

GEORGIA MOUNTAINS HEALTH SERVICES, INC.

**HIPAA
PRIVACY AND SECURITY
PROTECTION MANUAL**

**INCLUDING
BREACH NOTIFICATION RULE**

2018

HIPAA PRIVACY AND SECURITY PROTECTION MANUAL

TABLE OF CONTENTS

I.	GLOSSARY OF TERMS.....	1
II.	POLICIES AND PROCEDURES	
	A. PRIVACY	
	Policy 1 General Administrative Requirements	12
	Policy 2 Notice of Privacy Practice for PHI	17
	Policy 3 Uses and Disclosures for which Authorization is Required.....	21
	Policy 4 Uses and Disclosures Requiring an Opportunity for Individual to Agree or Object	24
	Policy 5 When Authorization and/or an Opportunity to Object is Not Required	27
	Policy 6 Other Requirements Relating to Uses/Disclosures of PHI.....	28
	Policy 7 Privacy of Health Information (Optional Policy)	32
	Policy 8 Right to Request Privacy Protection for PHI.....	36
	Policy 9 Access of Individuals to PHI	37
	Policy 10 Amendment of PHI	41
	Policy 11 Accounting of Disclosures of PHI	44
	Policy 12 Complaint and Compliance Procedures	47
	Policy 13 Business Associates	48
	Policy 13.1 Uses and Disclosures of PHI	49
	Policy 13.2 Covered Entity Uses & Disclosures of PHI	48
	B. SECURITY	
	Policy 14 Security Administrative Safeguards.....	56
	Policy 15 Security Physical Safeguards	60
	Policy 16 Security Technical Safeguards	62
	Policy 17 Security Policies/Procedures and Documentation.....	64
	Policy 17.3 Covered Entity General HIPAA Compliance	65
	Policy 17.4 Covered Entity Mobile Devices Policy	71
	Policy 17.5 Covered Entity Policy for Devices and Electronic Media.....	74
	Policy 17.6 Covered Entity Transaction Policy	76
	C. IDENTITY THEFT	
	Policy 18 Red Flag Rules	78
	Policy 19 Address Discrepancy Guidelines	82
	D. BREACH NOTIFICATION	
	Policy 20 Breach Notification	83
	Policy 21 Covered Entity Notification of Breach	87

III. FORMS

A. PRIVACY

Policy 1		
& 14.2	Confidentiality Agreement.....	91
	Confidentiality Agreement (Outside Vendors)	92
Policy 1.5		
& 14.10	Employee Training Form	93
Policy 2	Notice of Privacy Practices (Long Form)	94
	Notice of Privacy Practices (Short Form)	102
Policy 3.3	Authorization for Uses and Disclosures.....	104
Policy 7	Patient Consent Form (Optional)	104
Policy 8.1	Request for Limitations and Restrictions of Use	105
Policy 8.2	Confidential Communication Request	106
Policy 9.1	Request to Inspect and Copy	107
Policy 9.2/.3	Letter for Denial of Request for Access.....	108
Policy 10	Request for Amendment.....	110
Policy 11	Notice of Rights and Request for an Accounting.....	111
Policy 12.2	Complaint Form	112
Policy 13		
& 14.6	Safeguards Model Business Associate Agreement	113
	Business Associate Agreement	123
	Business Associate Subcontractor Agreement.....	125

B. SECURITY

Policy 14.1(4)	Information System Activity Review	132
Policy 14.2	Assigned Security Responsibility	133
Policy 14.3	Security Incident Policies and Procedures.....	134
Policy 14.3		
& 18.3	Security Incident Report	135
Policy 14.4	Contingency Plan.....	136
Policy 14.8	Workforce Security Policies and Procedures.....	137
Policy 14.8		
& 14.9	Levels of Access by Position Log.....	140
Policy 14.8		
& 16.1	Password Log.....	141
Policy 14.9	Information Access Management Form.....	142
Policy 14.9(2)	Access Establishment Policies and Procedures	143
Policy 14.10(2)	Procedures for Protection from Malicious Software	144
Policy 14.10(3)	Log-In Monitoring Procedures	145
Policy 14.10(4)	Password Management Procedures	146
Policy 14.11(2)	Application and Data Criticality Log	147
Policy 15.1	Workstation Use Policies and Procedures	148
Policy 15.3	Device and Media Controls Policies and Procedures	149
	Removable Media and Device Usage Agreement.....	153
Policy 15.3	IT Equipment Tracking Log.....	156
	Movement of IT Property Request Form.....	157

Policy 15.4	Facility Access Controls	158
Policy 15.4(4)	Facility Maintenance Log	159
Policy 16.2	Information Systems Audit.....	160
Policy 16.4(2)		
& 16.6	Encryption and Decryption/Transmission Security	161
Policy 16.5	Integrity of EPHI Policies and Procedures	162
 C. IDENTITY THEFT		
Policy 18.3	Examples of Identity Theft Red Flags.....	163
Policy 18.3	Patient Report of Identity Theft.....	166
Policy 18.5	Red Flag Alerts.....	167
Policy 18.5	John or Jane Doe file extraction	168
 D. BREACH NOTIFICATION		
Policy 20	Sample Letter of Breach Notification.....	169
	Identification of Breach and Activation of Notification.....	170

GLOSSARY OF TERMS

ACCESS- The ability to read, write, or communicate information.

ACCESS RIGHTS- Limited to that which is necessary to adequately perform one's specific job responsibilities. Access rights to protected health information are defined through the following:

- Employee job descriptions;
- Contract terms or job descriptions for independent contractors;
- Medical Staff By-Laws and Rules and Regulations for health care professionals;
or
- Policies and procedures.

ADMINISTRATIVE SAFEGUARDS- Administrative actions, policies and procedures to protect electronic protected health information.

AUDIT- To trace actions affecting system security back to the responsible party based on individual identity.

AUTHENTICATION- The corroboration that a person is the one claimed.

AUTHORIZATION- An authorization is a written document signed by a patient giving permission to the Health Center to disclose PHI for purposes other than treatment, payment and health care operation. For use and disclosure beyond treatment, payment, and operations, a specific authorization is required. An authorization must be obtained for any use or disclosure of psychotherapy notes except for use by the originator of the notes for treatment

AVAILABILITY- The accessibility of information upon demand by an authorized person.

BREACH- The unauthorized acquisition, access, use, or disclosure of protected health information which compromises the security or privacy of such information, not including unintentional good faith access by a workforce member, inadvertent disclosure to another similarly situated workforce member or business associate, or unauthorized disclosures to persons without the ability to retain the information.

BREACH NOTIFICATION RULES- Interim final breach notification regulations, issued in August 2009, implement section 13402 of the Health Information Technology for Economic and Clinical Health (HITECH) Act by requiring HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information. Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

BUSINESS ASSOCIATE- A business associate is any organization that performs services to or for the organization where the provision of the service involves the disclosure of PHI (any third party vendor to your organization with whom PHI is shared), including the following entities: (1) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of the Center. For all "business

associates" with which PHI is shared, a written agreement must be in place that provides for appropriate safeguarding of such information. This standard does not apply when information is being shared with a health care Center for the purpose of treatment. A business associate is any organization which performs a function or activity on behalf of, or provides a service to, the Center that involves the creation, use, or disclosure of electronic protected health information.

CONFIDENTIALITY- The property that information is neither made available nor disclosed to unauthorized persons.

CONSENT (OPTIONAL)- Relates to information used for treatment, payment, and healthcare related purposes. Practitioners may choose to get and retain evidence of a patient consent prior to the use or disclosure of health information (except in certain situations: emergency circumstances, identification of the body of a deceased person or the cause of death, public health needs, research, oversight of the health care system, judicial and administrative proceedings, limited law enforcement activities, and activities related to national defense and security). Please note, that use of a Consent form is not required under the Final Privacy Regulations.

COVERED ACCOUNT - An account that a creditor offers or maintains, that involves or is designed to permit multiple payments or transactions; and any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. Creditors that maintain covered accounts are subject to the Red Flag rules.

COVERED ENTITY- A health plan or a health care center that transmits any health information in electronic form in connection with a standard transaction.

CREDITOR – Any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Accepting credit cards as a method of payment does not by itself make an entity a creditor. If a health care provider extends credit to a consumer by establishing an account that permits multiple payments, that provider is a *creditor* offering a *covered account* and is subject to the Red Flag rules.

DESIGNATED RECORD SET- Includes the medical records and billing records.

DIRECT TREATMENT RELATIONSHIP- A treatment relationship between a patient and a health care Center that is not an indirect treatment relationship. The health care practice deals directly with the patient.

DISCLOSURE- Release, transfer, provision of access to, or divulging in any other manner of information outside the organization holding the information.

EMPLOYEES- As used in this manual, refers to all people who work in the Center (this includes temporary help, employees, independent contractors who work in the Center).

ENCRYPTION- Transforming information into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

EPHI- Electronic protected health information.

FACILITY- The physical premises, including the interior and exterior of a building.

HHS- The Department of Health and Human Services.

HEALTH CARE- Care, services or supplies related to the health of an individual including, but not limited to, the following: preventive, diagnostic, therapeutic, rehabilitative, maintenance or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body and sale or dispensing of a drug, device, equipment or other item with a prescription.

HEALTH CARE OPERATIONS- Includes general administrative and business functions necessary for an organization to remain a viable business, such as business planning and development, due diligence, internal grievance resolution and customer service to provide data and statistical analysis.

HEALTH CARE PROVIDER- A center of medical services including: *physician office* (including clinics and centers, physician group practices, clinical laboratories, pharmacies, nursing homes, licensed/certified health care practitioners and suppliers of durable medical equipment); *facilities and practitioners*; (such as hospitals, skilled nursing facilities, home health agencies, comprehensive outpatient rehabilitation facilities) and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

HIPAA- Health Insurance Portability and Accountability Act of 1996 and its implementing administrative simplification regulations (45 CFR §§ 160-164) (“HIPAA”) as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act and its implementing regulations, as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (the “HITECH Act”).

HITECH ACT/HITECH REVISIONS- refers to the Health Information Technology for Economic and Clinical Health Act, which was enacted on February 17, 2009, as part of the American Recovery and Reinvestment Act of 2009 (ARRA). The HITECH Act established new information security breach notification requirements that apply to covered entities and business associates and set forth substantially revised regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

INDIRECT TREATMENT RELATIONSHIP- A relationship between a patient and a health care center in which the health care center delivers health care to the patient based on the orders of a physician with a direct treatment relationship with the patient. The health care center typically provides services or products to the patient and reports the diagnosis or results associated with the health care to the physician who provides direct treatment to the patient.

INFORMATION SYSTEM- An interconnected set of information resources under the same direct management control. A system normally includes hardware, information, data,

applications, communications, and people.

INTEGRITY- The property that information has been neither altered nor destroyed in an unauthorized manner.

LIMITED DATA SET- Protected health information as defined in 45 C.F.R. § 164.514(e) that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (i) names; (ii) postal address information, other than town or city, State, and zip code; (iii) telephone numbers; iv) fax numbers; (v) electronic mail addresses; (vi) Social Security numbers; (vii) medical record numbers; (viii) health plan beneficiary numbers; (ix) account numbers; (x) certificate/license numbers; (xi) vehicle identifiers and serial numbers, including license plate numbers; (xii) device identifiers and serial numbers; (xiii) web Universal Resource Locators (URLs); (xiv) Internet Protocol (IP) address numbers; (xv) biometric identifiers, including finger and voice prints; and (xvi) full face photographic images and any comparable images

MALICIOUS SOFTWARE- Software designed to damage or disrupt a information system or network (ex: a virus).

MARKETING- A communication about a product or service the purpose of which is to encourage recipients of the communication to purchase or use the product or service. Marketing encompasses all treatment and health care operations communications where the covered entity (or business associate or subcontractor) receives financial remuneration for making such communications from a third party whose product or service is being marketed and, thus, requires prior authorization from the individual. All subsidized treatment communications that promote a health-related product or service will be treated as marketing communications that require authorization. One exception is that the covered entity (or business associate) may receive remuneration for refill reminders and other communications about currently prescribed drugs or biologics, but only if any financial remuneration received in exchange for making the communication is reasonably related to the cost of making the communication. "Financial remuneration" includes those direct and indirect financial payment made in exchange for making communications about a product or service that encourages individuals to buy or use such product or service. For purposes of the definition of marketing, it does not include non-financial benefits (e.g., in-kind benefits), nor does it include any payment for treatment of an individual.

MINIMUM NECESSARY CONCEPT- This applies to the use of health information and requires that reasonable efforts be made to limit the information to the "minimum necessary" to accomplish the intended purpose (for example, a Center may not use the contents of an entire medical record, except when the entire medical record is reasonably necessary). As a practical matter, Centers must evaluate how they use information within their own organization. They will need to consider whom they grant access to, and whether that person really needs access to all the information they currently get.

NETWORK SAFEGUARDS- Precautionary measures implemented to make sure the network is secure.

NOTICE OR NOTICE OF PRIVACY PRACTICES- All Centers must provide a "notice of privacy practice" to each patient or legal representative. The notice must describe the patient's rights and the entity's legal responsibilities with respect to PHI. All Practices must make a good

faith effort to obtain an "acknowledgment" from the patient or legal representative, indicating that notice has been made available to them. All acknowledgements obtained by the Center must be retained.

OCR – The Office of Civil Rights.

PASSWORD- Confidential authentication information composed of a string of characters.

PAYMENT- Information may be disclosed to payers or individual's health plans that will be responsible for all or part of a patient's bill, including preauthorization for proposed services. However, pursuant to the HITECH Revisions, the Center may not disclose an individual's information to his or her group health plan if the patient requests that the information not be disclosed, and the protected health information relates solely to a health care item or service for which the Center has been paid in full out-of-pocket.

PHYSICAL SAFEGUARDS- Physical measures, policies, and procedures to protect electronic information systems and related buildings and equipment from natural environmental hazards and unauthorized intrusion.

PRIVACY OFFICER- The Center must designate a privacy officer who is responsible for the implementation of and ongoing adherence to privacy policies and procedures. Responsibilities of the privacy officer include, but are not limited to:

1. Provide developmental guidance and assistance in identifying, implementing, and maintaining Center information as well as privacy policies and procedures.
2. Work with the Center to establish organization-wide privacy policies that comply with the HIPAA regulations.
3. Perform initial and periodic privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with the Center's other compliance and operational assessment functions.
4. Work with legal counsel and management to ensure the Center has and maintains appropriate notice of privacy practices, confidentiality agreements, authorization forms, and other materials reflecting current organization and legal Center requirements.
5. Oversees, directs, delivers initial and subsequent privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.
6. Participates in the development, implementation, and ongoing compliance monitoring of all business associate agreements to ensure all privacy concerns, requirements, and responsibilities are addressed.
7. Establishes a mechanism to track access to PHI, within the Center and as required by law and to allow qualified individuals to review or receive a report of such activity.
8. Oversee patient rights to inspect, amend, and restrict access to PHI when appropriate.
9. Administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the Center's privacy policies and procedures in coordination and collaboration when necessary with legal counsel.

10. Ensure compliance with notice of privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce and for all business associates, in cooperation with administration and legal counsel when needed.
11. Initiate, facilitate and promote activities to foster information privacy awareness within the Center.
12. Work with all Center personnel involved with any aspect of release of PHI, to ensure full coordination and cooperation under the Center's policies and procedures in addition to legal responsibilities.
13. Cooperate with the OCR, and other legal entities, and organization officers in any compliance review or investigation.

PRIVACY RULE- Part of the Health Information Portability and Accountability Act of 1996 (HIPAA) and is designed to protect medical records and other protected health information. The Privacy Rule is codified at 45 C.F.R. Part 164, and includes any amendments thereto, including, but not limited to, those amendments set forth in the Health Information Technology for Economic and Clinical Health Act (the HITECH Act), which is part of the American Recovery and Reinvestment Act of 2009 (ARRA) enacted on February 17, 2009.

PROTECTED HEALTH INFORMATION (PHI)-Any information, whether oral or recorded in any form or medium that is created or received by a health care Center, health plan, employer, public health authority, life insurer, school or university, healthcare clearinghouse and relates to the past, present, or future payment for the provision of health care to a patient.

RED FLAG – A pattern, practice, or specific activity that could indicate identity theft.

SAFEGUARDS- Means of protection.

SECURITY OR SECURITY MEASURES- All of the administrative, physical, and technical safeguards in an information system with respect to electronic protected health information.

SECURITY RULE- The third and final phase of the Health Information Portability and Accountability Act (HIPAA), designed to protect electronic protected health information.

SECURITY INCIDENT- The attempted or successful unauthorized access, use, disclosure, modification, or destruction of electronic protected health information.

SYSTEM ARCHITECTURE- Computer structure arranged to protect the information database from external interference or tampering.

SECURITY TESTING- Evaluation of protection mechanisms to confirm that they work properly.

TECHNICAL SAFEGUARDS- The technology, policy and procedures that protect electronic protected health information and control access to it.

TREATMENT- Health care information may be shared among caregivers involved in the care and treatment of the patient. Confidential health care information may also be disclosed to

health care professionals and organizations outside the hospital that will be involved in the patient's care after they leave the hospital.

Unsecured PHI- PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through either (i) the use of encryption for electronic PHI or (ii) destruction rendering hard copy PHI unreadable and unable to be reconstructed.

USER- A person or entity with authorized access to the information system.

WORKSTATION- A computer that has electronic media stored on it.

GEORGIA MOUNTAINS HEALTH SERVICES, INC

HIPAA PRIVACY AND SECURITY

POLICIES AND PROCEDURES

Policy One: General Administrative Requirements

Policy 1.1 Personnel Designations

Georgia Mountains Health shall designate a privacy official who is responsible for the development and implementation of the policies and procedures of the Center.

Policy 1.2 Designation of Privacy Officer/ Privacy Officer Responsibilities

Georgia Mountains Health shall designate a privacy officer who is responsible for the implementation of and ongoing adherence to privacy policies and procedures. Responsibilities of the privacy officer include, but are not limited to:

1. Provide developmental guidance and assistance in identifying, implementing, and maintaining Center information as well as privacy policies and procedures.
2. Work with the Center to establish organization-wide privacy policies that comply with the HIPAA regulations.
3. Perform initial and periodic privacy risk assessments and conduct related ongoing compliance monitoring activities in coordination with the Center's other compliance and operational assessment functions.
4. Work with legal counsel and management to ensure the Center has and maintains appropriate notice of privacy practices, confidentiality agreements, authorization forms, and other materials reflecting current organization and legal practice requirements.
5. Oversees, directs, delivers initial and subsequent privacy training and orientation to all employees, volunteers, medical and professional staff, contractors, alliances, business associates, and other appropriate third parties.
6. Participates in the development, implementation, and ongoing compliance monitoring of all business associate agreements to ensure all privacy concerns, requirements, and responsibilities are addressed.
7. Establishes a mechanism to track access to PHI, within the Center and as required by law and to allow qualified individuals to review or receive a report of such activity.
8. Oversee patient rights to inspect, amend, and restrict access to PHI when appropriate.
9. Administer a process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the Center's privacy policies and procedures in coordination and collaboration when necessary with legal counsel.
10. Ensure compliance with notice of privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce and for all business associates, in cooperation with administration and legal counsel when needed.
11. Initiate, facilitate and promote activities to foster privacy awareness within the Center.

12. Work with all Center personnel involved with any aspect of release of PHI, to ensure full coordination and cooperation under the Center's policies and procedures in addition to legal responsibilities.
13. Cooperate with the Office of Civil Rights (OCR), and other legal entities, and organization officers in any compliance review or investigation.

Policy 1.3 Documenting Personnel Designations

The Center must document the personnel designations as required by the Documentation section below (Policy 1.16).

Policy 1.4 Training

The Center must train all members of its workforce on the privacy policies and procedures as necessary and appropriate for its employees to carry out their job functions. The Center must provide training as follows:

1. To each member of the workforce by no later than the compliance date for the Center;
2. Thereafter, to each new member of the workforce within a reasonable period of time after the person joins the Center's workforce; and
3. To each member of the Center's workforce whose functions are affected by a material change in the policies or procedures, within a reasonable period of time after the material change becomes effective.

Policy 1.5 Documentation

The Center must document that the training has been provided and follow the Documentation Maintenance policy below (Policy 1.16).

