consenting patients should be photographed, filmed, and/or recorded, and that the Images shall not include the likeness or other information concerning any other patients, family members, RMC Health System visitors, RMC Health System staff, or medical staff members. I agree that the Images shall not include RMC Health System facilities and/or equipment, except as minimally necessary to capture the treatment interaction. I agree to de-identify the Images to the extent possible under the circumstances and to only capture and retain the minimum amount of identifiable health information necessary under the circumstances. Specifically, if the patient's face and other identifying characteristics are not required under the circumstances, such will not be captured.

3. I agree that the Images should only be captured on a device that has been approved by the RMC Health System Security Officer ("**Device**"). In that regard, prior to capturing any Images, I agree to submit the Device to the RMC Health System's Security Officer for review and approval. I understand that during the approval process, the RMC Health System Security Officer may install certain software, applications, or security measures designed to better protect and secure the Images, including, but not limited to, encryption software, remote wiping capability, anti-malware software, screen and automatic lock procedures, device management software, and password protections. By signing below, I hereby grant the Security Officer permission to install such software, applications, or security measures. I agree not to alter, amend, delete, or re-configure the software, applications, or security measures installed or implemented by the RMC Health System Security Officer without his/her prior written consent. I acknowledge and agree

that RMC Health System has the right to audit my Device at any time to ensure the appropriate software, applications, and security measures are installed therein and functioning adequately.

4. I agree not to share my Device with any other person and to retain the Device in my physical possession and control at all times.

5. I understand that a unique password and/or biometric is required for accessing the Device and the Images contained therein. I will not divulge my password to any other individual or entity or use my biometric to allow anyone else to access the Device, and I understand that my password and biometric are personal to me. I understand that I am responsible for any damages, including monetary damages, for the inappropriate access, use and/or disclosure of information by another individual using my Device. If I suspect that my password has been obtained by another individual, I will immediately change my password and inform RMC Health System's Security Officer so that appropriate action may be taken.

6. I agree to cooperate with RMC Health System regarding any investigations or audits concerning my Images and the Device. RMC Health System shall have the right, upon request, to access the Device, audit the Device, and review and remove Images from the Device.

7. I agree not to store or upload Images on the Device's "cloud" and agree to disable any automatic back-up or automatic recovery functions that would result in copies of the Images being uploaded from the Device. I agree to remove the Images from my Device in a secure manner at least once a week and prior to discarding the Device. In that regard, once the Images are removed from the Device, I agree to store the Images in a secure manner compliant with HIPAA and applicable industry standards.

8. I acknowledge that photographing/filming/recording patients without their written consent and using and/or disclosing the Images without the patient's written authorization is a breach of this Agreement and violates applicable law. Thus, before capturing any Images of any patient, I agree to notify RMC Health System's Security Officer of my intent to capture such Images, and I will ensure that the Patient Authorization for Use/Disclosure of Protected Health Information for Marketing/Educational Purposes Form and the Consent for Capturing Images, Recordings, or Videos Form have been properly executed by the patient (or the patient's personal representative) and included in the patient's record. I understand that if either form is revoked by the patient (or the patient's personal representative), the photographing, recording, and/or filming shall cease immediately and any Images captured shall not be further used and/or disclosed by me without additional patient authorization.

9. I understand that the Images captured (and the information related thereto) are private and confidential and shall be treated as such at all times. In that regard, I agree to abide by all rules, regulations, and laws relating to the privacy, confidentiality and security of patient health information, including, but not limited to, HIPAA and its implementing regulations.

10. I agree to be bound by the terms and conditions of RMC Health System's policies regarding the access, use, and disclosure of patient health information, as well as applicable policies and procedures regarding capturing Images while on the RMC Health System premises, as amended from time to time, including, but not limited to, the Photography/Videoing/Recording Policy. I understand that should I violate any provision of such policies, RMC Health System may discontinue my privilege to photograph/film/record on the RMC Health System premises and take other appropriate disciplinary action.

11. I agree to be bound by the terms of the following agreements related to the use, disclosure, licensing, distributing, etc. of the Images: _____
_____.

12. Prior to the disclosure of any Images to any production company, media developer, broadcast media producer, or similar entity or person (a "**Licensee**"), I agree to submit the Images, along with the name of the Licensee and purpose of the disclosure, to RMC Health System's Privacy Officer for review and approval, and agree not to disclose the Images to any Licensee without the prior written approval of RMC Health System's Privacy Officer. In other words, I shall only disclose Images to Licensees that have been reviewed and approved in writing by RMC Health System's Privacy Officer.

13. I understand that with regard to intellectual property rights, RMC Health System is the copyright holder and has the sole ability to license the Images. In that regard, I agree that I have no right to license and/or distribute the Images without the prior written consent of RMC Health System. To the extent necessary to confirm RMC Health System's title to the Images, I hereby assign to RMC Health System all right, title, and interest in and to the Images, including, without limitation, all copyright interests and goodwill embodied therein, to RMC Health System.

14. I will immediately report to RMC Health system's Security Officer any unauthorized access, use, or disclosure of the Images. I agree to actively mitigate, prevent, and cure any privacy breaches, and to work cooperatively with RMC Health System in its efforts to mitigate, prevent, and cure any privacy breaches.

15. I understand that this Agreement does not pertain to any Images captured by RMC Health System in the routine course of treatment (*e.g.*, endoscopy, laparoscopy, diagnostic images, telemedicine), and only relates to Images personally captured by me. Thus, I understand that RMC Health system will not retain the Images (except when the Images are captured for treatment purposes and made available to RMC Health System for incorporation into the medical record) and that it is my sole obligation to retain, maintain, use, and disclose the Images in accordance with applicable law. In that regard, I acknowledge that the Images will not be incorporated into RMC Health System's medical record (except as stated above) and will not be used by RMC Health System staff to make decisions regarding the patient's course of treatment.

16. I agree to undergo any additional training required by RMC Health System in connection with obtaining and/or retaining the privilege granted herein.

17. I agree to notify my professional liability insurance carrier that I am capturing and retaining Images and agree to obtain the carrier's permission before doing so.

18. I recognize that the privilege granted herein may be terminated by RMC Health System at any time, with or without cause

19. I acknowledge that this Agreement does not cover requests by third-parties (*e.g.*, TV crews, news media, etc.) to photograph, film, or record on RMC Health System's premises, and that such requests shall be submitted to and approved by RMC Health System Security Officer.

20. I agree to hold harmless, indemnify and defend RMC Health System, and its officers, directors, employees, successors, representatives and assigns, from and against any and all liabilities, costs, damages, suits, judgments, fines, losses, demands or expenses of any kind whatsoever (including, but not limited to, court costs, arbitration fees, if applicable, and attorneys' fees and expenses

actually and reasonably incurred) from or attributable to: (a) my breach of this Agreement, including, but not limited to, my failure to obtain appropriate consent and authorization to capture, use, and disclose the Images, or (b) my negligent or intentional acts and/or omissions with regard to the Device and the Images. By signing below, I acknowledge that I have read, understand, and agree with the conditions above.

Medical Staff Member's Signature: _____

Date: _____

To Be Completed by **RMC Health System.**

Device Reviewed and Approved On: _____ (insert date)

Device Reviewed and Approved By (print name): _____
(signature): _____

Permission Granted On: _____ (insert date)

Permission Granted By (print name) : _____
(signature): _____

Permission Terminated On: _____ (insert date)

Permission Terminated By (print name): _____
(signature): _____

Title: Photography/Videoing/Recording Policy

Effective Date: _01/01/2020__

Purpose:

1. To facilitate compliance with the Health Insurance Portability and Accountability Act ("HIPAA"), the Heath Information Technology for Economic and Clinical Health Act ("HITECH"), and their implementing regulations, and any and all other applicable Federal or state law, regulations and interpretive guidelines.

2. To establish guidelines for situations where patients, visitors, and/or workforce members may or may not be photographed, recorded, or otherwise imaged while on or within the premises of the RMC Health System

Definitions:

1. Recording: Recording an individuals' voice using video recording (*e.g.*, video cameras, cellular telephones), tape recorders, or other technologies capable of capturing audio or transmitting sound.

2. Authorization: The patient's or patient's legal representative's written authorization for the use and/or disclosure of protected health information. The authorization is only good for the type of protected health information indicated and the timeframe listed in the authorization. Otherwise, a new authorization form must be obtained. The appropriate authorization form is the Patient Authorization for Use/Disclosure of Protected Health Information or the Patient Authorization for Use/Disclosure of Protected Health Information for Marketing/Educational Purposes.

3. Consent: The patient's or patient's legal representative's written consent to being photographed or recorded. The consent is only good for the type of photographs, videos, or recordings indicated and the timeframe listed in the consent. Otherwise, a new consent form must be obtained. The appropriate consent form is the Consent for Capturing Images, Recordings, or Videos Form or the Conditions of Admission or Consent for Treatment Form (if capturing for security or general healthcare operations purposes).

4. Photography: Recording an individual's likeness (*e.g.,* image, picture) using photography (*e.g.*, cameras, cellular telephones), video recording (*e.g.*, video cameras, cellular telephones), digital imaging (*e.g.*, digital cameras, web cameras) or other technologies capable of capturing an image and/or video (*e.g.*, Skype).

5. Workforce Member: Employees, volunteers, and other persons whose conduct, in performance of work for RMC Health System, is under direct control of RMC Health System, whether or not they are paid by RMC Health System or the Health Care Authority of the City of Anniston. As used herein, providers are considered workforce members.

6. Provider: Anyone with authority granted by the Medical Staff Executive Committee to perform independent licensed patient care (*e.g.*, physician, CRNP, CRNA, etc.).

Policy Statement:

1. In General:

   a. RMC Health System shall take reasonable steps to protect patients, visitors, and workforce members from unauthorized photography or recording. Due to the sensitive nature of patient information and to protect patient privacy, RMC Health System and its workforce members must follow the guidelines and procedures outlined herein before allowing, or prior to, photographing or recording patients and workforce members.

   b. RMC Health System may refuse to permit any person or workforce member from photographing or recording any person if it violates the privacy or jeopardizes the safety of anyone or is determined to be disruptive to patient care or RMC Health System's operations.

   c. For violations of this policy, sanctions shall be applied in accordance with RMC Health System's Sanctions for Privacy and Information Security Violations policy.

   d. The following limited circumstances may be used to capture or record a patient's likeness or voice using photography and/or recording:

      i. Any workforce member intending to personally photograph or record a patient on a personal device for any reason (*i.e.*, a non-RMC Health system device) must first seek approval from the Medical Staff Executive Committee and execute the Medical Staff Photographing/Recording/Filming Permission Agreement. Personal cellular telephones, iPADs, cameras, etc. may only be used to capture or record a patient's likeness, image, or voice if they have been submitted to and approved by RMC Health System's Security Officer. During the approval process, as appropriate, the Security Officer may install certain software, applications, or security measures designed to better protect and secure the image captured. The software, applications, or security measures shall not be altered, amended, deleted, or re-configured without the prior written consent of RMC Health System's Security Officer. RMC Health System may audit the devices at any time.

      ii. RMC Health System policies and procedures address how devices should be securely stored, and how photographs or recordings shall be saved, securely stored, and disposed of by workforce members.

      iii. Photographs or recordings shall not be permanently stored on the device (*e.g.*, camera), on unencrypted memory cards, on the Device's "cloud," or in any other unsecure manner and must be deleted within one (1) week from the device. Any automatic back-up or automatic recovery functions that would result in copies of the photographs or recordings being uploaded from the device should be disabled.

iv. If the photograph or recording is being used for any purpose other than a clinical/treatment purpose, unless stated otherwise herein, RMC Health System will not retain a copy of the photograph or recording in the hospital medical record or in the patient's designated record set, as defined by HIPAA. A copy of the photograph or recording may be retained by the treating provider as appropriate under applicable law and in accordance with RMC Health System's policies and procedures.

v. Photographing and/or recording should cease immediately at the request of the patient and/or treating provider. The patient has the right to refuse to being photographed or recorded, and may withdraw his/her consent and/or authorization at any time in writing.

e. With regard to the disclosure of photographs or recordings, the following shall apply:

i. Photographs or recordings shall not be released without specific written authorization from the patient, unless the disclosure is for treatment, payment or health care operations purposes or is otherwise permitted under applicable law without patient authorization.

ii. Unless prohibited by law, photographs and recordings contained in the patient's designated record set, as defined by HIPAA, may be released to the patient in accordance with the Patients' Right to Access Policy. See Patient's Right to Access Policy.

iii. RMC Health System will retain all originals when photographs or recordings retained by RMC Health System are disclosed by RMC Health System.

iv. Photographs or recordings may not be disclosed to any production company, media developer, broadcast media producer or similar entity or person without RMC Health System's prior review and written approval.

v. With regard to the intellectual property rights, RMC Health System is the copyright holder and has the sole ability to license the photographs and recordings.

2. Photographing/Recording Patients in the Routine Course of Treatment Using RMC Health System-Owned Device or Equipment:

a. Written patient informed consent is required before workforce members may photograph or record a patient for treatment purposes. See Consent Policy and Procedure. Endoscopy or laparoscopy will require the Photography Consent NS 042 to be signed by the patient.

b. If written consent is obtained, workforce members may photograph and/or record patients in the routine course of treatment using an RMC Health System-owned device or equipment. This includes diagnostic imaging, endoscopy, laparoscopy, telemedicine, or images of specimens.

c. Photographs or records may be used and/or disclosed for treatment purposes without patient authorization.

d. A copy of the photograph or recording will be kept by RMC Health System and included in the hospital medical record.

e. A copy of the photograph or recording will be made available to the treating provider as appropriate under applicable law and in accordance with RMC Health System's policies and procedures.

3. Photographing/Recording Patients by Workforce Members for Treatment Purposes Using a Personal Device:

   a. Written patient informed consent is required before workforce members may photograph or record a patient for treatment purposes. See Consent Policy and Procedure.

   b. Photographs or records may be used and/or disclosed for treatment purposes without patient authorization.

   c. A copy of the photograph or recording will be kept by RMC Health System and included in the hospital medical record only if such photograph or recording is made available by the workforce member to RMC Health System. Refer to the RMC Health System Designated Record Set Policy to determine which photographs or recordings must be made available to RMC Health System and stored in the hospital medical record.

   d. A copy of the photograph or recording may be retained by the treating provider as appropriate under applicable law and in accordance with RMC Health System's policies and procedures.

4. Photographing/Recording Patients and Workforce Members by Patients, Family Members, and/or the Patient's Visitors:

   a. Photographing or recording a patient by a family member or visitor is permitted unless the patient objects. However, patients, family members, and/or visitors are not permitted to take photographs or recordings of other patients or in common areas of the facility. Workforce members should not be photographed or recorded without consent.

   b. To the extent a workforce member is aware of any inappropriate attempt to photograph or record a patient and/or workforce member, the workforce member must take reasonable steps to ensure that patients and/or workforce members are not inappropriately photographed or recorded within RMC Health System by a patient or the patient's family members or visitors.

   c. RMC Health System workforce members have the discretion and authority to require that such photographing or recording cease immediately and to contact security when necessary.

5. Photographing/Recording Patients by Workforce Members for Security or General Health Care Operations Purposes:

a. The Conditions of Admission or Consent for Treatment form advises patients that photographs or recordings may be taken for security or general health care operations purposes (*e.g.*, quality assurance).

b. Photographs or records may be used and/or disclosed for the general health care operations of RMC Health Systemwithout patient authorization.

c. Photographs or records may be used and/or disclosed for security purposes without patient authorization as long as such uses and/or disclosures are allowed by applicable state and federal law.

d. This policy does not apply to general security surveillance of public areas, which is permitted without patient consent. However, the use and/or disclosure of such surveillance videos and/or images must comply with applicable state and federal law.

6. Photographing/Recording Patients by Workforce Members to Document Abuse or Neglect:

   a. Patient consent or authorization is generally not required to document and report abuse or neglect; however, the photographs or recordings may not be used and/or disclosed for any other purpose beyond submission to the appropriate reporting agency unless otherwise permitted by federal or state law (*e.g.*, for treatment purposes). See Sanie Policy

   b. Documentation of the need/benefit to take photographs or recordings to document abuse or neglect should be retained in the medical record. A copy of the photograph or recording shall be included in the hospital medical record.

7. Photographing/Recording Patients by Workforce Members for Research:

   a. Written patient informed consent is required before workforce members may photograph or record a patient for research purposes.

   b. Any use and/or disclosure of photographs or recordings for research purposes will be in compliance with state and federal regulations concerning privacy and research.

   c. If a photograph or recording is determined to be identifiable, the Institutional Review Board overseeing the specific research project will determine if additional patient authorization is required.

   d. A copy of the photograph or recording shall be included in the hospital medical record.

8. Photographing/Recording Patients by Workforce Members for Educational, Publicity, or Marketing Purposes:

   a. RMC Health System must obtain written consent from the patient prior to photographing or recording a patient for educational, publicity, or marketing purposes.

b. RMC Health System must obtain an "Authorization for Use and Disclosure of PHI for Marketing/Educational Purposes" prior to using and/or disclosing any photograph or recording for marketing, publicity or educational purposes.

9. Photographing/Recording Patients by the News Media:

   a. RMC Health System may permit news media to photograph or record a patient if the patient consents in writing.

   b. RMC Health System may disclose photographs and/or recordings to the news media with patient authorization.

10. Photographing/Recording Patients by and/or for Law Enforcement:

   a. RMC Health System may permit law enforcement agencies to photograph or record a patient if the patient consents in writing, or if such consent is not required by applicable law.

   b. RMC Health System may disclose photographs and/or recordings to law enforcement without patient authorization when required by state law, such as child abuse and neglect, domestic violence, elder abuse, rape, and similar disclosures required and/or allowed by law. Documentation of the need/benefit to take photographs or recordings for law enforcement purposes should be retained in the medical record.

   c. As appropriate, a copy of the photograph or recording shall be included in the hospital medical record.

11. Photographing/Recording of Patients or the Patient's Visitors within RMC Health System by Workforce Members for Personal Use or Any Other Use Not Specified Herein:

   a. Workforce members are prohibited from photographing or recording patients or the patient's visitors within RMC Health System for personal use or for any use not specified herein, including, but not limited to,

      i. taking pictures to share with friends and/or co-workers,

      ii. to post on the internet using social media (*e.g.*, Facebook, YouTube, Twitter), etc.

   b. However, if the recording or posting is for educational or marketing purposes, such is permissible if the procedures outlined in Section 8 are followed.

12. Photographing/Recording of Patients for Gifts or Commemorative Purposes:

   a. In order for RMC Health System to photograph or record a patient when the photograph or record will be given as a gift or sold to the patient, written consent must be obtained.

   b. If the photograph or record is to be given or sold to anyone other than the patient, a patient authorization must be obtained.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

USE AND DISCLOSURE OF PHI FOR FUNDRAISING

1. General Rule.

(a) We may use, or disclose to a Business Associate or to an institutionally related foundation, the following protected health information for the purpose of raising funds for our own benefit, without an Authorization:

(i) Demographic information relating to an individual, including name, address, other contact information, age, gender, and date of birth;

(ii) Dates of health care provided to the individual;

(iii) The department or area of service that provided the individual treatment;

(iv) The individual's treating physician;

(v) Outcome information; and

(vi) Health insurance status.

(b) We have included a statement that we may contact individuals to raise funds in our HIPAA Privacy Notice.

(c) We will not condition treatment or payment on the individual's choice with respect to receiving fundraising communications.

2. Opportunity to Opt-Out of Fundraising.

(a) Each fundraising communication sent to individuals shall include information set out in a clear and conspicuous manner how the individual may elect not to receive ("opt-out") any further fundraising communications from our organization. The method for opting-out of further fundraising communications cannot cause the individual to incur an undue burden or more than nominal cost.

(b) When an individual elects to opt-out of receiving further fundraising communications, no further fundraising communications shall be sent to the individual by our organization.

(c) We may provide an individual who has elected to opt-out of receiving further fundraising communications with a method to opt back in to receive fundraising communications.

(d) All opt-out notices informing our organization that an individual does not wish to be contacted for fundraising purposes shall be forwarded to our HIPAA Privacy Officer.

(e) The HIPAA Privacy Officer shall be responsible for receiving, documenting, and ensuring that individuals who decide to opt-out of receiving future fundraising communications are not sent any additional fundraising materials.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

USE AND DISCLOSURE OF PHI CONTAINING PSYCHIATRIC/MENTAL INFORMATION

Records containing psychiatric/mental health information are considered privileged and require proper patient authorization before disclosing these records to any individual who is not afforded access by law.

A subpoena is not sufficient to release psychiatric/mental health information, regardless to how the subpoena reads, unless patient or proper authorization accompanies it. A court order will be required if there is no proper authorization along with the subpoena.

NOTE: The Health Care Authority does maintain psychotherapy notes, as defined by HIPAA.

1. **Use of an Authorization**. To the extent we maintain psychotherapy notes as defined by the Privacy Rule, we will obtain an Authorization for any use or disclosure of psychotherapy notes except:

(a) To carry out the following:

(i) Use by the originator of the psychotherapy notes for treatment;

(ii) Use or disclosure by us in our own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling; or

(iii) Use or disclosure by us to defend a legal action or other proceeding brought by a patient.

(b) Where the use or disclosure is to the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the Privacy Rules;

(c) Where the use or disclosure is required by Law, to the extent that such use or disclosure complies with and is limited to the relevant requirements of such law;

(d) Where the use or disclosure is for health oversight activities with respect to the oversight of the originator of the psychotherapy notes;

(e) Where the use or disclosure is to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties imposed by law; and to funeral directors as permitted by law and as necessary to carry out the funeral director's duties with respect to the decedent; or

(f) Where we believe, in good faith, that the use or disclosure is necessary to avert a serious threat to the health or safety of a person or the public and the use or disclosure is to persons reasonably able to prevent or lessen the threat, including the target of the threat, or is necessary for law enforcement authorities to identify or apprehend an individual.

(g) We will not combine an Authorization for disclosure of psychotherapy notes with any other document to create a compound Authorization, except where it is combined with another

Authorization for a use or disclosure of psychotherapy notes and such combination is permitted by the Privacy Rules.

The Health Care Authority also maintains mental health and behavioral health records that contain psychiatric/mental health information considered privileged and require proper patient authorization before disclosing these records to any individual who is not permitted access by law.

With very limited exceptions, a subpoena is not sufficient to release psychiatric/mental health information, regardless how the subpoena reads, unless patient authorization or other proper authorization accompanies it. Generally, a court order is necessary if there is no proper authorization along with the subpoena.

2. Psychiatrist/Physician Requesting.

If the physician has treated the patient here at The Health Care Authority, the physician may have access to the patient's record.

If the physician is not a treating physician of record, then patient authorization is required to access the patient's record.

3. Patient Requesting.

Notify psychiatric physician of request so physician can determine that the information will not have an adverse effect on the patient or any other individual if disclosed. Inform the patient that you must get authorization from their physician to disclose the records.

(a) Physician can agree to disclose copies of records. Should the physician agree to the disclosure, a statement of disclosure shall be secured and placed in the patient's record prior to disclosing any information to the patient.

(b) If the physician denies the request, the statement of nondisclosure must be secured from the physician and placed in the patient's record.

(c) If the physician denies the request, the patient may seek a second opinion.

- If the second physician denies the request, a statement of nondisclosure containing the reason(s) for the denial must be placed in the correspondence section of the patient's medical record. The patient must secure a court order in order to access the records.

- If the second physician approves disclosure of the records to the patient, the records may be disclosed after a written statement of release containing the approval for disclosure is placed in the correspondence section of the patient's medical record.

4. All Other Requestors.

Review the request to ensure proper authorization by the patient or legal representative. Walk-in request will need to have patient or proper authorization and photo identification. Reasonable copy/processing time should be allowed. Copying fees may be applied as appropriate and in accordance with state and federal law.

Psychiatric/mental information should not be transmitted via facsimile machine, E-mail, or disclosed over the telephone unless emergently needed for patient care.

5. **Emergency Situation.**

(a) Psychiatric/mental information may be disclosed to health care requestors without patient authorization if obtaining authorization would cause a potentially dangerous delay in treatment. The "Call-back" system shall be followed to verify identity and address of the health care provider requesting the information. Two employees must hear the information given by the requestor on call back. Information should include the following:

- Identity and credential of person requesting the information;
- Reason for the disclosure;
- Information needed; and
- Reason authorization could not be obtained.

(b) Information regarding disclosure should be documented on a proper authorization form and noted that it was an emergency request. The form should be signed and dated by the two employees and placed in the correspondence section of the patient's medical record.

6. **Alabama State Law.** We recognize that psychiatric/mental information may be further protected by Alabama law and/or other applicable law. Prior to using or disclosing psychiatric/mental information, we will determine if the use or disclosure is further restricted and protected beyond the standards imposed by HIPAA.

➢ **Form: Patient Authorization for Release of Psychotherapy Notes and/or Mental/Behavioral Health Records**

RMC
Regional Medical Center
Anniston

400 East Tenth Street, Post Office Box 2208
Anniston, Alabama 36202
256.235.5121
www.rmccares.org

HEALTH INFORMATION SERVICES

DATE: _____

Dear Dr. _____:

Please be advised that your patient, _____

(Medical Record # _____), has requested copies of medical

for the following dates of service:

_____

_____

_____

When psychiatric, drug or alcohol-related protected health information (PHI) is requested by the patient, it is our policy to secure approval from the physician who treated the patient prior to releasing this information. At no time will psychosocial notes be released.

To streamline this process, we developed this form for you to utilize in corresponding to this request.

If you would like to review the records prior to responding, you may utilize the ChartMaxx imaging system (if you have access in your office) or contact us at Extension #5763 and our correspondence personnel will assist you.

_____ **I authorize Health Information Services to release copies of the above requested medical records to the patient listed above.**

_____ **I do not authorize Health Information Services to release copies of the above requested medical records based upon the clinical determination that access would be detrimental to the patient's health or may cause harm to patient or others. [Code of Alabama, Section 22-56-4 (7)]**

_____ _____

Physician Signature Date

Please return to Health Information Services – Correspondence Section

Phone: (256) 235-5763 Fax: (256) 235-5094

RMC HEALTH SYSTEM

Consent for Disclosure of 42 C.F.R. Part 2 Records (Treatment, Payment, and Healthcare Operations)

Patient Name:	Date of Birth:

I understand that certain substance use disorder treatment records are protected under Federal law and may only be disclosed in certain instances with my written consent. I hereby consent to and authorize The Health Care Authority of the City of Anniston d/b/a Northeast Alabama Regional Medical Center and/or its healthcare providers, employees, contractors, and medical staff members ("RMC") to disclose the above-named patient's health information indicated below to my treatment providers, third party payors or others responsible for payment, and/or people and/or entities helping to operate the RMC Part 2 Program.