Policy 1.6 Safeguards

The Center must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and reasonably safeguard PHI from any intentional or unintentional use or disclosure, or violation of the requirements of the privacy regulation.

Policy 1.7 Complaints to the Center

The Center must provide a process for individuals to make complaints concerning its policies and procedures or its compliance with its policies and procedures or the requirements of the privacy regulation. The Center must document all complaints received, and the disposition of such complaints, if any.

Policy 1.8 Sanctions

The Center must have and apply appropriate sanctions against its employees who fail to comply with the Center's privacy policies and procedures or the regulations. The Center must document the sanctions that are applied, if any. Sanctions are not to be applied in certain situations, such as disclosures by whistleblowers, disclosures by workforce member crime victims, or as set forth in Policy 1.10 below.

Policy 1.9 Mitigation

The Center must mitigate, to the extent practicable, any harmful effect that is known to the Center of a use or disclosure of PHI in violation of its policies and procedures or the requirements of Policy One and by the Center or by its business associate.

All reports of actual or suspected privacy or security violations will be handled confidentially and persons reporting such violations will not face retaliation unless they have been directly involved in the deliberate breach of privacy or security practices.

In the event an actual or suspected privacy or security violation occurs, all access by person or persons committing or suspected of committing the violation(s) will be immediately suspended.

The Privacy or Security Officer will confer with the Chief Executive Officer, and contact legal counsel if necessary, to determine if any law enforcement and/or professional disciplinary authorities should be notified.

The Center will take appropriate disciplinary action as required.

The Center Privacy Officer will contact the actual or alleged recipient of wrongfully disclosed protected health information, will inform the recipient that he/she received the information in error, and will attempt to retrieve all records containing such information prior to any subsequent use or disclosure of the information by the recipient.

The Center will review all privacy and security policies and procedures and revise as appropriate to attempt to prevent a recurrence of any actual violation.

The Center will contact legal counsel to determine if the subject(s) whose protected health information has been violated will be contacted and told what action is being taken to correct the situation and prevent its recurrence.

A summary report of privacy and security activities, including violations, will be reported through the Corporate Compliance Committee to the Board of Directors.

If the violation occurs with regard to unsecured protected health information as defined by the Breach Notification Rules, the Center will follow its Breach Notification Policy.

Policy 1.10 Refraining from Intimidating or Retaliatory Acts

The Center may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by this subpart, including the filing of a complaint under this section;
2. Any individual or other person for:
 - a) Filing a complaint with the OCR;
 - b) Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI; or
 - c) Opposing any act or practice made unlawful by this subpart, provided the individual or person has a good faith belief that the Practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of this subpart.

Policy 1.11 Waiver of Rights

The Center may not require an individual to waive his or her right to file a complaint with the OCR as a condition of treatment or payment.

Policy 1.12 Implementation of Policies and Procedures

The Center must implement policies and procedures that are designed to comply with the privacy regulations. The privacy policies and procedures may be reasonably designed to take into account the Center's size and the Center's operations, to ensure compliance.

Policy 1.13 Changes to Policies and Procedures / Changes in Law

The Center must change its policies and procedures as necessary and appropriate to comply with any changes in the law. When a Center changes a privacy practice that is stated in its Notice of Privacy Practices, and makes corresponding changes to its policies and procedures, it may make the changes effective for PHI that it created or received prior to the effective date of the notice revision, if the Center has included in the notice a statement reserving its right to make such a change in its privacy practices; or the Center may make any other changes to policies and procedures at any time, provided that the changes are documented and implemented in accordance with the Center's policies and procedures.

Policy 1.14 Changes to Privacy Centers Stated in the Notice

If the Center has not reserved its right to change a privacy practice described in the Notice, the Center is bound by the privacy practices stated in the notice with respect to PHI created or received while the notice is in effect. The Center may change a privacy practice stated in the Notice without having reserved the right to do so, provided that the change meets the

implementation requirements described in the section and the change is effective only for PHI created or received after the effective date of the notice.

Policy 1.15 Changes to Other Policies or Procedures

The Center may change, at any time, a policy or procedure that does not materially affect the content of the Notice, provided that:

1. The policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of this subpart; and
2. Prior to the effective date of the change, the policy or procedure, as revised, is documented as required under Documentation below (Policy 1.16).

Policy 1.16 Documentation

The Center must maintain its policies and procedures in written or electronic form. If a communication is required by this subpart to be in writing, the Center must maintain such writing, or an electronic copy, as documentation. If an action, activity, or designation is required by this subpart to be documented, the Center must maintain a written or electronic record of such action, activity, or designation.

Policy 1.17 Retention Period

The Center must retain the required documentation for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

Policy Two: Notice of Privacy Practices for Protected Health Information

Policy 2.1 Generally

Georgia Mountains Health Services, “the Center”, has the duty to disclose to individuals the possible uses and disclosures of PHI and the individual's rights and the Center's legal duties with respect to PHI.

Policy 2.2 Required Elements of Notice

The notice must be written in plain language and contain a header reading: **"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."** The notice must also contain:

1. A description, including at least one example, of the types of uses and disclosures the Center is permitted to make for each of the following purposes: treatment, payment, and health care operations.
2. A description of each of the other purposes for which the Center is permitted or required to use or disclose PHI without the individual's written consent or authorization.
3. If a use or disclosure is prohibited or materially limited by other law, the description of such use or disclosure must reflect the more stringent law.
4. A description, including at least one example, of the types of uses and disclosures the Center is permitted to make for each of the following purposes: treatment, payment, and health care operations.
5. A description of each of the other purposes for which the Center is permitted or required to use or disclose PHI without the individual's written consent or authorization.
6. If a use or disclosure is prohibited or materially limited by other law, the description of such use or disclosure must reflect the more stringent law.
7. A statement that other uses and disclosures will be made only with the individual's written authorization, that the individual may revoke such authorization, and how the individual may revoke authorization.
8. A statement that the sale of protected health information and the use of such information for paid marketing require authorization from the individual.
9. A statement that other uses and disclosures not described in the Notice of Privacy Practice will be made only with a patient authorization.

Policy 2.3 Separate Statements for Certain Uses or Disclosures

If the Center intends to engage in any of the following activities, the notice must include a

separate statement, as applicable, that:

1. The Center may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual;
2. The Center may contact the individual to raise funds for the Center; or
3. The Center may contact the individual to authorize the use or disclosure of PHI for marketing activities supported by third parties.

Policy 2.4 Individual Rights

The notice must contain a statement of the individual's rights with respect to PHI and a brief description of how the individual may exercise these rights as follows:

1. The right to request restrictions on certain uses and disclosures of PHI including a statement that the Center is not required to agree to a requested restriction;
2. The right to receive confidential communications of protected information as applicable;
3. The right to inspect and copy PHI as provided;
4. The right to amend PHI as provided;
5. The right to receive an accounting of disclosures of PHI as provided;
6. The right to receive a security breach notification upon occurrence;
7. The right of an individual, including an individual who has agreed to receive the notice electronically, to obtain a paper copy of the notice from the Center upon request; and
8. The right of an individual to pay "out of pocket" and restrict disclosures to their health plan for services.

Policy 2.5 Center's Duties

A. The notice must contain:

1. A statement that the Center is required by law to maintain the privacy of PHI and to provide individuals with notice of its legal duties and privacy practices with respect to PHI;
2. A statement that the Center will notify the affected individuals of breaches of their PHI.
3. A statement that the Center is required to abide by the terms of the notice currently in effect; and
4. For the Center to apply a change in a privacy practice that is described in the notice to PHI that the Center created or received prior to issuing a revised notice, a statement that it reserves the right to change the terms of its notice and to make the

new notice provisions effective for all PHI that it maintains. The statement must also describe how it will provide individuals with a revised notice.

B. The notice must be made available to all patients and to and personal representative of a patient. The Center shall make the notice available to the patient by posting the notice on the wall and by providing copies of the notice upon request. The Center shall make a good faith effort to obtain the patient's acknowledgement that the notice has been made available to them. Copies of the patient acknowledgement shall be retained by the Center.

Policy 2.6 Privacy Complaints

With respect to privacy complaints, the notice of privacy practices must: (i) state that the individuals may file a complaint with the Center and/or with the OCR if they believe that the Center has violated their right to privacy, (ii) a brief description of how to file a complaint with the Center and the OCR, and (iii) a statement that the individual will not be retaliated against for filing a complaint.

Policy 2.7 Contact

The notice must have the name or title, and telephone number of a person or office to contact for further information.

Policy 2.8 Effective Date

The notice must have the effective date on it, which may not be earlier than the date on which the notice is printed or otherwise published.

Policy 2.9 Revisions

The notice must be revised whenever there is a material change to the uses or disclosures, the individual's rights, the Center's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term may not be implemented prior to the effective date of the notice in which such material change is reflected.

Policy 2.10 Implementation Requirements for Centers

A Center that has a direct treatment relationship with an individual must: provide the notice no later than the date of the first service delivery (including service delivered electronically). If the Center maintains a physical service delivery site: 1) Have the notice available at the service delivery site for individuals to request to take with them; and 2) Post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the Center to be able to read the notice.

Policy 2.11 Electronic Notice

If a Center maintains a web site, the Center must post its notice on the web site. The notice may

be sent to an individual via e-mail - if the individual agrees to electronic notice. If the Center becomes aware that notice by e-mail has failed, the Center must give the individual a paper copy of the notice. Updates can be sent by e-mail. The individual who gets notice via e-mail retains the right to obtain a paper copy of the notice upon request.

Policy 2.12 Joint Notice

A Center that participates in an organized health care arrangement may comply with Policy Two by using a joint notice, provided that:

1. The participating entities agree to abide by the terms of the notice created or received by the Center as part of its participation in the health care arrangement;
2. The notice reflects that it covers more than one Center; and
3. The notice describes with reasonable specificity the Center, or class of entities, to which the joint notice applies;
4. The notice describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies; and
5. If applicable, the notice must state that the Center will share PHI with each other, as necessary to carry out treatment, payment, or health care operations relating to the organized health care arrangement.

Policy 2.13 Documentation of Notice

The Center must document compliance with the notice requirements by retaining copies of the issued joint notices.

Policy 2.14 Notice Revisions

The Center must make notice revisions available to patients upon request after the effective date of revisions.

The Center must post the revised notice in a clear and prominent location in their facility.

Policy Three: Uses and Disclosures for which Authorization is Required

Policy 3.1 General Rule

Georgia Mountains Health Services may not use or disclose PHI without a valid authorization for situations that require an authorization (i.e. uses or disclosures made for reasons other than treatment, payment or operations). When the Center obtains a valid authorization, such use or disclosure must be consistent with such authorization.

Policy 3.2 Psychotherapy Notes

The Center must obtain an authorization for any use or disclosure of psychotherapy notes, except:

1. To carry out the following treatment, payment, or health care operations, consistent with consent requirements detailed in Part II above:
 - a) Use by originator of the psychotherapy notes for treatment;
 - b) Use or disclosure by the Center in 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 the Center to defend a legal action or other proceeding brought by the individual; and
2. A use or disclosure that is required or permitted with respect to the oversight of the originator of psychotherapy notes.

Policy 3.3 Valid Authorizations

A valid authorization must be written in plain language and must contain the following elements:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion;
2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom the Center may make the requested use or disclosure;
4. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure;
5. A statement of the individual's right to revoke the authorization in writing and the exceptions to the right to revoke, together with a description of how the individual may revoke the authorization;
6. A statement that PHI used or disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and no longer be protected by this rule;
7. Signature of the individual and date; and

8. If the authorization is signed by a personal representative, a description of such representative's authority to act for the individual.

Policy 3.4 Invalid Authorizations

An authorization is not valid if it does not meet the requirements set out directly above, or if:

1. The expiration date has passed, or the expiration is known by the Center to have occurred;
2. The authorization is known by the Center to have been revoked;
3. The authorization violates any of the rules relating to "Compound Authorizations" (Policy 3.5 below).
4. Any material PHI in the authorization is known by the Center to be false.

Policy 3.5 Compound Authorizations

An authorization may not be combined with any other document to create a compound authorization, except as follows:

1. An authorization for the use or disclosure of PHI created for research that includes treatment of the individual may be combined as permitted under "Research" (Policy 3.9 below); or
2. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes.

Policy 3.6 Prohibition on Conditioning of Authorizations

The Center may not condition the provision to an individual of treatment or payment, obtainment of an authorization, except:

1. A Center may condition the provision of research related treatment on provision of an authorization (see "Research" Policy 3.9 below); and
2. A Center 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 PHI to that third party.

Policy 3.7 Revocation of Authorizations

An individual may revoke an authorization at any time, provided that the revocation is in writing, except to the extent that:

1. The Center has taken action in reliance thereon; or
2. If the authorization was obtained as a condition of obtaining insurance coverage.

Policy 3.8 Documentation

The Center must document and retain all signed authorizations.

Policy 3.9 Research

- A. If PHI is used for research, such authorization must:
1. Meet the requirements listed in “Valid Authorization” (Policy 3.3);
 2. Contain:
 - a) A description of how the PHI will be used to carry out treatment, payment, or health care operations.
 - b) A description of any PHI that will not be used or disclosed for permitted purposes, provided that the Center may not include a limitation affecting its right to make a use or disclosure that is required by law.
 - c) If the Center has or intends to obtain the individual's consent, or has or intends to provide the individual with a notice, the authorization must refer to that consent or notice and state that the statements made are binding.
- B. A research authorization may be in the same document as a consent to participate in research, a consent to use or disclose PHI to carry out treatment, payment or health care operations, or a notice of privacy practices.

Policy Four: Uses and Disclosures Requiring an Opportunity For the Individual to Agree or Object

Policy 4.1 No Written Consent or Authorization Needed

The Center may use or disclose PHI without obtaining an authorization if the individual is informed in advance of the use or disclosure and has been given the opportunity to agree or object to the disclosure. The Center may orally inform the individual and/or obtain the individual's oral agreement or objection to a use or disclosure permitted by this section.

Policy 4.2 Written Consent or Authorization Exception

The Center must first obtain individual consent or authorization in order to use or disclose PHI for marketing purposes or to sell PHI.

Policy 4.2 Facility Directories — Uses and Disclosures

A. Generally, the Center may use the following PHI to maintain a directory of individuals in its facility:

1. The individual's name;
2. The individual's location in the Center's facility;
3. The individual's condition (described in general terms that does not communicate specific medical information about the individual); and
4. The individual's religious affiliation.

B. The Center may disclose for directory purposes the above information to:

1. Members of the clergy; or
2. Except for religious affiliation, to other persons who ask for the individual by name.

Policy 4.3 Exceptions

The Center must inform an individual of the PHI that the Center may include in a directory and the persons to whom it may disclose such information, and provide the individual with the opportunity to restrict or prohibit some or all of the uses or disclosures.

Policy 4.4 Emergencies

A. If circumstances prohibit the Center from giving the individual the right to object, then the Center may use or disclose some or all of the PHI permitted above for the facility's directory, if such disclosure is:

1. Consistent with a prior expressed preference of the individual, if any, that is known to the Center; and
2. In the individual's best interest as determined by a provider in the Center in his or her professional judgment.

B. The individual must be given the right to object.

Policy 4.5 Uses and Disclosures for Involvement in the Individual's Care

- A. The Center may disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care.
- B. The Center may use or disclose PHI to notify, or assist in the notification of a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death.
- C. If the individual has the capacity to object, the Center may use or disclose the protected information if it:
1. Obtains the individual's agreement;
 2. Provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or
 3. Reasonably infers from the circumstances, based on the exercise of professional judgment that the individual does not object to the disclosure.
- D. If the individual is not present, or does not have the capacity to object, then the Center may determine whether the disclosure is in the best interests of the individual. If the Center determines that it is in the best interest of the individual, it may only disclose PHI that is directly relevant to the person's involvement with the individual's health care.
- E. The Center may use or disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts.

Policy Five: When Authorization and/or an Opportunity To Object is Not Required

A. The Center may disclose PHI: (i) without written acknowledgement of receipt of the Notice of Privacy Practices and Notice of Individual Rights; and/or (ii) without providing the individual with the opportunity to agree or object in the following circumstances and under certain conditions:

1. When required by law;
2. To a public health authority 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, public health investigations, and public health interventions;
3. To an authority authorized by law to receive reports of abuse or neglect;
4. To a person subject to the jurisdiction of the Food and Drug Administration;
5. To a person who may have been exposed or could be exposed to a communicable disease;
6. As necessary to comply with laws relating to Workers' Compensation or other similar programs that provide benefits for work-related injuries or illness without regard to fault; and
7. In compliance with and as limited by the relevant requirements of:
 - a. A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer (See Organizational Policy and Procedure: Release of Protected Health Information Under Subpoena);
 - b. A grand jury subpoena; or
 - c. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law, provided that (a) the information sought is relevant and material to a legitimate law enforcement inquiry; (b) the request is specific and limited in scope to the purpose for which the information is sought; and (c) De-identified information could not be reasonably used.

B. Disclosures may also be permitted: as required by law; regarding victims of crime; regarding decedents; when there is a crime on the premises; reporting crime in emergencies; to avert a serious threat to health or safety; and to correctional institutions.

C. Before disclosing PHI to any of the entities listed above, employees of the Center must contact the Privacy Officer.

Policy Six: Other Requirements Relating to Uses and Disclosures of PHI

Policy 6.1 Generally

- A. PHI that has been de-identified can be released.
- B. PHI can be de-identified by removing:
 - 1. Names;
 - 2. All geographic indicators of a subdivision smaller than a state (city, street, county, etc.);
 - 3. All dates (except the year). However, if the individual is over 89 years old, then the birth year must also be removed;
 - 4. Telephone and fax numbers;
 - 5. E-mail addresses;
 - 6. Social security numbers;
 - 7. Medical record numbers;
 - 8. Health plan beneficiary numbers;
 - 9. Account numbers;
 - 10. Certificate/license numbers;
 - 11. Vehicle identifiers and serial numbers, including license plate numbers;
 - 12. Device identifiers and serial numbers;
 - 13. Web Universal Resource Locators (URLs);
 - 14. Internet Protocol (IP) address numbers;
 - 15. Biometric identifiers, including finger and voice prints;
 - 16. Full face photographic images and any comparable images; and
 - 17. Any other unique identifying number, characteristic, or code.
- C. To release de-identified PHI, the Center cannot have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.
- D. The Center can use a code system to re-identify the de-identified information provided that the codes are not related to or derived from information about the individual. In addition, the Center cannot disclose the code or method for re-identification to any party.
- E. The Center must identify those individuals within the entity that need to have access to PHI to carry out their duties. For each individual, or class of individuals, the entity must describe the categories of classified PHI to which each individual is allowed access.

F. When any PHI is disclosed, the Center must disclose the minimum amount of information necessary to accomplish the purpose for which disclosure is sought.

G. The Center must analyze each request for production to determine that the minimum amount of information needed is released unless the request is made by:

1. A public official;
2. Another Center;
3. A professional associated with the Center who is providing professional services to the Center; or
4. The person requesting the information has already documented the need for the release.

If the information is requested by one of the four classes of people listed above, then the Center may release the information without analyzing the specific request, but instead, rely on the request made by the party.

H. For a request that is made on a routine and recurring basis, the Center must implement policies and procedures (which may be standard protocols) that limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

I. Entire medical records cannot be requested unless the entire record is needed to accomplish the purpose for which the request is made.

Policy 6.2 Marketing

PHI can only be disclosed for marketing purposes to a business associate that assists the Center. When information for marketing is requested, the above protocols must be followed UNLESS the information is being disclosed to make a marketing communication to an individual that:

1. Occurs in a face-to-face encounter with the individual;
2. Concerns products or services of nominal value; or
3. Concerns the health-related products and services of the Center or of a third party and the communication meets the following requirements:
 - a) The communication must:
 - i. Identify the Center as the party making the communication;
 - ii. If the Center has received or will receive direct or indirect remuneration for making the communication, prominently state that fact; and
 - iii. Except when the communication is contained in a newsletter or similar type of general communication device that the Center distributes to a broad cross-section of patients, enrollees, or other broad groups of individuals, contain instructions describing how the individual may opt out of receiving future such communications.

- b) If the Center uses or discloses PHI to target the communication to individuals based on their health status or condition:
 - i. The Center must make a determination prior to making the communication that the product or service being marketed may be beneficial to the health of the type or class of individual targeted; and
 - ii. The communication must explain why the individual has been targeted and how the product or service relates to the health of the individual.
 - c) The Center must make reasonable efforts to ensure that individuals who decide to opt out of receiving future marketing communications are not sent such communications.
4. The Center may not receive direct or indirect payment in exchange for such marketing communications made on or after February 17, 2010, unless:
- a) Payment is for a communication regarding a drug currently prescribed for the recipient of the communication and the payment is “reasonable in amount”;
 - b) The communication is made with the patient’s authorization; or
 - c) The communication is made by the Center business associate on behalf of the Center and is consistent with the business associate agreement.

Policy 6.3 Fundraising.

The Center can release demographic information relating to an individual; and dates of health care provided to an individual to business associates or an institutionally related foundation.

The Center may not use or disclose PHI for fundraising purposes unless a statement disclosing that the Center can use the information for fundraising purposes has been signed by the individual.

The Center must include in any fundraising materials it sends to an individual a description of how the individual may opt out of receiving any further fundraising communications.

The Center must make reasonable efforts to ensure that individuals who decide to opt out of receiving future fundraising communications are not sent such communications. The decision to opt out is considered a revocation of authorization under the HITECH revisions.

Policy 6.4 Underwriting.

If a health plan receives PHI for the purposes of underwriting, premium rating, or other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and if such health insurance or health benefits are not placed with the health plan, such health plan may not use or disclose such PHI for any other purpose, except as may be required by law.

In order to release information under any of the circumstances listed above, the Center must verify the identity of the person requesting the information and the authority of such person to have access to the information, and obtain any documentation, statements, or representations,

whether oral or written, from the person requesting the information when required by this section. The Center may rely on presentation of a Center identification badge, other official credentials, proof of government status, government letterhead, warrant, subpoena, or other legal process to determine that the requesting party is asking with proper authority. Basically, the Center must show that it acted on a good faith belief or exercised professional judgment when releasing the information.

Policy 6.5 Limited Data Sets

The Center may not create and disclose a limited data set (a set of patient data that does not include directly identifiable information about the patient) for research, public health or for operational purposes, if the Center enters into a data use agreement. The data use agreement may take a form similar to the Confidentiality Agreement or the Business Associate Agreement.

Policy Seven: Privacy of Health Information

Policy 7.1 Consent

The Center must obtain an individual's consent before using or disclosing PHI to carry out treatment, payment, or health care operations unless:

1. The Center has an indirect treatment relationship with the individual; or
2. The Center created or received the protected information in the course of providing health care to an individual who is an inmate.
3. Situations Where a Personal Representative May Act for a Patient regarding Protected Health Information:
 - a. If a person, under applicable law, has authority to act on behalf of an individual who is an adult or an emancipated minor, the Center must treat such person as a personal representative, i.e., a person holding authority under a valid Durable Power of Attorney for Health Care Decisions falls within this category.
 - b. Health care information may be released to a patient's personal representative or relative for the purpose of providing health care to the patient if:
 - i. The patient has been notified of his/her right to object to the disclosure and the patient has not objected; or
 - ii. The patient is in a physical or mental condition such that the individual is not capable of objecting, and there are no prior indications that the individual would object.
 - c. If, under applicable law, a parent, guardian, or other person acting in *loco parentis* has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, the Center must treat such person as a personal representative. HOWEVER, the following conditions apply:
 - i. If the minor consents to such health care service – then no other consent is required, and the minor has not requested that such person be treated as the personal representative;
 - ii. The minor may lawfully obtain such health care service 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;
 - iii. A parent, guardian or other person acting in *loco parentis* assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.
 - iv. Deceased individuals: 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, the Center must treat such person as a personal representative.

- d. Deceased individuals: 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, the Center must treat such person as a personal representative. Georgia code provides for the following persons to receive a copy of the deceased medical record:
 - i. Each child (either minors or adults) of a deceased patient has an independent right to a copy of the deceased medical record.
 - ii. The surviving spouse if there are no children and no spouse living at the time of the patient's death, the patient's parents are each entitled to a copy.
 - iii. The administrator of the estate.
- e. Cases or suspected cases of abuse, neglect, or endangerment. Unless there is a conflict in an existing law, the Center may decide not to treat a person as the personal representative of the patient if there is a reasonable belief that:
 - i. The patient has been or may be subjected to domestic violence, abuse, or neglect by such person; or
 - ii. Treating such person as the personal representative could endanger the patient based on the Center professional judgment.

Policy 7.2 No Consent Needed

- A. The Center need not get consent:
 - 1. In emergency treatment situations, if the Center attempts to get consent as soon as is reasonably practicable after delivery of the treatment.
 - 2. If the Center is required by law to treat the individual, AND the Center attempts to get consent but is unable to do so.
 - 3. The Center attempts, but is unable to obtain consent due to substantial communication barriers, AND the Center decides that the individual's consent can be inferred from the circumstances.
- B. If the Center fails to receive consent, the Center must document its attempt to obtain consent and the reason why it was not obtained.

Policy 7.3 Consent from Another Entity

Consent obtained by the Center is not effective to permit another Center to use or disclose PHI.

Policy 7.4 Documentation

- A. Consent may not be combined in a single document with the notice of privacy practices for PHI.
- B. A consent for use or disclosure may be combined with other types of written legal permission if the consent:

1. Is visually and organizationally separate from such other written legal permission; and
 2. Is separately signed by the individual and dated.
- C. The consent may be combined with a research authorization.
- D. Consent must be documented and retained.

Policy 7.5 Revocation of Consent

- A. An individual may revoke consent at any time, except to the extent that action has been taken in reliance on the consent.
- B. Revocation must be in writing.

Policy 7.6 Formalities

Consent must be in plain language and:

1. Inform the individual that PHI may be used and disclosed to carry out treatment, payment, or health care operations;
2. Refer the individual to the Notice of Privacy Practices for PHI and state that the individual has the right to review the Notice before signing the consent;
3. State that the terms of the entity's notice may change and describe how the individual may obtain a revised notice;
4. State that:
 - a. The individual has the right to request that the Center restrict how PHI is used or disclosed to carry out treatment, payment, or health care operations;
 - b. The Center is not required to agree to requested restrictions; and
 - c. If the Center agrees to a requested restrictions, the restriction is binding on the Center;
5. State that the individual has the right to revoke the consent in writing, except to the extent that the Center has taken action in reliance thereon; and
6. Be signed by the individual and dated.

Policy 7.7 Void Consents

The consent is void if:

1. The consent lacks any of the formalities listed above; or
2. The consent has been revoked.

Policy 7.8 Conflicting Consents

- A. If the Center has received two conflicting consents, it must abide by the more restrictive consent, authorization, or other written legal permission from the individual.
- B. A consent can attempt to be resolved by:
 - 1. Obtaining a new consent from the individual;
 - 2. Communicating orally or in writing with the individual in order to determine the individual's preference. The preference must be documented.

Policy 7.9 Joint Consents

- A. A Center that participates in an organized health care arrangement and has a joint notice may comply with this section by using a joint consent.
- B. The joint consent must:
 - 1. Include the name or other specific identification of the Center, or classes of the Center, to which the joint consent applies; and
 - 2. Meet all requirements listed above in this Policy Seven.

Policy Eight: Right to Request Privacy Protection for PHI

Policy 8.1 Generally

The Center must permit an individual to request restrictions on the release of PHI. The Center is not required to agree to the restriction. However, if the Center does agree to restrict the release of the PHI, the Center must abide by that restriction unless a release is needed to provide emergency treatment. If PHI is released for emergency treatment reasons, then the Center must request that such health care center not further use or disclose the information.

The Center may terminate its agreement to a restriction if:

- the individual agrees to or requests the termination in writing;
- the individual orally agrees to the termination and the oral agreement is documented; or
- the Center tells the individual that it is terminating its agreement to a restriction, except that the termination is only effective with respect to information created or received after it has informed the individual.

Policy 8.2 Confidential Communication Requirements

The Center must permit individuals to request, and must accommodate reasonable requests, to receive communications of PHI from the Center by alternative means or at alternative locations. The Center can request that the accommodation be made in writing. The Center can condition a reasonable accommodation on: when appropriate, when information as to how payment, if any, will be handled; and specification of an alternative address or other method of contact. A covered health care Center may NOT require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis. A health plan may require that a request contain a statement that disclosure of all or part of the information to which the request pertains could endanger the individual.

Policy 8.3 Record-Keeping

The Center will maintain documentation of restrictions and termination of restrictions as it applies to this policy and procedure as part of the patient's permanent medical record.

Policy Nine: Access of Individuals to PHI

Policy 9.1 Right of Access Generally

An individual shall be allowed access to all PHI with the exception of psychotherapy notes, information compiled in anticipation of litigation for a formal proceeding, and information maintained subject to the Clinical Laboratory Improvements Amendments of 1988, 42 U.S.C. § 263a, or to the extent the provision of access to the individual would be prohibited by law.

All request for access to PHI must be forwarded to the Privacy Officer.

Policy 9.2 Unreviewable Grounds for Denial

Access may be denied without providing the individual an opportunity for review in the following circumstances:

1. The information is accepted from the right of access.
2. Access can be denied to an inmate if obtaining a copy of the information would jeopardize the health, safety, security, custody, or rehabilitation of the individual or of other inmates, or the safety of any officer, employee, or other person at the correctional institution or responsible for the transporting of the inmate.
3. Review can be denied during ongoing research projects, provided that the individual has agreed to the denial of access when consenting to participate in the research that includes treatment, and the Center has informed the individual that the right of access will be reinstated upon completion of the research.
4. Access to information contained in records that are subject to the Privacy Act, 5 U.S.C. §522a, may be denied, if the denial of access under the Privacy Act would meet the requirements of that law.
5. Access may be denied if the information was obtained from someone other than a health care center under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Policy 9.3 Reviewable Grounds for Denial

- A. This Center may deny an individual access in the following circumstances:
1. A licensed health care professional has determined that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;
 2. The information makes reference to another person (unless such other person is a health care center) and a licensed health care professional has determined that the access requested is reasonably likely to cause substantial harm to such other person;
or
 3. The request for access is made by the individual's personal representative, and a licensed health care professional has determined that the provision of access to such

personal representative is reasonably likely to cause substantial harm to the individual or another person.

B. If access is denied under one of the provisions above, the individual has the right to have the denial reviewed by a licensed health care professional who is designated by the Center to act as a reviewing official and who did not participate in the original decision to deny. This Center must provide or deny access in accordance with the determination of the reviewing official.

Policy 9.4 Requests for Access and Timely Action

A. This Center must allow individual's access to their PHI. However, the Center may require the individual to make requests for access in writing, provided that it informs individuals of such a requirement. The Center has thirty (30) days to respond to the request as follows:

1. If the request is granted, in whole or in part, the Center must inform the individual of the acceptance of the request and provide the access requested.
2. If the request is denied, in whole or in part, the Center must provide the individual with a written denial.

B. If the request is for information that is not maintained or accessible to the Practice on-site, it must respond as above within sixty (60) days rather than thirty (30) days. The Center can extend the response time for thirty (30) additional days provided that:

1. The Center, within the first thirty (30) or sixty (60) days as mandated above, provides the individual with a written statement or the reasons for the delay and the date by which the Center will complete its action on the request; and
2. The Center may have only one such extension.

Policy 9.5 Provision of Access

If access is granted in whole or in part, the following requirements must be met:

1. The Center must provide the access requested, including inspection or obtaining a copy, or both, of the information about them in designated record sets. If the information is maintained in more than one designated record set or at more than one location, the Center need only produce the protected information once in response to a request for access.
2. The Center must provide the individual with access to the information in the form or format requested by the individual if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by the Center and the individual.
3. The Center may provide the individual with a summary in lieu of providing access to the information or may provide an explanation of the PHI if:
 - a. The individual agrees in advance to such a summary or explanation; and
 - b. The individual agrees in advance to the fees imposed, if any, by the Center for such summary or explanation.

4. Pursuant to the HITECH Revisions, if the request is for protected health information that is used or maintained through an electronic health record, the Center will produce the record in electronic format if the individual so requests in a clear, conspicuous, and specific manner.

All request for PHI in an electronic format must be sent to the Privacy Officer.

Policy 9.6 Time and Manner of Access

The Center must provide the individual with a convenient time and place to inspect or copy the information or mail the information to the individual.

Policy 9.7 Fees

The Center can charge reasonable, cost-based fees, provided that the fee includes only the cost of:

1. Copying, including the cost of supplies for and labor of copying, the PHI requested by the individual;
2. Postage, when the individual has requested the copy, or the summary or explanation, be mailed; and
3. Preparing an explanation or summary of the PHI.

Policy 9.8 Denial of Access

If access is denied, in whole or in part, the Center must comply with the following requirements:

1. The Center must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI as to which the Center has a ground to deny access.
2. The Center must provide a timely, written denial to the individual. The denial must be in plain language and contain:
 - a. The basis of the denial;
 - b. If applicable, a statement of the individual's review rights including a description of how the individual may exercise such review rights; and
 - c. A description of how the individual may complain to the Center or to the OCR. The description must include the name, title, and telephone number of the contact person or office designated.
3. If the Center does not maintain the requested information, and the Center knows where the information is maintained, it must inform the individual where to direct the request.
4. If the individual requests a review of the denial, the Center must designate a licensed health care professional, who was not directly involved in the denial to review the decision to deny access. The Center must promptly refer a request for review to such

designated reviewing official. The designated reviewing official must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards. The Center must promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as required by this section to carry out the designated reviewing official's determination.

Policy 9.9 Documentation

The Center must document the designated record sets that are subject to access by individuals; and the titles of the persons or offices responsible for receiving and processing requests for access by individuals.

Policy Ten: Amendment of PHI

Policy 10.1 Right to Amendment

An individual has the right to request that the Center amend PHI or a record in a designated record set for as long as the information is maintained in the record set.

All requests for amendments of PHI must be sent to the Privacy Officer.

Policy 10.2 Denial of Amendment

The Center can deny the individual's request to amend if the information or record:

1. Was not created by the Center, unless the individual provides a reasonable basis to believe that the originator is no longer available to act on the requested amendment;
2. Is not part of the designated record set;
3. Access could be denied under Policy Nine above; or
4. Is accurate and complete.

Policy 10.3 Requests for Amendment and Timely Action

The Center may require individuals to make requests for amendment in writing and to provide a reason to support a requested amendment, provided that it informs individuals in advance of such requirements. It must act on the request no later than sixty (60) days after receipt of the request, and it may extend the time by no more than thirty (30) days if the Center provides the individual with a written statement of the reasons for the delay and the date by which the Center will complete its action on the request. The Center may have only one such extension.

Policy 10.4 Accepting the Amendment

If the Center accepts the requested amendment, in whole or in part, the entity must comply with the following requirements:

1. The Center must make the appropriate amendment 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.
2. The Center must timely inform the individual that the amendment is accepted and obtain the individual's identification of and agreement to have the entity notify the relevant persons with which the amendment needs to be shared.
3. The Center must make reasonable efforts to inform and provide the amendment within a reasonable time to:
 - a. Persons identified by the individual as having received PHI about the individual and needing the amendment; and
 - b. Persons, including business associates, that the Center knows 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 individual.

Policy 10.5 Denying the Amendment

If the request to amend is denied, in whole or in part, the Center must comply with the following:

1. The Center must provide the individual with a timely, written denial. The denial must use plain language and contain:
 - a. The basis for the denial;
 - b. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;
 - c. A statement that, if the individual does not submit a statement of disagreement, the individual may request that the entity provide the request and the denial with future disclosures of the information that is the subject of the amendment; and
 - d. A description of how the individual may complain to the entity or to the OCR. The description must include the name, or title, and telephone number of the contact person or office designated to receive complaints.
2. The Center must permit the individual to submit to the entity a written statement disagreeing with the denial of all or part of the requested amendment and the basis of such disagreement. The Center may reasonably limit the length of a statement of disagreement.
3. The Center may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the entity must provide a copy to the individual who submitted the statement of disagreement.
4. The Center may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, the Center must provide a copy to the individual who submitted the statement of disagreement.
5. The Center must, as appropriate, identify the record or PHI in the designated record set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment, the Center's denial of the request, the individual's statement of disagreement, if any, and the Center's rebuttal, if any, to the designated record set.
6. If a statement of disagreement has been submitted by the individual, the Center must include the material appended as described above (see "5." directly above), or an accurate summary of the information, with any subsequent disclosure of the PHI to which the disagreement relates. If the individual has not submitted a written statement of disagreement, the Center must include the individual's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the PHI *only* if the individual has requested such action. When a subsequent disclosure is made using a standard transaction that does not permit the additional material to be included with the disclosure, the Center may separately transmit the material, as applicable, to the ° recipient of the standard transaction.

7. The Center that is informed by another Center of an amendment to an individual's information must amend the information in its designated record sets.
8. The Center must document the titles of the persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation as required.

Policy Eleven: Accounting of Disclosures of PHI

Policy 11.1 Standard: Right to an Accounting of Disclosures of PHI

An individual has a right to receive an accounting of disclosures of information made by the Center in the six (6) years prior to the date the accounting is requested, except for disclosures:

1. To carry out treatment, payment and health care operations or pursuant to an authorization as provided in Policy 3;
2. To individuals of PHI about them, or incident to a use or disclosure otherwise permitted or required under these Policies;
3. For the facility's directory or to persons involved in the individual's care or other notification purposes;
4. For national security or intelligence purposes;
5. To correctional institutions or law enforcement officials;
6. That occurred prior to the compliance date for the Center or as part of a limited data set, as that phrase is defined under the Rule; and
7. Certain reports to law enforcement officials or health oversight agencies, in accordance with Policy 11.2 below and subject to applicable state laws that limit the disclosure of criminal reports.
8. Made through an electronic health record (in that case, the patient may request an accounting for disclosures made by the Center in the three years prior to the request for accounting).
9. That, in the good faith estimation of a member of the medical staff of the Centers, the request for accounting is made by the individual representative that is suspected of domestic or child abuse, and the medical staff member has a reasonable belief that such representative individual is the abuser or that providing the accounting could endanger the individual or the medical staff member making the report.

All requests for accounting of disclosures must be sent to the Privacy Officer.

Policy 11.2 Suspension

The Center must temporarily suspend an individual's right to receive an accounting of disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides the Center with a written statement that such an accounting would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

If the statement from the agency is made orally, it must:

1. Document the statement, including the identity of the agency or official making the statement;
2. Temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and
3. Limit the temporary suspension to no longer than thirty (30) days from the date of the oral statement, unless a written statement pursuant to this section is submitted during that time.

Policy 11.3 Time for Accounting

An individual may request an accounting of disclosures for a period of time less than six (6) years from the date of request.

Policy 11.4 Content of the Request

The entity must provide the individual with a written accounting that meets the following requirements:

1. The accounting must include disclosures for the time requested, or past six (6) years if no time limit is requested, including disclosures to or by business associates of the Center.
2. The accounting must include for each disclosure:
 - a. The date of the disclosure;
 - b. The name of the Center or person who received the PHI and, if known, the address of such entity or person;
 - c. A brief description of the information disclosed; and
 - d. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure; or, in lieu of such statement:
 - i. a copy of the individual's written authorization;
 - ii. a copy of a written request of disclosure, if any.
 - e. If the Center has made multiple disclosures of information to the same person or entity for a single purpose, or pursuant to authorization, the accounting may, with respect to such multiple disclosures, provide:
 - i. The information required under this number "2." as stated directly above, for the first disclosure during the accounting period;
 - ii. The frequency, periodicity, or number of the disclosures made during the accounting period; and
 - iii. The date of the last such disclosure during the accounting period.

Policy 11.5 Provisions of the Accounting

The Center must act on the request for an accounting, no later than sixty (60) days after receipt of such a request as follows:

1. The Center must provide the individual with the accounting requested; or
2. If the entity is unable to provide the accounting within the time required, the entity may extend the time to provide the accounting by no more than thirty (30) days, provided that:
 - a. The Center, within sixty (60) days, provides the individual with a written statement of the reasons for the delay and the date by which the Center will provide the accounting; and
 - b. The Center may have only one such extension of time for action on a request for an accounting.