The specific health information to be disclosed may include the above-named patient's entire medical record, or any sub-part thereof that is necessary for the relevant treatment, payment or healthcare operations purpose.

If the receiving entity is a covered entity or business associate, as defined by HIPAA, the information may be re-disclosed by the receiving entity in accordance with the permissions granted by applicable law, except for uses and disclosure for civil, criminal, administrative, and legislative proceedings against the above-named patient.

The health information is being disclosed for treatment, payment, and/or healthcare operations purposes.

By providing this Consent, I understand as follows:

1. **I understand that this Consent may result in the sending of clinical information with reference to the above-named patient's diagnosis and/or any substance abuse treatment services, behavioral or mental health services, physician notes and orders, evaluation and assessments, medical history, laboratory and test results, attendance and participation in substance abuse treatment programs, and date of discharge or status.**
2. I understand that I may also be asked to sign a HIPAA Authorization for the disclosure of protected heath information.
3. I understand that if any of the patient's information is protected by the psychotherapist-patient privilege, counselor-client privilege, or any other applicable privilege that I hereby waive such privileges with respect to the information disclosed.
4. I understand that information concerning the patient's presence and participation in an alcohol and drug treatment program, as well as substance abuse treatment records, are protected by Federal confidentiality regulations, codified at 42 C.F.R. Part 2, and that this information cannot be disclosed without written consent or unless otherwise disclosed in accordance with applicable law. I understand that applicable law will permit redisclosure under certain circumstances and that such information may no longer be protected by 42 C.F.R. Part 2.
5. I also understand that I may revoke this Consent at any time by notifying RMC in writing except to the extent that action has been taken in reliance on this Consent prior to receipt of the revocation.
6. I understand that this Consent is continuous in nature and is to be given full force and effect, including disclosing any and all of the foregoing information learned or determined after the date hereof but prior to the expiration date. If not previously revoked, this Consent shall expire automatically one (1) year following the end of my treatment by RMC.
7. I understand that this Consent is voluntary. If I refuse to sign this Consent, the above-named patient's treatment and/or payment obligations may be impacted by RMC's inability to provide protected healthcare information for treatment, payment and healthcare operations.
8. I understand that, upon request, I may receive a copy of this Consent form after I sign it.
9. I understand that a photocopy or facsimile of this Consent shall be valid and effective, just as the original.

By signing this Consent, I acknowledge that I have read and understand the information contained in this form and that I accept its terms, either on behalf of myself as the patient, or on behalf of the patient as his/her authorized legal representative.

Signature of Patient or Patient's Representative	Date
Printed Name of Patient's Representative (*if applicable*)	Representative's Relationship to Patient (*if applicable*)

If you are signing as the personal representative, you may be asked to submit proof of your authority to act as the personal representative of the patient.

NOTICE TO PERSON(S) AND/OR ORGANIZATION(S) RECEIVING CONFIDENTIAL PATIENT INFORMATION: 42 C.F.R. Part 2 prohibits unauthorized disclosure of these records.

RMC HEALTH SYSTEM

Patient Authorization for Use and/or Disclosure of Protected Health Information

Patient Name:	Date of Birth:

Address: _____ Phone Number _____

Email Address: _____

I hereby authorize the disclosure of the above-named patient's health information as follows:

☐ **use the following health information maintained by RMC Health System until:** _____ **Expiration Date/ will expire one year from signed date unless otherwise specified above.**	☐ **disclose the following health information to:** _____ **Address:** _____ **City, State, Zip:** _____ **Phone:** _____	☐ **obtain the following health information from:** _____ **Address:** _____ City, State, Zip _____ Phone: _____

Specific description of the health information to be used/disclosed/obtained (*include dates of service, i.e., appointment date, type of service, etc):* _____

This health information is used/disclosed/obtained for the following purpose (*if Authorization requested by the patient put: "At the request of the individual"*): _____

Specific health information to be disclosed (*check all that apply*): RMC Health System ☐ RMC Health Clinic ☐

- ☐ Complete Medical Record
- ☐ Discharge Summary
- ☐ History & Physical
- ☐ Emergency Room Records
- ☐ Labs
- ☐ Pathology
- ☐ Radiology Reports
- ☐ Specific Dates of Service (*please specify*): _____

The health information is being disclosed for the following purpose (*please check one*):

- ☐ Judicial/Administrative Proceedings
- ☐ Law Enforcement
- ☐ Investigation
- ☐ Health Oversight
- ☐ Coroner/Medical Examiner
- ☐ Personal
- ☐ Other: _____

By providing this Authorization, I understand as follows:

By providing this Authorization, I understand as follows:

1. I understand that RMC Health System may receive financial or in-kind compensation or remuneration in exchange for the use and/or disclosure of the above-named patient's protected health information.

2. I understand that this Authorization is continuous in nature and is to be given full force and effect, including disclosing and/or utilizing any and all of the foregoing information learned or determined after the date hereof but prior to the expiration date noticed below.

3. **I understand that this Authorization may result in the sending of clinical information and x-rays with reference to the above-named patient's diagnosis and/or any alcohol, drug or child abuse problems, behavioral or mental health services, reproductive health and/or information concerning sexually**

transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency syndrome (HIV). I understand that these records are strictly confidential and are solely for the information of the person to whom addressed.

4. I understand that this Authorization is voluntary. I may refuse to sign this Authorization and the above-named patient's treatment and/or payment obligations will not be affected unless either of the following applies:

   - The treatment is related to research and the use and/or disclosure is related to such research; or
   - The treatment is solely for the purpose of creating protected health information for disclosure to a third-party.

5. I understand that the health information to be released may be subject to redisclosure by the recipient of the health information and no longer protected by federal or state law.

6. I understand that I may revoke this Authorization at any time by notifying RMC Health System in writing, but if I do, it will not have any effect on uses or disclosures prior to the receipt of the revocation. Unless otherwise revoked, this Authorization will expire on _____ (date, event, or condition). If I fail to specify a date, event, or condition, this Authorization will expire in one (1) year.

7. I understand that, upon request, I may receive a copy of this Authorization form after I sign it.

8. I understand that a photocopy or facsimile of this Authorization shall be valid and effective, just as the original.

_____	_____
Signature of Patient or Patient's Representative	Date
_____	_____
Printed Name of Patient's Representative (*if applicable*)	Representative's Relationship to Patient (*if applicable*)

If you are signing as the personal representative, you may be asked by the Releasing Entity to submit proof of your authority to act as the personal representative of the patient.

RMC HEALTH SYSTEM

Patient Authorization for Disclosure of Protected Health Information

Patient Name:	Date of Birth:
Address:	Account Number:

I hereby authorize RMC Health System ("RMC") to disclose the above-named patient's health information, as described below, to the following:

Dr. Lola Johnston
Director of Counseling Services
Jacksonville State University
700 Pelham Road North
Jacksonville, AL 36265
256-782-8684

Specific description of the health information to be disclosed (*include dates of service, i.e., appointment date, type of service, etc):* **medical records regarding the treatment received by the above-named patient at RMC following referral from the JSU Health Clinic**.

This health information is used/disclosed/obtained for the following purpose (*if Authorization requested by the patient put: "At the request of the individual"*): **continuing monitoring, oversight, and care coordination of the above-named student/patient.**

By providing this Authorization, I understand as follows:

1. I understand that RMC Health System may receive financial or in-kind compensation or remuneration in exchange for the use and/or disclosure of the above-named patient's protected health information.

2. I understand that this Authorization is continuous in nature and is to be given full force and effect, including disclosing and/or utilizing any and all of the foregoing information learned or determined after the date hereof but prior to the expiration date noticed below.

3. **I understand that this Authorization may result in the sending of clinical information and x-rays with reference to the above-named patient's diagnosis and/or any alcohol, drug or child abuse problems, behavioral or mental health services, reproductive health and/or information concerning sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency syndrome (HIV). I understand that these records are strictly confidential and are solely for the information of the person to whom addressed.**

4. I understand that this Authorization is voluntary. I may refuse to sign this Authorization and the above-named patient's treatment and/or payment obligations will not be affected unless either of the following applies:

   - The treatment is related to research and the use and/or disclosure is related to such research; or
   - The treatment is solely for the purpose of creating protected health information for disclosure to a third-party.

5. I understand that the health information to be released may be subject to redisclosure by the recipient of the health information and no longer protected by federal or state law.

6. I understand that I may revoke this Authorization at any time by notifying RMC in writing, but if I do, it will not have any effect on uses or disclosures prior to the receipt of the revocation. Unless otherwise revoked, this Authorization will expire on _____ (date, event, or condition). If I fail to specify a date, event, or condition, this Authorization will expire in one (1) year.

7. I understand that, upon request, I may receive a copy of this Authorization form after I sign it.

8. I understand that a photocopy or facsimile of this Authorization shall be valid and effective, just as the original.

_____ _____
Signature of Patient or Patient's Representative Date

_____
Printed Name of Patient's Representative (*if applicable*)

_____
Representative's Relationship to Patient (*if applicable*)

RMC HEALTH SYSTEM

Consent for Disclosure of 42 C.F.R. Part 2 Records (Treatment, Payment, and Healthcare Operations)

Patient Name:	Date of Birth:

I understand that certain substance use disorder treatment records are protected under Federal law and may only be disclosed in certain instances with my written consent. I hereby consent to and authorize The Health Care Authority of the City of Anniston d/b/a Northeast Alabama Regional Medical Center and/or its healthcare providers, employees, contractors, and medical staff members ("RMC") to disclose the above-named patient's health information indicated below to my treatment providers, third party payors or others responsible for payment, and/or people and/or entities helping to operate the RMC Part 2 Program.

The specific health information to be disclosed may include the above-named patient's entire medical record, or any sub-part thereof that is necessary for the relevant treatment, payment or healthcare operations purpose.

If the receiving entity is a covered entity or business associate, as defined by HIPAA, the information may be re-disclosed by the receiving entity in accordance with the permissions granted by applicable law, except for uses and disclosure for civil, criminal, administrative, and legislative proceedings against the above-named patient.

The health information is being disclosed for treatment, payment, and/or healthcare operations purposes.

By providing this Consent, I understand as follows:

1. **I understand that this Consent may result in the sending of clinical information with reference to the above-named patient's diagnosis and/or any substance abuse treatment services, behavioral or mental health services, physician notes and orders, evaluation and assessments, medical history, laboratory and test results, attendance and participation in substance abuse treatment programs, and date of discharge or status.**
2. I understand that I may also be asked to sign a HIPAA Authorization for the disclosure of protected heath information.
3. I understand that if any of the patient's information is protected by the psychotherapist-patient privilege, counselor-client privilege, or any other applicable privilege that I hereby waive such privileges with respect to the information disclosed.
4. I understand that information concerning the patient's presence and participation in an alcohol and drug treatment program, as well as substance abuse treatment records, are protected by Federal confidentiality regulations, codified at 42 C.F.R. Part 2, and that this information cannot be disclosed without written consent or unless otherwise disclosed in accordance with applicable law. I understand that applicable law will permit redisclosure under certain circumstances and that such information may no longer be protected by 42 C.F.R. Part 2.
5. I also understand that I may revoke this Consent at any time by notifying RMC in writing except to the extent that action has been taken in reliance on this Consent prior to receipt of the revocation.
6. I understand that this Consent is continuous in nature and is to be given full force and effect, including disclosing any and all of the foregoing information learned or determined after the date hereof but prior to the expiration date. If not previously revoked, this Consent shall expire automatically one (1) year following the end of my treatment by RMC.
7. I understand that this Consent is voluntary. If I refuse to sign this Consent, the above-named patient's treatment and/or payment obligations may be impacted by RMC's inability to provide protected healthcare information for treatment, payment and healthcare operations.
8. I understand that, upon request, I may receive a copy of this Consent form after I sign it.
9. I understand that a photocopy or facsimile of this Consent shall be valid and effective, just as the original.

By signing this Consent, I acknowledge that I have read and understand the information contained in this form and that I accept its terms, either on behalf of myself as the patient, or on behalf of the patient as his/her authorized legal representative.

Signature of Patient or Patient's Representative	Date
Printed Name of Patient's Representative (*if applicable*)	Representative's Relationship to Patient (*if applicable*)

If you are signing as the personal representative, you may be asked to submit proof of your authority to act as the personal representative of the patient.

NOTICE TO PERSON(S) AND/OR ORGANIZATION(S) RECEIVING CONFIDENTIAL PATIENT INFORMATION: 42 C.F.R. Part 2 prohibits unauthorized disclosure of these records.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PROHIBITION ON SALE OF PHI

Except as permitted below, The Health Care Authority shall not directly or indirectly receive remuneration or payment in exchange for the release of any PHI unless The Health Care Authority Obtains a valid authorization from the patient who is the subject of the health information and such authorization includes a specification as to whether the health information can be further exchanged for remuneration or payment by the entity receiving the health information.

The prohibition against selling PHI shall not apply if the exchange is for:

(a) Public health activities, as described in 45 CFR § 164.512 or 164.514;

(b) Research, as defined and described in 45 CFR §§ 164.501 and 164.512, but only if the price charged reflects the costs of preparation and transmittal of the data for such purpose;

(c) Treatment and payment purposes;

(d) Health care operations associated with the sale, transfer, merger or consolidation of all or part of our organization and for related due diligence;

(e) To or by a Business Associate for activities that the Business Associate undertakes on our behalf, and the only remuneration provided is by us to the Business Associate for the performance of such activities;

(f) Providing a patient with a copy of and access to his/her health information pursuant to 45 CFR § 164.524;

(g) As required by law; or

(h) Any other purpose as determined and approved by HHS.

➢ **Form: Patient Authorization for Use and/or Disclosure of PHI**

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PERSONAL REPRESENTATIVES OF PATIENTS

Generally, where a person has the right to make a health care decision then he/she has the right to control the information associated with that decision. There may be times when patients are legally or otherwise incapable of exercising their rights, or simply choose to designate another person to act on their behalf with respect to their rights. A person authorized under Alabama law or other applicable law to act on behalf of an individual in making health care related decisions is generally referred to as the patient's "personal representative".

A personal representative is recognized and treated as the patient with respect to uses and disclosures of the patient's PHI when that person has the legal authority to act on a patient's behalf. Because a personal representative's power may be limited as to the manner in which he/she is legally authorized to act on matters related to health care, we shall exercise professional judgment in verifying the scope and extent of a representative's authority. This shall include consulting HIPAA, Alabama law, and any other applicable law, as well as ensuring that a personal representative has the necessary legal documentation to demonstrate his/her authority.

1. Adults and Emancipated Minors.

If, under applicable law, a person has legal authority to make health care related decisions on behalf of a patient who is an adult or "emancipated minor" (*i.e.*, an individual less than nineteen (19) years old, but who is deemed independent usually as a result of a court order or an event such as marriage), this person will be treated as a representative of the patient with respect to PHI relevant to such representation. Examples of individuals with legal authority to make health care decisions on behalf of an adult or emancipated minor include, but are not limited to, persons with a durable power of attorney and persons acting as court appointed legal guardians.

2. Unemancipated Minors.

A "minor" is generally defined as a person who has not realized full legal-age. In Alabama, this means a person who is under nineteen (19) years of age and who has not otherwise been "emancipated". (*See* Section 1 for a definition of an "emancipated minor".)

(a) **General Rule.** If, under applicable law, a parent, guardian, or other person acting *in loco parentis* ("in place of a parent") has authority to act and make health care decisions on behalf of an individual who is an unemancipated minor, such person will be treated as a personal representative of the minor with respect to PHI relevant to such representation, except in the following circumstances where a minor is deemed to have the authority to control the manner in which his/her PHI is used and disclosed:

(i) The minor consents to health care services and no other consent for such services is required by law, regardless of whether the consent of another person has been obtained (*e.g.*, where a minor's parent also consents to health care services), and the minor has not requested that such person be treated as his/her personal representative;

(ii) The minor lawfully obtains health care services without the consent of a parent, guardian, or other person acting *in loco parentis* and the minor, a court, or another person authorized by law consents to such health care service; or

(iii) A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between a health care provider and the minor with respect to health care services.

(b) **Circumstances Where A Minor's PHI May Be Further Disclosed, Accessed, and/or Restricted Pursuant to Alabama Law or Other Applicable Law.** Notwithstanding the general rule set forth in Section 2(a), there may be circumstances in which a minor's PHI may be further disclosed, accessed, and/or restricted pursuant to Alabama law or other applicable law, including applicable case law, even if a minor is legally authorized to control the use and disclosure of his/her PHI. For example, PHI of an unemancipated minor may be disclosed or accessed by a parent, guardian, or person acting *in loco parentis* to the extent permitted or required by Alabama law or other applicable law. Alternatively, where Alabama law or other applicable law prohibits such disclosure or access, we shall abide by those restrictions and prohibitions. In the event a parent, guardian or other person acting *in loco parentis* is not an unemancipated minor's personal representative and where Alabama law or other applicable law does not provide for access rights, we may provide or deny access to a parent, guardian, or other person acting *in loco parentis* if such action is consistent with Alabama law or other applicable law -- provided that such decision is made by a licensed health care professional in the exercise of professional judgment.

3. Deceased Individuals.

If the patient is deceased, we may disclose to a family member, relative, or a close personal friend of the patient, or any other person identified by the patient, who were involved in the patient's care or payment for healthcare prior to the patient's death, PHI of the patient that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the patient that is known to us. Otherwise, if, under applicable law, an executor, administrator or other person has authority to act on behalf of a deceased individual or of the individual's estate, such person will be treated as the personal representative with respect to PHI relevant to such representation. Prior to releasing such information, verification of authority should be obtained, preferably through Letters of Testamentary or Letter of Administration issued by the Probate Court and naming the individual who is authorized to act on behalf of a deceased individual or of his/her estate. We will comply with the requirements of the Privacy Rules and this Compliance Plan with respect to the PHI of a deceased patient for a period of 50 years following the death of the patient.

4. Persons Subject to Abuse, Neglect, or Endangerment.

Notwithstanding a provision under Alabama law or in this policy to the contrary, we may elect not to treat a person as a personal representative of a patient if we reasonably believe that:

(a) The patient has been or may be subjected to domestic violence, abuse, or neglect by such person, or where treating such person as the personal representative of the patient could endanger the patient; and

(b) In the exercise of professional judgment, the decision is made that it is not in the best interest of the patient to treat such person as the patient's personal representative.

- **Form: Personal Representatives of Patients Matrix**

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

HIPAA BREACH NOTIFICATION

The purpose of this policy is to establish procedures for determining the need for Breach notification, as well as for providing notification to appropriate parties in the event of a Breach of an individual's Unsecured PHI. The Health Care Authority shall comply with applicable law in determining the need for Breach notification, as well as for providing notification to appropriate parties in the event of a Breach of an individual's Unsecured PHI.

1. Definitions.

(a) **PHI.** "PHI" means Protected Health Information, whether oral, electronic or recorded in any form or medium, (i) that relates to the past, present or future physical or mental condition of an individual; or (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual; and (iv) that identifies the individual (or there is a reasonable basis to believe the information can be used to identify the individual).

(b) **Unsecured PHI.** "Unsecured PHI" means PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized individuals through the use of a technology or methodology identified by the Secretary of HHS. Unsecured PHI may be written, oral or electronic PHI. PHI which has been encrypted, destroyed or de-identified in accordance with the following standards is not considered Unsecured PHI and therefore is not subject to this policy:

(i) Encrypted PHI - Electronic PHI has been encrypted as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The encryption processes identified below have been tested by the National Institute of Standards and Technology (NIST) and judged to meet this standard.

(a) Data at Rest - Valid encryption processes for data at rest are consistent with NIST Special Publication 800-111;

(b) Data in Motion - Valid encryption processes for data in motion are those which comply, as appropriate, with NIST Special Publications 800-52.

(ii) Destroyed PHI. PHI which has been destroyed, through the destruction of the media on which it is stored or recorded. This shall require:

(a) Paper, film or other hard copy media to be shredded or destroyed such that the PHI cannot be read or reconstructed; and

(b) Electronic media to be cleared, purged, or destroyed consistent with NIST media sanitation standards, so that the PHI cannot be retrieved.

(iii) De-Identified. PHI which has been de-identified in accordance with the Privacy Rules' requirements such that the health information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual.

(c) **Breach.** A "Breach" means the unauthorized acquisition, access, use or disclosure of Unsecured PHI in a manner not permitted under the Privacy Rules which compromises the security or privacy of PHI. The following events do not constitute a Breach and therefore are not subject to this policy:

- Any unintentional acquisition, access or use of PHI by a Workforce member or person acting under The Health Care Authority's or a business associate, if such acquisition, access or use was made in good faith and within the scope of authority, and such PHI is not further used or disclosed in a manner not permitted by the Privacy Rules.

- Any inadvertent disclosure by a person who is authorized to access PHI within our organization or our business associate to another person authorized to access PHI within our organization or our business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rules.

- A disclosure of PHI where The Health Care Authority or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

(d) **Breach Presumed.** An acquisition, access, use, or disclosure of PHI in a manner not permitted under the Privacy Rules is presumed to be a Breach unless we or our business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

(i) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

(ii) The unauthorized person who used the PHI or to whom the disclosure was made;

(iii) Whether the PHI was actually acquired or viewed; and

(iv) The extent to which the risk to the PHI has been mitigated.

(e) **When Breach is Deemed Discovered.** We shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent of our organization.

2. Breach Reporting.

(a) **Reporting Breach.** Suspected Breaches of Unsecured PHI should be immediately reported to the Privacy Officer within forty-eight (48) hours of becoming aware of such event.

(b) The Privacy Officer shall be responsible for investigating the facts and circumstances of a suspected Breach, and for determining whether a reportable Breach has, in fact, occurred. At the conclusion of the investigation, the Privacy Officer will be responsible for documenting the investigation's outcome, including whether the reasons as to why a Breach notification is or is not determined to be necessary.

(c) **HIPAA Business Associates**. Our HIPAA business associates shall notify us in the event they discover or suspect any Breach. A Breach shall be treated as discovered by a business associate as of the first day on which such Breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the business associate. Such notifications shall be made in accordance with the terms of the HIPAA Business Associate Agreement between the parties and/or as otherwise directed by us.

3. Notification Process.

(a) **Notification to Individuals.**

(i) Timing. Following the discovery of a Breach of Unsecured PHI, except in the cases of a Law Enforcement Delay (defined in Section III.D. below) The Health Care Authority shall notify the individual(s) affected by the Breach without unreasonable delay (but in no event later than 60 calendar days after the date of the discovery of the Breach). Such notice shall be the responsibility of the Privacy Officer.

(ii) Content of Individual Notification. The notification shall be in plain language and shall include, to the extent possible, the following elements:

- Brief description of what happened, including the date the Breach occurred and was discovered;
- Description of the types of Unsecured PHI that were involved in the Breach, whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved. However, this description should not include the actual PHI that was breached and/or include any sensitive information;
- Any steps individuals should take to protect themselves from potential harm resulting from the Breach (*e.g.*, notice to a credit card company or engagement of credit monitoring services);
- Brief description of The Health Care Authority's efforts to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches; and
- Contact procedures for individuals to ask questions or learn additional information from The Health Care Authority, which shall include a toll-free telephone number, an E-mail address, web-site, or postal address.

(iii) Methods of Delivery for Individual Notification.

- Written Notice: Sufficient Contact Information. Individual notification shall be in written form, by first class mail, to the individual at the last known address of the individual, or by E-mail if the individual has agreed to receive such notices electronically. The notification may be provided in one or more notification as information becomes available. As appropriate and permitted by the Privacy Rules, individual notification may be sent to an individual's authorized personal representative.

- Substitute Notice: Insufficient Contact Information. In the case where there is insufficient or out-of-date contact information that precludes providing an individual notification in writing, a substitute form of individual notification reasonably calculated to reach the individual shall be provided.

    - Fewer than 10 Individuals. In the case in which there is insufficient or out-of-date contact information for fewer than ten (10) individuals, then such substitute notice may be provided by an alternative form of written notice, telephone, or other means.

    - 10 or More Individuals. In the case in which there is insufficient or out-of-date contact information for ten (10) or more individuals, then such substitute notice shall be in the form of either a conspicuous posting for a period of ninety (90) days on the The Health Care Authority web-site, or a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the Breach likely reside. Such a Web or media posting shall include a toll-free telephone number that remains active for at least 90 days where individuals can learn whether their Unsecured PHI may be included in the Breach.

- Urgent Situations. In any case deemed by The Health Care Authority to require urgency because of possible imminent misuse of Unsecured PHI, The Health Care Authority may provide information to the affected individual(s) by telephone or other means, as appropriate. However, this initial contact shall be followed by written notification to the affected individual(s) in accordance with this policy.

(b) **Media Notice.** In the event The Health Care Authority experiences a Breach of Unsecured PHI affecting more than 500 individual-residents of a state or jurisdiction, The Health Care Authority shall provide notice (*e.g.,* a press release) to prominent media outlets serving the state or jurisdiction ("Media Notice"). Except in cases of a Law Enforcement Delay (defined in Section III.D. below), the Media Notice shall be provided without unreasonable delay, and in no case later than sixty (60) days following the discovery of a Breach of Unsecured PHI and will include the same information required for an individual notification (as discussed in Section III.A. above). This Media Notice obligation is in addition to the individual notification obligations discussed in Section III.A. above.

(c) **Notice to Secretary of HHS.** In addition to notifying affected individuals and the media of a Breach of Unsecured PHI, The Health Care Authority shall notify the Secretary of HHS of a Breach of Unsecured PHI as follows:

(i) Breaches Affecting More than 500 Individuals. In the event a Breach of Unsecured PHI affects 500 or more individuals, The Health Care Authority shall, except in cases of a Law Enforcement Delay (defined in Section III.D. below), notify the Secretary of HHS contemporaneously with the Individual Notification, in the manner and method specified on the HHS web-site.

(ii) Breaches Affecting Less than 500 Individuals. For Breaches of Unsecured PHI that affect fewer than 500 individuals, The Health Care Authority will maintain a log or other documentation of such Breaches and shall notify the Secretary of HHS of such Breaches on an annual basis. All notifications of Breaches affecting fewer than 500 individuals shall be submitted within sixty (60) days of the end of the calendar year in which the Breaches occur. The Health Care Authority shall submit these Breach notifications, in the manner and method specified on the HHS web-site.

(d) **Law Enforcement Delay.** Notification required under this policy may be delayed if a law enforcement official states that notification, notice, or posting would impede a criminal investigation or cause damage to national security ("Law Enforcement Delay").

(i) If the statement is in writing and specifies the time for which a delay is required, The Health Care Authority may delay such notification, notice or posting for the time period specified by the office.

(ii) If the statement is made orally, The Health Care Authority shall document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily, but no longer than thirty (30) days from the date of the oral statement, unless a written statement meeting the requirements above is submitted by the official during that time.

(e) **Notification Documentation.** The Privacy Officer shall be responsible for maintaining and retaining copies of any Breach notifications to individuals, the media, and Secretary of HHS, as well as any Law Enforcement Delay Statement. Such documentation shall be maintained and retained in accordance with the Compliance Plan's documentation requirements and standards. (See Policy: *Recordkeeping and Retention*).

4. Mitigation; Training and Education; Sanctions.

(a) **Mitigation.** The Health Care Authority shall take corrective action to mitigate and cure, if feasible, any Breach of Unsecured PHI.

(b) **Training.** Training and education on this policy shall be provided to workforce members and associates as appropriate and necessary for such individuals to carry out their respective duties and responsibilities to our organization. Failure to comply with this policy can result in disciplinary action, including possible termination.

(c) **Sanctions.** Failure to comply with this policy can result in disciplinary action, including possible termination. (See Policy: *Workforce Member Sanctions for Violations of the Compliance Plan and Progressive Sanctions Policy*).

(d) **Complaints.** The Privacy Officer shall be responsible for implementing a process and procedure for addressing complaints concerning the handling of a Breach of Unsecured PHI.

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 741-6456

Privacy Problem/Concern Report

The Privacy Problem/Concern Report form is to be used by members of our Workforce to report their good faith belief of violations of the Privacy Rules, our HIPAA Privacy Compliance Plan, applicable law, as well as other ethical standards regarding the protection and privacy of protected health information. **We will take every measure to ensure the confidentiality of the information outlined below. However, there may be circumstances where disclosure of this information may become necessary.**

1. **Name** (*unless you wish to remain anonymous*): _____

2. **Date**: _____

3. **Time**: _____ AM or PM (*circle one*)

4. **Your position/job description**: _____

5. **Department**: _____

6. **Detailed description of the problem/concern/possible privacy violation** (*Include dates, location(s) of incident, names of persons involved, general description of the health information disclosed, and duration of event(s)):*_____
_____
_____
_____
_____
_____
_____
_____
_____

7. **How did you become aware of the problem?** _____
_____
_____
_____

8. **Others with knowledge of the problem/concern/possible violation:**_____
_____
_____

This report was received by the Privacy Officer on _____.

_____ _____

Signature of Privacy Officer Date

Do Not Write Below This Line: For Administrative Use Only

The following information is to be completed after an investigation is conducted.

Date Investigation Initiated: _____

Privacy Problem/Concern/Violation Valid? Yes OR No (*circle one*)

General Description of Problem/Concern/Violation Found: _____

_____

_____

_____

_____

Action taken: _____

_____

_____

_____

_____

Date Investigation Closed: _____

Approved: _____ _____

Signature of Privacy Officer Date

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
HIPAA PRIVACY COMPLIANCE PLAN

Workforce Member Privacy Training Acknowledgement

I acknowledge that I have received education and training regarding the Privacy Rules and its impact on Northeast Alabama Regional Medical Center (RMC). I understand that the Privacy Rules govern the manner in which protected health information (PHI) can be used and disclosed by RMC, and that I am required to follow the policies and procedures of RMC pertaining to such use and disclosure.

As necessary, I will seek advice from my supervisor or the Privacy Officer concerning the appropriateness of my actions or those of others and any questions that I may have regarding privacy compliance activities. I will also report to my supervisor, the Privacy Officer or the Compliance Line any suspected violations of the Privacy Rules or the Privacy Compliance Plan.

My signature acknowledges my understanding of the above information and my agreement to comply fully with the HIPAA compliance policies, procedures and plan.

_____ _____

Print Name Date

_____ _____

Signature Clock # (If applicable)

_____

Department/Unit/Service

STRINGFELLOW MEMORIAL HOSPITAL
ANNISTON, AL 36207

PRIVACY NOTICE ACKNOWLEDGEMENT
(April 2003 Privacy Notice)

Place label here

PRINOT

BY SIGNING BELOW, I HEREBY ACKOWLEDGE RECEIPT OF THE PRIVACY NOTICE FOR NORTHEAST ALABAMA REGIONAL MEDICAL CENTER

_____ _____
Printed Name of Patient Date

_____ _____
Signature of Patient or Patient's Representative Medical Record Number

_____
Printed Name of Patient's Representative (*if applicable)*

_____
Representative's Relationship to Patient (*if applicable)*

To be completed by Northeast Alabama Regional Medical Center only if Acknowledgement Refused:

After a good faith attempt to obtain this Acknowledgement, the patient or his/her representative, refused or was unable to acknowledge receipt of our Privacy Notice for the following reason(s):

_____

_____

_____ _____
Signature of Hospital Representative Date

This form is to be maintained as a permanent part of the patient's medical record.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

DISTRIBUTING, POSTING AND REVISING THE PRIVACY NOTICE

The Privacy Rules provide that a patient, or his/her personal representative, has a right to receive a notice of our privacy practices ("Privacy Notice"). This notice addresses, among other items, our legal duty to protect PHI, its possible uses and disclosures, patients' rights with respect to PHI, how to file complaints for privacy violations, who to contact with privacy questions/concerns, and the effective date of the Privacy Notice.

In compliance with the Privacy Rules, the Privacy Notice was developed for distribution to all patients, or their representatives, no later than the date of their first service delivery, on or after April 14, 2003, or in an emergency treatment situation, as soon as reasonably possible after the emergency treatment situation. Patients may be provided a copy of the Privacy Notice via E-mail only if they agree to such transmission. However, patients are still entitled to receive a paper copy of our Privacy Notice, even if they have agreed to receive the Privacy Notice electronically.

Except in emergencies, a good faith effort will be made to obtain no later than the first date of service a written Acknowledgement from all patients, or their representatives, of their receipt of our Privacy Notice. This good faith effort will be made even where we provide the Privacy Notice electronically. If unable to obtain an Acknowledgement of receipt, an appropriate notation will be made in the patient's medical record and on the copy of the Privacy Notice presented to the patient. The notation shall document the fact that the patient refused or failed to acknowledge receipt of our Privacy Notice, as well as our good faith efforts to obtain the patient's written Acknowledgment. In an emergency situation, we will make a good faith effort to obtain the written Acknowledgment after the emergency has been resolved. We may not condition provision of services on obtaining an Acknowledgment of the receipt of the Privacy Notice.

In compliance with the Privacy Rules, a copy of the Privacy Notice will be posted in a clear and prominent location in our facility where it is reasonable to expect patients seeking care and services to be able to see and read it. It is recognized that this may require posting the Privacy Notice in several key locations or points-of-entry around our facility. In addition, a copy of the Privacy Notice will be posted on our web site and available for any patient who requests a copy.

Whenever a material change is required regarding PHI uses or disclosures, patients' rights, our privacy duties/obligations or other privacy practices, revised copies of the Privacy Notice will be promptly distributed to all new patients at their first visit following the revision, placed on our web-site, posted at our facility, and made available for any patient who requests a copy. There is no requirement, however, to obtain a new Acknowledgment from an existing patient or his/her representative. In accordance with the Privacy Rules, the Privacy Officer will be responsible for retaining, on file, copies of the original, as well as all revised Privacy Notices, and any written Acknowledgments or documentation of our good faith efforts to obtain such written Acknowledgments, for six (6) years after their creation date or after the date when they last were effective, whichever is later. (See Policy: *Recordkeeping and Retention*).

Except to the extent patient care might be compromised, we shall not use or disclose identifiable health information in a manner inconsistent with the Privacy Notice.

- **Form: Privacy Notice and Acknowledgment**

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

OBTAINING BUSINESS ASSOCIATE AGREEMENTS

From time to time, assistance is obtained from a variety of persons or entities to provide certain functions, activities or services on our behalf, which involve the creation, use and/or disclosure of PHI, including EPHI. These persons or entities are called "Business Associates" and they perform an assortment of tasks on our behalf, including legal, accounting, consulting, data aggregation, management and administrative services.

There is an obligation under HIPAA to ensure that these persons and entities are performing their delegated functions, activities and services on our behalf in compliance with HIPAA. To accomplish this purpose, HIPAA requires us to enter into a written Business Associate Agreement ("BA Agreement") with each of our Business Associates. These BA Agreements contain specific language setting out the Business Associates' contractual obligations to us, as well as their responsibility to conduct activities in compliance with HIPAA.

1. **General Obligations of a BA Agreement.**

(a) The BA Agreement shall establish the permitted and required uses and disclosures of PHI by the Business Associate. The BA Agreement may not authorize the Business Associate to use or further disclose the information in a manner that would violate the requirements of the HIPAA Privacy Rules, if done by us, except that:

(i) The BA Agreement may permit the Business Associate to provide data aggregation services relating to our healthcare operations;

(ii) The BA Agreement may permit the Business Associate to use the PHI received by the Business Associate in its capacity as a Business Associate, if necessary (1) for the proper management and administration of the Business Associate; or (2) to carry out the legal responsibilities of the Business Associate;

(iii) The BA Agreement may permit the Business Associate to disclose the PHI received by the Business Associate in its capacity as a Business Associate, if: (1) the disclosure is required by law; or (2)(a) the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person; and (2)(b) the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(b) The BA Agreement shall provide that:

(i) The Business Associate will use and disclose PHI only for the purposes for which it has been engaged by us and as required by law;

(ii) The Business Associate will use appropriate safeguards and comply, where applicable, with the HIPAA Security Rules with respect to electronic PHI, to

prevent use or disclosure of the information other than as provided for by BA Agreement;

(iii) The Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the PHI that it creates, receives, maintains, or transmits;

(iv) The Business Associate agrees to mitigate, to the extent practicable, any harmful effect involving the use and/or disclosure of PHI;

(v) The Business Associate will report to us any use and/or disclosure of PHI not provided for in the BA Agreement, any Breach, or any security incident of which it becomes aware, including breaches of unsecured protected health information;

(vi) The Business Associate will ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the Business Associate agree to comply with the applicable requirements of HIPAA by entering into a written contract or other arrangement with the Business Associate that complies with HIPAA;

(vii) The Business Associate will help us comply with our duty to provide patients or their designee with access to their PHI including electronic PHI. If the PHI that is the subject of a request for access is maintained in a designated record set electronically and if the patient or the patient's designee requests an electronic copy of such information, the Business Associate must provide us the PHI in the electronic form and format requested by the patient or the patient's designee, if the PHI is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by us and the patient or patient's designee;

(viii) The Business Associate will help us comply with our duty to permit patients to amend their PHI;

(ix) The Business Associate will help us comply with our duty to provide patients with an accounting of their PHI;

(x) The Business Associate will make its internal practices, books and records relating to the use and disclosure of PHI that is created or received by the Business Associate on our behalf, available to the Secretary of HHS for the purpose of determining our compliance with HIPAA; and

(xi) Upon termination of the BA Agreement, the Business Associate, if feasible, will return or destroy all PHI created and received by the Business Associate on our behalf, retaining no copies of such information. Where such return or destruction is not feasible, the Business Associate will extend the protections of the BA Agreement to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible; and

(xii) If we determine that the Business Associate has violated a material term of the BA Agreement, authorize us to terminate the contract.

2. Obligation to Address Material Breaches and Violations.

(a) Where we know of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligation under a BA Agreement or other arrangement, we shall take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, terminate the BA Agreement, if feasible.

(b) Where a Business Associate knows of a pattern of activity or practice of a subcontractor that constitutes a material breach or violation of the subcontractor's obligation under a BA Agreement or other arrangement, the Business Associate must take reasonable steps to cure the breach or end the violation, as applicable, and if such steps are unsuccessful, terminate its contract or agreement with the subcontractor, if feasible.

3. Obtaining Business Associate Agreements.

PHI may only be shared with Business Associates pursuant to an approved written BA Agreement. The Privacy Officer shall be responsible for overseeing the review of all agreements, contracts and relationships with persons or entities performing services, functions and activities on our behalf, to determine if a BA Agreement is necessary. If the Privacy Officer determines that a BA Agreement is warranted, the Privacy Officer shall require the Business Associate to enter into a BA Agreement. (See *Business Associate Agreement* form). Where a BA Agreement is provided by the Business Associate, the Privacy Officer shall review the contract to ensure that the language contained therein is sufficient to meet the requirements of HIPAA, as well as to address our particular privacy needs and concerns. As necessary, we shall engage legal counsel to assist in the process of preparing, reviewing and implementing all BA Agreements to ensure compliance with HIPAA.

- **Forms: Business Associate Agreement with Existing Contract**

  Business Associate Agreement without Existing Contract

  Business Associate Agreement (Law Firm)

  Business Associate Agreement (Accounting Firm)

  Amendment to Business Associate Agreement

HIPAA BUSINESS ASSOCIATE AGREEMENT
(No Written Contract Exists)

THIS BUSINESS ASSOCIATE AGREEMENT ("BA Agreement") is effective as of the Effective Date by and between Regional Medical Center Board d/b/a Northeast Alabama Regional Medical Center ("Covered Entity") and the person or entity listed as the business associate on the signature page hereto ("Business Associate").

WHEREAS, Covered Entity has determined that it is a covered entity under HIPAA or has components covered by HIPAA; and

WHEREAS, Covered Entity and Business Associate are parties to the Agreement, pursuant to which Business Associate performs functions, activities, or services for Covered Entity, and, in connection with those functions, activities, and/or services, Business Associate creates, receives, maintains, or transmits PHI that is subject to protection under HIPAA.

NOW, THEREFORE, in consideration of the foregoing and of the covenants and agreements set forth herein, the parties, intending to be legally bound, agree as follows:

Section 1. **Definitions.** The terms used, but otherwise not defined, in this BA Agreement shall have the same meaning as those terms in HIPAA.

(a) "Agreement" shall mean that certain oral agreement by and between Covered Entity and the Business Associate, as more fully described on Exhibit A attached hereto.

(b) "Breach" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA.

(c) "Designated Record Set" shall have the meaning set forth in 45 CFR § 164.501, including, without limitation, a group of records maintained by or for Covered Entity that consist of: (i) the medical records and billing records about individuals maintained by or for a Covered Entity; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) records used, in whole or in part, by or for Covered Entity to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for Covered Entity.

(d) "Effective Date" shall mean the ___ day of _____, 20___.

(e) "HIPAA" shall mean: (i) the Health Insurance Portability and Accountability Act of 1996, and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164, and any subsequent amendments or modifications thereto, and (ii) the HITECH Act, and regulations promulgated thereunder, and any subsequent amendments or modifications thereto.

(f) "HITECH Act" shall mean the provisions applicable to business associates under the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

(g) "PHI" shall mean Protected Health Information which Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity in connection with the performance of functions, activities, and/or services pursuant to the Agreement.

(h) "Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, as may be amended, modified, or superseded from time to time.

(i) "Protected Health Information" shall have the meaning set forth in 45 CFR § 160.103, including, without limitation, any information, whether oral, electronic or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual; and (iv) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(j) "Required by Law" shall have the meaning set forth in 45 CFR § 164.103, including, without limitation, a mandate contained in law that compels Covered Entity or Business Associate to make a use or disclosure of Protected Health Information and that is enforceable in a court of law.

(k) "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

(l) "Security Incident" shall have the meaning set forth in 45 CFR § 164.304, including without limitation, the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI.

(m) "Security Rules" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, as may be amended, modified, or superseded from time to time.

(n) "Unsecured PHI" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, Protected Health Information not secured through the use of encryption, destruction or other technologies and methodologies identified by the Secretary to render such information unusable, unreadable, or indecipherable to unauthorized persons.

Section 2. Obligations of Business Associate.

(a) Permitted Uses. Business Associate shall not use PHI in any manner except for the purpose of performing functions, activities, or services pursuant to the Agreement; provided, however, that Business Associate shall not use PHI in any manner that would constitute a violation of HIPAA if so used by Covered Entity. Business Associate may use PHI: (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; or (iii) as Required by Law.

(b) Permitted Disclosures. Business Associate shall not disclose PHI in any manner except for the purpose of performing functions, activities, or services pursuant to the Agreement; provided, however, that Business Associate shall not disclose PHI in any manner that would constitute a violation of HIPAA if so disclosed by Covered Entity. Business Associate may disclose PHI: (i) for the proper management and administration of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; (ii) to carry out the legal responsibilities of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; or (iii) as Required by Law. To the extent that Business Associate discloses PHI to a third party pursuant to Section 2(b)(i) or (ii) above under Reasonable Assurances, Business Associate must obtain in writing, prior to making any such disclosure: (x) reasonable assurance from the third party that such PHI will be held in a confidential manner; (y) reasonable assurance from the third party that such PHI will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to such third party; and (z) an agreement from the third party to immediately notify Business Associate of any breaches of confidentiality of such PHI, to the extent the third party has obtained knowledge of such breach (collectively, "Reasonable Assurances"). Except as Required by Law, Business Associate shall not disclose PHI to a health plan for payment or healthcare operations if the individual subject to the PHI has requested such restriction and the individual (or designee) pays out of pocket in full for the health care item or service to which the PHI relates.

(c) De-identification. Business Associate shall not de-identify PHI without Covered Entity's prior written consent.

(d) Appropriate Safeguards. Business Associate shall comply with the applicable provisions of the Security Rules and shall implement appropriate administrative, technical, physical, and security safeguards in compliance with HIPAA that reasonably and appropriately safeguard and protect the confidentiality, integrity and availability of PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. As required by HIPAA, Business Associate shall maintain policies, procedures and documentation that address these safeguards and the requirements of HIPAA and which are appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its services.

(e) Business Associate's Subcontractors and/or Agents. To the extent Business Associate uses one or more subcontractors or agents to perform a function, activity or service for the Covered Entity, and such subcontractors or agents create, receive, maintain, or transmit PHI, Business Associate shall first require in accordance with 45 CFR § 164.308(b) and 164.502(e) that each subcontractor or agent agree in writing to be bound by the terms of this BA Agreement and HIPAA, to the same extent as Business Associate. Business Associate shall report to Covered Entity in writing, as soon as possible, but in no event later than three (3) days following the discovery of non-compliance by a subcontractor or agent of any of its obligations with respect to PHI. Notwithstanding the above, Business Associate shall not delegate to a subcontractor or agent any functions, activities, or services it provides on behalf of Covered Entity pursuant to the Agreement without Covered Entity's prior, written consent.

(f) Access to PHI. Within five (5) days of receipt of a request by Covered Entity, Business Associate shall make PHI maintained by Business Associate in a Designated Record Set available to Covered Entity for inspection and/or copying to enable Covered Entity to fulfill its obligations under 45 CFR § 164.524. If a request for access to PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity. Business Associate shall provide access to a copy of electronic PHI maintained by Business Associate in a Designated Record Set to the Covered Entity in accordance with the provisions of this Section and HIPAA.

(g) Amendment of PHI. Within five (5) days of receipt of a request by Covered Entity, Business Associate shall

amend PHI maintained by Business Associate in a Designated Record Set as directed by Covered Entity to enable Covered Entity to fulfill its obligations under 45 CFR § 164.526. If a request for amendment of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity.

(h) Accounting of PHI Disclosures. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Within five (5) days of receipt of a request by Covered Entity, Business Associate shall make available to Covered Entity the information required to provide an accounting of such disclosures. Any accounting information shall include the information described in 45 CFR § 164.528(b), including, without limitation: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the written request for disclosure. If a request for an accounting of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity.

(i) Governmental Access to Records. Business Associate shall make PHI and his/her/its facilities, internal practices, books, records, accounts, and other information relating to the use and disclosure of PHI available to the Secretary in a time and manner designated by the Secretary and shall cooperate with the Secretary concerning any investigation designed to determine Covered Entity's or Business Associate's compliance with HIPAA. Unless the Secretary directs otherwise, Business Associate shall promptly notify Covered Entity of Business Associate's receipt of a request for information from the Secretary or a notice concerning an investigation by the Secretary.

(j) Minimum Necessary Use and Disclosure Requirement. Business Associate shall only request, use and disclose the minimum amount of PHI necessary to reasonably accomplish the purpose of the request, use or disclosure in accordance with 45 CFR § 164.502(b). Further, Business Associate will restrict access to PHI to those employees, contractors, or agents of Business Associate who are actively and directly participating in performing functions, activities, or services pursuant to the Agreement and who need to know such PHI in order to fulfill such responsibilities.

(k) Retention of PHI. Business Associate shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under Section 2(h) of this BA Agreement for a period of six (6) years from its creation.

(l) Notification Obligations; Mitigation. During the term of this BA Agreement, Business Associate shall notify Covered Entity as soon as possible, but in no event later than three (3) days (or such shorter time period as required by applicable state law) after discovery of any use and/or disclosure of PHI not permitted by this BA Agreement, a Breach of Unsecured PHI, or any material Security Incident of which it becomes aware. This notification obligation shall include the information required by HIPAA and, at a minimum, shall provide Covered Entity with the following information: (i) a description of the facts and circumstances concerning the improper use or disclosure, Breach or Security Incident; (ii) a description of the PHI affected; and (iii) the names and identity of the individual(s) affected. Business Associate shall take prompt corrective action to mitigate and cure, if possible, any harmful effect that is known to Business Associate of an improper use and/or disclosure of PHI, Breach or Security Incident. Business Associate shall cooperate with Covered Entity regarding any Breach notification to third parties, and shall reimburse Covered Entity for any costs incurred by Covered Entity in complying with the applicable requirements of HIPAA resulting from a Breach of Unsecured PHI by Business Associate. Business Associate shall be deemed to discover a Breach of Unsecured PHI as of the first day on which such Breach is known, or should have been known, by Business Associate.

(m) Additional Obligations. Business Associate shall comply with the requirements of HIPAA which are applicable to business associates, including all regulations which are issued to implement such requirements, as may be amended, modified, or superseded from time to time. To the extent Business Associate carries out one or more of Covered Entity's obligation(s) under 45 CFR Part 164, Subpart E, in the performance of such obligations, Business Associate shall comply with the requirements of 45 CFR Part 164, Subpart E, that apply to Covered Entity to the same extent as required by Covered Entity. Business Associate shall comply with all applicable state and federal laws that affect the privacy or security of PHI received from the Covered Entity.

(n) Compliance with Standard Transactions. If Business Associate conducts, in whole or in part, Standard Transactions (as such term is defined in the Standards for Electronic Transactions Rule at 45 CFR Parts 160 and 162, as may be amended, modified or superseded, from time to time) for or on behalf of Covered Entity, Business Associate will comply, and will require any of its subcontractors or agents involved with such Standard Transactions on behalf of Covered Entity to comply, with each applicable requirement of 45 CFR Parts 160 and 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any agreement in connection with the conduct of Standard

Transactions for or on behalf of Covered Entity that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked "not used" in a Standard Transaction or are not in the Standard Transactions' implementation specification; or (iv) changes the meaning or intent of the Standard Transactions' implementation specifications.

(o) Data Jurisdiction. Business Associate may not create, receive, maintain, transmit, or store PHI in any jurisdiction outside of the United States, including, but not limited to, on any server (physical, cloud or otherwise) located outside of the United States.

Section 3. Obligations of Covered Entity.

(a) Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation(s) may affect Business Associate's use or disclosure of PHI.

(b) Restrictions on Use or Disclosure. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individuals to use and/or disclose PHI, to the extent such changes or revocations may affect Business Associate's permitted or required uses and/or disclosures of PHI. Further, Covered Entity shall notify Business Associate of any restriction to the use and/or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent such restriction may affect Business Associate's permitted or required uses and/or disclosures of PHI.

Section 4. Term and Termination.

(a) Term. This BA Agreement shall commence on the Effective Date and will remain effective for the entire term of the Agreement, unless earlier terminated in accordance with the terms herein.

(b) For Cause Termination Due to Material Breach. Either party may terminate this BA Agreement by notice in writing to the other party, if the other party materially breaches this BA Agreement in any manner and such material breach continues for a period of thirty (30) days after written notice is given to the breaching party by the other party specifying the nature of the breach and requesting that it be cured. A material breach of this BA Agreement shall constitute a breach of the Agreement. If termination of this BA Agreement is not feasible, the non-breaching party shall report the breach to the Secretary, if required by HIPAA.

(c) Effect of Termination. Upon termination of this BA Agreement, Business Associate shall return or destroy all PHI (regardless of form or medium), including all copies thereof and any data compilations derived from PHI and allowing identification of any individual who is the subject of the PHI. The obligation to return or destroy all PHI shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. If the return or destruction of PHI is not feasible, Business Associate shall provide Covered Entity written notification of the conditions that make return or destruction not feasible. Upon notification that return or destruction of PHI is not feasible, Business Associate shall continue to extend the protections of this BA Agreement to such information and limit further uses or disclosures of such PHI to those purposes that make the return or destruction of such PHI not feasible, for as long as Business Associate maintains such PHI. If Business Associate elects to destroy the PHI, Business Associate shall notify Covered Entity in writing that such PHI has been destroyed.

(d) Injunction. In the event of a breach by Business Associate of any of its obligations hereunder, Covered Entity shall have, in addition to any other rights and remedies available at law or in equity, the right to obtain injunctive relief without the necessity of proving actual damages or that any irreparable harm would or might result from a failure to obtain injunctive relief, it being acknowledged and agreed to by all parties hereto that any such breach will cause irreparable harm to Covered Entity and that monetary damages alone will not provide an adequate remedy.

Section 5. Enforcement, Civil Monetary Penalties. The parties hereby acknowledge that in providing services pursuant to the Agreement, Business Associate is at all times acting as an independent contractor and not as an agent of the Covered Entity. In accordance with HIPAA, Business Associate hereby acknowledges that it/he/she will be directly liable for civil money penalties for: (i) impermissible uses and disclosures of PHI; (ii) failure to provide notifications of Breaches of Unsecured PHI to the Covered Entity; (iii) failure to provide access to a copy of electronic PHI to either the Covered Entity, the individual subject to the electronic PHI or the individual's designee, as designated by the Covered Entity; (iv) failure to disclose PHI where required by the Secretary to investigate or determine the Covered Entity's or Business Associate's compliance with HIPAA; (v) failure to provide an accounting of disclosures of PHI in accordance with the requirements of HIPAA; (vi) failure to comply with the requirements of the Security Rule; (vii) failure to limit PHI used and/or disclosed to the minimum amount necessary to accomplish the intended purpose; and (viii) failure to obtain the written agreement of its subcontractors or agents to be bound by the terms of this BA Agreement and applicable law to the same extent as Business Associate.

Section 6. Indemnification.

(a) Business Associate agrees to indemnify, defend and hold harmless Covered Entity and its owners, officers, employees and agents from any and all claims, penalties, fines, costs, liabilities or damages, including but not limited to reasonable attorneys' fees, arising from or based upon any violation of this BA Agreement and/or HIPAA by Business Associate or any of its owners, officers, employees, agents and subcontractors.