Policy 11.6 Extensions

The Center may have only one such extension of time.

Policy 11.7 Accounting

The Center must provide the first accounting to an individual in any 12-month period without charge. The Center may impose a reasonable, cost-based fee for each subsequent request by the same individual within the twelve (12) month period, provided that it informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

Policy 11.8 Documentation

The Center must document the following and retain the documentation as required under Policy 1.16 Documentation:

1. The information required to be included in an accounting for disclosures of information that are subject to an accounting;
2. The written accounting that is provided to the individual under this section; and
3. The titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

Policy 11.9 Disclosures

Disclosures made six (6) years prior to the request for disclosure or disclosures made three (3) years prior to the request for disclosure if disclosed through an electronic health record.

Policy Twelve: Complaint and Compliance Procedures

Policy 12.1 Compliance and Enforceability

- A. The Center is required to cooperate with the OCR and DHHS to insure compliance with the HIPAA regulations.
- B. The OCR may provide technical assistance to the Center to help them comply voluntarily. In that case, the Center shall make every effort to cooperate.

Policy 12.2 Comments and Complaints

If a patient, or a representative of a patient, feels the Center is not complying with the Privacy Rule, he or she may file a comment or complaint with the Office for Civil Rights ("OCR") pursuant to § 160.306. The Privacy Officer will instruct the patient on the proper way to file a comment with the Center using Form 12.2 (attached). If the patient desires to file a complaint with the Office for Civil Rights, then the Privacy Officer shall assist the patient in that process.

Policy 12.3 Compliance Reviews

- A. The OCR has the right to conduct compliance reviews to determine whether the Center is in compliance.
- B. The Center must provide records and compliance reports to the OCR when and if they are requested during a compliance review.
- C. The Center and its employees must cooperate with the OCR during complaint investigations and compliance reviews.
- D. The Center and its employees must permit access to the OCR during normal business to its facilities, books, records, accounts, and other sources of information, including PHI, that are pertinent to ascertaining compliance with the Privacy Rule.
- E. **If any PHI is requested from the Center by the OCR, or anyone else involved in a compliance review, the employee receiving the request is to notify the Privacy Officer immediately.**

Policy Thirteen: Business Associates

Policy 13 Generally

A. The Center may disclose PHI to a business associate who performs a function or provides services to the Center. The Center may allow a business associate to create or receive PHI on their behalf only if the Center obtains satisfactory assurance that this business associate will safeguard the PHI.

B. In order to disclose PHI to a business associate, the Center will need to have a written contract with the business associates (Form 13).

C. A business associate is any person or organization that provides certain functions, activities, or services for the Center, involving the use and/or disclosure of PHI. A business associate is not a member of the workforce of the Center.

D. A business associate includes, but is not limited to, the following:

- Claims processing or administration
- Data analysis
- Processing
- Utilization review
- Quality assurance
- Billing
- Benefit management
- Center management
- Legal
- Actuarial
- Accounting
- Consulting
- Data Aggregation
- Management
- Accreditation

Business associate also includes patient safety organizations (PSOs), health information organizations (HIOs) and subcontractors. A governmental health benefit program (e.g. Medicare, Medicaid) is not a business associate.

E. The Center may rely on a business associate's representations as to the amount of information that is minimally necessary for the business associate to perform its functions.

F. The Center should require that a request for PHI from a business associate have a stated purpose and a representation that the information requested is the minimum necessary.

G. The Center should prohibit disclosure of any information pursuant to a request that does not meet these requirements.

Policy 13.1: Uses and Disclosures of Protected Health Information

A. Purpose.

The purpose of the Policy for the Retention of Protected Health Information (“The Policy”) is to prevent the risk of unauthorized disclosures of Protected Health Information (“PHI”) by the Center, any member of the Center (“Member”) or any independent contractor (“Independent Contractor”).

B. General Introduction.

The Center serves as a business associate each time it enters into a business associate agreement with a covered entity to help the covered entity carry out its health care activities and functions involving PHI. This Policy is to prevent any disclosure by the Center, Members, or Independent Contractors that is not authorized under 45 CFR § 164.502.

C. Individuals Subject to this Policy.

This Policy applies to all Members of the Center, including all employees, volunteers, interns and any other person whose conduct is under the direct control of the Center in the performance of work for or on behalf of the Center, including but not limited to Independent Contractors.

D. Permitted Uses and Disclosures.

The Center, Members, and Independent Contractors may only disclose PHI as permitted by the business associate contract or any other arrangement with a covered entity or as required by law.

E. Required Uses and Disclosures.

The Center shall disclose PHI when required by the Secretary of Health and Human Services to investigate or determine the Center’s compliance with HIPAA. The Center shall also disclose PHI to the covered entity, individual, or designee of the individual upon request.

F. Sale of PHI.

The sale of PHI by the Center, Members, and Independent Contractors is forbidden.

G. Minimum Necessary Standard.

When using or disclosing PHI or when requesting PHI from another covered entity or business associate, the Center, Members, and Independent Contractors must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. However, the Minimum Necessary standard does not apply to disclosures to or requests by a health care provider for treatment, uses or disclosures made to the individual, disclosures made to the Secretary of Health and Human Services, and disclosures required by law.

Policy 13.2: Covered Entity Policy for Uses and Disclosures of Protected Health Information

A. Purpose.

The purpose of the Policy for the Retention of Protected Health Information (“The Policy”) is to prevent the risk of unauthorized disclosures of Protected Health Information (“PHI”) by Georgia Mountains Health Services (“Covered Entity”).

B. General Introduction.

Georgia Mountains Health Services serves as a business associate each time it enters into a business associate agreement with a covered entity to help the covered entity carry out its health care activities and functions involving PHI. This Policy is to prevent any disclosure by Georgia Mountains Health Services, Members, or Independent Contractors that is not authorized under the HIPAA Security Rule.

C. Individuals Subject to this Policy.

This Policy applies to all Members of Georgia Mountains Health Services, including all employees, volunteers, interns and any other person whose conduct is under the direct control of Georgia Mountains Health Services in the performance of work for or on behalf of Georgia Mountains Health Services, including but not limited to Independent Contractors.

D. Permitted Uses and Disclosures.

Georgia Mountains Health Services is permitted to disclose PHI as follows:

- (i) To the individual;
- (ii) For treatment, payment, or health care operations;
- (iii) Incident to a use or disclosure otherwise permitted or

E. Required Uses and Disclosures.

Georgia Mountains Health Services shall disclose PHI when required by the Secretary of Health and Human Services to investigate or determine compliance with HIPAA. Georgia Mountains Health Services shall also disclose PHI to the covered entity, individual, or designee of the individual upon request.

F. Uses and Disclosures Requiring Authorization.

(a) Psychotherapy Notes

An Individual’s written authorization is required for any use or disclosure of Psychotherapy Notes except in the following circumstances:

- (1) To carry out the following treatment, payment or health care operations:
 - i. Use by the originator of the psychotherapy notes for treatment;
 - ii. Use or disclosure by Covered Entity for its own training programs in which

students, trainees or practitioners in mental health learn under supervision to practice or improved their skills in group, joint, family or individual counseling; or

iii. Use or disclosure by Covered Entity to defend itself in a legal action or other proceeding brought by the Individual;

- (2) To an Individual per the Individual's request or to provide the Individual with an accounting of disclosures required under HIPAA;
- (3) As may be required by law;
- (4) To a medical examiner or coroner;
- (5) To avert a serious threat to health or safety.

(b) Marketing

Georgia Mountains Health Services may not disclose an Individual's PHI for marketing purposes without the Individual's written authorization unless:

- (1) the marketing communication is in the form of a face-to face communication from Covered Entity to the Individual; or
- (2) the communication is in the form of a promotional gift of nominal value provided by Covered Entity. In addition, if the marketing involves direct or indirect remuneration to Covered Entity from a third party then the authorization must state that such remuneration is involved.

G. Uses and Disclosures for Which An Authorization is Not Required, but for which the Individual Must Have an Opportunity to Agree or Object.

The following uses and disclosures of PHI do not require an authorization, but require Covered Entity to give the individual an opportunity to agree or object to the use or disclosure:

- (a) Use and disclosure for facility directories;
- (b) Use and disclosure to persons involved in an individual's care and for notification purposes.

H. Uses and Disclosures Requiring Neither Authorization Nor Opportunity for the Individual to Agree or Object.

The following uses and disclosures of PHI require neither authorization nor an opportunity for the individual to agree or object to the use or disclosure:

- (a) Uses and disclosures to carry out treatment, payment or health care operations, except for the disclosure of psychotherapy notes or the disclosure of PHI for marketing purposes;
- (b) Uses and disclosures for public health activities;
- (c) Disclosures about victims of abuse, neglect or domestic violence;
- (d) Uses and disclosures for health oversight activities;
- (e) Disclosures for judicial and administrative proceedings;
- (f) Disclosures for law enforcement purposes;
- (g) Uses and disclosures about decedents;
- (h) Uses and disclosures for cadaveric organ, eye or tissue donation purposes;
- (i) Uses and disclosures for research purposes;

- (j) Uses and disclosures to avert a serious threat to health or safety;
- (k) Uses and disclosures for specialized government functions
- (l) Disclosures for workers' compensation purposes.

I. Disclosures by Whistleblower and Workforce Member Crime Victims.

Covered Entity is not considered to have violated the requirements of HIPAA if a member of its workforce or Business Associate discloses PHI that:

- (a) The workforce member or Business Associate believes in good faith that Covered Entity engaged in unlawful conduct that violates professional or clinical standards, or that the care, services, or conditions provided by Covered Entity potentially endangers patients, workers, or the public;
- (b) The disclosure is to:
 - (1) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee relevant conduct or conditions of Covered Entity or to appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by Covered Entity;
 - (2) An attorney retained by or on behalf of the workforce member or Business Associate for the purpose of determining legal options of workforce member or Business Associate with regard to the alleged conduct;
- (c) The workforce member disclosing PHI was the victim of a criminal act provided that PHI disclosed is about suspected perpetrator of the criminal act.

J. Valid Authorization.

In order to be valid, an authorization must contain the following elements:

- (a) A written form in plain language that provides that the Individual who signs the form will be provided with a copy of the signed document and that Covered Entity also will retain a copy of the document. Verbal authorization is not valid.
- (b) A description of the PHI to be used or disclosed that identifies the information in a specific and meaningful fashion.
- (c) The name or other specific identification of the person(s) or class of persons, authorized to make the requested use or disclosure
- (d) The name or other specific identification of the person(s), or class of persons, to whom Covered Entity may make the requested use or disclosure.
- (e) A description of each purpose of the requested use or disclosure.
- (f) An expiration date or expiration event that relates to the Individual or the purpose of the use or disclosure. [Note: The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of PHI for research, including for the creation and maintenance of a research database or research repository.]
- (g) The signature of the Individual and date, or if the authorization is to be signed by a personal representative of the Individual, the representative's signature along with a statement of the representative's authority to act for such individual.

- (h) A statement of the Individual's right to revoke the authorization in writing along with a description of how the Individual may revoke the authorization along with a description of any HIPAA-permitted fashion in which PHI may be used after revocation, e.g., use of PHI obtained in while authorization was in effect.
- (i) A statement as to whether or not treatment, payment or enrollment will or will not be conditioned upon signing the authorization.
- (j) A statement of the potential for information disclosed pursuant to the authorization to be re-disclosed by the person(s) who receive the information and no longer be protected by HIPAA requirements.
- (k) If the authorization is for research purposes and the researcher wants to defer the Individual's right to access his/her research records until the end of the research study, then a statement to this effect must also be included in the Authorization.

K. Defective Authorization.

An authorization will be invalid if it contains any of the following defects:

- (a) The expiration date has passed or Covered Entity knows that the expiration event has occurred;
- (b) The authorization has not been filled out completely such that one of the mandatory elements is not present;
- (c) The authorization is inappropriately combined with another document or inappropriately conditions treatment, payment, enrollment or eligibility on signing the authorization;
- (d) Covered Entity knows that any material information that is set forth in the authorization is false.

L. Prohibition Against Combining Authorizations with Other Documents.

An authorization may not be combined with any other document, except as follows:

- (a) An authorization to be used in a research project may be combined with the informed consent document that will be used in the research project;
- (b) An authorization for the use or disclosure of psychotherapy notes may only be combined with another authorization for the use or disclosure of psychotherapy noted;
- (c) An authorization that does not pertain to psychotherapy notes and that is not conditioned on anything may be combined with another authorization.

M. Prohibition Against the Conditioning of Authorizations.

Covered Entity may not condition treatment, payment, enrollment in a health plan or eligibility for benefits on an individual signing an authorization except as follows:

- (a) For research-related treatment;
- (b) For health plan enrollment, eligibility, risk rating or underwriting determination, provided that the authorization doesn't ask for the use or disclosure of psychotherapy notes.
- (c) For providing health care solely for the purpose of creating PHI for disclosure to a third party (e.g., conducting a physical on behalf of an employer for determining fitness related to performance of a job duty).

- (d) **Revocation of Authorization:** An Individual may revoke his/her authorization at any time by sending a written notice of revocation to the party to whom the authorization was provided or to party designated in the notice of privacy practices (i.e., medical records department of the facility at which the Individual received his/her care). Revocation, however, will not be effective with regard to any action that the Emory Covered Component has taken in reliance on the authorization, or if the authorization was obtaining as a condition of obtaining insurance.

N. Sale of PHI.

The sale of PHI by Covered Entity is forbidden.

O. Minimum Necessary Standard.

When using or disclosing PHI or when requesting PHI from another covered entity or business associate, the Center, Members, and Independent Contractors must make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. However, the Minimum Necessary standard does not apply to disclosures to or requests by a health care provider for treatment, uses or disclosures made to the individual, disclosures made to the Secretary of Health and Human Services, and disclosures required by law.

Policy Fourteen: Security Administrative Safeguards

The Final Security Rule requires establishment of a formal security management process to create, administer and provide oversight of policies to address the full range of security issues and to ensure the prevention, detection, containment, and correction of security violations. This process is to include implementation features consisting of risk analysis, risk management, and sanction and security policies.

See IT Security Policies.

I. REQUIRED SPECIFICATIONS

Policy 14.1 Security Management Process

- 1) **Risk Analysis:** The Center must conduct a thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of the EPHI controlled by the Center.
- 2) **Risk Management:** The Center must implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. *See IT Security Policies.*
- 3) **Sanction Policy:** The Center must apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the Center.
- 4) **Information System Activity Review:** The Center must implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident reports.

Policy 14.2 Assigned Security Responsibility

The Security Rule requires designation of an Information Security Officer who is responsible for the implementation of and ongoing adherence to information security policies and procedures. Responsibilities of the information security officer include, but are not limited to:

- 1) Provide guidance and assistance in identifying, implementing, and maintaining organization-wide information security policies and procedures that comply with the Final Security Rule.
- 2) Provide direct training and oversight to all employees, contractors, alliance, or other third parties with information security clearance on the information security policies and procedures.
- 3) Initiate activities to create information security awareness within the organization.
- 4) Perform and document information security risk analysis and audit.
- 5) Serve as the information security liaison to clinical administration and behavioral systems as they integrate with their data users.
- 6) Review all system-related security planning throughout the network and act as a liaison to information technology professionals.
- 7) Monitor compliance with the security policies and procedures.

Policy 14.3 Security Incident Procedures

The Security Rule requires implementation of policies and procedures to address security incidents.

In accordance with the Breach Notification Rules, the Center must identify, and respond to, suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the Center; and document security incidents and their outcomes.

Policy 14.4 Contingency Plan (Required)

The Security Rule requires establishment (and implementation as needed) of policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.

- 1) **Data Backup Plan:** The Center must establish and implement procedures to create and maintain retrievable exact copies of EPHI.
- 2) **Disaster Recovery Plan:** The Center must establish (and implement as needed) procedures to restore lost data.
- 3) **Emergency Mode Operation Plan:** The Center must establish (and implement as needed) procedures to enable continuation of critical processes to ensure the security of EPHI while operating in emergency mode.

Policy 14.5 Evaluation

The Security Rule requires the performance of periodic technical and nontechnical evaluations, based initially upon the standards implemented under the Security Rule, and subsequently in response to environmental or operational changes affecting the security of EPHI. These evaluations should measure the Center's compliance with the HIPAA Security Rule.

Policy 14.6 Business Associate Agreements

The Center, in accordance with the Security Rule, may permit a business associate to create, receive, maintain, or transmit EPHI on the Center's behalf only if the Center obtains satisfactory assurances that the business associate will appropriately safeguard the information through a written contract. Any Center which violates the satisfactory assurances it provides as a business associate of another Center will be in noncompliance with the standards, implementation specifications and requirements of the Security Rule.

- 1) **Business Associate Contracts:** The Center will establish contracts with its business associates which will:
 - a. Provide that the business associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the EPHI that it creates, receives, maintains, or transmits on behalf of the Center;
 - b. Ensure that any agent, including a subcontractor, to whom the business associate provides such information, agrees to implement reasonable and appropriate safeguards to protect it;

- c. Report to the Center any security incident of which the business associate becomes aware; and
- d. Authorize termination of the contract by the Center if the Practice determines that the business associate has violated a material term of the contract.

2) **Business Associates Required by Law:** The Center may permit a business associate to create, receive, maintain, or transmit EPHI on its behalf to the extent necessary to comply with a legal mandate without meeting the requirements above, provided that the Center attempts in good faith to obtain satisfactory assurances as required by the Security Rule, and documents the attempts and the reasons that these assurances cannot be obtained.

3) **Non-Compliance:** The Center is not in compliance with the standards in the Security Rule and this policy if the Center knew of a pattern of activity of a business associate which constitutes a material breach or violation of the business associate’s obligation under the contract or other arrangement, unless the Center took reasonable steps to cure the breach or end the violation, as applicable, and if such steps were unsuccessful then:

- a. Terminated the contract or arrangement, if feasible; or
- b. If termination is not feasible, reported the problem to the Secretary of Health and Human Services.

Policy 14.7 Exceptions to this Standard

Satisfactory assurances in a written contract need not be obtained for:

- 1) The transmission by the Center of EPHI to another healthcare Center concerning treatment of an individual;
- 2) The transmission of EPHI by a group health plan or an HMO or health insurance carrier on behalf of a group health plan to a plan sponsor, to the extent which the requirements of the Security Rule apply and are met; or
- 3) The transmission of EPHI from or to other agencies providing the services when the entity is a health plan which is a government program providing public benefits, if the requirements of the Security Rule are met.

II. ADDRESSABLE SPECIFICATIONS

Policy 14.8 Workforce Security

The first addressable specification under the Security Rule deals with ensuring that personnel are supervised by a knowledgeable person, maintaining a record of access authorizations, and ensuring that operating and maintenance personnel have proper access authorization by establishing personnel clearance procedures, establishing and maintaining personnel security policies and procedures, and ensuring that systems users have proper training.

- 1) **Authorization and/or Supervision:** The Center shall implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed.
- 2) **Workforce Clearance Procedures:** The Center shall implement procedures to determine whether the access of a workforce member to EPHI is appropriate.

- 3) **Termination Procedures:** The Center shall implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by the Security Rule.

Policy 14.9 Information Access Management (Addressable)

Two other addressable specifications under the Security Rule involve the establishment and maintenance of formal, documented policies and procedures defining levels of access for all personnel authorized to access EPHI and how that access is granted and modified.

- 1) **Access Authorization:** The Center shall implement policies and procedures for granting access to EPHI through access to a workstation, transaction, program, process, or other mechanism.
- 2) **Access Establishment and Modification:** The Center shall implement policies and procedures that, based upon the Center's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.

Policy 14.10 Security Awareness and Training

The Security Rule's next addressable specifications are the implementation of a security awareness and training program for all members of the workforce, including management.

- 1) **Security Reminders:** The Center shall post periodic security updates.
- 2) **Protection from Malicious Software:** The Center shall establish procedures for guarding against, detecting, and reporting malicious software.
- 3) **Log-in Monitoring:** The Center shall establish procedures for monitoring log-in attempts and reporting discrepancies.
- 4) **Password Management:** The Center shall establish procedures for creating, changing, and safeguarding passwords.