(b) Covered Entity agrees to indemnify, defend and hold harmless Business Associate and its owners, officers, employees and agents from any and all claims, penalties, fines, costs, liabilities or damages, including but not limited to reasonable attorneys' fees, arising from or based upon any violation of this BA Agreement and/or HIPAA by Covered Entity or any of its owners, officers, employees, agents and subcontractors.

Section 7. **Construction.** This BA Agreement shall be construed as broadly as necessary to implement and comply with HIPAA. The parties agree that any ambiguity in this BA Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA. In the event the terms of this BA Agreement conflict with the terms of the Agreement, the terms of this BA Agreement shall control.

Section 8. **Captions.** The captions contained in this BA Agreement are included only for convenience of reference and do not define, limit, explain or modify this BA Agreement or its interpretation, construction or meaning and are in no way to be construed as part of this BA Agreement.

Section 9. **Notice.** All notices and other communications required or permitted pursuant to this BA Agreement shall be in writing, addressed to the party at the address set forth at the end of this BA Agreement, or to such other address as any party may designate from time to time in writing in accordance with this Section. All notices and other communications shall be sent by: (i) registered or certified mail, return receipt requested, postage pre-paid; (ii) overnight mail by reputable carrier; (iii) facsimile with a copy sent by First Class Mail, postage pre-paid; or (iv) hand delivery. All notices shall be effective as of the date of delivery if by hand delivery or overnight mail, two (2) days following the date of facsimile, or if by certified mail on the date of receipt, whichever is applicable.

Section 10. **Assignment.** This BA Agreement and the rights and obligations hereunder shall not be assigned, delegated, or otherwise transferred by either party without the prior written consent of the other party and any assignment or transfer without proper consent shall be null and void.

Section 11. **Governing Law and Venue.** This BA Agreement shall be governed by, and interpreted in accordance with HIPAA, and the internal laws of the State in which the Covered Entity has its principal place of business, without giving effect to any conflict of laws provisions.

Section 12. **Binding Effect; Modification.** This BA Agreement shall be binding upon, and shall enure to the benefit of, the parties hereto and their respective permitted successors and assigns. This BA Agreement may only be amended or modified by mutual written agreement of the parties; provided, however, that in the event provisions of this BA Agreement shall conflict with the requirements of HIPAA, this BA Agreement shall automatically be deemed amended as necessary to conform to such legal requirements at all times.

Section 13. **Waiver.** The failure of either party at any time to enforce any right or remedy available hereunder with respect to any breach or failure shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

Section 14. **Severability.** In the event that any provision or part of this BA Agreement is found to be totally or partially invalid, illegal, or unenforceable, then the provision will be deemed to be modified or restricted to the extent and in the manner necessary to make it valid, legal, or enforceable, or it will be excised without affecting any other provision of this BA Agreement, with the parties agreeing that the remaining provisions are to be deemed to be in full force and effect as if they had been executed by both parties subsequent to the expungement of the invalid provision.

Section 15. **No Third-Party Beneficiaries.** Nothing express or implied in this BA Agreement is intended to confer, nor shall anything herein confer, upon any person or entity other than Covered Entity, Business Associate and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

Section 16. **Counterparts.** This BA Agreement may be executed in multiple counterparts, each of which shall constitute an original and all of which together shall constitute but one BA Agreement.

Section 17. **Entire Agreement.** This BA Agreement constitutes the entire agreement between the parties with respect to the matters contemplated herein and supersedes all previous and contemporaneous oral and written negotiations, commitments, and understandings relating thereto.

[Signatures on following page]

IN WITNESS WHEREOF, Covered Entity and Business Associate have each caused this BA Agreement to be executed in their respective names by their duly authorized representatives as of the Effective Date.

BUSINESS ASSOCIATE:

_____

Signature: _____

Print Name/Title _____

Address: _____

_____

_____

Telephone: _____

Facsimile: _____

Contact Person: _____

COVERED ENTITY:

Regional Medical Center Board d/b/a
Northeast Alabama Regional Medical Center

Signature: _____

Print Name/Title: _____

Address: Post Office Box 2208
Anniston, Alabama 36202

Telephone: _____

Facsimile: _____

Contact Person: _____

Exhibit A

Description of Agreement

1. Effective date of oral agreement between Business Associate and Covered Entity: _____

_____

_____

2. Business Associate provides the following goods and/or services to Covered Entity: _____

_____

_____

_____

3. Business Associate has access to the following PHI in order to provide the goods and/or services to Covered Entity: _

_____

_____

_____

_____

HIPAA BUSINESS ASSOCIATE AGREEMENT
(Written Contract Exists)

THIS BUSINESS ASSOCIATE AGREEMENT ("BA Agreement") is effective as of the Effective Date by and between The Health Care Authority of the City of Anniston d/b/a Northeast Alabama Regional Medical Center ("Covered Entity") and the person or entity listed as the business associate on the signature page hereto ("Business Associate").

WHEREAS, Covered Entity has determined that it is a covered entity under HIPAA or has components covered by HIPAA; and

WHEREAS, Covered Entity and Business Associate are parties to the Agreement, pursuant to which Business Associate performs functions, activities, or services for Covered Entity, and, in connection with those functions, activities, and/or services, Business Associate creates, receives, maintains, or transmits PHI that is subject to protection under HIPAA.

NOW, THEREFORE, in consideration of the foregoing and of the covenants and agreements set forth herein, the parties, intending to be legally bound, agree as follows:

Section 1. Definitions. The terms used, but otherwise not defined, in this BA Agreement shall have the same meaning as those terms in HIPAA.

(a) "Agreement" shall mean that certain _____ Agreement by and between Covered Entity and the Business Associate dated the ____ day of _____, 20___.

(b) "Breach" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA.

(c) "Designated Record Set" shall have the meaning set forth in 45 CFR § 164.501, including, without limitation, a group of records maintained by or for Covered Entity that consist of: (i) the medical records and billing records about individuals maintained by or for a Covered Entity; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) records used, in whole or in part, by or for Covered Entity to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes Protected Health Information and is maintained, collected, used or disseminated by or for Covered Entity.

(d) "Effective Date" shall mean the effective date of the Agreement.

(e) "HIPAA" shall mean: (i) the Health Insurance Portability and Accountability Act of 1996, and regulations promulgated thereunder, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 CFR Parts 160 and 164, and any subsequent amendments or modifications thereto, and (ii) the HITECH Act, and regulations promulgated thereunder, and any subsequent amendments or modifications thereto.

(f) "HITECH Act" shall mean the provisions applicable to business associates under the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

(g) "PHI" shall mean Protected Health Information which Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity in connection with the performance of functions, activities, and/or services pursuant to the Agreement.

(h) "Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Parts 160 and 164, as may be amended, modified, or superseded from time to time.

(i) "Protected Health Information" shall have the meaning set forth in 45 CFR § 160.103, including, without limitation, any information, whether oral, electronic or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual; and (iv) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

(j) "Required by Law" shall have the meaning set forth in 45 CFR § 164.103, including, without limitation, a mandate contained in law that compels Covered Entity or Business Associate to make a use or disclosure of Protected Health Information and that is enforceable in a court of law.

(k) "Secretary" shall mean the Secretary of the U.S. Department of Health and Human Services or his/her designee.

(l) "Security Incident" shall have the meaning set forth in 45 CFR § 164.304, including without limitation, the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI.

(m) "Security Rules" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Parts 160 and 164, as may be amended, modified, or superseded from time to time.

(n) "Unsecured PHI" shall have the meaning set forth in 45 CFR § 164.402, including, without limitation, Protected Health Information not secured through the use of encryption, destruction or other technologies and methodologies identified by the Secretary to render such information unusable, unreadable, or indecipherable to unauthorized persons.

Section 2. Obligations of Business Associate.

(a) Permitted Uses. Business Associate shall not use PHI in any manner except for the purpose of performing functions, activities, or services pursuant to the Agreement; provided, however, that Business Associate shall not use PHI in any manner that would constitute a violation of HIPAA if so used by Covered Entity. Business Associate may use PHI: (i) for the proper management and administration of Business Associate; (ii) to carry out the legal responsibilities of Business Associate; or (iii) as Required by Law.

(b) Permitted Disclosures. Business Associate shall not disclose PHI in any manner except for the purpose of performing functions, activities, or services pursuant to the Agreement; provided, however, that Business Associate shall not disclose PHI in any manner that would constitute a violation of HIPAA if so disclosed by Covered Entity. Business Associate may disclose PHI: (i) for the proper management and administration of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; (ii) to carry out the legal responsibilities of Business Associate if such disclosure is Required by Law or if "Reasonable Assurances" are obtained; or (iii) as Required by Law. To the extent that Business Associate discloses PHI to a third party pursuant to Section 2(b)(i) or (ii) above under Reasonable Assurances, Business Associate must obtain in writing, prior to making any such disclosure: (x) reasonable assurance from the third party that such PHI will be held in a confidential manner; (y) reasonable assurance from the third party that such PHI will be used or further disclosed only as Required by Law or for the purpose for which it was disclosed to such third party; and (z) an agreement from the third party to immediately notify Business Associate of any breaches of confidentiality of such PHI, to the extent the third party has obtained knowledge of such breach (collectively, "Reasonable Assurances"). Except as Required by Law, Business Associate shall not disclose PHI to a health plan for payment or healthcare operations if the individual subject to the PHI has requested such restriction and the individual (or designee) pays out of pocket in full for the health care item or service to which the PHI relates.

(c) De-identification. Business Associate shall not de-identify PHI without Covered Entity's prior written consent.

(d) Appropriate Safeguards. Business Associate shall comply with the applicable provisions of the Security Rules and shall implement appropriate administrative, technical, physical, and security safeguards in compliance with HIPAA that reasonably and appropriately safeguard and protect the confidentiality, integrity and availability of PHI that it creates, receives, maintains or transmits on behalf of Covered Entity. As required by HIPAA, Business Associate shall maintain policies, procedures and documentation that address these safeguards and the requirements of HIPAA and which are appropriate to the size and complexity of the Business Associate's operations and the nature and scope of its services.

(e) Business Associate's Subcontractors and/or Agents. To the extent Business Associate uses one or more subcontractors or agents to perform a function, activity or service for the Covered Entity, and such subcontractors or agents create, receive, maintain, or transmit PHI, Business Associate shall first require in accordance with 45 CFR § 164.308(b) and 164.502(e) that each subcontractor or agent agree in writing to be bound by the terms of this BA Agreement and HIPAA, to the same extent as Business Associate. Business Associate shall report to Covered Entity in writing, as soon as possible, but in no event later than three (3) days following the discovery of non-compliance by a subcontractor or agent of any of its obligations with respect to PHI. Notwithstanding the above, Business Associate shall not delegate to a subcontractor or agent any functions, activities, or services it provides on behalf of Covered Entity pursuant to the Agreement without Covered Entity's prior, written consent.

(f) Access to PHI. Within five (5) days of receipt of a request by Covered Entity, Business Associate shall make PHI maintained by Business Associate in a Designated Record Set available to Covered Entity for inspection and/or copying to enable Covered Entity to fulfill its obligations under 45 CFR § 164.524. If a request for access to PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity. Business Associate shall provide access to a copy of electronic PHI maintained by Business Associate in a Designated Record Set to the Covered Entity in accordance with the provisions of this Section and HIPAA.

(g) Amendment of PHI. Within five (5) days of receipt of a request by Covered Entity, Business Associate shall

amend PHI maintained by Business Associate in a Designated Record Set as directed by Covered Entity to enable Covered Entity to fulfill its obligations under 45 CFR § 164.526. If a request for amendment of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity.

(h) Accounting of PHI Disclosures. Business Associate agrees to document disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528. Within five (5) days of receipt of a request by Covered Entity, Business Associate shall make available to Covered Entity the information required to provide an accounting of such disclosures. Any accounting information shall include the information described in 45 CFR § 164.528(b), including, without limitation: (i) the date of disclosure of PHI; (ii) the name of the entity or person who received PHI and, if known, the address of the entity or person; (iii) a brief description of PHI disclosed; and (iv) a brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the written request for disclosure. If a request for an accounting of PHI is delivered directly to Business Associate, Business Associate shall as soon as possible, but no later than five (5) days after receipt of the request, forward the request to Covered Entity.

(i) Governmental Access to Records. Business Associate shall make PHI and his/her/its facilities, internal practices, books, records, accounts, and other information relating to the use and disclosure of PHI available to the Secretary in a time and manner designated by the Secretary and shall cooperate with the Secretary concerning any investigation designed to determine Covered Entity's or Business Associate's compliance with HIPAA. Unless the Secretary directs otherwise, Business Associate shall promptly notify Covered Entity of Business Associate's receipt of a request for information from the Secretary or a notice concerning an investigation by the Secretary.

(j) Minimum Necessary Use and Disclosure Requirement. Business Associate shall only request, use and disclose the minimum amount of PHI necessary to reasonably accomplish the purpose of the request, use or disclosure in accordance with 45 CFR § 164.502(b). Further, Business Associate will restrict access to PHI to those employees, contractors, or agents of Business Associate who are actively and directly participating in performing functions, activities, or services pursuant to the Agreement and who need to know such PHI in order to fulfill such responsibilities.

(k) Retention of PHI. Business Associate shall retain all PHI throughout the term of the Agreement and shall continue to maintain the information required under Section 2(h) of this BA Agreement for a period of six (6) years from its creation.

(l) Notification Obligations; Mitigation. During the term of this BA Agreement, Business Associate shall notify Covered Entity as soon as possible, but in no event later than three (3) days (or such shorter time period as required by applicable law) after discovery of any use and/or disclosure of PHI not permitted by this BA Agreement, a Breach of Unsecured PHI, or any material Security Incident of which it becomes aware. This notification obligation shall include the information required by HIPAA and, at a minimum, shall provide Covered Entity with the following information: (i) a description of the facts and circumstances concerning the improper use or disclosure, Breach or Security Incident; (ii) a description of the PHI affected; and (iii) the names and identity of the individual(s) affected. Business Associate shall take prompt corrective action to mitigate and cure, if possible, any harmful effect that is known to Business Associate of an improper use and/or disclosure of PHI, Breach or Security Incident. Business Associate shall cooperate with Covered Entity regarding any Breach notification to third parties, and shall reimburse Covered Entity for any costs incurred by Covered Entity in complying with the applicable requirements of HIPAA resulting from a Breach of Unsecured PHI by Business Associate. Business Associate shall be deemed to discover a Breach of Unsecured PHI as of the first day on which such Breach is known, or should have been known, by Business Associate.

(m) Additional Obligations. Business Associate shall comply with the requirements of HIPAA which are applicable to business associates, including all regulations which are issued to implement such requirements, as may be amended, modified, or superseded from time to time. To the extent Business Associate carries out one or more of Covered Entity's obligation(s) under 45 CFR Part 164, Subpart E, in the performance of such obligations, Business Associate shall comply with the requirements of 45 CFR Part 164, Subpart E, that apply to Covered Entity to the same extent as required by Covered Entity. Business Associate shall comply with all applicable state and federal laws that affect the privacy or security of PHI received from the Covered Entity.

(n) Compliance with Standard Transactions. If Business Associate conducts, in whole or in part, Standard Transactions (as such term is defined in the Standards for Electronic Transactions Rule at 45 CFR Parts 160 and 162, as may be amended, modified or superseded, from time to time) for or on behalf of Covered Entity, Business Associate will comply, and will require any of its subcontractors or agents involved with such Standard Transactions on behalf of Covered Entity to comply, with each applicable requirement of 45 CFR Parts 160 and 162. Business Associate will not enter into, or permit its subcontractors or agents to enter into, any agreement in connection with the conduct of Standard

Transactions for or on behalf of Covered Entity that: (i) changes the definition, data condition, or use of a data element or segment in a Standard Transaction; (ii) adds any data elements or segments to the maximum defined data set; (iii) uses any code or data element that is marked "not used" in a Standard Transaction or are not in the Standard Transactions' implementation specification; or (iv) changes the meaning or intent of the Standard Transactions' implementation specifications.

(o) Data Jurisdiction. Business Associate may not create, receive, maintain, transmit, or store PHI in any jurisdiction outside of the United States, including, but not limited to, on any server (physical, cloud or otherwise) located outside of the United States.

Section 3. Obligations of Covered Entity.

(a) Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's Notice of Privacy Practices in accordance with 45 CFR § 164.520, to the extent that such limitation(s) may affect Business Associate's use or disclosure of PHI.

(b) Restrictions on Use or Disclosure. Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by individuals to use and/or disclose PHI, to the extent such changes or revocations may affect Business Associate's permitted or required uses and/or disclosures of PHI. Further, Covered Entity shall notify Business Associate of any restriction to the use and/or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent such restriction may affect Business Associate's permitted or required uses and/or disclosures of PHI.

Section 4. Term and Termination.

(a) Term. This BA Agreement shall commence on the Effective Date and will remain effective for the entire term of the Agreement, unless earlier terminated in accordance with the terms herein.

(b) For Cause Termination Due to Material Breach. Either party may terminate this BA Agreement by notice in writing to the other party, if the other party materially breaches this BA Agreement in any manner and such material breach continues for a period of thirty (30) days after written notice is given to the breaching party by the other party specifying the nature of the breach and requesting that it be cured. A material breach of this BA Agreement shall constitute a breach of the Agreement. If termination of this BA Agreement is not feasible, the non-breaching party shall report the breach to the Secretary, if required by HIPAA.

(c) Effect of Termination. Upon termination of this BA Agreement, Business Associate shall return or destroy all PHI (regardless of form or medium), including all copies thereof and any data compilations derived from PHI and allowing identification of any individual who is the subject of the PHI. The obligation to return or destroy all PHI shall also apply to PHI that is in the possession of subcontractors or agents of Business Associate. If the return or destruction of PHI is not feasible, Business Associate shall provide Covered Entity written notification of the conditions that make return or destruction not feasible. Upon notification that return or destruction of PHI is not feasible, Business Associate shall continue to extend the protections of this BA Agreement to such information and limit further uses or disclosures of such PHI to those purposes that make the return or destruction of such PHI not feasible, for as long as Business Associate maintains such PHI. If Business Associate elects to destroy the PHI, Business Associate shall notify Covered Entity in writing that such PHI has been destroyed.

(d) Injunction. In the event of a breach by Business Associate of any of its obligations hereunder, Covered Entity shall have, in addition to any other rights and remedies available at law or in equity, the right to obtain injunctive relief without the necessity of proving actual damages or that any irreparable harm would or might result from a failure to obtain injunctive relief, it being acknowledged and agreed to by all parties hereto that any such breach will cause irreparable harm to Covered Entity and that monetary damages alone will not provide an adequate remedy.

Section 5. Enforcement, Civil Monetary Penalties. The parties hereby acknowledge that in providing services pursuant to the Agreement, Business Associate is at all times acting as an independent contractor and not as an agent of the Covered Entity. In accordance with HIPAA, Business Associate hereby acknowledges that it/he/she will be directly liable for civil money penalties for: (i) impermissible uses and disclosures of PHI; (ii) failure to provide notifications of Breaches of Unsecured PHI to the Covered Entity; (iii) failure to provide access to a copy of electronic PHI to either the Covered Entity, the individual subject to the electronic PHI or the individual's designee, as designated by the Covered Entity; (iv) failure to disclose PHI where required by the Secretary to investigate or determine the Covered Entity's or Business Associate's compliance with HIPAA; (v) failure to provide an accounting of disclosures of PHI in accordance with the requirements of HIPAA; (vi) failure to comply with the requirements of the Security Rule; (vii) failure to limit PHI used and/or disclosed to the minimum amount necessary to accomplish the intended purpose; and (viii) failure to obtain the written agreement of its subcontractors or agents to be bound by the terms of this BA Agreement and applicable law to the same extent as Business Associate.

Section 6. Indemnification.

(a) Business Associate agrees to indemnify, defend and hold harmless Covered Entity and its owners, officers, employees and agents from any and all claims, penalties, fines, costs, liabilities or damages, including but not limited to reasonable attorneys' fees, arising from or based upon any violation of this BA Agreement and/or HIPAA by Business Associate or any of its owners, officers, employees, agents and subcontractors.

(b) Covered Entity agrees to indemnify, defend and hold harmless Business Associate and its owners, officers, employees and agents from any and all claims, penalties, fines, costs, liabilities or damages, including but not limited to reasonable attorneys' fees, arising from or based upon any violation of this BA Agreement and/or HIPAA by Covered Entity or any of its owners, officers, employees, agents and subcontractors.

Section 7. **Construction.** This BA Agreement shall be construed as broadly as necessary to implement and comply with HIPAA. The parties agree that any ambiguity in this BA Agreement shall be resolved in favor of a meaning that complies and is consistent with HIPAA. In the event the terms of this BA Agreement conflict with the terms of the Agreement, the terms of this BA Agreement shall control.

Section 8. **Captions.** The captions contained in this BA Agreement are included only for convenience of reference and do not define, limit, explain or modify this BA Agreement or its interpretation, construction or meaning and are in no way to be construed as part of this BA Agreement.

Section 9. **Notice.** All notices and other communications required or permitted pursuant to this BA Agreement shall be in writing, addressed to the party at the address set forth at the end of this BA Agreement, or to such other address as any party may designate from time to time in writing in accordance with this Section. All notices and other communications shall be sent by: (i) registered or certified mail, return receipt requested, postage pre-paid; (ii) overnight mail by reputable carrier; (iii) facsimile with a copy sent by First Class Mail, postage pre-paid; or (iv) hand delivery. All notices shall be effective as of the date of delivery if by hand delivery or overnight mail, two (2) days following the date of facsimile, or if by certified mail on the date of receipt, whichever is applicable.

Section 10. **Assignment.** This BA Agreement and the rights and obligations hereunder shall not be assigned, delegated, or otherwise transferred by either party without the prior written consent of the other party and any assignment or transfer without proper consent shall be null and void.

Section 11. **Governing Law and Venue.** This BA Agreement shall be governed by, and interpreted in accordance with HIPAA, and the internal laws of the State in which the Covered Entity has its principal place of business, without giving effect to any conflict of laws provisions.

Section 12. **Binding Effect; Modification.** This BA Agreement shall be binding upon, and shall ensure to the benefit of, the parties hereto and their respective permitted successors and assigns. This BA Agreement may only be amended or modified by mutual written agreement of the parties; provided, however, that in the event provisions of this BA Agreement shall conflict with the requirements of HIPAA, this BA Agreement shall automatically be deemed amended as necessary to conform to such legal requirements at all times.

Section 13. **Waiver.** The failure of either party at any time to enforce any right or remedy available hereunder with respect to any breach or failure shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

Section 14. **Severability.** In the event that any provision or part of this BA Agreement is found to be totally or partially invalid, illegal, or unenforceable, then the provision will be deemed to be modified or restricted to the extent and in the manner necessary to make it valid, legal, or enforceable, or it will be excised without affecting any other provision of this BA Agreement, with the parties agreeing that the remaining provisions are to be deemed to be in full force and effect as if they had been executed by both parties subsequent to the expungement of the invalid provision.

Section 15. **No Third-Party Beneficiaries.** Nothing express or implied in this BA Agreement is intended to confer, nor shall anything herein confer, upon any person or entity other than Covered Entity, Business Associate and their respective successors or permitted assigns, any rights, remedies, obligations or liabilities whatsoever.

Section 16. **Counterparts.** This BA Agreement may be executed in multiple counterparts, each of which shall constitute an original and all of which together shall constitute but one BA Agreement.

Section 17. **Entire Agreement.** This BA Agreement constitutes the entire agreement between the parties with respect to the matters contemplated herein and supersedes all previous and contemporaneous oral and written negotiations, commitments, and understandings relating thereto.

[Signatures on following page]

IN WITNESS WHEREOF, Covered Entity and Business Associate have each caused this BA Agreement to be executed in their respective names by their duly authorized representatives as of the Effective Date.

BUSINESS ASSOCIATE:

_____

Signature: _____

Print Name/Title_____

Address: _____
_____
_____

Telephone: _____
Facsimile: _____

Contact Person: _____

COVERED ENTITY:

The Health Care Authority of the City of Anniston
d/b/a Northeast Alabama Regional Medical Center

Signature: _____

Print Name/Title: _____

Address: Post Office Box 2208
Anniston, Alabama 36202

Telephone: _____
Facsimile: _____

Contact Person: _____

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PATIENT'S RIGHT TO INSPECT AND/OR COPY PHI

A patient has a right of access to inspect and/or copy PHI in our designated record set except for:

(a) Psychotherapy notes;

(b) Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and

1. Processing Patient Requests.

Patient requests for access to inspect and/or copy PHI will be processed in the following manner.

a. Request in Writing. A patient seeking to gain access to inspect and/or copy his/her PHI must submit a request in writing to Health Information Services on the *Patient Request to Inspect and/or Copy PHI* or the *Patient Authorization For Use and/or Disclosure of PHI* forms. Requests for access submitted on a form or in a format other than prescribed above will not be accepted. Rather, patients who submit non-compliant access requests will be advised of this policy and will be provided the necessary form to complete and sign. The use of standardized forms for this request is meant to ensure that we receive all the necessary information from a patient in order that we may process the request in a timely manner. If the covered entity does not maintain the PHI that is the subject of the request for access, and we know where the requested information is maintained, we must inform the individual where to direct the request for access.

b. Format of PHI. We must provide the individual with access to the PHI in the form and format requested by the individual, if it is readily producible in such form and format, or, if not, in a readable hard copy form or such other form and format as agreed to by the covered entity and the individual. If the protected health information that is subject of a request for access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information the covered entity must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it readily producible in such form and format; or if not, in a readable electronic form and format as agreed to by the covered entity and the individual. If directed by the patient we shall send a copy of the patient's PHI in electronic form to an entity or person designated by the patient to receive the information. Such designation shall be clear, conspicuous, and specific. Please reference the *Administrative Policy: Guidance to Staff on the Disclosure of PHI While Patient is Currently Being Treated, P-*

(a) Please reference the *Administrative Policy: Guidance to Staff on the Disclosure of PHI While Patient is Currently Being Treated.*

(b) Summary/Explanation of PHI Requested. A summary of a patient's requested PHI may be provided, in lieu of providing access to the PHI, or an explanation of the PHI to which

access has been given may be provided. The patient must agree in advance to a summary or explanation of his/her PHI and to the fees imposed for providing such summary or explanation.

(c) Time and Manner of Access. We will provide the access requested by a patient in a timely manner, including arranging with the patient for a convenient time and place to inspect or obtain a copy of his/her PHI, or mailing a copy of PHI upon request. We may discuss the scope, format, and other aspects of the request with the patient, as necessary to facilitate the timely provision of access.

(d) Fees. If a patient requests a copy of their PHI or agrees to a summary or explanation of such information, we may impose a reasonable cost-based fee, provided that the fee includes only the cost that the OCR has given guidance upon.

If a patient requests a copy (or summary or explanation) of his/her PHI in electronic form, we may impose a reasonable cost based fee following OCR guidance for responding to such request, provided that the fee is and in accordance with applicable law. If the patient requests access in an electronic format and such access can be achieved within the guidelines of HIPAA, such electronic access is granted, regardless of whether or not the information is contained in the EMR or otherwise stored electronically in a designated record set. The hospitals also provide patient's electronic information though patient portals.

(e) Third-Party Recipient. If a patient's request for access directs us to transmit a copy of the PHI directly to another individual designated by the patient we will provide the copy to the designated individual. However, the patient's request must be in writing on the *Patient Request to Inspect and/or Copy PHI*, signed by the patient and clearly identify the designated person and where to send the copy of PHI.

(f) Documentation. We will document the following and retain such documentation for six (6) years after its creation date or after the date when it was last effective, whichever is later (See Policy: *Recordkeeping and Retention*):

- The designated record sets that are subject to access by patients; and
- The titles of the persons or offices responsible for receiving and processing requests for access by patients.

(g) Right to have information disclosed upon request. You have the right to have us disclose your protected health information to another named by you or a third party in writing.

(h) Right to direct where copies will be sent to health and claims records to a third party. If you wish us to send a copy of your health and claims records to a third party please notify us by completed the patient authorization for use and disclosure form.

2. Timely Action for Handling Patient Requests.

Patient requests for access to inspect and/or copy PHI in a designated record set will be responded to in a timely manner by Health Information Services staff.

(a) Time-Frame. We shall act on a patient's request for access no later than thirty (30) days after receipt of the request.

- If we grant the request, in whole or in part, we will inform the patient of the acceptance of the request and provide the access requested.

- If we deny the request, in whole or in part, we will provide the patient with a written denial.

(b) Extension. If we are unable to act on a request for access within the 30-day timeline prescribed above, we may extend the time to respond only once and by no more than thirty (30) days, provided that we provide the patient within the original 30-day time limit, whichever is applicable, with a written statement of the reasons for the delay and the date by which we will complete our response.

3. Unreviewable Grounds for Denial of Access.

We may deny a patient the right to access his/her PHI in a designated record set, without providing the patient an opportunity to seek a review of such a denial, under the following circumstances:

(a) PHI Generally Accepted from a Patient's Right of Access. A patient may be denied the right of access to PHI where it constitutes:

- Psychotherapy notes which are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session at a group, joint, or family counseling session and that are separated from the rest of the individual's medical records. Psychotherapy notes do not include medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date;

- Information compiled by us in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;

(b) PHI Used by Correctional Institutions. A patient who is serving time at a correctional institution may be denied, in whole or in part, access to his/her PHI, if obtaining a copy would jeopardize the health, safety, security, custody, rehabilitation of the patient or other inmates, or the safety of any officer, employee, or other person at the correctional institution or who is responsible for the transport of the patient.

(c) PHI Used in Research. A patient may be denied access to PHI created or obtained in the course of research, provided that the patient has agreed, as part of the research protocol, to the limitation on access during the duration of the research and the patient's right of access will be reinstated upon completion of the research. This request will be coordinated with the hospital Research Nurse.

(d) PHI Subject to the Privacy Act. A patient may be denied access to PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a and meet the denial of access requirements contained therein.

(e) PHI Obtained Confidentially. A patient may be denied access if the PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

4. Reviewable Grounds for Denial of Access.

We may deny a patient access to his/her PHI in a designated record set provided that the patient is given a right to have such denials reviewed, in the following circumstances:

(a) A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;

(b) The PHI makes reference to another person (unless such person is a licensed health care professional) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

(c) The request is made by the patient's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the patient or another person.

When access is denied, a patient has a right to have the denial reviewed by a licensed health care professional who has been designated by us to act as a reviewing official and who did not participate in the original decision to deny access. We will promptly refer a request for review to such designated reviewing professional who then must determine, within a reasonable period of time, whether or not to deny the access requested based on the reviewable grounds for denial of access. After the designated reviewing official reaches a decision, we will then promptly provide written notice to the patient of the determination of the reviewing professional and shall act in accordance with such determination.

5. Implementing a Denial of Access.

In the event we deny a patient access, in whole or in part, to his/her PHI in a designated record set, we will implement the following procedures:

(a) Make Other Information Accessible. We will, to the extent possible, give the patient access to any other PHI requested, after excluding the PHI for which we have a ground to deny access.

(b) Provide Written Denial to Patient. We will provide a timely written denial to the patient in plain language and which contains the basis of the denial; a statement of the patient's review rights, if applicable, including a description of how the patient may exercise such rights; and a description of how the patient may complain to us or to the Secretary of HHS. We will use the *Written Denial to Copy and/or Inspect Protected Health Information* form. In addition, the patient will be provided the name, or title, and the telephone number of the Health Care Authority personnel who would receive complaints.

(c) Guidance on Where to Direct Request. If we do not maintain the PHI that is the subject of the request and we know where the information is maintained, we will inform the patient where to direct their request.

- **Forms: Patient Request to Inspect and/or Copy PHI**

  Written Denial to Copy and/or Inspect PHI

  Patient Authorization For Use and/or Disclosure of PHI

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

Patient Request to Inspect and/or Copy Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

I hereby request that RMC grant me access to

Check One: _____ Inspect _____ Copy _____ Inspect & Copy

my personal health information maintained by RMC.

Provide a specific description of the personal health information you are seeking to access (*include dates of service, type of service, etc.*):_____
_____
_____
_____

By submitting this request I understand:

1. That RMC may deny my request to access my health information, with or without review, depending on the type of information I am seeking and whether RMC actually maintains this information.

2. If I agree, I may be provided with a summary or explanation of the health information requested, in lieu of being provided access to the information. By initialing below, I am indicating that I am willing to receive a summary or explanation of the health information I have requested and to pay all fees associated with this request.

   Your Initials: _____ Please send me a summary or explanation of my health information. I agree to pay all fees associated with this request.

3. That RMC may impose a reasonable fee for accessing my health information, provided that the fee includes only the cost of:

   (a) Copying, including the cost of supplies and labor;
   (b) Postage, where I have requested that the copy or the summary/explanation be mailed; and
   (c) Preparing an explanation or summary of my health information, where I have agreed to and requested such material.

BY SIGNING THIS FORM, I ACKNOWLEDGE THAT I HAVE READ THIS FORM AND UNDERSTAND THE TERMS AND CONDITIONS OF REQUESTING MY HEALTH INFORMATION.

_____ _____
Signature of Patient or Patient's Representative Date

_____
Printed Name of Patient's Representative (*if applicable*)

_____
Representative's Relationship to Patient (*if applicable*)

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

Written Denial to Copy and/or Inspect Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

We have denied your request to inspect and/or copy your Protected Health Information ("PHI") for the following reason(s) *(check all that apply)*:

1. Unreviewable Grounds for Denial.

☐ The PHI involves Psychotherapy Notes;

☐ The PHI was compiled by us in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding;

☐ The PHI is:
(1) Subject to the Clinical Laboratory Improvements Amendments of 1988, 42 USC. 263a, or
(2) Exempt from the Clinical Laboratory Improvements Amendments of 1988, 42 CFR 493.3(a)(2).

☐ As an inmate in a correctional institution, it has been determined that the disclosure of PHI would jeopardize the health, safety, security, custody, rehabilitation of you or other inmates, or the safety of any officer, employee or other person at the correctional institution;

☐ The PHI was created or obtained in the course of research and you agreed to the denial of access when consenting to participate in the research;

☐ The PHI is subject to the Privacy Act, 5 USC § 552a, and cannot be disclosed; or

☐ The PHI was obtained by us from someone other than a health care provider under a promise of confidentiality and access would likely reveal the source of the information.

2. Reviewable Grounds for Denial of Access.

☐ A licensed health care professional has determined, in the exercise of professional judgment, that access is reasonably likely to endanger your life or physical safety or that of another person;

☐ The PHI makes reference to another person (other than a healthcare provider) and a licensed health care professional has determined, in the exercise of professional

☐ The request is made by your personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that access by such personal representative is reasonably likely to cause substantial harm to you or another person.

If we deny access, in part, we will make other requested information accessible. If we do not maintain the PHI that is the subject of your request and we know where the information is maintained, we will inform you where to direct your request.

3. Review of Denial of Access.

(a) If access is denied under Paragraph 2 above, you have the right to have the denial reviewed by a licensed health care professional who is designated by us to act as a reviewing official and who did not participate in the original decision to deny access. You must promptly notify us within thirty (30) days of the date of this Written Denial of your request to have the denial reviewed. We will promptly refer any timely request for review to such designated reviewing professional who will determine, within a reasonable period of time, whether to permit or deny access. After the designating reviewing official reaches a decision, we will promptly provide you with a written notice informing you of the determination of the reviewing professional. We will grant or deny access in accordance with the determination of the reviewing professional.

(b) If you wish to have a denial of a request to inspect and/or copy PHI reviewed, you must submit a request for review in writing to our Privacy Officer at the following address:

400 E. 10TH ST
P.O. Box 2208
ANNISTON, AL 36202
(256) 741-6456
Attn: Privacy Officer

Our Privacy Officer shall be responsible for receiving and processing all such requests.

(c) If you wish to submit a complaint regarding our unwillingness to grant you access to your PHI, please submit your complaint in writing to our Privacy Officer or to the Secretary of the Department of Health and Human Services.

_____ _____

Signature of Privacy Officer Date

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PATIENT'S RIGHT TO REQUEST RESTRICTIONS ON USE AND DISCLOSURE OF PHI

A patient may request restrictions on the use or disclosure of their PHI to carry out treatment, payment or health care operations, as well as restrictions on disclosures to persons involved in the patient's care. However, we are not required to agree to a requested restriction, unless such agreement is required by applicable law. For example, we must comply with a restriction where the disclosure is to a health plan for purposes of carrying out payment or health care operations and the PHI pertains solely to a health care item or service for which The Health Care Authority has been paid by the patient, out of pocket, in full. *Except in unusual circumstances or where required by law, it is our general policy not to agree to any patient requests for restrictions on the use or disclosure of PHI.*

1. Process for Seeking a Restriction.

Patients seeking to restrict the use or disclosure of their PHI must submit their requests in writing to us. Only requests made on the *Patient Request for Restrictions on Use and Disclosure of PHI* form will be reviewed. Patients will not be required to elaborate upon the circumstances or provide an explanation or the reason for the restriction. Patients who submit restriction requests on an improper form will be advised of this policy and will be provided the necessary form to complete and sign. The use of a standardized form for requesting restrictions is meant to ensure that we receive all the necessary information, in order that we may properly process and document requests in a timely and thorough manner.

The Privacy Officer shall be responsible for overseeing the approval or denial of all such restriction requests. Patients will be notified of the denial of such requests through the *Written Denial to Restrict the Use and/or Disclosure of PHI* form. All requests granted will be abided by. When responding to others seeking PHI, including Business Associates, we will exercise appropriate care not to reveal the restricted information when disclosing that a restriction is in place. In accordance with HIPAA, the Privacy Officer will retain, on file, copies of granted requests for restrictions on use and disclosure of PHI for six (6) years after their creation date or after the date when they were last effective, whichever is later. (See Policy: *Recordkeeping and Retention*).

2. Exceptions to Restrictions.

Although not required to agree to a restriction, if a restriction request of patient is granted, we must abide by that agreement unless one of the following exceptions apply.

(a) Patient in Need of Emergency Treatment. Where a patient who has requested a restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment and care, we may use the restricted PHI, or may disclose such information to a health care provider, to provide treatment to the patient. However, in such circumstances, we will request that the health care provider not use or disclose the information further.

(b) Individual Requests Access to the Restricted PHI. A restriction is not effective where a patient requests information pursuant to his/her right to inspect and/or copy PHI or requests an accounting of PHI disclosures. In such circumstances, we may disclose PHI

to the patient regardless of the restriction, except when the restricted information is privileged. In this case, we would secure the authorization of the physician/psychiatrist prior to disclosure.

(c) Facility Uses Information for Directory Purposes. A restriction is not effective for PHI that is used and disclosed for facility directories, where a patient has been previously given an opportunity to verbally agree or object to such disclosure.

(d) Authorization or Opportunity to Agree or Object Not Required. A restriction is not effective for the use and disclosure of PHI for public purposes where an authorization or opportunity to agree or object is not required under the Privacy Rules. (See Policy: *Use and Disclosure of PHI Without Authorization or Opportunity to Verbally Agree or Object*).

(e) Secretary of HHS. A restriction is not effective for the use and disclosure of PHI when required by the Secretary of HHS to investigate or determine The Health Care Authority's compliance with HIPAA.

3. Terminating a Restriction.

A restriction may be terminated if:

(a) The patient agrees to or requests the termination in writing;

(b) The patient orally agrees to the termination and the oral agreement is documented; or

(c) We inform the patient that we are terminating the agreement to a restriction, except that such termination is only effective with respect to PHI created or received after we have informed the patient.

➢ **Forms: Patient Request for Restrictions on Use and/or Disclosure of PHI**

Written Denial to Restrict the Use and/or Disclosure of PHI

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

Patient Request for Restrictions on Use and/or Disclosure of Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

I hereby request that RMC restrict the

Check One: _____ Use _____ Disclosure _____ Use & Disclosure

of my health information as follows:

Specific description of health information not to be used or disclosed (*include type of service, person/entity to whom disclosure should not be made, etc.*):

_____
_____
_____

Provide description of scope of the requested restriction (*include description of parties who should not* receive health information described above, etc.):

_____
_____
_____

Please note: We will carefully consider your request, but we are not obligated to accept your request.

BY SIGNING BELOW, I ACKNOWLEDGE THAT I HAVE READ THIS FORM AND UNDERSTAND THE TERMS AND CONDITIONS OF REQUESTING A RESTRICTION ON THE USE AND/OR DISCLOSURE OF MY PROTECTED HEALTH INFORMATION.

_____ _____
Signature of Patient or Patient's Representative Date

_____
Printed Name of Patient's Representative (*if applicable*)

_____
Representative's Relationship to Patient (*if applicable*)

To Be Completed by RMC

The requested restrictions on the use and/or disclosure of the patient's health information are:

_____ Accepted _____ Denied (complete "Written Denial to Restrict Use/Disclosure of PHI" form)

_____ _____
Signature of RMC Representative Date

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER (RMC)
400 East 10TH ST ANNISTON, ALABAMA 36207 (256) 235-5763

Written Denial to Restrict the Use and/or Disclosure of Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

We have received your request to restrict the use and/or disclosure of your health information dated _____. After consideration, we have decided to deny your request for the following reasons:

_____

_____

_____

_____

If you have any questions and/or concerns, you may contact our Privacy Officer at (256) 741-6456.

_____ _____

Privacy Officer Date

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

Patient Request for Restrictions on Use and/or Disclosure of Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

I hereby request that RMC restrict the

Check One: _____ Use _____ Disclosure _____ Use & Disclosure

of my health information as follows:

Specific description of health information not to be used or disclosed (*include type of service, person/entity to whom disclosure should not be made, etc.*):

_____
_____
_____

Provide description of scope of the requested restriction (*include description of parties who should not* receive health information described above, etc.):

_____
_____
_____

Please note: We will carefully consider your request, but we are not obligated to accept your request.

BY SIGNING BELOW, I ACKNOWLEDGE THAT I HAVE READ THIS FORM AND UNDERSTAND THE TERMS AND CONDITIONS OF REQUESTING A RESTRICTION ON THE USE AND/OR DISCLOSURE OF MY PROTECTED HEALTH INFORMATION.

_____ _____
Signature of Patient or Patient's Representative Date

_____
Printed Name of Patient's Representative (*if applicable*)

_____
Representative's Relationship to Patient (*if applicable*)

To Be Completed by RMC

The requested restrictions on the use and/or disclosure of the patient's health information are:

_____ Accepted _____ Denied (complete "Written Denial to Restrict Use/Disclosure of PHI" form)

_____ _____
Signature of RMC Representative Date

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER (RMC)
400 East 10TH ST ANNISTON, ALABAMA 36207 (256) 235-5763

Written Denial to Restrict the Use and/or Disclosure of Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

We have received your request to restrict the use and/or disclosure of your health information dated _____. After consideration, we have decided to deny your request for the following reasons:

_____

_____

_____

_____

If you have any questions and/or concerns, you may contact our Privacy Officer at (256) 741-6456.

_____ _____

Privacy Officer Date

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PATIENT'S RIGHT TO REQUEST AN AMENDMENT OF PHI

A patient has the right to request an amendment of his/her PHI for as long as the PHI is maintained in a designated record set. The Privacy Officer shall be responsible for receiving and processing all such requests for amendment. The Privacy Officer, in conjunction with the attending physician and/or the Medical Director shall be responsible for approving or denying all such requests for amendment.

Patients are notified of their right to request an amendment of their PHI in our Privacy Notice. Patients seeking to amend their PHI must submit their requests in writing to us on the *Patient Request for Amendment of PHI* form. The patient's request should specify the reason to support a requested amendment. The completed *Patient Request for Amendment of PHI* form shall be maintained for six (6) years from the date it was created, or after the date when it was last effective, whichever is later. (See Policy: *Recordkeeping and Retention*).

1. Reasons for Denial of Request.

A patient's request for amendment may be denied if we determine that the PHI that is the subject of the request:

(a) Was not created by us, unless the patient provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment;

(b) Is not part of the designated record set;

(c) Would not be available for inspection (See Policy: *Patient's Right to Inspect and/or Copy PHI*); or

(d) Is accurate and complete.

2. Time to Respond.

A patient's request for an amendment will be acted upon by the Privacy Officer no later than sixty (60) days after receipt of such request. If, however, we are unable to act on the amendment within sixty (60) days, we may extend the time for such action by no more than thirty (30) days, provided that:

(a) We provide the patient, no later than sixty (60) days after receipt of such request, with a written statement of the reasons for the delay and the date by which we will complete the action on the request, and

(b) We shall only have one such extension of time for action on a request for amendment.

3. Acceptance of Amendment.

If requested amendment is accepted, in whole or in part, we will take the following actions:

(a) We will make the appropriate amendment to the PHI that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the

amendment and appending or otherwise providing a link to the location of the amendment;

(b) Timely informing the patient that the amendment is accepted and obtain the patient's identification of an agreement to have us notify the relevant persons (discussed below) with whom the amendment needs to be shared in a timely fashion; and

(c) Provide the amendment within a reasonable time to: (i) persons identified by the patient as having received PHI about the patient needing amendment, and (ii) persons, including Business Associates, that we know have the PHI that is the subject of the amendment and that may have relied or could foreseeably rely, on such information to the detriment of the patient.

4. **Denial of Amendment.**

(a) If the requested amendment is denied, in whole or in part, we must provide the patient with a timely, written denial using the *Written Denial to Amend PHI* form, which contains the following items:

- The basis for the denial;
- The patient's right to submit a written statement disagreeing with the denial and how the patient may file such statement;
- A statement that, if the patient does not submit a statement of disagreement, the patient may request that we provide the patient's request for amendment and our denial with any future disclosures of the PHI that is the subject of the amendment; and
- A description of how the patient may complain to us pursuant to the complaint procedures established by these policies and procedures and the Privacy Notice. The description will include the name or title and telephone number of our Privacy Officer.

(b) We must permit the patient to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement.

(c) We may prepare a written rebuttal to the patient's statement of disagreement. If a written rebuttal is prepared, a copy must be given to the patient who submitted the statement of disagreement.

(d) We shall identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the patient's request for amendment, our denial, the patient's statement of disagreement, if any, and our rebuttal, if any, to the designated record set.

(e) If a patient submits a statement of disagreement we shall include the material appended in accordance with 4(d) above, or, at our election, an accurate summary of any such information, with any subsequent disclosure of PHI to which the disagreement relates. If a written statement of disagreement has not been received we shall include the patient's request for amendment and our denial, or an accurate summary of such information, with

any subsequent disclosure of the PHI only if the patient has requested such action. If a Standard Transaction does not permit the additional material to be included with the disclosure, we may separately transmit the material required by this section, to the recipient of the Standard Transaction.

(f) When we are informed by another covered entity of an amendment to a patient's PHI, we shall amend the PHI in the designated record set.

➢ **Forms: Patient Request for Amendment of PHI**

Written Denial to Amend PHI

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

Written Denial to Amend Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

We have denied your request dated _____ to amend your protected health information ("PHI") for the following reasons:

? The PHI was not created by us;
? The PHI is not part of a designated record set;
? The PHI is not available for inspection, under the Privacy Rules or
? The PHI is accurate and complete.

_____

_____

_____

You have the following rights regarding the denial of your request to amend your health information:

a) **Right to submit a statement of disagreement.** You have the right to submit a statement of disagreement disputing the denial. You may submit the statement of disagreement to our Privacy Officer at the following address:

400 E. 10TH ST
P.O. Box 2208
ANNISTON, AL 36202
(256) 741-6456

The Privacy Officer is responsible for receiving and processing all such statements of disagreement. Any statement of disagreement will be included with your health information. If you decide not to submit a statement of disagreement, you may ask that we include your request for amendment and our denial with any future disclosures of your health information. You should submit this request to our Privacy Officer.

a) **Rebuttal statement.** We may prepare a written rebuttal to your statement of disagreement, if any, and will provide you with a copy of the rebuttal statement.

b) **Complaint Process.** If you wish to submit a complaint regarding our decision not to amend your health information please submit your complaint to the Privacy Officer. You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services. Please see our Privacy Notice for more information.

_____ _____
Privacy Officer Date

_____ _____
Medical Director Date

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER (RMC)
400 East 10TH ST ANNISTON, ALABAMA 36207 (256) 235-5763

Patient Request for Amendment of Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

I hereby request that RMC amend my health information in the following manner and for the following reasons:

- Specific description of health information to be amended (*include type of service, scope of amendment, etc.)*:

  _____

  _____

  _____

- Provide detailed explanation for requested amendment:

  _____

  _____

  _____

  _____

I understand that I have the right to request an amendment of my health information, maintained by or for RMC, and that RMC may deny my request if it determines that I have asked to amend information that: was not created by RMC unless the person or entity that created the information is no longer available; is not health information maintained as part of a designated record set; is information that I am not permitted to inspect or copy; or RMC determines that the information is accurate and complete. If RMC disagrees with my requested amendment, it will provide me with a written explanation of the reasons for the denial, an opportunity to submit a statement of disagreement, and a description of how I may file a complaint.

BY SIGNING THIS FORM, I ACKNOWLEDGE THAT I HAVE READ THIS FORM AND THE PRIVACY NOTICE AND UNDERSTAND THE TERMS AND CONDITIONS OF REQUESTING AN AMENDMENT OF MY HEALTH INFORMATION.

_____ _____

Signature of Patient or Patient's Representative Date

_____

Printed Name of Patient's Representative (*if applicable*)

_____

Representative's Relationship to Patient (*if applicable*)

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PATIENT'S RIGHT TO AN ACCOUNTING OF DISCLOSURES OF PHI

Beginning April 14, 2003, a history of disclosures of PHI will be maintained. Patients may request an accounting for a period of up to six (6) years prior to the date of the request if the information is maintained in paper form or up to three (3) years prior if the information is maintained in electronic form. In addition, a patient may request an accounting of such information for a shorter period, such as one year.

1. Exceptions.

Accounting of Disclosures of PHI will not be recorded on the following:

(a) Disclosures for purposes of treatment, payment or health care operations if the released information is contained in paper form (if contained in an electronic health record, they will be accounted as required by applicable law);

(b) Disclosures to law officials or correctional institutions;

(c) Disclosures for facility directories, if applicable;

(d) Disclosures to the patients themselves;

(e) Disclosures pursuant to an authorization;

(f) Disclosures for national security or intelligence purposes;

(g) Disclosures to people involved in a patient's care or payment for care;

(h) Disclosures for notification purposes;

(i) Disclosures to health oversight agencies contingent on the agency's submission to us of a statement that indicates that an accounting of disclosures will impede an investigation that involves the patient in question. The statement must include a time frame for the exclusion period. The statement may be oral, but appropriate documentation must be received by us within thirty (30) days;

(j) Disclosures that are part of a Limited Data Set;

(k) Incidental disclosures; or

(l) Any other reason exempted by applicable law.

2. Process to Request an Accounting.

A patient requesting an accounting of their PHI must submit their requests in writing to Health Information Services on the *Patient Request for an Accounting of Disclosures of PHI* form. The Privacy Officer shall be responsible for receiving, processing and approving or denying all such requests for accounting. The completed *Patient Request for an Accounting of PHI* form shall be maintained for six (6)

years from the date it was completed by the patient. A patient is allowed to request one accounting within any 12-month period free of charge. A reasonable cost-based fee may be charged for more frequent accounting requests, provided the patient is notified of the fee in advance. For subsequent accountings provided in paper form, the patient may be charged a fee for copying, compiling, and mailing the accounting. For subsequent accountings provided in electronic form, the patient may be charged a fee not to exceed our labor costs in processing the request.

3. Responding to a Request for an Accounting.

An accounting of disclosures will be provided within sixty (60) days from receiving the written request. If an accounting of disclosures cannot be honored within the sixty (60) days, then the reason for the delay and the expected completion date will be provided to the requestor. Only one 30-day extension of time will be acceptable per request.

4. Included in an Accounting.

An accounting shall include the following information:

(a) The date of the disclosure;

(b) The name of the entity or person who received the PHI and, if known, the address of such entity or person;

(c) A brief description of the PHI disclosed; and

(d) A brief statement of the purpose of the disclosure that reasonably informs the patient of the basis for the disclosure; or in lieu of such statement, a copy of the patient's written authorization/request for a disclosure.

5. Accounting of Disclosure Procedure.

Each department that discloses PHI that is not exempted will account for these disclosures. The following shall occur when accounting for a disclosure:

(a) Obtain the Accounting of Disclosures for PHI – Tracking Log Form;

(b) Complete all of the information required for the disclosure as outlined above (Section 4);

(c) Forward the *Tracking Log Form* to Health Information Services where it will be entered into a computerized tracking log, The Wizard, by the Health Information Services staff.

Inquiries related to the accounting of disclosures should be directed to Health Information Services.

Refer also to Table 1 for a non-inclusive list of disclosures requiring an accounting.

6. Summary Accounting Procedure.

Multiple disclosures to the same entity or individual recorded on a regular interval or an authorization with multiple disclosures may have a summary entry on the tracking log. The summary entry requires all information as described above for the first disclosure, an indication of periodic interval (monthly, weekly, etc.), and the date of the last disclosure.