Policy 14.11 Contingency Plan (Addressable)

- 1) **Testing and Revision Procedures:** The Center shall implement procedures for periodic testing and revision of contingency plans.
- 2) **Application and Data Criticality Analysis:** The Center shall assess the relative criticality of specific applications and data in support of contingency planning.

Policy Fifteen: Security Physical Safeguards

The HIPAA Security Rule requires documentation of physical safeguards to protect data integrity, confidentiality, and availability by providing medical controls, physical access controls, policies and guidelines on workstation use, a secure workstation location, and security awareness training.

See IT Security Policies.

I. REQUIRED SPECIFICATIONS

Policy 15.1 Workstation Use

The Security Rule requires the implementation of policies and procedures which specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation which can access EPHI.

Policy 15.2 Workstation Security

Access to EPHI must be restricted to authorized users.

Policy 15.3 Device and Media Controls (Required)

The Security Rule requires the implementation of policies and procedures governing the receipt and removal of hardware and electronic media which contain EPHI into and out of a facility, and the movement of these items within the facility.

- 1) **Disposal:** The Center must implement policies and procedures to address the final disposition of electronic media on which EPHI is stored in accordance with the Breach Notification Rules.
- 2) **Media Re-use:** The Center must implement procedures for removal of EPHI from electronic media before that media is made available for re-use.

II. ADDRESSABLE SPECIFICATIONS

Policy 15.4 Facility Access Controls

The Security Rule mandates that the Center address the implementation of policies and procedures which limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.

- 1) **Contingency Operations:** The Center shall establish (and implement as needed) procedures which allow facility access for the purpose 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:** The Center shall implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- 3) **Access Control and Validation Procedures:** The Center shall implement procedures to control and validate access to facilities based on a person's role or function, including visitor control and control of access to software programs for testing and revision.

- 4) **Maintenance Records:** The Center shall implement policies and procedures to document repairs and modifications to the physical components of a facility related to security (for example: hardware, walls, doors, and locks).

Policy 15.5 Device and Media Controls (Addressable)

- 1) **Accountability:** The Center shall maintain a record of the movements of hardware and electronic media and any person responsible therefore.
- 2) **Data Backup and Storage:** The security and integrity of the data residing on the Center's computer systems and data stored for archival purposes will be maintained by an adequate backup process and will be properly secured in accordance with the Breach Notification Rules. The Center shall create a retrievable, exact copy of EPHI, when needed, before movement of equipment.

Policy Sixteen: Security Technical Safeguards

The HIPAA Security Rule requires implementation of technical safeguards to allow access only to those persons or software programs which have been granted access rights as specified in the Administrative Safeguards.

See IT Security Policies.

I. REQUIRED SPECIFICATIONS

Policy 16.1 Access Control (Required)

- 1) **Unique User Identification:** The Center must assign a unique name and/or number for identifying and tracking user identity.
- 2) **Emergency Access Procedure:** The Center must establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency.

Policy 16.2 Audit Controls

Under the Security Rule, the Center must establish audit controls in the form of hardware, software, and/or procedural mechanisms that record and examine activity in information systems which contain or use EPHI.

Policy 16.3 Person or Entity Authentication

The Security Rule requires that procedures be in place to verify that a person or entity seeking access to EPHI is the one claimed.

II. ADDRESSABLE SPECIFICATIONS

Policy 16.4 Access Control (Addressable)

- 1) **Automatic Logoff:** The Center shall establish electronic procedures which terminate an electronic session after a predetermined time of inactivity.
- 2) **Encryption and Decryption:** The Center shall establish a mechanism to encrypt and decrypt EPHI in accordance with the Breach Notification Rules.

Policy 16.5 Integrity

Covered entities must address implementation of policies and procedures to protect EPHI from improper alteration or destruction.

- 1) **System Security:** The security and integrity of the data residing on the Center's computer systems will be maintained by tracking, recording and auditing of access to protected health information (PHI) and responding to unauthorized access attempts in accordance with the Breach Notification Rules.

- 2) **Mechanism to Authenticate EPHI:** The Center shall establish and implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner.

Policy 16.6 Transmission Security

The Security Rule requires the addressing of technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network.

- 1) **Integrity Controls:** The Center shall establish and implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of.
- 2) **Encryption:** The Center shall establish and implement a mechanism to encrypt EPHI in accordance with the Breach Notification Rules.

Policy Seventeen: Security Policies/Procedures and Documentation

Policy 17.1 Policies and Procedures

The Center must establish and implement reasonable and appropriate policies and procedures to comply with the Security Rule. The Center may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with the Security Rule.

See IT Security Policies.

Policy 17.2 Documentation

The Center will establish and maintain the policies and procedures implemented to comply with the Security Rule in written (may be electronic) form.

If an action, activity or assessment is required by the Security Rule, the Center will maintain a written (may be electronic) record of the action, activity or assessment.

- 1) **Time Limit:** The Center will retain the documentation required by the Security Rule for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.
- 2) **Availability:** The Center will make the documentation available to those persons responsible for implementing the procedures to which the documentation pertains.
- 3) **Updates:** The Center will review the documentation periodically, updating it as needed, in response to environmental or operational changes affecting the security of its EPHI.

Policy 17.3: Covered Entity General HIPAA Compliance and Administrative Safeguard Policy

Introduction

Georgia Mountains Health Services, Inc adopted this HIPAA Compliance Plan in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act of 2009, as well as all implementing regulations.

Assumptions

Georgia Mountains Health Services, Inc recognizes its status as a Covered Entity under HIPAA.

Georgia Mountains Health Services, Inc will comply with HIPAA.

Policy

It is the policy of Georgia Mountains Health Services, Inc to become and remain in full compliance with all requirements of HIPAA applicable to Covered Entities.

It is the policy of Georgia Mountains Health Services, Inc to fully document all HIPAA compliance-related activities and efforts.

All owners, officers, employees, volunteers, independent contractors, and other persons whose conduct, in the performance of work for Georgia Mountains Health Services, Inc, is under the direct control of Georgia Mountains Health Services, Inc (collectively, the “Workforce” of Georgia Mountains Health Services, Inc) are responsible for following this HIPAA Compliance Plan. Workforce members who violate this HIPAA Compliance Plan may be subject to discipline up to and including termination.

This HIPAA 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 Georgia Mountains Health Services’ PHI Compliance Plan are:

To assist Georgia Mountains Health Services in identifying PHI.

To assist Georgia Mountains Health Services in avoiding improper uses and disclosures of PHI.

To establish compliance standards and procedures for members of Georgia Mountains Health Services’ Workforce that are reasonably capable of reducing the prospect of violating HIPAA.

To appoint a Privacy Officer and Security Officer who are high-level and trustworthy employees with the responsibility to implement and oversee Georgia Mountains Health Services’ compliance with the standards and procedures set forth in this HIPAA Compliance Plan.

To effectively communicate the compliance standards, policies and procedures set forth

in this HIPAA Compliance Plan to all members of Georgia Mountains Health Services' 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 HIPAA 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 Georgia Mountains Health Services' Workforce can report perceived wrongful uses and disclosures of PHI by others without fear of retribution. *See Reporting of Non-Compliance and Non-Retaliation Policy.*

To respond appropriately to non-compliance after detection and to prevent recurrence, which may require modifications to this HIPAA Compliance Plan.

Definitions

For purposes of this HIPAA Compliance Plan, the following terms shall have the following meanings:

"Breach" shall mean the unauthorized acquisition, access, use, or disclosure of PHI in a manner not permitted by HIPAA.

"Business Associate" shall mean a person or entity who performs certain functions or activities on behalf of a "covered entity," as such term is defined by HIPAA (i.e., a healthcare provider, health plan, healthcare clearinghouse or personal health record vendor), which involve the creation, receipt, maintenance, or transmission of PHI on behalf of the covered entity.

"Business Associate Agreement" shall mean an agreement which addresses Covered Entity's use, disclosure, creation, receipt, maintenance, or transmission of PHI on behalf of a HIPAA Client.

"Designated Record Set" shall mean a group of records maintained by or for a HIPAA Client that consist of: (a) the medical records and billing records about individuals; (b) the enrollment, payment, claims adjudication, and case or medical management record systems; or (c) records used, in whole or in part, by or for a HIPAA Client to make decisions about individuals. For purposes of this definition, the term "record" means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for a HIPAA Client.

"HIPAA" shall mean: (a) the Health Insurance Portability and Accountability Act of 1996, and regulations promulgated there under, including the Privacy, Security, Breach Notification and Enforcement Rules at 45 C.F.R. Parts 160 and 164, and any subsequent amendments or modifications thereto, and (b) the HITECH Act, and regulations promulgated there under, and any subsequent amendments or modifications thereto.

"HIPAA Client" shall mean one of the following types of persons or entities for which Covered Entity does work for:

Health Care Providers, which are persons or entities who furnish, bill or are paid for health care services in the normal course of business. (Examples include: physician practices, hospitals, skilled nursing facilities, surgery centers, outpatient rehabilitation facilities, home health agencies, pharmacies, and durable medical equipment providers.)

Health Plans, which are individual or group plans that provide or pay the cost of medical care. (Examples include: HMOs, private health insurers, group health plans, and employee welfare benefit plans.)

Health Care Clearinghouses, which are entities that process PHI in a non-standard HIPAA format or containing non-standard data into a standard format. (Examples include: billing companies, repricing companies, and value added networks.)

Personal Health Record Vendors, which are entities offering or maintaining an electronic record of PHI on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual.

"HITECH Act" shall mean 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.

"PHI" or "Protected Health Information" shall mean any information, whether oral, written or electronic: (a) that relates to the past, present or future physical or mental condition of an individual; or (b) the provision of health care to an individual; or (c) the past, present or future payment for the provision of health care to an individual; and (d) 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.

"Privacy Rules" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and 164, as may be amended, modified or superseded, from time to time.

"Required by Law" shall have the meaning set forth in 45 C.F.R. § 164.103, including, without limitation, a mandate contained in law that compels a HIPAA Client or Covered Entity to make a use or disclosure of PHI and that is enforceable in a court of law.

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

"Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification or destruction of electronic PHI.

"Security Rules" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 C.F.R. Parts 160 and 164, as may be amended, modified or superseded from time to time.

"Unsecured PHI" shall have the meaning set forth in the HITECH Act, including, without limitation, PHI 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 individuals.

"Workforce" shall include Covered Entity's owners, officers, employees, volunteers and other persons whose conduct, in the performance of work for Covered Entity, is under Covered Entity's direct control, whether or not they are paid by Covered Entity, such as independent contractors.

Privacy Officer Policy

Introduction

This policy governs the designation and duties of a HIPAA Privacy Officer for Georgia Mountains Health Services, Inc. The Privacy Officer shall be a high-level and trustworthy employee of Georgia Mountains Health Services.

Assumptions

To the extent required for Business Associates, Georgia Mountains Health Services must comply with HIPAA concerning the assignment of HIPAA responsibilities to a Privacy Officer.

The assignment of overall HIPAA responsibility is an important and integral part of our overall risk management process.

Policy

It is the policy of Georgia Mountains Health Services to designate a HIPAA Privacy Officer.

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 HIPAA activities.

The Privacy Officer shall work closely with the Security Officer in carrying out his/her duties. The position of Privacy Officer and Security Officer may be held by one person.

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

The responsibilities and duties of the Privacy Officer shall focus on the privacy of PHI and include the following:

To assist with the development of our HIPAA 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 HIPAA

Compliance Plan to ensure our compliance with HIPAA.

To keep apprised of changes to HIPAA. As part of this responsibility, the Privacy 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 HIPAA Compliance Plan, new HIPAA 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 HIPAA 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 HIPAA issues and to report suspected violations of our HIPAA Compliance Plan or HIPAA.

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

To receive and investigate all complaints relating to possible HIPAA violations and/or violations of our HIPAA Compliance Plan, and to record/document the results of any such complaints.

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

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

Security Officer Policy

Introduction

This policy governs the designation and duties of a HIPAA Security Officer for Georgia Mountains Health Services. The Security Officer shall be a high-level and trustworthy employee of Georgia Mountains Health Services.

Assumptions

To the extent required for Georgia Mountains Health Services, the organization must comply with HIPAA concerning the assignment of PHI security responsibilities to the Security Officer.

The assignment of overall HIPAA security responsibility is an important and integral part of our overall risk management process.

Policy

It is the policy of Georgia Mountains Health Services to designate a HIPAA Security Officer.

The Security Officer is responsible for the overall implementation and operation of the security of PHI, both electronic and other forms, and shall have authority to review all documents and other information relevant to HIPAA security activities.

The Security Officer shall work closely with the Privacy Officer in carrying out his/her duties. The position of Privacy Officer and Security Officer may be held by one person.

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

The responsibilities and duties of the Security Officer shall focus on the security of PHI and include the following:

To assist with the development of our HIPAA Compliance Plan, which sets forth the legal and ethical standards, policies and procedures to be followed by members of Covered Entity's Workforce.

To implement and enforce the standards, policies and procedures set forth in our HIPAA Compliance Plan to ensure compliance with the Security Rules.

To keep apprised of changes to the Security Rules. 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 assist the Privacy Officer in the investigation of alleged violations of Covered Entity's HIPAA Compliance Plan and HIPAA, and to work with appropriate parties to handle violations promptly, properly and consistently.

In conjunction with the Privacy Officer, to report to Covered Entity's Governing Body on the operation and implementation of this HIPAA Compliance Plan.

Policy 17.4: Covered Entity Mobile Devices Policy

EXECUTIVE SUMMARY: All mobile devices (both personal mobile devices and mobile devices supplied by a covered entity) used to access PHI should be password-protected to ensure the security of PHI and other sensitive information.

Covered Entity Mobile Devices Policy

A. Purpose.

The purpose of this Mobile Devices Policy is to allow for the authorized use of laptops, smart phones, and other portable computing and communications devices (“Mobile Devices”) at the covered entity (“Covered Entity”) by Covered Entity’s employees (“Employees”), officers (“Officers”), independent contractors (“Independent Contractors”), and business associates (“Business Associates”) with whom Covered Entity has a written business associate agreement (“Business Associate Agreement”).

B. General Introduction.

The use of Mobile Devices allows for greater efficiency in dealing with Georgia Mountains Health Services’ clients, but the use of Mobile Devices poses potential risks to digital information such as Protected Health Information (“PHI”). The Mobile Devices Policy (“The Policy”) intends to manage such potential risks.

The use of Mobile Devices under the Policy is a privilege that may be terminated at any time for any violation, or as a sanction for violating any other Georgia Mountains Health Services policies. Violation of the Policy may also be grounds for other sanctions. In accordance with 45 CFR § 164.306, Covered Entities shall take measures to protect PHI and other digital information while considering the Covered Entity’s size, financial capabilities technical infrastructure, hardware and software security capabilities, and the probability and criticality of potential risks to PHI.

C. Individuals Subject to this Policy.

This Policy applies to all Officers, Employees, Volunteers, Interns, and Independent Contractors of Georgia Mountains Health Services, any other persons whose conduct is under the direct control of Georgia Mountains Health Services, and Business Associates subject to a written Business Associate Agreement with Georgia Mountains Health Services.

D. Information Subject to this Policy.

This Policy applies to all information owned by the Center, as well as all private, sensitive or confidential information that the Center is obliged by law or contract to protect against unauthorized use, disclosure, copying or alteration. This includes, without limitation:

- Protected Health Information.
- All intellectual property.
- Confidential personal or organizational information, such as employee records and financial information.
- Sensitive visual information, such as patient faces or physical security safeguards that may be subject to photographing or video capture.
- Metadata pertaining to events and activities occurring in or by use of a Mobile Device, or any other electronic computing or communication device.

E. Devices Subject to this Policy.

This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and is capable of receiving, processing, or transmitting digital information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Portable Device, or any equipment capable of recording, storing or transmitting digital information (such as copiers or medical devices). Mobile Devices therefore include but are not limited to smart phones, digital music players, hand-held computers, laptop computers, tablet computers, and personal digital assistants (PDAs).

This Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased and provided by Covered Entity or any other Business Associate or Covered Entity.

F. Encryption.

All sensitive data subject to this Policy shall be encrypted to prevent unauthorized access. For these purposes, encryption shall be in the form of password protection.

G. Password or other user authentication.

Access to each Mobile Device must be controlled by a password or PIN number. Persons subject to this Policy may not share the password or PIN number used to access a Mobile Device with anybody.

H. Use of Wireless Networks.

When sending, accessing, or receiving data subject to this Policy, persons subject to this Policy shall use a secure WI-FI network that uses a password and secure encryption methods to send data wirelessly between a Mobile Device and the Internet connection point. Persons subject to this Policy shall never send, access, or receive any data subject to this policy over a public WI-FI network unless it is through a virtual private network (VPN).

I. File-sharing Applications.

Persons subject to this Policy may not use file-sharing applications for any digital

data covered by this Policy.

J. Maintaining Physical Control of Mobile Device.

Persons subject to this Policy shall physically secure a Mobile Device when it is not in use to prevent unauthorized users from accessing data through or on the device. When a Mobile Device is not in use, persons subject to this policy shall lock the screen of the Mobile Device. Persons subject to this policy shall keep the Mobile Device in physical possession, or keep it physically secured if it cannot be kept in physical possession. Persons subject to this policy shall not allow others to use or access the Mobile Device.

K. Deleting Stored Information Before Discarding a Mobile Device.

Before any Mobile Device is discarded, all information stored on the Mobile Device that is subject to this Policy shall be deleted.

L. Covered Entity Capacity.

Covered Entity cannot guarantee with full certainty that Covered Entity has the technical or financial capacity to do the following:

- Provide a firewall for a wireless network.
- Provide security software for Mobile Devices.
- Provide the ability to remotely wipe or erase all data from a lost or stolen Mobile Device.
- Provide auditing of Mobile Devices.

M. Mobile Device Auditing.

Covered Entity may audit Covered Entity's Mobile Devices, as well as any other Mobile Devices through which PHI entrusted to Covered Entity has been transacted (including Mobile Devices of Employees, Officers, Independent Contractors, and Business Associates).

Policy 17.5: Covered Entity Policy for Devices and Electronic Media

A. Purpose.

The purpose of this Electronic Media Policy (“The Policy”) is to allow for the authorized use of electronic media (“Electronic Media”) at the covered entity (“Covered Entity”) by Covered Entity’s employees (“Employees”), officers (“Officers”), independent contractors (“Independent Contractors”), and business associates (“Business Associates”) with whom Covered Entity has a written business associate agreement (“Business Associate Agreement”).

B. General Introduction.

The HIPAA Security Rule defines Electronic Media as the following:

- (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card;
- (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

The use of Electronic Media under this Policy is a privilege that may be terminated at any time for any violation, or a sanction for violating any other Covered Entity policies. Violation of the Policy may also be grounds for other sanctions. In accordance with 45 CFR § 164.306, the Center shall take measures take to protect PHI and other digital information while considering Covered Entity’s size, financial capabilities technical infrastructure, hardware and software security capabilities, and the probability and criticality of potential risks to PHI.

C. Individuals Subject to this Policy.

This Policy applies to all Officers, Employees, Volunteers, Interns, and Independent Contractors of Covered Entity, any other persons whose conduct is under the direct control of Covered Entity, and Business Associates subject to a written Business Associate Agreement with Covered Entity.

D. Information Subject to this Policy.

This Policy applies to all information owned by Covered Entity, as well as all private, sensitive or confidential information that the Center is obliged by law or contract to protect against unauthorized use, disclosure, copying or alteration. This includes, without limitation:

- Protected Health Information.
- All intellectual property.
- Confidential personal or organizational information, such as employee records and financial information.
- Sensitive visual information, such as patient faces or physical security safeguards that may be subject to photographing or video capture.

E. Removal of Information.

Any information subject to this policy shall be removed from Electronic Media before the Electronic Media is made available for re-use.

F. Data Backup and Storage.

Individuals subject to this policy shall create a retrievable, exact copy of any information subject to this policy, when needed, before the movement of equipment or Electronic Media.

G. Encryption.

Whenever possible, information subject to this policy on a device or Electronic Media shall be encrypted. However, encryption in this scope may be limited to the use of a password or PIN for user authentication.