7. Accounting for Disclosures for Research Purposes.

If research is conducted (1) pursuant to a valid waiver of authorization, (2) for preparatory research purposes, or (3) using only records of deceased individuals, and involves at least fifty (50) records, accounting to the patient for the disclosure of PHI will be accomplished by providing the patient with a list of all protocols for which the patient's PHI may have been disclosed, and when requested by the patient, the researcher's name and contact information. The list of protocols that we shall provide to the patient shall include:

(a) The name of the study;

(b) A description of the purpose and criteria of the study;

(c) The type of PHI sought and disclosed;

(d) The time frame of disclosures in response to the request;

(e) Name, address and telephone number of the sponsor and the researcher; and

(f) A statement that PHI may or may not have been disclosed for a particular protocol or research activity.

For more information regarding cancer research protocols, contact the Cancer Research Nurse.

- **Forms: Patient Request for an Accounting of Disclosures of PHI**

  Disclosure of PHI Tracking Log

Table 1 – The following disclosures will be accounted for (but are not limited to):	
➢ Adoption Services	➢ Environmental Protection Agency
➢ Adult Protective Services	➢ Food and Drug Administration (FDA) (adverse events, product defects, recalls, product tracking)
➢ Alabama Department of Public Health, including: Bureau of Vital Statistics, Cancer Registry, Trauma Registry	➢ Federal HMO Act
➢ Alabama Organ Center	➢ Funeral Directors
➢ AQAF (QIO)	➢ Immigration
➢ Birth Defect Registry	➢ Medical Examiner/Coroner
➢ Centers for Disease Control (CDC)	➢ Occupational Safety and Health Administration (OSHA)
➢ Dept of Human Resources (DHR), Child Protective Services	➢ Organ Procurement Bank (Cadaveric organ, eye or tissue donations)

➢ Clinical Licensing boards, including but not limited to: Board of Medical Examiners, Board of Nursing, Pharmacy Board	➢ Poison Control
➢ County public health departments, including: sexually transmitted diseases, animal bites, etc.	➢ Probate courts
➢ Court order, subpoena, warrant	➢ Reporting of wounds or other physical injuries as required by law
➢ Court-appointed guardians	➢ Research, if no authorization or Institutional Review Board (IRB) waiver
➢ Death due to suspected crime	➢ To avert a serious threat to health or safety
➢ Department of Health and Human Services (HHS)	➢ Workers' Compensation (disclosures to carriers or employers)
➢ Department of Justice	➢ Drug Enforcement Administration (DEA)
➢ Department of Public Safety	➢ Employers (medical surveillance, work injury follow-up)

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

Patient Request for an Accounting of Disclosures of Protected Health Information

Patient Name:	
Social Security Number:	Date of Birth:

I hereby request that RMC provide me with an accounting of the disclosures of my health information made by RMC for the time period from _____ to _____. I understand that RMC cannot provide an accounting of disclosures of health information dating back earlier than six (6) years from the date of my request. I further understand that the accounting will not include: disclosures related to treatment, payment or health care operations; disclosures to me; disclosures based on my Authorization; disclosures that are part of a Limited Data Set; incidental disclosures; disclosures to persons involved in my care or payment for my care; disclosures to correctional institutions or law enforcement officials; disclosures for facility directories; or disclosures that occurred prior to April 14, 2003.

BY SIGNING THIS FORM, I ACKNOWLEDGE THAT I HAVE READ THIS FORM AND THE PRIVACY NOTICE AND UNDERSTAND THE TERMS AND CONDITIONS OF REQUESTING AN ACCOUNTING OF MY HEALTH INFORMATION.

_____ _____
Signature of Patient or Patient's Representative Date

_____
Printed Name of Patient's Representative (*if applicable*)

_____
Representative's Relationship to Patient *(if applicable)*

To Be Completed by RMC

The request for an accounting on the use and/or disclosure of the patient's health information is (are):

___ Accepted ____Denied ____ Other (explain: _____)

_____ _____
Signature of RMC's Representative Date

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PATIENT'S RIGHT TO REQUEST CONFIDENTIAL COMMUNICATIONS

A patient has the right to request that communications from us regarding PHI be transmitted by alternative means or to alternative locations. We shall accommodate reasonable requests for alternative communications.

Patients seeking to have communications transmitted by alternative means or to alternative locations must submit their requests in writing to us on the *Patient Request for Confidential Communications* form. The Privacy Officer shall be responsible for receiving, processing, and approving or denying all such requests.

Patients requesting restrictions on the manner and method by which confidential communications are transmitted must specify reasonable, alternative means or methods by which they would prefer to receive PHI and must explain, if applicable, how they will handle payment. However, we will not require an explanation from a patient of the basis for the request as a condition for providing communications on a confidential basis.

If we agree to communicate with a patient by alternative means or at alternative locations, a copy of the *Patient Request for Confidential Communications* form must be placed in the patient's file, as well as in any other location where notice of such restriction is appropriate. A copy of the form will also be provided to the patient.

- **Form: Patient Request for Confidential Communications**

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

Patient Request for Confidential Communications

Patient Name:	
Social Security Number:	Date of Birth:

I hereby request that communications to me from RMC concerning my personal health information be transmitted by the following alternative means or to the alternative locations:

- Please use the following alternative means:

  _____

  _____

  _____

- Please send to the following locations:

  _____

  _____

  _____

  We will honor all reasonable requests.

BY SIGNING THIS FORM, I ACKNOWLEDGE THAT I HAVE READ THIS FORM AND THE PRIVACY NOTICE AND UNDERSTAND THE TERMS AND CONDITIONS OF REQUESTING RESTRICTIONS ON THE MANNER AND METHOD OF CONFIDENTIAL COMMUNICATIONS.

_____ _____
Signature of Patient or Patient's Representative Date

_____
Printed Name of Patient's Representative (*if applicable*)

_____
Representative's Relationship to Patient

To Be Completed by RMC

The request for confidential communications on the disclosure of the patient's health information is (are):

___ Accepted ___Denied ___ Other (Explain: _____)

_____ _____
Signature of RMC's Representative Date

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

SAFEGUARDING COMMUNICATION OF PHI

1. Safeguarding PHI Contained in Printed Information.

We are committed to safeguarding printed information containing PHI. To reduce the risks of any inappropriate or unlawful disclosures of PHI, we require that all printed information be handled, distributed, stored, and disposed of in a manner, which minimizes the possibility that PHI will be disclosed or used improperly. To help ensure the proper handling, distribution, use, storage and disposal of PHI, the following procedures shall be followed:

(a) Where appropriate, all desks and work stations shall be cleared of documents, paperwork, files, etc., at the close-of-business or the end of a Workforce member's shift, to help eliminate the possibility of unauthorized personnel having access to PHI;

(b) Authorized Workforce members shall act as designated conduits for all incoming correspondence and mail, to ensure that this material is distributed to the appropriate and intended recipient(s) for processing;

(c) Duplicates and/or photocopies of documents containing PHI shall be kept to the minimum number necessary to accomplish the intended purpose of a project; and

(d) Access to storage files, cabinets, rooms, etc., shall be restricted to authorized Workforce members and appropriately secured during and after work hours.

2. Safeguarding PHI Disclosed by Telephone and in Conversations.

A telephone system has been installed to facilitate both internal and external business communications. This system is our property, and we retain the right to inspect the system, as well as monitor its use.

Because every telephone call and conversation presents an opportunity for PHI to be improperly disclosed, members of our Workforce will conduct calls and conversations in a manner that will minimize the risk of unnecessary and inappropriate disclosures. To help ensure the protection of PHI, the following procedures shall be followed when disclosing PHI verbally:

(a) We will identify the person(s) requesting PHI by telephone, as well as their authority to receive and/or discuss PHI;

(b) Person(s) requesting PHI on patients must provide the patient identification number ("PIN") of the patient in order to receive PHI on the patient;

(c) Any PHI disclosed by telephone and in conversations shall be kept to the minimum necessary to accomplish the communication's intended and lawful purpose;

(d) Telephone calls and conversations will be conducted in a manner which minimizes the possibility of the conversation being overheard by persons other than the intended recipient, *i.e.*, other personnel, patients, or visitors within hearing range of the conversation;

(e) When possible, physical barriers such as doors and partitions will be utilized to help prevent conversations from being overheard by unauthorized persons; and

(f) To prevent access by unauthorized recipients, PHI will not be left on voicemail systems or disclosed to answering services without prior authorization and approval from the patient and the Privacy Officer, in accordance with HIPAA.

(g) Information left on voicemail for scheduling purposes is based on the wishes of the patient. Under no circumstances is information specific to a test communicated on voicemail or provided to anyone other than the patient.

Please refer to the *Administrative Policy: Electronic Mail and Voice Mail Policy,* in order to ensure the general protection and confidentiality of PHI communicated or received.

3. Safeguarding PHI Transmitted or Received by Facsimile ("Fax").

We are committed to safeguarding PHI transmitted or received by fax. Although fax machines and fax software can enhance the quality of health care by permitting the rapid transmission of information, we recognize that this equipment cannot ensure that information will always be transmitted to the intended or authorized recipient. Accordingly, where it is appropriate to transmit or receive PHI by facsimile, we will do so in the manner outlined below. **However, unless disclosure is for an emergent medical care issue, at no time shall we transmit or request that information regarding sexually transmitted diseases, chemical or substance dependency, HIV/AIDS, mental health status, or other highly sensitive health information be communicated by fax.**

All faxes containing PHI must include a *Confidential Fax Cover Page*, which directs the recipient to safeguard the contents of the document and makes certain the fax is only distributed to the intended recipient.

PHI should not be faxed unless at least one of the following exists: (i) an authorized staff member is on hand at the receiving site to promptly handle the materials, (ii) receiving fax machine is located in a secured area with limited access, or (iii) a password protected fax machine is used and restricts unauthorized release of the materials.

Please refer to the *Administrative Policy: Facsimile Transmission,* in order to ensure the general protection and confidentiality of PHI transmitted or received.

4. Safeguarding PHI Transmitted Via E-Mail.

An electronic mail system has been installed to facilitate internal and external business communications. This system and the computer equipment necessary to operate it are our property, and we retain the right to inspect the system and the manner in which it is being used.

We recognize that, although E-Mail permits the rapid communication of administrative and clinical data, there are enormous risks associated with this practice. Specifically, information can be inadvertently communicated to unintended third parties, where it can be improperly distributed to others. **Accordingly, we strictly prohibit the communication of PHI by E-Mail, except as provided below.**

All E-Mail communications transmitting PHI must contain the following disclaimer language:

> Confidentiality Notice: This e-mail is intended only for the use of the individual or entity named above and may contain information this is privilege and confidential. Unauthorized re-disclosure or a failure to maintain the confidentiality of the information contained herein could subject you to penalties under state and federal law. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, the reader is hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited. If you have received this communication in error, please notify us immediately by telephone.

In addition to the above disclaimer, all E-mail communications of PHI are strictly prohibited, except under the following conditions:

(a) The PHI transmitted by E-mail is the minimum necessary to accomplish the communication's intended purpose;

(b) The E-Mail communication is to an authorized recipient and is protected in such a way that, if improperly intercepted or re-transmitted, the information contained therein will not reveal the patient's identity;

(c) The E-Mail communication is encrypted and accomplished using secure communication links;

(d) The patient has signed an *E-Mail Consent* form, which sets out the risks of E-Mail communication and the patient's acceptance of such risks. The *E-Mail Consent* form shall be maintained in the patient's medical chart; and

(e) All E-Mails will be printed out and included in the patient's medical record.

Please refer to the *Administrative Policies: Electronic Mail and Voice Mail Policy,* in order to ensure the general protection and confidentiality of PHI transmitted or received.

5. Incidental Uses and Disclosures of PHI.

Incidental uses and disclosures of PHI that occur as a by-product of a use or disclosure otherwise permitted by the Privacy Rules are not a violation of our Compliance Plan or the Privacy Rules to the extent that we have applied reasonable safeguards and complied with our "minimum necessary" standards. (See Policy: *Minimum Necessary Requirements*). For example, it is not a violation if a healthcare practitioner, who is discussing PHI, is overheard by other patients or employees if he/she has taken appropriate precautions not to be overheard. However, it is a violation if a healthcare provider permits a Workforce member unimpeded access to a patient's medical record, where such access is not necessary for the employee to do his/her job.

6. Verification.

Prior to any disclosure of PHI to any individual, the authority of the individual to receive such information should be verified. Verification can include photo identification, signature comparisons, statements, legal documents, or other acceptable documents. Should a question or concern arise regarding the release of PHI to an individual or whether proper verification has been received, contact the Privacy Officer.

7. Removal of PHI Off Premises.

Other than appropriate and approved remote access to the EHR system, which must comply with the terms of this Compliance Plan, PHI shall not be physically removed from The Health Care Authority's premises unless absolutely necessary to provide treatment or to carry out one's job-related duties. When PHI is physically removed from The Health Care Authority's premises, it should be properly protected and secured at all times. Any PHI removed from The Health Care Authority's premises must be immediately returned once it is no longer needed off the premises.

- **Forms: Confidential Fax Cover Page**

  E-Mail Consent Form

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 235-5763

E-Mail Consent Form

Patient Name:	
Social Security Number:	Date of Birth:

Please read the following statements carefully:

1. **Risks of Using E-Mail:** Transmitting patient information by E-mail has many significant risks that you should consider before asking us to use E-mail as a means of communicating your personal health information. These risks include, but are not limited to, the following:

   a. E-mail can be circulated, forwarded and stored in numerous paper and/or electronic files without your knowledge;
   b. E-mail can be sent immediately worldwide and received by large numbers of unintended individuals;
   c. E-mail addresses can be misaddressed causing the information to be sent to the wrong individuals; or
   d. E-mail can be intercepted, changed and redistributed to others.

2. **Conditions for Use of E-Mail:** We will use reasonable means to protect the security and confidentiality of E-mail sent and received. However, because of the risks, some of which are outlined above, we cannot guarantee the security and confidentiality of E-mail communications, and will not be responsible for improper disclosures of your health information. Accordingly, you must consent to the use of E-mail for sending your personal health information. Consent to the use of E-mail includes your agreement with the following conditions:

   a. All E-mails concerning your diagnosis or treatment will be made a part of your medical record. Because they are a part of the medical record, other individuals authorized to access the medical record will have access to these E-mails;
   b. We may forward E-mails internally to our staff and agents as necessary for diagnosis, treatment, reimbursement, and other appropriate purposes. We will not, however, forward E-mails to independent third parties without your prior written consent, except as authorized by law;
   c. We cannot guarantee that any particular E-mail from you will be read and responded to within any particular time. Thus, you should not use E-mail for medical emergencies or other time sensitive matters;
   d. If your E-mail requires or invites a response from us, and you have not received a response from us within a reasonable period of time, it is your responsibility to follow-up to determine whether the intended recipient received the E-mail and when the recipient will respond;

e. You should not use E-mail for communication of sensitive medical information including, without limitation, sexually transmitted diseases, HIV/AIDS, mental health conditions, substance abuse or other developmental disabilities;
f. You are responsible for informing us of any type of information that you do not want sent by E-mail;
g. We shall not engage in unlawfully practicing medicine across state lines; and
h. We will not be responsible for the occurrence of any of the items set forth in Paragraph 1 above.

BY SIGNING THIS FORM, I HEREBY ACKNOWLEDGE THAT I HAVE READ AND FULLY UNDERSTAND THIS CONSENT TO USE AND/OR DISCLOSE MY HEALTH INFORMATION VIA E-MAIL. I UNDERSTAND THE RISKS AND CONSENT TO THE CONDITIONS OUTLINED HEREIN AND ANY OTHER INSTRUCTIONS OR CONDITIONS NORTHEAST ALABAMA REGIONAL MEDICAL CENTER MAY IMPOSE CONCERNING THE USE OF E-MAIL COMMUNICATIONS.

_____ _____

Signature of Patient or Patient's Representative Date

_____

Printed Name of Patient's Representative (*if applicable*)

_____

Representative's Relationship to Patient (*if applicable)*

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

RECORDKEEPING AND RETENTION

Efforts to comply with HIPAA will be documented through our Privacy Officer, Security Officer, and our Workforce members. For example, where we, in our efforts to comply with HIPAA, request advice from an appropriate government agency (including the Office of Civil Rights), we shall document, in writing, the request and any written or oral response, the latter of which will be confirmed in writing with the government agency, if possible. **In order for us to rely on any advice from a government agency, written record(s) of the advice and written confirmation of the advice is extremely important.**

All HIPAA compliance documentation will be maintained in written or electronic form. This shall include, but not be limited to, all forms, privacy policies and procedures, as well as the following information:

- *Patient Requests for Accounting of Disclosures of PHI;*
- *Patient Requests for Amendments of PHI;*
- Complaints of possible privacy violations or violations of our privacy policies and procedures, and their disposition;
- Privacy training material;
- *Privacy Notice;*
- *Patient Request for Restrictions on Use and/or Disclosure of PHI;*
- Designated Record Sets subject to access by patients and the title of the person or office for receiving and processing requests for access by patients;
- Signed *Authorizations;*
- Any sanctions for non-compliance;
- Any use or disclosure of PHI for research without the patient's Authorization;
- *Privacy Notice Acknowledgements* or documentation of our efforts to obtain written acknowledgement; and
- The name of our Privacy Officer
-

This documentation will be retained for at least six (6) years from the date of its creation or the date when it last was in effect, whichever is later. If any action, activity or assessment is required to be taken and documented, such documentation shall be maintained (in written or electronic form) for six (6) years from the date of its creation or the date when it last was in effect, whichever is later. Additional documentation to be maintained includes:

(1) All records required by state or federal law (*e.g.*, clinical and medical records and claims documentation), and

(2) All records necessary to protect the integrity of our Compliance Plan and confirm the effectiveness of the Plan (*e.g.*, documentation that Workforce members are adequately trained; reports of possible violations, including the nature and results of any investigation conducted; modification of the Compliance Plan; and the results of our auditing and monitoring efforts).

Records that are no longer required and have satisfied the required periods of retention are to be destroyed in an appropriate manner in accordance with our standard organizational practice and policy. The

destruction of records is to be carried out only upon the authority of the Privacy Officer or Security Officer and a list of all destroyed records must be retained. Records relevant to any legal action are to be retained pursuant to instructions from the Privacy Officer.

All documentation shall be made available to those persons responsible for implementing the procedures to which the documentation pertains.

Documentation will be reviewed periodically, and updated as needed, in response to environmental or operational changes affecting the security of PHI.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

DESIGNATED RECORD SET

The Health Care Authority maintains a designated record set that is defined as a group of records generated, collected, or maintained by the hospital that are the medical and billing records used to make decisions about our patients. PHI contained in our designated record set is individually identifiable health information on our patients that can be accessed, amended, and inspected by and copied for our patients.

The designated record set includes the following:

- The health information contained in the legal paper-based medical record and computer-based health record used to make clinical decisions about the patient's care and treatment, e.g., medical reports, radiographic images, tracings, monitor strips, videotapes, photographs, scanned documents.
- The summary and detailed bills located in the paper-based and computer-based patient accounts folders.

Health information not included in the designated record set is as follows:

- Health information generated, collected or maintained for purposes that do not include decision making about the patient's care and treatment, i.e. surgery schedules, registers, indexes, peer review data, performance improvement data, and risk management data.
- Source data interpreted or summarized in the patient's medical record, i.e. pathology slides, diagnostic images, cardiac tracings, etc.
- Psychotherapy notes that may be maintained separate and apart from the regular medical record.
- Information compiled in reasonable anticipation of or for use in civil, criminal, or administrative actions or proceedings.
- Employer records.
- Education records.
- Business associate records that meet the definition of the designated record set but that merely duplicate information maintained by The Health Care Authority.
- Correspondence regarding the use/disclosure of PHI, not related to direct patient care.
- Coding attestation sheets, records from other agencies or healthcare facilities.

Exception: Access to or copies of source data not considered part of the designated record set will be provided to patients for emergent/urgent reasons whenever possible, as long as the access would not violate state or federal laws or regulations, and would not endanger the privacy, health, or safety of the patient or another patient.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

INTERNAL AND EXTERNAL COMPLAINT PROCESS FOR REPORTING AND INVESTIGATING PRIVACY RIGHTS VIOLATIONS

1. Workforce Members' Responsibility to Report Possible Privacy Violations.

It is the responsibility of all members of our Workforce to abide by the standards set forth in this Compliance Plan and the Privacy Rules and to support our privacy efforts. **All members of our Workforce are required to report their good faith belief of any violation of this Compliance Plan.**

Open discussions of ethical and legal issues without fear of retribution or retaliation is the cornerstone of our privacy efforts. We will ***not*** tolerate retaliation against a Workforce member who, in good faith, reports an ethical and/or legal concern. On the contrary, we will look favorably on Workforce members who report suspected violations and who are committed to privacy efforts and ethical behavior.

A Workforce member whose report of misconduct contains an admission of a personal violation, however, cannot be guaranteed protection against disciplinary action. In determining whether, and to what extent, to discipline a Workforce member who reports wrongdoing for which he or she is partly or fully responsible, we will consider as a favorable factor the fact that the member volunteered the information. A Workforce member may be subject to discipline if we determine that a report of wrongdoing was knowingly fabricated, in whole or in part.

To the extent possible under the circumstances and taking into account investigational requirements, we will provide anonymity to Workforce members who file a report of a possible violation. There may, however, come a point when the identity of the member becomes obvious or may have to be revealed as part of the investigation or to adequately address the wrongdoing.

2. Methods to Report Possible Violations.

A Workforce member can report his/her good faith belief of violations of this Compliance Plan, Privacy Rules, or ethical standards:

(a) Orally to his or to her supervisor or to the Privacy Officer;

(b) In writing by using the *Privacy Problem/Concern Report* form, and providing the report to the Privacy Officer at Northeast Regional Medical Center. By calling the Privacy Officer directly at (256) 235-5373; or

(c) By mailing his or her written concern(s) to the Privacy Officer at the following address: PO Box 2208, Anniston, AL 36202.

All reports of possible misconduct shall be forwarded immediately to the Privacy Officer.

3. Complaints of Privacy Violations By Patients.

Patients have the right to file a complaint that we have violated the Privacy Rules, and/or our own privacy policies and procedures. The patient may file a complaint either directly with us (an "internal" complaint) or with the Secretary of HHS (an "external" complaint). Complaints filed by patients shall be documented

on the *Privacy Problem Concern Report for Patients Form*. Complaints filed by patients with the Secretary must be made in writing, name/identify us, describe the alleged acts or omissions, and must be filed within 180 days of the time the patient became aware of or should have been aware of the violation.

We will fully cooperate with investigations by the Secretary, his/her designee or the Office of Civil Rights, by permitting access, as appropriate and in accordance with applicable law, to information requested by any such investigator.

4. Response and Prevention.

The purpose of this section is to set forth the procedures that we will use to respond to reports or concerns by our Workforce members or other patients that an activity may be contrary to the standards and procedures of this Compliance Plan and/or the Privacy Rules.

(a) Receipt, Documentation and Investigative Oversight.

- All complaints or reports of privacy violations shall be immediately forwarded to the Privacy Officer. Upon receipt of a complaint or report of a possible privacy violation, the Privacy Officer shall complete the *Privacy Problem/Concern Report* form, if one is not already completed.

- The Privacy Officer, with the assistance of outside legal counsel and the Vice President of Human Resources, where appropriate, will be responsible for directing the investigation of the alleged violation. If outside legal counsel is involved, the investigation shall be conducted to maintain, to the extent possible, attorney-client and work product privilege over documents uncovered and reports prepared in the course of the investigation.

- As necessary, individual Workforce members may be asked to assist in the investigation and the Privacy Officer, the Vice President of Human Resources, and/or our outside legal counsel may request that third parties with appropriate expertise also provide assistance.

(b) Investigative Process.

- Upon learning of a possible privacy violation, the Privacy Officer, the Vice President of Human Resources, and/or our legal counsel, shall begin a formal investigation of the matter. The investigation shall be started as soon as possible.

- Generally, an investigation shall be conducted in accordance with the following procedures, unless the Privacy Officer, the Vice President of Human Resources, and/or our legal counsel decides that an alternative approach is in the furtherance of the standards and procedures set forth in this Compliance Plan.

  (i) Step One. If the Privacy Officer, the Vice President of Human Resources, or our legal counsel, believes the integrity of the investigation may be at stake because of the presence of a Workforce member allegedly involved in the misconduct, such an individual shall be temporarily removed from his/her current work activity until the investigation is concluded.

(ii) Step Two. The Privacy Officer, the Vice President of Human Resources, and/or our legal counsel, shall interview, as appropriate, the person(s) filing the report of wrongdoing, and other persons who may have knowledge of the alleged violation.

(iii) Step Three. In order to assess the complaint of conduct, the Privacy Officer, the Vice President of Human Resources, and/or our legal counsel, shall review applicable sections of this Compliance Plan, the Privacy Rules and relevant local, state and federal law.

(iv) Step Four. The Privacy Officer, the Vice President of Human Resources, and/or our legal counsel, shall review the information obtained under Steps Two and Three to determine whether or not the conduct in question occurred and, if such conduct did occur, whether it is permitted by this Compliance Plan, the Privacy Rules and applicable law.

(v) Step Five. If the Privacy Officer, the Vice President of Human Resources, and/or our legal counsel determines that there is not a violation of the standards and procedures set forth in this Compliance Plan, the Privacy Rules, and applicable law, or if the conduct which allegedly resulted in a violation did not occur, the investigation shall be closed. If, however, there is a probable violation, or if additional facts are necessary to make a proper determination about the validity or invalidity of the complaint of conduct, the investigation shall proceed to Step Six.

(vi) Step Six. As applicable, the Privacy Officer, the Vice President of Human Resources, and/or our legal counsel, or retained outside expert, shall identify and review in more detail the complaint of conduct. The purpose of such review shall be to identify the problem, including its scope, duration and frequency, and to gather information to address the problem and prevent its recurrence.

(vii) Step Seven. As necessary, the Privacy Officer, the Vice President of Human Resources, our legal counsel, or retained outside expert, shall interview any additional person(s) who may have information related to the complaint of conduct. The purpose of the interview(s) will be to verify information learned through Step Two and to gather additional information relevant to assess the complete situation, including, for example: (i) intent, of the persons involved, (ii) identity of other persons with information relevant to the conduct, (iii) mechanisms necessary to prevent recurrence of the complaint of conduct, and (iv) potential civil and/or criminal liability.

(c) Our Response.

In the event the investigation reveals what appears to be conduct that is a violation of the standards and procedures set forth in this Compliance Plan, the Privacy Rules and/or applicable law, we shall, as appropriate:

- Immediately stop the activities until such time as the offending practices are corrected;
- Correct the improper practice;
- Discipline the person(s) responsible for the offending practice(s), in accordance with potential disciplinary actions set forth in *Workforce Member Sanctions For Violations of the Compliance Plan and Progressive Sanctions Policy*;
- Institute training, education and other actions to avoid recurrence of the problem;
- If the violation results in a Breach of Unsecured PHI, follow the procedures outlined in the *HIPAA Breach Notification Policy*; and/or
- Initiate such other actions and steps deemed necessary and appropriate under the circumstances (*e.g.*, offer credit monitoring assistance to the patient when applicable).

(d) At the conclusion of the investigation, the Privacy Officer will be responsible for documenting the investigation's outcome, including any disciplinary and/or corrective action taken in the matter.

(e) In the event the investigation reveals that the conduct may have resulted in a violation of the Security Rules, the Privacy Officer will notify the Security Officer of such findings.

➢ **Form: Privacy Problem/Concern Report**

Privacy Problem/Concern Report for Patients

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
400 East 10TH ST. ANNISTON, ALABAMA 36207 (256) 741-6456

Privacy Problem/Concern Report

The Privacy Problem/Concern Report form is to be used by members of our Workforce to report their good faith belief of violations of the Privacy Rules, our HIPAA Privacy Compliance Plan, applicable law, as well as other ethical standards regarding the protection and privacy of protected health information. **We will take every measure to ensure the confidentiality of the information outlined below. However, there may be circumstances where disclosure of this information may become necessary.**

1. **Name** (*unless you wish to remain anonymous*): _____
2. **Date**: _____
3. **Time**: _____ AM or PM (*circle one*)
4. **Your position/job description**: _____
5. **Department**: _____
6. **Detailed description of the problem/concern/possible privacy violation** (*Include dates, location(s) of incident, names of persons involved, general description of the health information disclosed, and duration of event(s)*): _____
7. **How did you become aware of the problem?** _____
8. **Others with knowledge of the problem/concern/possible violation:** _____

This report was received by the Privacy Officer on _____.

_____ _____

Signature of Privacy Officer Date

Do Not Write Below This Line: For Administrative Use Only

The following information is to be completed after an investigation is conducted.

Date Investigation Initiated: _____

Privacy Problem/Concern/Violation Valid? Yes OR No *(circle one)*

General Description of Problem/Concern/Violation Found: _____

_____

_____

_____

_____

Action taken: _____

_____

_____

_____

_____

Date Investigation Closed: _____

Approved: _____ _____

Signature of Privacy Officer Date

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PROGRESSIVE SANCTIONS POLICY

The Health Care Authority committed to compliance with all applicable laws and regulations governing the confidentiality of PHI. The Health Care Authority has enacted policies to educate and instruct employees on The Health Care Authority's requirements for compliance with HIPAA. The Health Care Authority recognizes that this Progressive Sanctions Policy (the "Policy") will assist The Health Care Authority in efficiently and fairly addressing situations where an The Health Care Authority employee or staff member (an "Employee") has been found in violation of the Compliance Plan or any HIPAA regulation promulgated by a federal agency (a "Violation"). The Health Care Authority's Privacy Officer, in conjunction with The Health Care Authority human resources personnel, will enact the following procedures for sanctioning of such violations:

(a) In the event that an Employee has been found to have committed a Violation, the Privacy Officer will, after investigation of the matter, determine the severity of the Violation based upon the following factors:

(i) Whether the Violation was intentional;

(ii) Whether PHI was improperly accessed, reviewed, or disclosed;

(iii) To whom any improper disclosure was made;

(iv) Whether the Employee committed the Violation for personal gain of any person;

(v) Whether the Employee committed the Violation with malicious intent;

(vi) If the Employee has a history of noncompliance with any The Health Care Authority policies;

(vii) Whether the Violation resulted in a HIPAA Breach as defined by the Health Information Technology for Economic and Clinical Health ("HITECH") Act; and

(viii) Any other factors revealed in the investigation which the Privacy Officer believes are relevant to the administration of Employee sanctions.

(b) Pursuant to The Health Care Authority's HIPAA/Peer Review Designation Policy, the Privacy Officer will, after the investigation, make a recommendation to the appropriate The Health Care Authority management personnel regarding sanctions for the Employee. The Privacy Officer may, depending on the severity of the Violation, recommend the following when appropriate:

(i) Verbal warning;

(ii) Written reprimand;

(iii) Notation in Employee's employment record;

(iv) Mandatory attendance at continuing education programs regarding PHI privacy and security;

(v) Disciplinary probation or suspension;

(vi) Reduction in salary;

(vii) Demotion; or

(viii) Termination.

(c) The Privacy Officer may recommend any of the above sanctions to address the severity of any Violation. The Health Care Authority reserves the right to terminate an Employee without prior sanction if the Privacy Officer and other appropriate The Health Care Authority management personnel determine that the severity of the Violation warrants such termination.

(d) This Policy shall apply to all The Health Care Authority employees and staff, including Medical Staff, except to the extent that it conflicts with the Health Care Authority Medical Staff Bylaws.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PRIVACY EDUCATION AND TRAINING FOR WORKFORCE MEMBERS

Training and education will be provided for all of our Workforce members as appropriate for their duties in order to promote compliance with the Privacy Rules and the standards, policies and procedures set forth in this Compliance Plan. Attendance and participation at training programs is mandatory and a condition of continued employment and failure to comply with training requirements could result in disciplinary action, including possible termination.

In addition to our privacy training activities, Workforce members may also receive additional training and education through participation in local, state and/or national seminars or conferences, attendance at meetings or workshops at which privacy activity is discussed, review of training manuals, publications or videos which discuss privacy issues, or other activity related to the promotion of the ideas and concepts set forth in this Compliance Plan. *All Workforce members are required to notify and provide proof of attendance at any non-workplace privacy training and education event to the Privacy Officer.*

1. General Privacy Training and Education.

All Workforce members shall receive training on the following topics:

(a) The components of this Compliance Plan;

(b) The essential characteristics of an effective HIPAA Compliance Program, including the means to report possible violations;

(c) An overview of our privacy policies and procedures and uses of our privacy forms; and

(d) The Workforce member sanctions/ legal sanctions for violations of the Privacy Rules.

Thereafter, if we determine that certain Workforce members are routinely failing to comply with the federal Privacy Rules or our privacy policies and procedures, we will require said Workforce members to undergo additional training. This Compliance Plan will be made available to all hospital leaders/managers and Workforce members via the hospital information system's public (P) drive in the HIPAA folder. The hard copy manual will be located in the office of the Privacy Officer.

In addition to general privacy training and education, each Workforce member whose functions are affected by a change in our privacy policies and procedures will undergo appropriate training within a reasonable period of time after the change becomes effective.

2. New Employee Training and Education.

New employees are provided privacy training and education at the time of general orientation. As needed, the Privacy Officer shall provide new employees such general and specific privacy training as deemed appropriate. In concert with the school affiliates, students are provided privacy training and education.

3. Documentation of Training and Education.

All Workforce members who receive privacy training and education from us shall sign a *Workforce Member Privacy Training Acknowledgment* or a *Student Nondisclosure Agreement/Privacy Training Acknowledgement* form.

- **Forms: Workforce Member Privacy Training Acknowledgement**

  Student Nondisclosure Agreement/Privacy Training Acknowledgement

  HIPAA Training Handbook for Students/Workforce and Competency Exam

NORTHEAST ALABAMA REGIONAL MEDICAL CENTER
HIPAA PRIVACY COMPLIANCE PLAN
POLICY AND PROCEDURE

STUDENT NONDISCLOSURE AGREEMENT

Northeast Alabama Regional Medical Center has a legal and ethical responsibility to safeguard the privacy of all patients and protect the confidentiality of their heath information. During the course of my student affiliation at Northeast Alabama Regional Medical Center, I may come into contact with protected health information (PHI), even though I may not be directly involved in providing patient services.

I understand that such PHI must be maintained in the strictest confidence. As a condition of my affiliation, I hereby agree that, unless directed by my clinical supervisor, I will not at any time during or after my affiliation with Northeast Alabama Regional Medical Center disclose any PHI to any person whatsoever or permit any person whatsoever to examine or make copies of any patient reports or other documents prepared by me, coming into my possession, or under my control, or use patient information, other than as necessary in the course of my affiliation. I also understand that during my clinical affiliation I will access only the minimum necessary PHI in order to perform my duties/responsibilities.

I understand that my computer identification code (if issued) is my access to computer-generated PHI and is to be used only by me. I will not permit any other person to use my I.D. code nor will I use anyone else's I.D. code, including physician codes.

When discussing PHI with other health care practitioners in the course of my studies, I will use discretion to assure that others who are not involved in the patient's care cannot overhear such conversations.

I understand that violation of this agreement and failure to comply with the hospital's policy regarding patient confidentiality, security, and electronic access may result in corrective action, up to and including termination of my student affiliation.

_____ _____

Signature of Student Date

_____

School/Program Affiliate

.....

WORKFORCE MEMBER PRIVACY TRAINING ACKNOWLEDGEMENT

I acknowledge that I have received education and training regarding the Health Insurance Portability and Accountability Act (HIPAA) and Privacy Rules and their impact on Northeast Alabama Regional Medical Center (RMC). I understand that the Privacy Rules govern the manner in which protected health information (PHI) can be used and disclosed by RMC, and that I am required to follow the policies and procedures of RMC pertaining to such use and disclosure.

As necessary, I will seek advice from my clinical supervisor or the Privacy Officer concerning the appropriateness of my actions or those of others and any questions that I may have regarding privacy compliance activities. I will also report to my clinical supervisor, the Privacy Officer or the Privacy Compliance Line (256-741-6456) any suspected violations of the Privacy Rules or the Privacy Compliance Plan.

My signature acknowledges my understanding of the above information and my agreement to comply fully with the HIPAA compliance policies, procedures and plan.

_____ _____

Signature of Student Date

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

HIPAA SECURITY RULE COMPLIANCE

The Health Care Authority committed to complying with all local, state, and federal laws pertaining to the security of health information and to consistently operate with the highest standards of business and professional ethics. This policy is designed to adopt, implement, and enforce fundamental principles which are integral to complying with the Security Rules.

The Security Rules set out the following four (4) general requirements ("General Requirements") which The Health Care Authority shall satisfy in order to ensure the security of electronic protected health information ("EPHI") and its compliance with the Security Rules.

(1) Ensure the confidentiality, integrity, and availability of all EPHI The Health Care Authority creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rules.

(4) To ensure compliance with the Security Rules by its Workforce.

The Health Care Authority may use any security measures which allow it to reasonably and appropriately implement the Standards and Implementation Specifications set forth in the Security Rules. In selecting which security measures to use for compliance, The Health Care Authority shall take into account the following factors:

(1) The size, complexity, and capabilities of the organization;

(2) The organization's technical infrastructure, hardware, and software security capabilities;

(3) The costs of security measures; and

(4) The probability and criticality of potential risks to EPHI.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

SECURITY MANAGEMENT PROCESS

This policy is designed to establish and implement procedures to prevent, detect, contain and correct security violations. This Standard includes four (4) Implementation Specifications:

- Risk analysis (*required*)
- Risk management (*required*)
- Sanction policy (*required*)
- Information system activity review (*required*)

The following procedures shall be followed by The Health Care Authority for purposes of establishing a security management process which prevents, detects, contains, and corrects security violations:

(a) Risk Analysis. On a periodic basis, an accurate and thorough assessment will be conducted of the potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI, including, but not limited to, all relevant losses that could occur if security measures were not put in place.

(b) Risk Management. Security measures shall be implemented to sufficiently reduce the risks and vulnerabilities to EPHI to a reasonable and appropriate level so as to achieve the general requirements of the Security Rules and the Compliance Plan.

(c) Sanctions. Any violation of the Security Rules or the Compliance Plan will subject a Workforce member to disciplinary action, which may include the following (See Policies: *Workforce Member Sanctions for Violations of the Compliance Plan and Progressive Sanctions Policy*):

(i) An oral or written warning;

(ii) Notation in employment records, if applicable;

(iii) Mandatory attendance at continuing education programs regarding EPHI privacy and security;

(iv) Disciplinary probation;

(v) Suspension;

(vi) Reduction in salary;

(vii) Demotion; or

(viii) Termination.

(d) Information System Activity Review. A regular review will be conducted of the information system activity including, but not limited to, audit logs, access reports and

security incident tracking reports. The extent, frequency and nature of such reviews will occur from time to time as deemed necessary by the Security Officer.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

SECURITY OFFICER JOB DESCRIPTION

Job Class: **SECURITY OFFICER**

Appointment: The Security Officer is a high-level and trustworthy employee. Reasonable inquiries into the prior conduct and background of the appointed individual should be made and it should be determined that the appointed individual is qualified to serve as THE HEALTH CARE AUTHORITY's Security Officer.

Position Summary.

The Security Officer is responsible for the security of EPHI, and shall have authority to review all EPHI and other information relevant to security activities, including, but not limited to patient records, billing records, and records concerning arrangements with other parties, including employees, independent contractors, physicians, agents, suppliers, business associates, etc.

Security activities are a significant component of the Security Officer's job description, and therefore his/her performance will be judged, in part, on security compliance activity and the effectiveness of such activity.

Essential Job Functions:

- To assist with the development of the Compliance Plan, which sets forth legal and ethical standards, policies and procedures to be followed by members of our Workforce;
- To implement and enforce the standards, policies and procedures set forth in the Compliance Plan to ensure compliance with the Security Rules, state security laws, and applicable business and professional ethical policies;
- To keep apprised of changes to the Security Rules and state security and privacy laws. As part of this responsibility, the Security Officer will keep track of new regulatory developments, including new HIPAA bulletins and initiatives, many of which can be found at: http://www.hhs.gov/ocr/hipaa.
- To communicate the contents of this Compliance Plan, new legal developments, and new policies and procedures to members of our Workforce through training programs, memoranda, and other appropriate means;
- To establish and coordinate regular training programs designed to ensure compliance with the standards and procedures set forth in this Compliance Plan and to document the regularity and consistency of such training programs, as well as attendance;
- To assist with the development and communication of a system for Workforce members to seek guidance on security issues and to report suspected violations of the Security Rules or our Compliance Plan;

- To investigate alleged violations of the Compliance Plan and Security Rules, and work with appropriate parties to handle violations promptly, properly and consistently;

- To establish a record-keeping system designed to document the ongoing security of EPHI, including documentation of certification of compliance by all Workforce members;

- To receive and investigate all complaints relating to possible violations of the Security Rules and/or violations of our Compliance Plan, and record/document the result of any such complaint; and

- To report to our Governing Body on the operation and implementation of this Compliance Plan.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

WORKFORCE SECURITY

It is the policy of The Health Care Authority that access to EPHI is restricted on a "need-to-know" basis and technical mechanisms shall be implemented to protect the confidentiality of EPHI. This policy is designed to implement procedures to ensure that all members of The Health Care Authority's Workforce have access to EPHI as needed to perform their work responsibilities and to prevent those Workforce members who do not require access for their job duties from obtaining access to EPHI. This Standard includes three (3) Implementation Specifications:

- Authorization and/or supervision (*addressable*)
- Workforce clearance procedure (*addressable*)
- Termination procedures (*addressable*)

To ensure that Workforce members are given appropriate access to EPHI, the following measures shall be implemented:

1. **Authorization and/or Supervision.**

   (a) Workforce members may only have access to the minimum amount of EPHI necessary to perform their job duties or responsibilities. Reasonable efforts will be made to limit a Workforce member's use of and access to EPHI to the "minimum necessary" to accomplish the intended purpose of the Workforce member's job duties and responsibilities. (See Policy: *Minimum Necessary Requirements*).

   (b) All Workforce members who are not authorized to have access to EPHI will either obtain prior authorization from the Security Officer to access EPHI or must be supervised when working with EPHI or when working in an area where EPHI is accessible.

2. **Workforce Clearance.**

   (a) Individuals with unrestricted access to EPHI are limited to accessing participant information only to the extent necessary to carry out his/her duties.

   (b) Individuals with restricted access to EPHI who need to see any portion of restricted EPHI must request permission from the Security Officer before viewing such information.

3. **Workforce Termination.** The following steps must be taken once a Workforce member is terminated or no longer provides services for the organization.

   (a) The Human Resources manager must immediately inform the Security Officer of the departure of a Workforce member.

   (b) The Security Officer (or designee) must immediately perform the following actions in regard to the departing Workforce member:

      - Remove all access to all computers and computer systems;

- Remove all access to the mainframe applications;
- Remove all access to the network;
- Remove all access to network applications;
- Remove all access to routers and switches;
- Remove any entries in router access lists;
- Revoke all user-IDs associated with the individual;
- Remove access capabilities to outside Vendors;
- Retrieve all PC hardware and software;
- Retrieve all home based equipment, including terminals, modems, etc.;
- Retrieve any magnetic card key and other facility access items;
- Retrieve pagers or cell phones;
- Notify the organization's Administrator of any missing hardware or software;
- Archive all Workforce member data files on workstations and file servers;
- Remove security system password of PIN for access to facility;
- Archive all E-mail per The Health Care Authority's E-mail retention policies; and
- Report any violations to the appropriate personnel.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

INFORMATION ACCESS MANAGEMENT

THE HEALTH CARE AUTHORITY desires to limit access to EPHI to only those appropriate Workforce members. This policy is designed to implement procedures for authorizing access to EPHI which are consistent with requirements with the Privacy Rules and Security Rules. This Standard includes two (2) Implementation Specifications:

- Access authorization (*addressable*)
- Access establishment and modification (*addressable*)

1. Access Authorization.

(a) Workforce members must obtain prior authorization or the appropriate clearance level from the Security Officer before accessing any EPHI.

(b) Workforce members may only have access to the minimum amount of EPHI necessary to perform their job duties or responsibilities. (See Policy: *Minimum Necessary Requirements*). Reasonable efforts should be made to limit a Workforce member's use of and access to EPHI to the "minimum necessary" to accomplish the intended purpose of the Workforce member's job duties and responsibilities. (See also *Workforce Security Policy*).

2. Access Establishment and Modification. The following procedures shall be followed to ensure that Workforce members have appropriate access to EPHI:

(a) Use and Access of EPHI by Workforce Members. In order to determine the appropriate access to EPHI by each Workforce member, the Security Officer shall:

(i) Identify the persons or groups of persons who need access to EPHI to carry out their job function (role-based or user-based access);

(ii) Identify the type of EPHI to which each person or group needs access, as well as the conditions under which they need access; and

(iii) Make reasonable efforts to limit access to EPHI to only the information appropriate for the job requirements of each Workforce member.

(b) Access Limitations.

(i) Individuals with unrestricted access to EPHI are limited to accessing such information for patients for which they are responsible for the provision of health care. Individuals are not permitted to access EPHI for patients for which they are not responsible.

(ii) Individuals with restricted access to EPHI who need to see any portion of restricted EPHI must request permission from the Security Officer before viewing such information.

(c) Remote Access.

(i) The following security measures must be implemented for any remote access connection into a secure network containing EPHI:

a) Mechanisms to bypass authorized remote access mechanisms are strictly prohibited.

b) Remote access systems must employ a mechanism to "clear out" cache and other session information upon termination of session.

c) Remote access workstation must employ a virus detection and protection mechanism.

d) All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to 128-bit encryption.

(d) Wireless Access. Wireless access to networks containing EPHI is permitted so long as the following security measures have been implemented:

(i) Encryption must be enabled.

(ii) MAC-based (Media Access Control) or user ID/password authentication must be enabled.

(iii) All console and other management interfaces have been appropriately secured or disabled.

(iv) Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing EPHI-based systems and applications.

(v) All wireless LANs (Local Area Networks) do not utilize standard 2.4GHz, 5.0GHz or microwave radio frequencies. Wireless LANs and devices may utilize infrared frequencies and may not support the typical wireless LAN encryption and security mechanisms. For instance, the use of infrared ports on PDAs, laptops, and printers to transmit EPHI may not allow encryption of that data stream. This is considered to be a low risk concern because implementation of infrared is very short.

(e) Modification. Access to EPHI will be modified by the Security Officer when a Workforce member's job function or requirements change.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

SECURITY AWARENESS AND TRAINING

It is the policy of The Health Care Authority that training and education must be provided to all Workforce members as appropriate for their duties in order to promote compliance with the Security Rules and the standards, policies and procedures set forth in this Compliance Plan. Attendance and participation at training programs is mandatory and a condition of continued employment. Failure to comply with training requirements can result in disciplinary action, including possible termination. This policy is designed to ensure that Workforce members are properly made aware of and trained on the Security Rules, the Compliance Plan, and potential threats to EPHI.

In addition to our security training activities, Workforce members may also receive additional training and education through participation in local, state and/or national seminars or conferences, attendance at meetings or workshops at which security activity is discussed, review of training manuals, publications or videos which discuss security issues, or other activity related to the promotion of the ideas and concepts set forth in this Compliance Plan. *All Workforce members are required to notify and provide proof of attendance at any non-workplace security training and education event to the Security Officer.*

This Standard includes four (4) Implementation Specifications:

- Security reminders (*addressable*)
- Protection from malicious code and software (*addressable*)
- Log-in monitoring (*addressable*)
- Password management (*addressable*)

The following measures shall be implemented to provide security awareness and training.

(1) General Security Training and Education. All Workforce members shall receive training on the following topics:

- The components of this Compliance Plan;
- The essential characteristics of an effective HIPAA Compliance Program, including the means to report possible violations;
- An overview of our security policies and procedures and uses of our security forms; and
- The Workforce member sanctions/ legal sanctions for violations of the Security Rules.

Thereafter, if we determine that certain Workforce members are routinely failing to comply with the Security Rules or our security policies and procedures, we will require said Workforce members to undergo additional training.

In addition to general security training and education, each Workforce member whose functions are affected by a change in our security policies and procedures will undergo

appropriate training within a reasonable period of time after the change becomes effective.

(2) New Employee Training and Education. New employees are provided security training and education at the time of general orientation. As needed, the Security Officer shall provide new employees such general and specific security training as deemed appropriate. In concert with the school affiliates, students are provided security training and education.

(3) Security Reminders. Training will be ongoing and will respond and evolve according to environmental and operational changes affecting the security of EPHI. Warnings will be issued to Workforce members as a reminder of the Security Rules and as a notification of potential threats or other Security incidents

(4) Protection from Malicious Code and Software. The Security Officer must notify Workforce members of new and potential threats from malicious code such as viruses, spyware, worms, denial of service attacks, or any other computer program or code designed to interfere with the normal operation of a system or its contents. The Security Officer must also notify Workforce members of the procedures for protecting systems from the malicious software, including security patches and virus protection mechanisms.

(5) Log-in Monitoring. The Security Officer is responsible for monitoring and reporting log-in attempts and reporting and documenting any discrepancies. All Workforce members must immediately report to the Security Officer any failed log-in attempts or error messages received by the Workforce members while attempting to log-in.

(6) Password Management. The Security Officer is responsible for the password management process. All Workforce members that access, receive, transmit, or otherwise use EPHI or setup, manage, or maintain systems and workstations that access, receive, transmit, or store EPHI are required to protect passwords and log-in identifications.

(7) Documentation of Training and Education. All security training efforts shall be documented and retained by the Security Officer in accordance with the *Recordkeeping and Retention Policy*.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

SECURITY INCIDENT PROCEDURES

This policy covers "security incidents" which are defined by the Security Rules to mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of EPHI or interference with system operations in an information system. This policy is designed to establish procedures to identify and address suspected or known security incidents involving EPHI. This Standard includes one (1) Implementation Specification:

- Response and reporting (*required*)

To ensure that security incidents are properly identified and addressed, the following measures shall be implemented:

1. **General Requirements.** For purposes of identifying and addressing suspected or known security incidents, THE HEALTH CARE AUTHORITY will develop and put into practice procedures to:

(a) Identify and report suspected or known security incidents;

(b) Mitigate, to the extent practicable, harmful effects of security incidents that are known; and

(c) Document security incidents and their outcomes.

2. **Oversight.** The Security Officer, in coordination with the Information Technology ("IT") administrator (where applicable), will be responsible for monitoring all electronic information systems for reported or known security incidents. In addition, the Security Officer shall document security incidents and their outcomes in accordance with the requirements and procedures set forth in this policy.

3. **Reporting Requirements.**

(a) It is the responsibility of all Workforce members to abide by the standards set forth in the Security Rules and to support the security efforts. All Workforce members are required to report their good faith belief of any security incidents.

(i) Open discussions of ethical and legal issues without fear of retribution or retaliation is the cornerstone of our compliance efforts. We will ***not*** tolerate retaliation against a Workforce member who, in good faith, reports an ethical and/or legal concern. On the contrary, we will look favorably on Workforce members who report suspected violations and who are committed to compliance efforts and ethical behavior.

(ii) A Workforce member whose report of misconduct contains an admission of a personal violation, however, cannot be guaranteed protection against disciplinary action. In determining whether, and to what extent, to discipline a Workforce member who reports wrongdoing for which he or she is partly or fully responsible, we will consider as a favorable factor the fact that the member volunteered the information. A Workforce

member may be subject to discipline if we determine that a report of wrongdoing was knowingly fabricated, in whole or in part.

(iii) To the extent possible under the circumstances and taking into account investigational requirements, we will provide anonymity to Workforce members who file a report of a possible violation. There may, however, come a point when the identity of the member becomes obvious or may have to be revealed as part of the investigation or to adequately address the wrongdoing.

(b) A Workforce member can report suspected or known security incidents:

(i) Orally to his/her supervisor or to the Security Officer;

(ii) In writing to the Security Officer;

(iii) By calling the Security Officer directly at (256) 235-5862; or

(iv) By mailing his or her written concerns to the Security Officer at the following address: Post Office Box 2208, Anniston, Alabama 36202.

All reports of possible security incidents shall be forwarded immediately to the Security Officer. Upon receipt of a report of a suspected or known security incident, the Security Officer shall document the security incident.

4. Complaints of Security Violations By Patients.

Patients have the right to file a complaint that we have violated the Security Rules and/or our own security policies and procedures. The patient may file a complaint either directly with us (an "internal" complaint) or with the Secretary of HHS (an "external" complaint). Complaints filed by patients shall be documented in writing. Complaints filed by patients with the Secretary must be made in writing, name/identify us, describe the alleged acts or omissions, and must be filed within 180 days of the time the patient became aware of or should have been aware of the violation.

We will fully cooperate with investigations by the Secretary, his/her designee or the Office of Civil Rights, by permitting access, as appropriate and in accordance with applicable law, to information requested by any such investigator.

5. Response and Prevention.

The purpose of this section is to set forth the procedures that we will use to respond to reports or concerns by our Workforce members or other patients that an activity may be contrary to the standards and procedures of this Compliance Plan and/or the Security Rules.

(a) Receipt, Documentation and Investigative Oversight.