Policy 17.6: Covered Entity Transaction Policy

A. Purpose.

The purpose of this Transaction Policy is to allow for a safe transaction of Protected Health Information (“PHI”) while preventing unauthorized access to such information. The covered entity (“Covered Entity”) and any employee (“Employee”), officer (“Officer”), (“Member”), business associate (“Business Associate”) subject to a business associate agreement (“Business Associate Agreement”) with Covered Entity, and independent contractor (“Independent Contractor”) of Covered Entity is subject to this policy.

B. Individuals Subject to this Policy.

This Policy applies to Covered Entity, including all employees, volunteers, interns and any other person whose conduct is under the direct control of Covered Entity in the performance of work for or on behalf of the Covered Entity, including but not limited to Independent Contractors, as well as Business Associates with whom Covered Entity has a written Business Associate Agreement.

C. Protected Health Information.

This Policy applies to all information owned by the Center, as well as all private, sensitive or confidential information that the Center is obliged by law or contract to protect against unauthorized use, disclosure, copying or alteration. This includes, without limitation:

- Protected Health Information.
- All intellectual property.
- Confidential personal or organizational information, such as employee records and financial information.
- Sensitive visual information, such as patient faces or physical security safeguards that may be subject to photographing or video capture.
- Metadata pertaining to events and activities occurring in or by use of a Mobile Device, or any other electronic computing or communication device.

D. Use of Wireless Networks.

When sending, accessing, or receiving information subject to this Policy, an individual subject to this policy shall use a secure WI-FI network that uses a password and secure encryption methods to send data wirelessly between any electronic device and the Internet connection point. An individual subject to this policy shall never send, access, or receive any information subject to this policy over a public WI-FI network unless it is through a virtual private network (VPN).

Public WI-FI networks include, but are not limited to, WI-FI networks available at airports, hotels, coffee shops, and other locations. Public WI-FI networks also include in-flight WI-FI networks onboard aircrafts.

D. Mobile Hotspot Connections.

Encrypted information subject to this policy may be transmitted over a private, secured mobile hotspot connection. However, an individual subject to this policy must never use a default password generated by a device or mobile phone, but must the individual must create a password to use. No individual subject to this policy may transact any information subject to this policy over a mobile hotspot connection that is not secured or that is secured using a password generated by the device or mobile phone.

D. Encryption of Information.

All information subject to this policy that is sent electronically shall be encrypted by means of either password protection or PIN authentication.

E. File-sharing Applications.

Individuals subject to this Policy may never use any file-sharing application to transmit any information subject to this policy.

Policy Eighteen: Identity Theft Detection, Prevention, and Mitigation (Red Flag Rules)

The Federal Trade Commission requires each *creditor* that offers or maintains one or more *covered accounts* to develop and provide for the continued administration of a written Identity Theft Prevention Program (the Program) to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. If a Center extends credit to a consumer by establishing an account that permits multiple payments, that provider is a creditor offering a covered account and is subject to the Red Flag rules.

Policy 18.1 The Program

In designing its Program, the Center may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to patients or to the safety and soundness of the Center from identity theft.

Policy 18.2 Methods for Administering the Program

- (a) **Initial Approval:** The Center must obtain initial approval of the Program from either its board of directors or an appropriate committee of the board of directors.
- (b) **Oversight of Program.** Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:
- (1) Assigning specific responsibility for the Program's implementation;
 - (2) Reviewing reports prepared by staff regarding compliance by the Center with the Red Flag rules;
 - (3) Approving material changes to the Program as necessary to address changing identity theft risks.
- (c) **Reports.**
- (1) In general. Staff of the Center responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the Center with the Red Flag rules.
 - (2) Contents of report. The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the Center in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.
- (d) **Oversight of service provider arrangements.** Whenever the Center engages a service provider to perform an activity in connection with one or more covered accounts the Center should take steps to ensure that the activity of the service provider is conducted in accordance with policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, the Center could require the service

provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the Center, or to take appropriate steps to prevent or mitigate identity theft.

(e) **Training:** The Center must train staff, as necessary, to effectively implement the Program.

Policy 18.3 Identifying Relevant Red Flags

(a) **Risk Factors:** The Center should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

- (1) The types of covered accounts it offers or maintains;
- (2) The methods it provides to open its covered accounts;
- (3) The methods it provides to access its covered accounts; and
- (4) Its previous experiences with identity theft.

(b) **Sources of Red Flags:** The Center should incorporate relevant Red Flags from sources such as:

- (1) Incidents of identity theft that the Center has experienced;
- (2) Methods of identity theft that the Center has identified that reflect changes in identity theft risks; and
- (3) Applicable supervisory guidance.

(c) **Categories of Red Flags:** The Program should include relevant Red Flags from the following categories, as appropriate.

- (1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- (2) The presentation of suspicious documents;
- (3) The presentation of suspicious personal identifying information, such as a suspicious address change;
- (4) The unusual use of, or other suspicious activity related to, a covered account;
- (5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the Center.

Examples of Identity Theft Red Flags (Policy 18.3):

- Only Centers that are *creditors* that offer or maintain *covered accounts* (see Glossary for definitions) must have a written Identity Theft Prevention Program.
- The Program must be designed to detect, prevent, and mitigate identity theft.
- Because methods of identity theft and identity theft detection are continually evolving, no list can be considered comprehensive, and the Program must therefore be updated regularly.
- The examples provided in this document can serve as a guide for the types of events or activities that may constitute Red Flags for identity theft.
- This list may be used for training purposes.
- The World Privacy Forum maintains a regularly updated collection of materials and news about medical identity theft, including detailed FAQs, reports, public comments, speeches, and other materials at:

Policy 18.4 Detecting Red Flags

The Center should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

- (a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account
- (b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

Policy 18.5 Preventing and Mitigating Identity Theft

The Center should provide for appropriate responses to the Red Flags the Practice has detected that are commensurate with the degree of risk posed. In determining an appropriate response, the Center should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a patient's account records held by the Center or third party, or notice that a patient has provided information related to a covered account held by the Center to someone fraudulently claiming to represent the Center or to a fraudulent website. Appropriate responses may include the following:

- (a) Monitoring a covered account for evidence of identity theft;
- (b) Contacting the patient;
- (c) Changing any passwords, security codes, or other security devices that permit access to a covered account;
- (d) Reopening a covered account with a new account number;
- (e) Not opening a new covered account;
- (f) Closing an existing covered account;
- (g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- (h) Notifying law enforcement;
- (i) Placing a Red Flag alert in the victim's health care records;
- (j) John or Jane Doe file extraction; or
- (k) Determining that no response is warranted under the particular circumstances.

Examples of Centers for Mitigating Identity Theft:

- A Red Flag alert is a mechanism or tool that makes employees aware that there may be a problem with a particular chart or account.
- John or Jane Doe file extraction is a method for purging a medical record of all information that was entered as the result of fraudulent activity, in the case of substantiated identity theft.

Policy 18.6 Updating the Program

The Center should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to patients or to the safety and soundness of the Center from identity theft, based on factors such as:

- (a) The experiences of the Center with identity theft;
- (b) Changes in methods of identity theft;
- (c) Changes in methods to detect, prevent, and mitigate identity theft;
- (d) Changes in the types of accounts that the Center offers or maintains;
- (e) Changes in the business arrangements of the Center, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Policy Nineteen: Address Discrepancy Rule

A Center comes under the Address Discrepancy Rule if they use consumer credit reports. A *Notice of Address Discrepancy* is a notice sent to a Center by a consumer reporting agency (also known as a *credit bureau*) that informs the Center of a substantial difference between the address for the consumer that the Center provided to request the credit report and the address in the credit bureau's file for the consumer. The Notice of Address Discrepancy is required by the Fair Credit Reporting Act, and triggers obligations under the new rules. Any health care provider that orders a credit report on a consumer (even if only for Human Resources purposes) must comply with those obligations, regardless of whether the provider is a creditor subject to the Red Flag rules.

Policy 19.1 Address Discrepancy Obligations for Centers That Use Credit Reports

(a) **Verification:** When the Center receives a Notice of Address Discrepancy, the Center must have policies and procedures in place designed to enable the Center to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report. Examples of these policies and procedures may include:

(i) Comparing the information in the consumer report provided by the credit bureau with information the Center:

-Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP); and

-Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or

-Obtains from third-party sources; or

(ii) Verifying the information in the consumer report provided by the credit bureau with the consumer.

(b) **Reporting:** The Center must furnish an address for the consumer that the Center has reasonably confirmed is accurate to the credit bureau from whom it has received the Notice of Address Discrepancy if ALL of the following conditions are met:

(i) The Center can form a reasonable belief that the consumer report relates to the consumer about whom the Center requested the report, based on one of the methods in (a)(i) above or other reasonable means;

(ii) The Center establishes a continuing relationship with the consumer; and

(iii) The Center regularly and in the ordinary course of business furnishes information to the credit bureau (consumer reporting agency) from which the Notice of Address Discrepancy relating to the consumer was obtained.

Policy 19.2 Training

The Center must train staff, as necessary, to effectively respond to Notices of Address Discrepancy.

Policy Twenty: Breach Notification

Policy Statement

Protected health information should be secured to maintain confidentiality.

Purpose

In accordance with the Breach Notification Rules, the Center must make required breach notifications following the discovery of a breach of unsecured protected health information. The Privacy Officer is responsible for performing all risk assessments, keeping all documentation, and making all notifications as required by this Breach Notification Policy.

Procedures

For each individual whose unsecured protected health information (PHI) potentially has been breached, the Center will use the following three (3) step process to determine if breach notification is required:

Step One: The Center will determine whether there has been a breach of unsecured PHI.

A breach of unsecured PHI occurs if an individual's unsecured PHI is acquired, accessed, used, or disclosed, or is reasonably believed to have been accessed, acquired, used, or disclosed in an impermissible manner (*i.e.*, a manner not permitted under Subpart E of the Privacy Rule¹) which compromises the security or privacy of the unsecured PHI.

A breach of unsecured PHI has not occurred if:

The PHI was secured through the use of a technology or methodology specified in guidance from the U.S. Department of Health and Human Services to render PHI unusable, unreadable, or indecipherable to unauthorized individuals, such as by using encryption or destruction ; or

If a breach of unsecured PHI has not occurred:

No breach notification is required. The Center should balance the need to mitigate harm and protect the individual whose unsecured PHI has been breached with the potential to cause the patient unnecessary concern when no harm is anticipated in determining whether or not to give breach notification.

If a breach of unsecured PHI has occurred:

The Center will follow Step Two.

Step Two: The Center will determine, and should document, whether the incident is excluded from the definition of "breach" because it is:

¹ Subpart E of the Privacy Rule is codified at 45 C.F.R. Part 164. Permitted uses and disclosures of PHI pursuant to the Privacy Rule include: (i) to the individual; (ii) for treatment, payment, or health care operations as permitted by the HIPAA Privacy Rule; (iii) incident to a use or disclosure otherwise permitted or required, provided that applicable requirements are complied with respect to such otherwise permitted use or disclosure; (iv) pursuant to and in compliance with a valid authorization; (v) pursuant to an agreement or as permitted by an individual; (vi) as otherwise permitted by and in compliance with the HIPAA Privacy Rule, including as required by law, for public health activities, for disclosures involving victims of abuse or domestic violence, for health oversight activities, for judicial and administrative proceedings, for law enforcement purposes, about decedents to coroners or medical examiners and funeral directors, for organ or tissue donation, for research when permitted by the HIPAA Privacy Rule, in a limited data set, for fundraising as permitted by the HIPAA Privacy Rule, and for underwriting and related purposes.

1. An unintentional use or acquisition of unsecured PHI by a Workforce Member acting in good faith within the scope of his or her authority, and the unsecured PHI is not further used or disclosed improperly;
2. An inadvertent disclosure of unsecured PHI by an authorized person to another authorized person, and the unsecured PHI is not further used or disclosed improperly; or
3. A disclosure of unsecured PHI to an unauthorized person where there is a good faith belief that the unauthorized person would not reasonably have been able to mentally or physically retain the unsecured PHI.

In accordance with the Breach Notification Rules, the Center bears the burden of demonstrating that an incident is excluded from the definition of “breach” because it meets one of the three exclusion criteria set forth above.

If the incident is excluded from the definition of “breach” because it meets one of the three exclusion criteria, then:

No breach notification is required.

If the incident is not excluded from the definition of “breach” because it does not meet one of the three exclusion criteria, then:

The Center will follow Step Three.

Step Three: The Center will perform a reasoned, fact-specific risk assessment to determine if there is a low probability that the PHI has been compromised, rather than demonstrating that there is no significant risk of harm to the individual.

The Center will document the risk assessment, which should at least consider 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 of PHI has been mitigated.

In accordance with the Breach Notification Rules, the Center bears the burden of demonstrating that there is a low probability that the PHI has been compromised.

If there is a low probability that the PHI has been compromised:

No breach notification is required.

If the PHI has probably been compromised:

The Center will make the required breach notification set forth below.

Required Breach Notification

1. **Breach Notification to Affected Individuals:** Following the discovery of a breach of unsecured PHI, the Center will notify the affected individuals.
 - a. **Content of Notification:** Notifications must be written in plain language and must include:
 - i. a brief description of what happened, including the date of the breach and the date of discovery of the breach, if known;

- ii. a description of the types of unsecured PHI subject to the breach;
 - iii. steps individuals should take to protect themselves from potential harm resulting from the breach;
 - iv. a brief description of the steps the Center is taking to investigate the breach, mitigate the harm, and protect against future breaches; and
 - v. contact information for individuals to ask questions or obtain additional information, including a toll-free phone number, email address, website, or postal address.
- b. **Methods of Notification:** Notifications must be delivered by first-class mail to the last known address of the affected individual or via email if the affected individual has agreed to email and has not withdrawn such agreement. Further:
- i. If the Center does not have sufficient contact information for some or all of the affected individuals, or if some notices are returned as undeliverable, the Center must provide substitute notice for the unreachable individuals in the following manner:
 - 1) If there are fewer than ten (10) individuals for whom the Center has insufficient or out-of-date contact information, the Center must provide substitute notice through an alternative form of written notice, by telephone, or other means, such as a conspicuous posting on the home page of its website.
 - 2) If there are ten (10) or more individuals for whom the Center has insufficient or out-of-date contact information, the Provider must provide substitute notice in one of the following forms:
 - a) Conspicuous posting on the home page of its website for a period of no fewer than ninety (90) days; or
 - b) Conspicuous notice in major print or broadcast media in the geographic areas where the individuals affected by the breach likely reside.
2. **Breach Notification to Media:** If a breach of unsecured PHI of five hundred (500) or more individuals who reside in the same state or jurisdiction, the Center must notify prominent local media outlets of the breach in addition to notifying affected individuals whose unsecured PHI has been breached as set forth above.
3. **Breach Notification to the U.S. Department of Health and Human Services:** the Center must notify the U.S. Department of Health and

Human Services upon the occurrence of a breach of unsecured PHI in the following manner:

- a. If the breach involves five hundred (500) or more individuals, the Center must notify the U.S. Department of Health and Human Services concurrently with notifying affected individuals as set forth above.
- b. If the breach involves less than five hundred (500) individuals, the Center must maintain a log or other documentation of the breach, which it submits annually to the Secretary of the U.S. Department of Health and Human Services within sixty (60) days of the end of each calendar year for breaches of unsecured PHI discovered in the preceding calendar year.

4. **Timing of Breach Notification:** The Center must deliver required breach notification to individuals, media, and the U.S. Department of Health and Human Services without unreasonable delay, but no later than sixty (60) days after the date of discovery of the breach of unsecured PHI.

- a. Breaches are treated as “discovered” under the HIPAA Privacy and Security Rules on the first day that the breach is known by the Center, a business associate serving as the Center agent, or a Workforce Member serving as the Center agent, or when, by exercising reasonable diligence, the breach would have been known to the Center or one of its agents.
- b. **Law Enforcement Delay.** If a law enforcement official states that a notification, notice, or posting required by the Breach Notification Rules would impede a criminal investigation or cause damage to national security, the Center will delay the notification, notice, or posting. If the statement is in writing, the Center will delay the notification for as long as requested during the time period specified by the law enforcement official.

If the statement is made orally, the Center will document the statement, including the official’s identity, and delay the notification, notice, or posting temporarily and no longer than thirty (30) days from the date of the oral statement unless a written statement is submitted during that time.

Policy 21: Covered Entity Policy for Notification of Breach

A. Purpose.

The purpose of this Notification of Breach Policy (“The Policy”) is to establish procedures that the covered entity (“Covered Entity”) should take following the discovery of a breach of unsecured protected health information (PHI).

B. General Introduction.

The Center may act as a business associate for covered entities when it enters into a written business associate agreement with a covered entity to help it carry out its health care activities and functions. In the event of a breach of unsecured PHI, the Center is required to notify the covered entity with whom it has entered into a business associate agreement. This policy follows the required procedures established by 45 CFR § 164.410.

C. Breach.

A breach is the acquisition, access, use, or disclosure of PHI in a manner not permitted under a business associate agreement of the Center that compromises the security or privacy of the PHI.

D. Discovery.

A breach of information shall be treated as discovered as of the first day the breach is known to the business associate. If the breach is known, the business associate shall be presumed to have knowledge of it.

E. Notification to Individual.

Covered Entity must notify affected individuals following a breach of unsecured PHI. Covered Entity must provide affected individual a written notice by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically.

(a) Contents of Notification to Individual.

A notification to an individual must be provided in no case later than 60 days following the discovery of a breach and must include, to the extent possible, the following:

- (i) a brief description of the breach;
- (ii) a description of the types of information that were involved in the breach;
- (iii) the steps affected individuals should take to protect themselves from potential harm;
- (iv) a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches;

- (v) contact information for Covered Entity (or Business Associate, as applicable).

(b) Insufficient or Out-Of-Date Contact Information for 10 or More Individuals

If Covered Entity has insufficient or out-of-date contact information for 10 or more individuals, Covered Entity must provide substitute individual notice by either posting the notice on the home page of its web site for at least 90 days or by providing the notice in major print or broadcasting media where the affected individuals likely reside.

(c) Insufficient or Out-Of-Date Contact Information for Fewer than 10 Individuals

If Covered Entity has insufficient or Out-Of-Date contact information for fewer than 10 individuals, Covered Entity may provide substitute notice by an alternative form of written notice, by telephone, or other means.

(d) Delegation of Individual Notices to Business Associate

Covered Entity may delegate to a Business Associate the responsibility of providing notification to individuals. Covered Entities and Business Associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, including the functions performed by the Business Associate on behalf of Covered Entity and which entity has the relationship with the individual affected by the breach.

F. Media Notice

If a Covered Entity experiences a breach that affects more than 500 residents of a State or jurisdiction, the Covered Entity must provide notice to prominent media outlets serving the State or jurisdiction no later than 60 days following discovery of the breach.

A notification by Covered Entity to media outlets must include the following:

- (i) a brief description of the breach;
- (ii) a description of the types of information that were involved in the breach;
- (iii) the steps affected individuals should take to protect themselves from potential harm;
- (iv) a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches;
- (v) contact information for Covered Entity.

G. Notice to the Secretary.

(a) Breach Affecting 500 or More Individuals.

If a breach affects 500 or more individuals, Covered Entity must notify the United States Secretary of Health and Human Services (“Secretary”) of the breach no later than 60 days following a breach. Covered Entity will notify the Secretary by filling out and electronically submitting the breach report form on the web site of

the U.S. Department of Health and Human Services (“HHS”). The URL for the web site with the form is the following:
https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true.

(b) Breach Affecting Fewer than 500 Individuals.

If a breach affects fewer than 500 individuals, Covered Entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. Covered Entity may report all of its breaches affecting fewer than 500 individuals on one date, but Covered Entity must complete a separate notice for each breach incident. Covered Entity will notify the Secretary by filling out and electronically submitting the breach report form on the web site of HHS. The URL for the web site with the form is the following:
https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true.

H. Law Enforcement Delay.

Following a breach of PHI, a law enforcement official may make a statement to Covered Entity that a notification of a breach would impede a criminal investigation or cause damage to national security.

- (a) If the statement by the law enforcement official is in writing and specifies the time for which a delay is required, Covered Entity shall delay such notification for the time period specified by the official.
- (b) If the statement by the law enforcement official is made orally, Covered Entity shall document the statement, including the identity of the official making the statement, and delay the notification no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

Forms



CONFIDENTIALITY AGREEMENT
Policy 1 and 14.2

I have reviewed Georgia Mountains Health Services' HIPAA Privacy and Security Policies and Procedures and understand that the Center has a legal responsibility to protect patient privacy. To do that, it must keep patient information confidential and safeguard the privacy of patient information and the privacy of electronic health information.