- All complaints or reports of security violations shall be immediately forwarded to the Security Officer. Upon receipt of a complaint or report of a possible security violation, the Security Officer shall document the complaint or report.

- The Security Officer, with the assistance of outside legal counsel and the Vice President of Human Resources, where appropriate, will be responsible for directing the investigation of the alleged violation. If outside legal counsel is involved, the investigation shall be conducted to maintain, to the extent possible, attorney-client and work product privilege over documents uncovered and reports prepared in the course of the investigation.

- As necessary, individual Workforce members may be asked to assist in the investigation and the Security Officer, the Vice President of Human Resources, and/or our outside legal counsel may request that third parties with appropriate expertise also provide assistance.

6. Investigation and Response.

(a) An investigation shall begin as soon as possible after the Security Officer learns of a security incident. Generally, an investigation shall be conducted in accordance with the following procedures, unless the Security Officer decides that an alternative approach is in the furtherance of the standards set forth in the Compliance Plan and Security Rules:

(i) Step One. If the Security Officer, the Vice President of Human Resources, or our legal counsel believes the integrity of the investigation may be at stake because of the presence of a Workforce member allegedly involved in the security incident, such individual shall be temporarily removed from his/her current work activity until the investigation is concluded.

(ii) Step Two. The Security Officer, the Vice President of Human Resources, and/or our legal counsel shall interview, as appropriate, the person(s) filing the security incident report and other persons who may have knowledge of the incident. In addition, the Security Officer, in coordination with the IT administrator (where applicable), will examine and evaluate any affected components of the organization's information system.

(iii) Step Three. In order to assess the complained of activity, the Security Officer, the Vice President of Human Resources, and/or our legal counsel shall review applicable sections of the Compliance Plan, Security Rules, and relevant local, state, and federal law (where applicable).

(iv) Step Four. The Security Officer, the Vice President of Human Resources, and/or our legal counsel shall review the information obtained under Steps Two and Three to determine whether or not the conduct in question occurred and, if such conduct did occur, whether it is permissible under the Compliance Plan, Security Rules, and/or other applicable law.

(v) Step Five. If the Security Officer, the Vice President of Human Resources, and/or our legal counsel determines that there is not a violation of the standards and procedures set forth in the Compliance Plan, Security Rules, and/or applicable law, or if the conduct which allegedly resulted in a security incident did not occur, the investigation shall be closed. If, however, there is a probable security incident, or if additional facts are necessary to make a proper determination about the validity or invalidity of the complained of conduct, the investigation shall proceed to Step Six.

(vi) Step Six. As applicable, the Security Officer, the Vice President of Human Resources, and/or our legal counsel, or retained outside expert (where applicable), shall identify and review in more detail the complained of security incident. The purpose of such review shall be to identify the problem, including its scope, duration and frequency, and to gather information to address the problem and prevent its reoccurrence.

(vii) Step Seven. As necessary, the Security Officer, the Vice President of Human Resources, and/or our legal counsel, or retained outside expert (where applicable), shall interview any additional person(s) who may have information related to the complained of security incident. The purpose of the interview(s) will be to verify information learned through Step Two and to gather additional information relevant to assess the complete situation, including, for example: (i) intent of the persons involved, (ii) identify of other persons with information relevant to the complaint of conduct, (iii) mechanisms necessary to prevent reoccurrence of the complaint or conduct, and (iv) potential civil and/or criminal liability. In addition, the Security Officer or expert will examine and evaluate any affected components of the organization's information system.

(b) Where an investigation reveals a security incident, we shall, as appropriate:

(viii) Immediately take steps to mitigate, to the extent practicable, harmful effects of the security incident(s) that are known;

(ix) Correct the activity leading up to the security incident, as well as any problems identified in The Health Care Authority's information system;

(x) Discipline the person(s) responsible for the security incident, in accordance with potential disciplinary actions set forth in *Workforce Member Sanctions for Violations of the Compliance Plan and Progressive Sanctions Policy*;

(xi) Institute training, education, and other actions to avoid recurrence of the problem;

(xii) If the security incident results in a Breach of Unsecured PHI, follow the procedure outlined in the *HIPAA Breach Notification Policy*; and/or

(xiii) Initiate such other actions and steps deemed necessary and appropriate under the circumstances.

(c) At the conclusion of the investigation, the Security Officer will be responsible for documenting the investigation's outcome, including any disciplinary and/or corrective action taken in the matter.

(d) In the event the investigation reveals that a security incident has or may have resulted in a violation of the Privacy Rules, the Security Officer will notify the Privacy Officer of such findings.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

CONTINGENCY PLAN

The Health Care Authority desires to continue to protect EPHI during certain disaster or emergency events. This policy is designed to establish and implement, as needed, procedures for protecting the availability, integrity, and security of EPHI in the event of a security incident (*e.g.,* an emergency, disaster, or other negative occurrence, including, but not limited to, fire, floods, vandalism, terrorism, system failure, or natural disasters). This Standard includes five (5) Implementation Specifications:

- Data backup plan (*required*)
- Disaster recovery plan (*required*)
- Emergency mode operation plan (*required*)
- Testing and revision procedures (*addressable*)
- Applications and data criticality analysis (*addressable*)

To ensure that proper procedures are in place for responding to an emergency, security incident, or other occurrence, the following measures shall be implemented:

1. **Data Backup Plan.**

(a) For purposes of ensuring the availability of EPHI in the event of an emergency, disaster, or other negative occurrence, procedures will be established and implemented to create and maintain retrievable, exact copies of EPHI (hereinafter referred to as the "Data Backup Plan").

(b) The Data Backup Plan shall cover all original PHI stored electronically (that is, PHI which is not a copy of information stored in the paper medical record) and which has been identified as requiring backup, as part of the risk analysis and risk management assessments. Information requiring backup shall include, but not be limited to: files, records, images, voice or video files, and E-mail which contains EPHI.

(c) All media and equipment used for backing up EPHI must be stored in a physically secure location which is separate and apart from all original EPHI software and data being backed up. If an off-site storage facility or vendor is used for backup services, a BA Agreement must be in place with the entity/individual to ensure that the EPHI is protected, handled and stored in an appropriate and secure manner. (See Policy: *Business Associate Agreements*).

(d) As appropriate, all data backup procedures and mechanisms will be tested to ensure that exact copies of EPHI can be retrieved and made available in an efficient manner.

(e) The Security Officer will be responsible for overseeing and implementing the organization's Data Recovery Plan and for ensuring that the organization performs routine, retrievable backups of EPHI, as appropriate.

2. **Disaster Recovery Plan.**

(a) For purposes of ensuring the availability and integrity of EPHI in the event of an emergency, disaster, or other negative occurrence, procedures must be established and implemented to restore any loss of data resulting from such events (hereinafter referred to as the "Disaster Recovery Plan").

(b) The Disaster Recovery Plan will include, but not be limited to:

(i) A Data Backup Plan;

(ii) Procedures to restore EPHI from data backups in the event of a disaster or negative occurrence resulting in a data loss;

(iii) Procedures, where appropriate, to periodically test the operation and recovery functionality of the Disaster Recovery Plan;

(iv) Procedures, where appropriate, to periodically perform an application and data criticality analysis; and

(v) Procedures to train the appropriate personnel to implement the Disaster Recovery Plan.

(c) The Security Officer will be responsible for overseeing and implementing the Disaster Recovery Plan, as well as ensuring that the plan is properly documented and easily accessible to Workforce members in the event of a disaster or negative occurrence resulting in a data loss.

3. **Emergency Mode Operation Plan.**

(a) For purposes of ensuring the availability of EPHI in the event of an emergency, procedures must be established and implemented to enable continuation of critical business processes for protection of the security of EPHI during and immediately after a crisis situation (hereinafter referred to as an "Emergency Mode Operation Plan").

(b) With the assistance of the Security Officer, an Emergency Mode Operation Plan will be developed, which identifies critical business processes, applications, data and information which will allow the organization to function and operate in the event of an emergency.

(c) The Security Officer will be responsible for overseeing and implementing the Emergency Mode Operation Plan.

4. **Testing and Revision Procedures.** As appropriate and necessary, procedures will be implemented for periodic testing and revision of Data Backup, Disaster Recovery, and Emergency Mode Operation Plans.

5. **Applications and Data Criticality Analysis.** As appropriate and necessary, procedures will be implemented to assess the scope and make-up of EPHI and data applications to determine what should be considered "critical" when developing Data Backup and Disaster Recovery Plans.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

EVALUATION

It is the policy of the Health Care Authority that periodic evaluations must be conducted of information systems, security practices, and security policies to ensure that practices and procedures are compliant with the Security Rules and other applicable local, state, and federal laws affecting the security of EPHI. This policy is designed to establish procedures to conduct periodic technical and non-technical evaluations of security policies based initially on Security Rule Standards and then in response to environmental or operational changes affecting EPHI to ensure that the policies continue to comply with the Security Rules and other applicable laws. This Standard is *required.*

To carry out these evaluations, the following measures shall be implemented:

1. **Security Evaluations.** Security evaluations must be conducted annually, at a minimum, or whenever environmental or operational changes affect the security of EPHI. The following events will trigger a review of the security policies and practices:

   (a) Significant modifications and/or updates to the Security Rules or security components of the Privacy Rules;

   (b) New local, state, or federal laws and regulations which impact the Security Rules and/or the security of EPHI;

   (c) Changes to environmental, operational, or business processes which affect security practices; and/or

   (d) A serious security violation or security incident which has been investigated and determined valid by the organization.

2. **Security Officer.** The Security Officer will be responsible for overseeing, conducting, and documenting security evaluations. Where appropriate, the Security Officer may appoint an individual and/or a Security Committee to assist him/her in conducting such evaluations.

3. **Compliance Tools.** The Security Officer will develop security compliance guidelines, models, and/or tools for assessing and documenting compliance with the security policies and Security Rules. Where appropriate, such materials may be developed in coordination with an outside vendor or professional association. In the event an external vendor is selected and he/she/it has access to EPHI maintained by or on behalf of the organization, the vendor will be asked to enter into a BA Agreement with The Health Care Authority. (See Policy: *Business Associate Agreements*).

4. **Modifications.** The following steps will be taken where a security evaluation finds changes are needed to the security policy:

   (a) The Security Officer will review the security evaluation's findings and assess the potential effect on the Compliance Plan and security practices;

   (b) Following an assessment, the Security Officer and The Health Care Authority's Administrator will develop and make any necessary revisions and modifications to the security policies;

(c) All security evaluation findings and necessary changes to the security policies will be documented and kept on file; and

(d) All Workforce members directly affected by changes to the security policies will be notified of such changes and will be provided training and education, as appropriate.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

FACILITY ACCESS CONTROLS

As appropriate, The Health Care Authority shall implement and document procedures for safeguarding and limiting access to its information systems and EPHI. This policy is designed to establish and implement procedures to limit physical access to The Heath Care Authority's electronic information systems and the areas or locations in which they are housed, while ensuring that properly authorized access is allowed. This Standard includes four (4) Implementation Specifications:

- Contingency operations (*addressable*)
- Facility security plan (*addressable*)
- Access control and validation procedures (*addressable*)
- Maintenance records (*addressable*)

1. **Contingency Operations.**

   (a) As appropriate, we will establish (and implement as needed) procedures that allow access in support of restoration of lost data under the Disaster Recovery Plan and Emergency Mode Operations Plan in the event of an emergency.

2. **Facility Security Plan.**

   (a) As appropriate, we will implement procedures to safeguard its facility and the equipment therein from unauthorized physical access, tampering, and theft (hereinafter referred to as the "Facility Security Plan").

3. **Access Control and Validation Procedures.**

   (a) As appropriate, we will implement procedures to control and validate a person's access to The Health Care Authority's information systems and EPHI based on their role or function, including visitor control, and control of access to software programs for testing and revision.

4. **Maintenance Records.**

   (a) As appropriate, we will implement procedures to document repairs and modifications to the physical components related to security (for example, hardware, walls, doors, and locks).

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

WORKSTATION USE

This policy requires all workstations to have physical safeguards in place which restrict access to authorized users who must utilize workstations and EPHI for purposes of completing assigned job functions. A "workstation" is defined by the Security Rules to mean an electronic computing device and the electronic media stored in its immediate environment, such as a desktop or laptop computer. This policy is designed to establish and implement policies and procedures of The Health Care Authority to ensure that all workstations which are used to send, receive, store, or access EPHI are used in a secure and appropriate manner. This Standard is *required.*

To ensure that workstations are used in a secure and appropriate manner, the following measures shall be implemented:

1. **Facility Workstations.** The Health Care Authority has installed workstations for use by its Workforce members to facilitate both internal and external business communications. These devices and the electronic media stored therein are property of The Health Care Authority, and as such, The Health Care Authority retains the right to inspect, as well as monitor their use. Workforce members shall have no expectation of privacy when utilizing workstations and The Health Care Authority's information system.

2. **User Responsibilities.** Workforce members have an obligation to use workstations in an appropriate and lawful manner. To help ensure proper access and use of workstations, the following procedures shall be followed:

   (a) Each Workforce member shall be provided a unique, individual password for utilizing workstations and The Health Care Authority's information system. Passwords are confidential and shall not be disclosed to others;

   (b) Workstations which are used to access and store EPHI shall be located in non-public access areas;

   (c) Workstation monitors shall be positioned in a manner so as to restrict viewing to authorized personnel only;

   (d) Active workstations shall not be left unattended for prolonged periods of time, except where specifically authorized by The Health Care Authority;

   (e) EPHI shall not be permanently stored on the local hard drive of any portable workstations (laptops, tablet PCs, and handheld PCs) which are not permanently assigned to a specific Workforce member. If a server is available, original EPHI will reside on the server and a copy will be available on workstation(s), where needed;

   (f) Where appropriate, backup of workstation data, programs and computer systems shall be performed on a regular basis to protect against business interruption;

   (g) At the close of business or at the end of a Workforce member's shift, all workstations shall be turned off or locked-out, as appropriate; and

(h) Transportable workstations (*e.g.*, laptops, notebooks, tablets, etc.) should not be unattended at any time and should never be checked with luggage in airline luggage systems.

3. Improper and Unauthorized Uses. Disciplinary action and sanctions may be initiated against a Workforce member where it is determined that the member has engaged in an improper or unauthorized use of a workstation. Improper and unauthorized uses include, but are not limited to, the following:

(a) Improper disclosure of user password(s);

(b) Access or attempted access to a workstation for which access authority has not been granted;

(c) Use of a workstation for personal gain;

(d) Use of a workstation and/or programs and software in connection to a workstation which can or will compromise the integrity and security of The Health Care Authority 's information system and/or is in violation of other The Health Care Authority policies. (For example, promulgating computer viruses, sending chain letters, or participating in communications which are perceived to be illegal, harassing, and/or offensive); or

(e) Downloading or installing software programs and data on a workstation which is unauthorized, inappropriate, and/or not organization approved.

4. Monitoring and Oversight. The Security Officer, in coordination with the Information Technology ("IT") administrator (where applicable), will be responsible for monitoring workstation access and use, as well as ensuring that Workforce members adhere to organization guidelines regarding permitted workstation practices. These monitoring and oversight activities will include, but not be limited to, the following:

(a) Maintaining accurate inventories of workstations, their location, and authorized users, including portable workstations such as laptops, tablet PCs, and handheld PCs;

(b) Conducting routine security assessments of workstation locations and configurations to check compliance with the Security Rules;

(c) Implementing and tracking password-protected programs and screen-savers for all workstations;

(d) Monitoring remote access to The Health Care Authority's information system, data, and workstations to verify access is being provided only to authorized users in accordance with the Security Rules;

(e) Conducting routine workstation security audits to assess compliance with the Security Rules; and

(f) Addressing improper and unauthorized uses of Workstations by workforce members, including instituting disciplinary action and sanctions where appropriate.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

WORKSTATION SECURITY

All workstations and servers that access EPHI systems must have physical safeguards in place that will restrict access to unauthorized users. This policy is designed to implement physical safeguards for all workstations that access EPHI and to restrict access to authorized users. This Standard is *required.*

To ensure that all workstations and servers are secure, the following measures will be implemented:

1. **Workstations.**

   (a) Workstations that are used to access EPHI must not be setup in a public access area.

   (b) Workstation monitors that are used to access EPHI should not face in a direction that makes visual access available to unauthorized users.

   (c) All workstations must use a password for access. Users should not share their password.

   (d) All applications workstations must have an automatic log-off capability after inactivity.

   (e) User accounts must be permanently disabled once the user no longer needs access to a workstation or network resources.

   (f) EPHI must not be stored on the local hard drive of a portable workstation that is not permanently assigned to a specific individual, which includes laptops, tablet PCs, and handheld PCs.

   (g) All users who remove workstations or media from The Health Care Authority's premises shall take reasonable precautions to physically secure the device(s) and media.

2. **Servers.**

   (a) All servers used to maintain EPHI must not be set up in a public access area, and must be located in a secured location.

   (b) All servers must use a password for access. Access to the server is limited to network administrators and other authorized personnel. Users should not share their password.

   (c) All unattended servers must be secured by a password or automatically lock-out user access after a certain number of minutes of inactivity. A valid password will be required to regain access to the servers.

   (d) All EPHI will be stored on the servers for security, availability, and data back-up purposes.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

DEVICE AND MEDIA CONTROLS

This policy covers the use of organization hard drives, storage systems, removable disks, floppy drives, CD-ROMs, PCMCIA cards, memory sticks, and all other forms of removable media and storage devices. This policy is designed to establish policies and procedures of The Health Care Authority which govern the receipt and removal of hardware and electronic media containing EPHI into, out of, and within a facility, and the movements of these items within the facility. This Standard includes four (4) Implementation Specifications:

- Disposal (*required*)
- Media re-use (*required*)
- Accountability (*addressable*)
- Data backup and storage (*addressable)*

To ensure that EPHI is handled, stored, and transmitted securely, the following measures shall be implemented:

1. **Disposal.**

   (a) Prior to destroying or disposing of any EPHI storage device or removable media, care must be taken to ensure that the device or media does not contain EPHI. If the device or media contains EPHI that is required or needed, a retrievable, exact copy of the EPHI must be made prior to disposal.

   (b) Prior to disposing of any EPHI storage device or removable media, a data destruction tool must be used to irretrievably destroy the data on the device or media. A typical reformat is not sufficient as it does not overwrite the data. The precise mechanism to destroy the EPHI will be dictated by the nature of the device or media.

2. **Media Re-use.**

   (a) Prior to making a storage device or removable media available for re-use, care must be taken to ensure that the device or media does not contain EPHI. If the device or media contains EPHI that is required or needed, a retrievable, exact copy of the EPHI must be made prior to re-use.

   (b) Prior to the re-use of any storage device or removable media, a data destruction tool must be used to irretrievably destroy the data on the device or media. A typical reformat is not sufficient as it does not overwrite the data. The precise mechanism to destroy the EPHI will be dictated by the nature of the device or media.

   (c) If re-using removable media for the purpose of system backups and disaster recovery and the removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.

3. **Accountability.** These Accountability requirements can be accomplished manually (for example, by keeping written logs of persons involved in the receipt and movement of EPHI storage devices or removable media) or through other means taking into account the size of The Health Care Authority.

(a) A procedure shall be implemented to track the movement of storage devices and removable media containing EPHI into and out of the organization.

(b) A procedure shall be implemented to document those persons involved in the movement of storage devices and removable media containing EPHI.

4. **Data Back-up and Storage.**

(a) All original PHI stored electronically (that is, PHI that is not a copy of information stored in the paper medical record), must be backed up on a regular basis. Backup mechanisms must be tested regularly to verify that EPHI can be efficiently retrieved.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

ACCESS CONTROL

Access to EPHI shall be restricted on a "need-to-know" basis and technical mechanisms must be implemented to protect the confidentiality of EPHI. This policy is designed to implement technical procedures of The Health Care Authority for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been given access rights. This Standard includes four (4) Implementation Specifications:

- Unique user identification (*required*)
- Emergency access procedure (*required*)
- Automatic logoff (*addressable*)
- Encryption and decryption (*addressable*)

To ensure that only authorized users or software programs are given access to EPHI, the following measures shall be implemented:

1. **Unique User Identification.**

   (a) All users shall be assigned a unique name and/or number which will allow for the identification and tracking of the user's access to EPHI.

   (b) Access to systems containing EPHI must be limited based on the user's identification, role, or context of a particular request.

   (c) Access control must be modified and/or terminated when an individual's role within the organization changes or when an individual is no longer a member of The Health Care Authority's Workforce.

2. **Emergency Access Procedure.**

   (a) Mechanisms must be developed to access all original EPHI (that is, PHI that is not a copy of information stored in the paper medical file) during emergencies, such as power outages.

3. **Automatic Logoff.**

   (a) All applications workstations must have an automatic log-off capability after inactivity.

4. **Encryption and Decryption.**

   (a) The use of mechanisms to encrypt and decrypt EPHI shall be assessed on a case-by-case basis in order to prevent unauthorized access. The need to incorporate encryption and decryption mechanisms will increase in the event the EPHI is sent to a third-party electronically.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

AUDIT CONTROLS

This policy is designed to implement hardware, software, and/or procedural mechanisms to record and examine activity in information systems that contain or use EPHI. This Standard is *required*.

To ensure that proper audit controls are in place, the following measures will be implemented:

(1) All network log-on successes and failures must be logged.

(2) Any electronic information systems or software containing EPHI that have the ability to monitor an individual's activity must be activated.

(3) All audit logs and records must be kept for a minimum of ninety (90) days.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

INTEGRITY (DATA AUTHENTICATION)

Appropriate data authentication mechanisms must be implemented to ensure that EPHI is not altered or destroyed in an unauthorized manner. Data authentication is a process to validate data integrity and verify that the same data sent is the same data that is received. Data authentication mechanisms can also be used to ensure the integrity of data storage and retrieval. This policy is designed to establish electronic mechanisms to protect EPHI from improper alteration or destruction. This Standard includes one (1) Implementation Specification:

- Mechanism to authenticate EPHI (*addressable*)

To ensure that proper integrity controls are in place, the following measures will be implemented:

(1) Security measures set forth in the Transmission Security Policy will be followed to ensure EPHI data integrity during transmission.

(2) Mechanisms such as error-correcting memory and magnetic disk storage will be used to authenticate data storage and retrieval.

(3) For all systems containing EPHI, a mechanism will be implemented to ensure that EPHI has not been altered or destroyed by a virus or other malicious code.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

PERSON OR ENTITY AUTHENTICATION

The Health Care Authority desires to ensure that persons accessing EPHI are properly authenticated. This policy is designed to implement procedures to verify that a person or entity seeking access to EPHI is the one claimed and has the appropriate authentication. This Standard is *required.*

To ensure that all individuals or entities which access EPHI have been properly authenticated, the following procedures shall be implemented:

(1) Individuals seeking access to any workstation or server that contains EPHI must satisfy a user authentication mechanism including, for example:

(a) A password system;

(b) A personal identification number;

(c) A biometric identification system; or

(d) A user identification card system or other "token" system that uses a physical device for identification.

(2) Individuals seeking access to any workstation or server must not misrepresent themselves by using another person's user ID, password, identification card or other item of identification.

(3) Individuals are not permitted to allow other persons or entities to use their unique user ID, password, identification card or other item of identification.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

TRANSMISSION SECURITY

Measures must be implemented to protect the security of electronic PHI when transmitted electronically from one point to another. This policy is designed to implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network. This Standard includes two (2) Implementation Specifications:

- Integrity controls (*addressable*)
- Encryption (*addressable*)

To ensure that proper transmission security controls are in place, the following measures will be implemented:

1. **Integrity Controls.**

   (a) Security measures will be followed to ensure that EPHI that is transmitted electronically is not improperly modified without detection.

   (b) All data networks containing EPHI will be secured behind a firewall to prevent any unauthorized access to EPHI.

   (c) Security measures set forth in the *Safeguarding Communication of Protected Health Information* will be followed when EPHI is transmitted by E-mail.

2. **Encryption.**

   (a) When EPHI is transmitted from one point to another, it must be protected in a manner commensurate with the associated risk of unauthorized access.

   (b) EPHI must not be transmitted over the Internet without the use of an approved encryption tool or method.

   (c) Only the minimum required amount of EPHI should be transmitted electronically.

   (d) Employees that send E-mail containing EPHI must ensure that the EPHI is being transmitted in the most secure manner possible and must comply with the security measures set forth in the *Safeguarding Communication of Protected Health Information Policy*.

   (e) The use of "point-by-point" connections (*e.g.*, dial-up lines) is deemed to be secure and no encryption is necessary.

   (f) Wireless access points within the Local Area Network (LAN) must use encryption security and other wireless security best practices.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

COMPLIANCE PLAN MODIFICATION

The Privacy Officer, Security Officer, designated Workforce members, and our legal counsel, if necessary, shall review the terms and requirements of this Compliance Plan, at a minimum, on an annual basis. Based on such review, the Privacy Officer and/or Security Officer shall recommend any necessary changes and/or revisions to this Compliance Plan for adoption by the Chief Executive Officer, as member of the Board of Directors.

In an emergency situation, the Chief Executive Officer, the Privacy Officer, or the Security Officer shall have the authority to unilaterally amend any portion of this Compliance Plan to comply with HIPAA, or any amendment thereto, and any local, state or federal law. If amendments to this Compliance Plan are made by the Privacy Officer or Security Officer, such amendments are subject to acceptance or rejection by the Chief Executive Officer, as member of the Board of Directors.

Each Workforce member whose functions are affected by a material change in our policies and procedures will undergo appropriate training within a reasonable period of time after the material change becomes effective.

NORTHEAST ALABAMA THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

EFFECT OF POLICIES AND PROCEDURES

The HIPAA Compliance Plan contains important information about The Health Care Authority's policies and procedures. However, it is not intended to be, and may not be construed to be, a contract, whether of employment or any other type, or a promise that The Health Care Authority will be bound by the policies and procedures contained herein. The Health Care Authority expressly reserves the right to revise, add to, delete from, or otherwise amend the policies and procedures contained herein. While The Health Care Authority generally will provide notice to employees of any such changes, a change without notice is nevertheless effective.

Under the policy of employment-at-will, employment relationships with The Health Care Authority are voluntary and can be terminated by either party, at any time, with or without notice or cause. No contract of employment on any other terms is valid unless it is styled a contract of employment, clearly sets forth the terms and conditions of employment, is signed by the President of The Health Care Authority, and has received such other approvals as may be necessary under the circumstances.

In the event of any conflict between any policy or procedure in this manual and any valid federal, state, or local law or regulation, such law or regulation shall govern.

THE HEALTH CARE AUTHORITY
HIPAA COMPLIANCE PLAN

QUESTIONS

Any questions regarding the HIPAA Program and this Compliance Plan shall be directed to either the Privacy Officer or the Security Officer.