In addition, I understand that during the course of my employment or other work at Georgia Mountains Health, I may see or hear other Confidential Information, including operational and financial information, pertaining to the Center that the Center must maintain as confidential.

Regardless of the capacity, I understand that I must sign and comply with this Agreement in order to continue to work with the Georgia Mountains Health.

By signing this Agreement, I understand and agree that:

I will keep patient information confidential, and I will disclose patient information only under the conditions described in the HIPAA Privacy and Security Policies and Procedures. Regarding other types of important information to the Center, I will keep such information confidential and will only disclose such information if it is required for the performance of my job. Additionally, I will only use the Center's equipment for business purposes which are related to my job functions.

I will not discuss any information, either patient-related or relating to the Center's operations, in public areas (even if specifics such as a patient's name are not used), unless that public area is an essential place for the performance of my job.

I will keep all security codes and passwords used to access the facility, equipment or computer systems, confidential at all times. I will not share my passwords with anyone and will safeguard my passwords at all times.

I will only access or view patient information, including my own, for that which is required to do my job. If I have any question about whether access to certain information is required for me to do my job, I will immediately ask my supervisor or the Center' Privacy Officer for assistance.

I will not disclose, copy, transmit, inquire, modify, or destroy patient information or other System confidential information without permission from my supervisor or the Center' Privacy Officer. This especially includes transmissions from the Center to my home.

I recognize that I have a duty to report any suspicious activity to my manager, the Help Desk, the Privacy Officer, or to the Security Officer immediately. I recognize that I have duty to report anyone who violates the HIPAA Privacy and Security Policies and Procedures to the Privacy Officer or the Security Officer. I will escort anyone who does not have an ID Badge to the front desk or the office manager immediately.

Once my job with Georgia Mountains Health services is terminated, I will immediately return all property (e.g. keys, documents, ID badges, etc.) to the Center. Even after my job is terminated, I agree to meet my obligations under this Agreement.

I understand that violation of this Agreement or the HIPAA Privacy and Security Policies and Procedures may result in disciplinary action, up to and including termination of my employment or relationship with the Center, and this may include civil and criminal legal penalties as a result of the final Privacy and Security Rules issued by the federal government.

I have read the above agreement and the HIPAA Privacy and Security Policies and Procedures and agree to comply with it so that I can continue to work with Georgia Mountains Health Services.

Signature

Date

Print Your Name

Title



CONFIDENTIALITY AGREEMENT — OUTSIDE VENDORS

Policy 1

I understand that Georgia Mountains Health has a legal responsibility to protect patient privacy. To do that, it must keep patient information confidential and safeguard the privacy of patient information.

In addition, I understand that during the course of my relationship with Georgia Mountains Health, I may see or hear other Confidential Information, including operational and financial information, pertaining to the Center that the Center must maintain as confidential.

Regardless of the capacity, I understand that I must sign and comply with this Agreement in order to continue to work with the Center.

By signing this Agreement, I understand and agree that:

I will keep patient information confidential, and I will disclose patient information only at the direct request of Georgia Mountains Health. Regarding other types of important information related to the Center, I will keep such information confidential and will only disclose such information if it is required for the performance of my job.

I will not discuss any information, either patient-related or relating to the Center's operations, in public areas (even if specifics such as a patient's name are not used), unless that public area is an essential place for the performance of my job.

I will only access or view patient information for that which is required to do my job. If I have any question about whether access to certain information is required for me to do my job, I will immediately ask the Center's Privacy Officer for assistance.

I will not disclose, copy, transmit, inquire, modify, or destroy patient information or other Center confidential information that I may become aware of, incidentally or intentionally, as a result of my relationship with the Center. This especially includes transmissions from the Center to my home.

Even after my job is terminated, I agree to meet my obligations under this Agreement .

I understand that violation of this Agreement may result in disciplinary action, up to and including termination of my relationship with the Center, and this may include civil and criminal legal penalties as a result of the final Privacy Rule issued by the federal government.

I have read the above agreement and agree to comply with it so that I can continue to work with the Center.

Signature

Date

Name

Title

Print Your



EMPLOYEE TRAINING FORM

Policy 1.5, 14.10, 18.2 and 19.2

Employee Name

Employee Position

In order to ensure the ongoing confidentiality of our patients' medical records, **Georgia Mountains Health** will provide data security training for all employees who have access to health information specific to a patient.

I have reviewed the HIPAA Privacy and Security Manual of **Georgia Mountains Health** and understand that I have a legal responsibility to protect patient privacy and the security of patients' electronic PHI. To do that, I must keep patient information confidential and safeguard the privacy of patient information, as well as protect against improper access to, or disclosure of, electronic PHI.

I have received training from **Georgia Mountains Health** to better understand how to better carry out my responsibilities within this organization. I understand that based on my duties, access to PHI will be limited only to information which is the minimum necessary to perform my functions a **Georgia Mountains Health**.

Employee Signature

Position

Karen Driskill

Training Official

Date of Training



NOTICE OF PRIVACY PRACTICES

This Notice Describes How Personal Information about You May Be Used and Disclosed and How You Can Get Access to this Information.

PLEASE REVIEW IT CAREFULLY.

HOW WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU.

The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures, we will elaborate on the meaning and provide specific examples. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories.

- **For Payment.** We may use and disclose medical information about you so that the treatment and services you receive at Georgia Mountains Health may be billed to and payment may be collected from you, an insurance company or a third party. For example, it may be essential that you provide us with your health plan information regarding care you receive at Georgia Mountains Health so that your health plan will pay us or reimburse you for those services. In addition, we may tell your health plan about a treatment you are going to receive in order to obtain necessary approval or to determine whether your plan will cover the treatment. You may restrict the disclosure of your Personal Health Information (PHI) to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which you have paid out of pocket in full.
- **For Treatment.** We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, medical students, or other Center personnel who are involved in taking care of you at Georgia Mountains Health. For example, a doctor treating you for a broken leg may need to know if you have diabetes so that he/she can arrange for an appropriate diet. Different departments of the Center also may share medical information about you in order to coordinate the different services you need, such as prescriptions, lab work and x-rays. We also may disclose medical information about you to people outside the Center who may be involved in your medical care after you leave our Center, such as family members, clergy or other persons that are part of your care.
- **For Health Care Operations.** We may use and disclose medical information about you for Center operations. These uses and disclosures are necessary to run Georgia Mountains Health and ensure that all of our patients receive quality care. For example, we may combine medical information about a variety of Center patients to decide what additional services the Center should offer, what services are not needed, and whether certain new treatments are effective. We may also disclose information to doctors, nurses,

technicians, medical students, and other Center personnel for review and learning purposes. We may combine the medical information we have along with medical information from other Centers to compare how we are doing and thus, evaluate where we can make improvements in the care and services we provide. We may remove information that identifies you from this set of medical information so that others may use it to study health care and health care delivery, without learning the identity of the patients.

WHO WILL FOLLOW THIS NOTICE.

This notice describes all Health Centers of Georgia Mountains Health Services and that of:

- Any health care professional authorized to enter information into your chart.
- All departments and units of Georgia Mountains Health.
- All employees, staff and other Georgia Mountains Health personnel.
- All of these entities, sites and locations follow the terms of this notice. In addition, these entities, sites and locations may share medical information with each other for treatment, payment or Center operations purposes described in this notice.

POLICY REGARDING THE PROTECTION OF PERSONAL INFORMATION.

We understand that medical information pertaining to you and your health is personal. We are committed to protecting your medical information. We create a record of the care and services you receive at Georgia Mountains Health. We need this record in order to provide you with quality care and to comply with certain legal requirements. This notice applies to all of the records of your care generated by the Center, whether made by Center personnel or by your healthcare providers. Your healthcare providers may have different policies or notices regarding the doctor's use and disclosure of your medical information created in the doctor's office or clinic.

This notice will inform you about the different ways in which we may use and disclose medical information about you. We also describe your rights and certain obligations we have regarding the use and disclosure of medical information.

The law requires us to:

- Make sure that medical information that identifies you is kept private;
- Acquire your authorization before any use or disclosure of any psychotherapy notes, Protected Health Information (PHI) for marketing purposes, and sales of PHI;
- Give you this notice of our legal duties and privacy practices with respect to medical information about you; and
- Follow the terms of the notice that is currently in effect.

OTHER CATEGORIES OF INFORMATION THAT WE MAY USE OR DISCLOSE INCLUDE.

Appointment Reminders. We may use and disclose medical information to contact you as a reminder that you have an appointment for treatment or medical care at the Center.

As Required By Law. We will disclose medical information about you when required to do so by federal, state or local law.

Fundraising Activities. We may use medical information about you to contact you in an effort to raise money for the Center and its operations. We may disclose medical information to a foundation related to the Center so that the foundation may contact you in raising money for the Center. We would only release contact information, such as your name, address and phone number and the dates you received treatment or services at the Center. However, you have the right to opt out of receiving such fundraising communications. If you do not want the Center to contact you for fundraising efforts, you must notify us in writing.

Health-Related Benefits and Services. We may use and disclose medical information to tell you about health-related benefits or services that may be of interests to you.

Center Directory. We may include certain limited information about you in the Center directory while you are a patient at the Center. This information may include your name, location in the Center, and your general condition (e.g. fair, stable, etc.). The directory information may also be released to people who ask for you by name. This is so your family, friends and clergy can call the Center about you and generally know how you are faring.

Individual Involved in Your Care or Payment for Your Care. We may release medical information about you to a friend or family member who is involved in your medical care. We may also give information to someone who helps pay for your care. We may also inform your family or friends about your condition. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.

Research. Under certain circumstances, we may use and disclose medical information about you for research purposes. For example, a research project may involve comparing the health and recovery of all patients who received another treatment, for the same condition. All research projects, however, are subject to a special approval process. This process evaluates a proposed research project and its use of medical information in order to balance the research needs with patients' need for privacy of their medical information. Before we use or disclose medical information for research, the project will have been approved through this research approval process, but we may, however, disclose medical information about you to people preparing to conduct a research project, for example, to help them look for patients with specific medical needs, as long as the medical information they review does not leave the Center. We will almost always ask for your specific permission if the researcher obtains access to your name, address or other information that reveals who you are, or will be involved in your care at Georgia Mountains Health.

To Avert a Serious Threat to Health or Safety. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or the health and

safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

Treatment Alternatives. We may use and disclose medical information to inform you about, recommend possible treatment options or alternatives that may be of interest to you.

LESS FREQUENT USES AND DISCLOSURES OF YOUR PERSONAL INFORMATION INVOLVING THOSE NOT DIRECTLY INVOLVED IN YOUR CARE COULD INCLUDE:

- **Coroners, Medical Examiners and Funeral Directors.** We may release medical information to a coroner or medical examiner, in order to identify a deceased person or determine the cause of death. We may also release medical information about patients of the Center to funeral directors as necessary to carry out their services.
- **Health Oversight Activities.** We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.
- **Inmates.** If you are an inmate of a correctional institution or under the custody of a law enforcement official, we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary: (1) for the institution to provide you with health care; (2) to protect your health and safety or the health and safety of others; or (3) for the safety and security of the correctional institution.
- **Law Enforcement.** We may release medical information if asked to do so by a law enforcement official:
 - In response to a court order, subpoena, warrant, summons or similar process;
 - To identify or locate a suspect, fugitive, material witness, or missing person;
 - About the victim of a crime if, under certain limited circumstances, we are unable to obtain the person's agreement;
 - About a death we believe may be the result of criminal conduct;
 - About criminal conduct at the Center; and
 - In emergency circumstances to report a crime; the location of the crime or victims; or to identify, description or location of the person who committed the crime.
- **Lawsuits and Disputes.** If you are involved in a lawsuit or a dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.

- **Military and Veterans.** If you are a member of the armed forces, we may release medical information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority.
- **National Security and Intelligence Activities.** We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.
- **Organ and Tissue Donation.** If you are an organ donor, we may release medical information to organizations that handle organ procurement or organ, eye or tissue transplantation or to an organ donation bank, as necessary, to facilitate organ or tissue donation and transplantation.
- **Protective Services for the President and Others.** We may disclose medical information about you to authorized federal officials so they may provide protection to the President, other authorized persons, and foreign heads of state or conduct special investigations.
- **Public Health Risks.** We may disclose medical information about you for public health activities. These activities generally include the following, but are not limited to:
 - Preventing or controlling disease, injury or disability;
 - Reporting births and deaths;
 - Reporting child abuse or neglect;
 - Reporting reactions to medications or problems with products;
 - Notifying people of recalls of products they may be using;
 - Notifying a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition;
 - Notifying the appropriate government authority if we believe a patient has been a victim of abuse, neglect or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.
- **Worker's Compensation.** We may release medical information about you for worker's compensation or similar programs. These programs provide benefits for work-related injuries or illness.

Uses and disclosures not described in this Notice of Privacy Practices will be made only with your authorization.

NOTICE OF INDIVIDUAL RIGHTS

You have the following rights regarding medical information we maintain about you:

- **Right to an Accounting of Disclosures.** You have the right to request an "accounting of disclosures." This is a list of the disclosures we made of medical information about you.

To request this list or accounting of disclosures, you must submit your request in writing to the Center's Privacy Officer. Your request must state a time period, which may not be longer than six years and may not include dates before February 26, 2003. Your request should indicate in what form you want the list (for example, on paper, electronically). The first list you request within a 12-month period will be free. For additional lists, we may charge you for the cost of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- **Right to Amend.** If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for the Center. To request an amendment, your request must be made in writing and submitted to the Center's Privacy Officer. In addition, you must provide a reason that supports your request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- Was not created by us, unless the person or entity that created the information is no longer available to make the amendment;
 - Is not part of the medical information kept by or for the Center;
 - Is not part of information which you would be permitted to inspect and copy; or
 - Is accurate and complete.
- **Right to Inspect and Copy.** You have the right to inspect and copy medical information that may be used to make decisions about your care. You may access Personal Health Information maintained electronically in one or more designated record sets, whether or not the designated record set is an electronic health record. Usually, this includes medical and billing records, but does not include psychotherapy notes.

To inspect and copy medical information that may be used to make decisions about you, you must submit your request in writing to the Center's Privacy Officer. If you request a copy of the information, we are entitled to charge a reasonable fee for the costs of copying, mailing or other supplies associated with your request, whether it is in paper or electronic form.

If you request an electronic copy of PHI that is maintained electronically in one or more designated record sets, we will provide you with access to the electronic information in the electronic form and format that you requested, if it is readily producible, or if not, in a readable electronic form and format as agreed.

If so requested, we will transmit the requested copy of PHI directly to a designated person, if your request is: (1) in writing; (2) signed by you; and (3) clearly identifies the designated person and where we should send the PHI.

We will respond to your request within 30 days. If the information cannot be gathered within the initial 30-day period, then we will respond with a written notice of the reasons for the delay and the expected date, no later than 60-days from the original request. However, we may deny your request to inspect and copy in certain very limited circumstances. If you are denied access to medical information, you may request that the denial be reviewed. Another licensed health care professional chosen by the Center will review your request and the denial. The person conducting the review will not be the person who denied your request. We will comply with the outcome of the review.

- **Right to a Paper Copy of this Notice.** You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time. Even if you have agreed to receive this notice electronically, you are still entitled to a paper copy of this notice. You may obtain a copy of this notice at our website, www.gamtnhealth.org. To obtain a paper copy of this notice contact the front desk staff.
- **Right to Request Confidential Communications.** You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.

To request confidential communications, you must make your request in writing in the Center's Privacy Officer. We will not ask you the reason for the request and will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

- **Right to Restrict Disclosures to Health Plan.** You have the right to restrict disclosures of PHI to a health plan if the disclosure is for payment or health care operations and pertains to a health care item or service for which you have paid out of pocket in full.
- **Right to be Notified of Breach.** You have the right to or you will be notified following a breach of unsecured PHI if you are affected by the breach.
- **Right to Request Restrictions.** You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery you had. ***We are not required to agree to your request.*** If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment.

To request restrictions, you must make your request in writing to the Privacy Officer. In your request, you must tell us (1) what information you want to limit; (2) whether you want to limit our use, disclosure or both; and (3) to whom you want the limits to apply, for example, disclosures to your spouse.

We will honor your request to restrict disclosure of your PHI to a health plan if (1) the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law and (2) the PHI pertains solely to a health care item or service for which you, or a person other the health plan on your behalf (such as a family member), has paid the covered entity for in full.

CHANGES TO THIS NOTICE

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for medical information we already have about you as well as any information we receive in the

future. We will post a copy of the current notice in the Center. The notice will contain on the first page, in the top right-hand corner, the effective date. In addition, each time you visit the Center for treatment or health care services, we will offer you a copy of the current notice in effect.

COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with Georgia Mountains Health Services or with the Secretary of the Department of Health and Human Services. To file a complaint with the Center, contact Karen Driskill, Business Development & Compliance Manager at 706-946-5605. This should be the same person or department listed on the first page as the contact for more information about this notice. All complaints must be submitted in writing. **You will not be penalized for filing a complaint.**

OTHER USES OF MEDICAL INFORMATION

Other uses and disclosures of medical information not covered by this notice or the laws that apply to use will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provide to you.

If you have any questions about this notice, please contact Karen Driskill, Business Development & Compliance Manager.

Effective Date: March 26, 2013.

NOTICE OF PRIVACY PRACTICES

**THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.
PLEASE REVIEW IT CAREFULLY.**

HOW WE MAY USE AND DISCLOSE MEDICAL INFORMATION ABOUT YOU. The following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures, we will elaborate on the meaning and provide more specific examples, if you request. Not every use or disclosure in a category will be listed. However, all of the ways we are permitted to use and disclose information will fall within one of the categories. We must obtain your authorization before the use and disclosure of any psychotherapy notes, uses and disclosures of PHI for marketing purposes, and disclosure that constitute a sale of PHI. Uses and disclosures not described in this Notice of Privacy Practices will be made only with authorization from the individual.

For Payment. We may use and disclose medical information about you so that the treatment and services you receive at the Center may be billed to and payment may be collected from you, an insurance company or a third party. For example: we may disclose your record to an insurance company, so that we can get paid for treating you.

For Treatment. We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, technicians, medical students, or other personnel who are involved in taking care of you at the Center or the hospital. For example, we may disclose medical information about you to people outside the Center who may be involved in your medical care, such as family members, clergy or other persons that are part of your care.

For Health Care Operations. We may use and disclose medical information about you for health care operations. These uses and disclosures are necessary to run the Center and ensure that all of our patients receive quality care. We may also disclose information to doctors, nurses, technicians, medical students, and other Center personnel for review and learning purposes. For example, we may review your record to assist our quality improvement efforts. **WHO WILL FOLLOW THIS NOTICE.** This notice describes our Center's policies and procedures and that of any health care professional authorized to enter information into your medical chart, any member of a volunteer group which we allow to help you, as well as all employees, staff and other Center personnel.

POLICY REGARDING THE PROTECTION OF PERSONAL INFORMATION. We create a record of the care and services you receive at the Center. We need this record in order to provide you with quality care and to comply with certain legal requirements. This notice applies to all of the records of your care generated by the Center, whether made by Center personnel or by your personal doctor. The law requires us to: make sure that medical information that identifies you is kept private; give you this notice of our legal duties and privacy practices with respect to medical information about you; and to follow the terms of the notice that is currently in effect. Other ways we may use or disclose your protected healthcare information include: appointment reminders; as required by law; for health-related benefits and services; to individuals involved in your care or payment for your care; research; to avert a serious threat to health or safety; and for treatment alternatives. Other uses and disclosures of your personal information could include disclosure to, or for: coroners, medical examiners and funeral directors; health oversight activities; law enforcement; lawsuits and disputes; military and veterans; national security and intelligence activities; organ and tissue donation; and others; public health risks; and worker's compensation.

NOTICE OF INDIVIDUAL RIGHTS

You have the following rights regarding medical information we maintain about you:

Right to a Paper Copy of this Notice. You have the right to a paper copy of this notice. You may ask us to give you a copy of this notice at any time.

Right to Inspect and Copy. You have the right to inspect and copy medical information that may be used to make decisions about your care. We may deny your request to inspect and copy in certain very limited circumstances.

Right to Amend. If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by, or for, the Center. To request an amendment, your request must be made in writing and submitted to the Privacy Officer and you must provide a reason that supports your request. We may deny your request for an amendment.

Right to Request Restrictions. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. *We are not required to agree to your request.* If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment. To request restrictions, you must make your request in writing to the Privacy Officer.

Right to Request Removal from Fundraising Communications. You have the right to opt out of receiving fundraising communications from the Center.

Right to Restrict Disclosures to Health Plan. You have the right to restrict disclosures of PHI to a health plan if the disclosure is for payment of health care operations and pertains to a health care item or service for which the individual has paid out of pocket in full.

Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. You must make your request in writing and you must specify how or where you wish to be contacted.

Right to an Accounting of Disclosures. You have the right to request an "accounting of disclosures." This is a list of the disclosures we made of medical information about you. To request this list or accounting of disclosures, you must submit your request in writing to the Privacy Officer. **CHANGES TO THIS NOTICE.** We reserve the right to change this notice. We will post a copy of the current notice in the Center's waiting room. **COMPLAINTS.** If you believe your privacy rights have been violated, you may file a complaint with the Center or with the Secretary of the Department of Health and Human Services. To file a complaint with the Center, contact _____, Privacy Officer, [Phone Number], [Center Address]. All complaints must be submitted in writing. **You will not be penalized for filing a complaint.** **OTHER USES OF MEDICAL INFORMATION.** Other uses and disclosures of medical information not covered by this notice or the laws that apply to use will be made only with your written authorization. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time.

If you have any questions about this notice or would like to receive a more detailed explanation, please contact our Privacy Officer.

[Center Administrators: If you choose to have patients or their personal representatives sign this Notice, please use the lines below. Otherwise, the lines below should be removed.]

I acknowledge by signing below that I have received the Notice of Privacy Practices and Notice of Individual Rights.

Patient or Patient's Personal Representative

Date



Authorization for Release of Health Information

Complete all sections of this authorization as appropriate to your request.

Patient Name: _____ Medical Record Number: _____

Address: _____ Date of Birth: _____
(street address)

(city, state, zip code) Phone Number: _____

I hereby authorize Georgia Mountains Health Services to take the following action:

Check all that apply:

- Provide a copy of My Health Information to me. Let me look at My Health Information.

- Release My Health Information to: Discuss My Health Information with: Obtain copies of My Health Information from:

Name of other person or entity: _____

Address: _____
(street address) (city) (state) (zip code)

Phone Number: _____ Fax Number: _____

For this Authorization, "My Health Information" means (check all that apply):

- Clinical Office Notes Emergency Room Record Outpatient Record
- Inpatient Hospital Notes History & Physical Pathology Report
- Billing Record Immunization Record Diagnostic Test Results
- Mental Health Records HIV Status or Test Results Other: _____

_____ By initialing here, I authorize for "My Health Information" to include Substance Abuse Records/Information.

For the date(s) of service from: _____ to _____ (records will be provided for all dates of service if left blank.)

I understand there may be a fee for a copy of My Health Information. All fees will be in compliance with applicable law. I agree to pay this fee.

I understand that:

- This Authorization is voluntary.
- This Authorization is valid for one year from the date signed, unless I revoke/withdraw it or unless an earlier date is specified here: _____ I may revoke/withdraw this Authorization by sending a written notice to the health center.
- When My Health Information is disclosed as requested, it may no longer be protected by federal and state privacy laws, and could be re-disclosed by the person(s) receiving it.
- The medical information released may contain information related to HIV status, AIDS, sexually transmitted diseases, mental health, and drug and alcohol abuse.

Signature of Patient: _____ Date: _____

Witness Signature: _____ Date: _____

If you are NOT the patient but are signing on behalf of the patient, please complete the following:

I, _____, am (check which applies)
(print your name)

- Parent with Parental Rights (not sufficient for substance abuse records)
- Court Appointed Guardian
- Legally Appointed Healthcare Agent (not sufficient for substance abuse records)
- Medical Power of Attorney (not sufficient for substance abuse records)
- Other _____

Representative's Signature: _____ Date: _____

Address: _____ Phone: _____

You MUST attach proof of your authority to act on behalf of the patient as checked above (other than parent).



Policy 7

**CONSENT FOR USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION
FOR PAYMENT, TREATMENT AND HEALTH CARE OPERATIONS**

By signing below, you hereby consent for Georgia Mountains Health Services, Inc to use or disclose information about yourself (or another person for whom you have the authority to sign) that is protected under federal law, for the sole purposes of treatment, payment and health care operations. You may refuse to sign this consent form.

You should read the Notice of Privacy Practices for PHI attached to this form before signing the Consent. The terms of the Notice may change from time to time, and you may always get a revised copy of it by asking the Privacy Officer for this Center.

You have the right to request that the Center restrict how PHI is used or disclosed to carry out treatment, payment, or health care operations. The Center is not required to agree to requested restrictions, however; if the Center agrees to your requested restrictions, the restriction is binding on it.

Information about you is protected under federal law, and you have the right to revoke this Consent, unless we have taken action in reliance on your authorization (as determined by our Privacy Officer). By signing below, you recognize that the protected health information used or disclosed pursuant to this Consent may be subject to re-disclosure by the recipient and may no longer be protected under federal law.

You may communicate with the following individuals regarding my condition or course of treatment: _____

You may communicate confidential information to me, including invoices for services, to the following address and/or phone numbers: _____

Individual Signature

Date

As a personal representative, I have authority to act for the individual because I am the individual's



FORM REQUEST FOR LIMITATIONS AND RESTRICTIONS OF USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

You have the right under the Health Insurance Portability and Accountability Act of 1996 to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. ***We are not required to agree to your request.*** If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment. To request limitations and restrictions, you must complete this form and return it to us.

Patient Name: _____

Date of Birth: _____

Please describe as specifically as possible the *type of information* that you would like for us to restrict or limit. _____

Please describe as specifically as possible *how* you would like this information to be restricted or limited.

Signature of Patient or Legal Guardian

Date

For Use by *the Center* only:

Date Received _____

Request Has Been: Accepted _____

Denied _____

Comments:

Privacy Officer

Date



Policy 8.2

CONFIDENTIAL COMMUNICATION REQUEST

Patient Name: _____

Date of Birth: _____

SSN: _____

_____ I would like to receive confidential communications of my protected health information.

_____ The disclosure of all or part of my protected health information could endanger me if not disclosed at an alternate location or at an alternative telephone number.

Please provide us with the **alternative address** or the **alternative telephone number** where or at which you would like for us to contact you.

Alternative Address:

Alternative Phone Number:

_____ I understand that this alternate location must be reasonable and that if our office does not believe it to be reasonable, this request may not be accepted.

Signature of Patient or Legal Guardian

Date

For Use by *the Center* only:

Date Received _____

Request Has Been:

Accepted _____

Denied _____

Comments:

Privacy Officer

Date



Policy 9.1

Authorization for Release of Health Information

Complete all sections of this authorization as appropriate to your request.

Patient Name: _____ Medical Record Number: _____

Address: _____ Date of Birth: _____
(street address)

_____ Phone Number: _____
(city, state, zip code)

I hereby authorize Georgia Mountains Health Services to take the following action:

Check all that apply:

- Provide a copy of My Health Information to me. Let me look at My Health Information.

- Release My Health Information to: Discuss My Health Information with: Obtain copies of My Health Information from:

Name of other person or entity: _____

Address: _____
(street address) (city) (state) (zip code)

Phone Number: _____ Fax Number: _____

For this Authorization, "My Health Information" means (check all that apply):

- Clinical Office Notes Emergency Room Record Outpatient Record
Inpatient Hospital Notes History & Physical Pathology Report
Billing Record Immunization Record Diagnostic Test Results
Mental Health Records HIV Status or Test Results Other: _____

By initialing here, I authorize for "My Health Information" to include Substance Abuse Records/Information.

For the date(s) of service from: _____ to _____ (records will be provided for all dates of service if left blank.)

I understand there may be a fee for a copy of My Health Information. All fees will be in compliance with applicable law. I agree to pay this fee.

I understand that:

- This Authorization is voluntary.
This Authorization is valid for one year from the date signed, unless I revoke/withdraw it or unless an earlier date is specified here:
I may revoke/withdraw this Authorization by sending a written notice to the health center.
When My Health Information is disclosed as requested, it may no longer be protected by federal and state privacy laws, and could be re-disclosed by the person(s) receiving it.
The medical information released may contain information related to HIV status, AIDS, sexually transmitted diseases, mental health, and drug and alcohol abuse.

Signature of Patient: _____ Date: _____

Witness Signature: _____ Date: _____

If you are NOT the patient but are signing on behalf of the patient, please complete the following:

I, _____, am (check which applies)
(print your name)

- Parent with Parental Rights (not sufficient for substance abuse records)
Court Appointed Guardian
Legally Appointed Healthcare Agent (not sufficient for substance abuse records)
Medical Power of Attorney (not sufficient for substance abuse records)
Other _____

Representative's Signature: _____ Date: _____

Address: _____ Phone: _____

You MUST attach proof of your authority to act on behalf of the patient as checked above (other than parent).



Policies 9.2 And 9.3

FORM LETTER FOR DENIAL OF REQUEST FOR ACCESS

Date: _____

Patient's Name
Address
City, State, Zip

Dear _____:

In accordance with federal law, Georgia Mountains Health Services (the Center) cannot fully respond to your request to inspect and obtain a copy of your protected health information (PHI). Because one of the following reason(s) listed below applies to the PHI that you requested, the Center has "blacked out" the information that falls into one of these categories (check one):

_____ Part of the records that you have requested contain psychotherapy notes, as defined in the Privacy Rule, and we are not required to allow you to inspect and obtain a copy of the part of your record that contains psychotherapy notes.

_____ The Privacy Rule does not require the Center to permit you to inspect and obtain a full copy of the record because it contains information that has been compiled in anticipation of, or for use in a civil, criminal or administrative action or proceeding.

_____ The Privacy Rule does not require the Center to permit you to inspect and obtain a full copy of the requested information because it contains information that was obtained from someone other than a healthcare Center under a promise of confidentiality, and the access requested would be reasonably likely to reveal the source of the information.

_____ The Privacy Rule does not require the Center to permit you to inspect and obtain a full copy of the requested information because part of your records contains information that was/is being created or obtained in the course of on-going research that includes treatment, and you agreed to denial of access when you consented to participate in the research. Your right of access will be reinstated upon the completion of the research.

_____ The requested information is contained in records subject to the federal Privacy Act, 5 U.S.C. Sec.552a, and this partial denial meets the requirements of that law.

_____ The Center does not possess the information requested.

If the Center denies you access to requested information for any of the reasons listed below, you have the right to have the denial reviewed by another licensed healthcare professional who did not participate in this denial.

_____ A licensed healthcare professional has determined in his/her professional judgment that full access to the requested information is reasonably likely to endanger your life or physical safety or the life or physical safety of another person.

_____ Part of the requested information makes reference to another person and a licensed healthcare professional has determined, in the exercise of reasonable judgment, that the requested access is reasonably likely to cause substantial harm to such other person.

_____ You are the personal representative of the subject of the requested information, and a licensed healthcare professional has determined, in the exercise of professional judgment that part of the requested information should not be provided to you.

If you choose to have this partial denial reviewed, please submit a written request to our Privacy Officer at _____.

The Center's Privacy Officer will decide whether to grant or deny you access to the requested PHI within a reasonable period of time. You may file a complaint regarding this denial with the Privacy Officer at 706-946-5605 or with the Secretary of the U.S. Department of Health and Human Services. Complaints to the Secretary must be in writing, name the Center, describe the acts/omissions believed to violate the Privacy Rule, and be filed within 180 days of the alleged violation.

Sincerely,

Georgia Mountains Health Services, Inc



FORM REQUEST FOR AMENDMENT OF PATIENT INFORMATION

Patient Name: _____ Date of Birth: _____

Patient Address: _____ SSN: _____
Street

City, State, Zip

Type of Information to be Amended: _____ (visit record (clinical), visit record (admin.), hospital record, prescription data, patient history./ complaint)

Please tell us what the information should say to be accurate or complete AND WHY:

Signature of Patient or Legal Guardian Date

Georgia Mountains Health Services has reviewed your request for amendment, and it will _____ (accept, deny or partly accept, partly deny) your request.

Part acceptances and denials can be based on the following: the information was not created by this organization, the information is not available to the patient for inspection, the information is not a part of patient's designated record set, or the information is accurate and complete.

Based on your request, the support for our decision is the following:

Privacy Officer: _____

*If your request has been denied, in whole or in part, you have the right to submit a written statement disagreeing with the denial to the Center in, the same way that you submitted your request. If you do not send us a letter or form stating that you disagree, you may tell us that we should provide your original request for amendment, along with our denial, with any future disclosures of the information that is the subject of the original request for an amendment. Also, you may file a complaint with our Privacy Officer or the Secretary of the U.S. Department of Health & Human Services.



Policy 11

FORM NOTICE OF RIGHTS AND REQUEST FOR AN ACCOUNTING

Federal rules protecting the privacy of patient information give you the right to receive an accounting of Georgia Mountains Health Services' disclosures of certain types of your information.

Your request must state a time period, which may not be longer than six (6) years and may not include dates before April 14, 2003.

The Center will conduct the first accounting you request within a 12-month period free of charge. If you make an additional request for an accounting during the same 12-month period, the Center will charge you with the costs of performing the accounting. The Center will notify you of the cost involved before that, however, and you may choose to withdraw or change your request.

To request an accounting of disclosures made by the Center, you must submit your request in writing to _____.

Patient Name: _____

Date of Birth: _____

Patient Address: _____
Street

SSN: _____

City, State, Zip

Time period of accounting requested: _____

Signature of Patient or Guardian

Date



PRIVACY COMPLAINT

Georgia Mountains Health Services values the privacy of its patients and is committed to operating our Center in a manner that promotes patient confidentiality while providing high quality patient care.

If the staff at the Center have in any way given you the impression that they are not protecting your right to privacy, we want you to notify us. Please be assured that your complaint will be kept confidential. Please use the space provided below to describe your complaint. It is our intent to use this feedback to better protect your rights to patient confidentiality.

Name of Patient

Date

Signature of Patient

Phone Number

You may send this complaint to our office and/or the Office of Civil Rights pursuant to 45 C.F.R. §160.306. If you wish for assistance in filing this complaint, please do not hesitate to contact our Privacy Officer at 165 Blue Ridge Overlook, Blue Ridge, GA 30513.



BUSINESS ASSOCIATE AGREEMENT

The Final Privacy Rule at 45 C.F.R. §164.502(e) and the Final Security Rule at 45 C.F.R. § 164.314 permit the Center to disclose protected health information to a business associate who performs a function or activity on behalf of, or provides a service to the Center that involves the creation, use, or disclosure of protected health information, provided that the Center obtains satisfactory assurances that the business associate will appropriately safeguard the information.

The Privacy and Security Rules require that the satisfactory assurances obtained from the business associate be in the form of a written contract, a model of which is attached, between Georgia Mountains Health Services and the business associate that contains the elements specified at §164.504 (e).

In addition, the Privacy and Security Rules also provide that where the Center knows of a material breach or violation by the business associate of the contract or agreement, the Center must take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, terminate the contract or arrangement. If termination of the contract or arrangement is not feasible, the Center is required to report the problem to the Secretary of Health and Human Services. This requirement does not oblige the Center to monitor and be responsible for the actions of its business associates with respect to the privacy and safeguarding of protected health information. Rather, once the Center knows of a pattern of activity that constitutes a material breach or violation of the business associate's obligation under the contract, it must take steps to cure the breach or end the violation.

This is only model language. These provisions are designed to help covered entities more easily comply with the business associate contract requirements of the Privacy and Security Rules. However, use of these model provisions is not required for compliance with the Privacy and Security Rules. The language may be amended to more accurately reflect business arrangements between the Center and the business associate.

Furthermore, the Center may want to include other provisions that are related to the Privacy and Security Rules but that are not required by the Rules. For example, the Center may want to add provisions in a business associate contract such that it can rely on the business associate to help the Center meet its obligations under the Privacy and Security Rules. These and other types of issues will need to be worked out between the parties.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (this “Agreement”) is made as of _____, 20___, (the “Effective Date”), and is entered into between _____ (“Covered Entity”) and _____ (“Business Associate”), (individually, a “Party” and collectively, the “Parties”) and supersedes and amends any prior business associate agreement, and any amendments thereto between the Parties.

RECITALS

WHEREAS, Covered Entity and Business Associate have entered into, or are entering into, or may subsequently enter into, agreements or other documented arrangements (collectively, the “Business Arrangements”), including but not limited to a _____ Agreement, dated _____, 20___ (the “Underlying Agreement”), pursuant to which Business Associate may provide services for Covered Entity that require Business Associate to access, create and use health information that is protected by state and/or federal law;

WHEREAS, Business Associate will create or receive from or on behalf of Covered Entity, or have access to, Protected Health Information (“PHI”) in the course of providing services (“Services”); and

WHEREAS, pursuant to the Health Insurance Portability and Accountability Act of 1996 and its implementing administrative simplification regulations (45 CFR §§ 160-164) (“HIPAA”) as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act and its implementing regulations, as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (the “HITECH Act”), Covered Entity is required to enter into this Agreement with Business Associate.

NOW THEREFORE, in consideration of the foregoing recitals and the mutual covenants contained herein, the Parties, intending to be legally bound, agree as follows:

I. DEFINITIONS

A. Catch-all definition:

- i. The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

B. Specific definitions:

- i. Business Associate. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Business Associate].
- ii. Covered Entity. “Covered Entity” shall generally have the same

meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean [Insert Name of Covered Entity].

- iii. HIPAA Rules. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

II. EFFECT OF AGREEMENT

The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Parties to comply with HIPAA.

III. BUSINESS ASSOCIATE OBLIGATIONS AND ACTIVITIES

(A) Business Associate agrees to:

- i. Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law;
- ii. Use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by the Agreement;
- iii. Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware; [The parties may wish to add additional specificity regarding the breach notification obligations of the Business Associate, such as a stricter timeframe for the Business Associate to report a potential breach to the Covered Entity.]
- iv. In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information;
- v. Make available protected health information in a designated record set to the Covered Entity as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.524;
- vi. Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.526; Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy Covered Entity’s obligations under 45 CFR 164.528;
- vii. To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and
- viii. Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

- (B) Permitted Uses and Disclosures: Except as otherwise limited in this Agreement, Business Associate may use or disclose PHI to (1) perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Underlying Agreement, provided that such use or disclosure would not violate HIPAA if made by Covered Entity or (2) as required or permitted by applicable law, rule, regulation, or regulatory agency or by any accrediting or credentialing organization to whom a Party is required to disclose such PHI. In addition, Business Associate may:
- (i) use PHI, if necessary, for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate;
 - (ii) disclose PHI, if necessary, if the following requirements are met:
 - (a) the disclosure is required by law; or
 - (b) 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 purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the PHI has been breached; and
 - (iii) use PHI to provide Data Aggregation services to Covered Entity as permitted by HIPAA.
- (C) Restrictions: Business associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity except for the specific uses and disclosures set forth below.
- (D) Business Associate Agents: Business Associate shall ensure that its agents, including subcontractors, to whom it provides PHI agree to the same restrictions and conditions that apply to Business Associate pursuant to this Agreement with respect to PHI and Electronic PHI. Notwithstanding the foregoing, the Underlying Agreement shall determine and control whether and under what conditions, if any, that the Business Associate may utilize agents and/or subcontractors.
- (E) Appropriate Safeguards; Security: Business Associate shall implement appropriate and commercially reasonable safeguards to prevent use or disclosure of PHI other than as permitted in this Agreement. Effective as of the date Covered Entity is required to comply with 45 C.F.R. Part 164 Subpart C, Business Associate shall implement Administrative, Physical and Technical Safeguards that reasonably and appropriately protect the Integrity, Availability, and Confidentiality of Electronic PHI. Business Associate shall report to Covered Entity in writing within twenty-four (24) hours of any Security Incident of which it becomes aware.

- (F) Government Access to Records: Business Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary of the Department of Health and Human Services for purposes of determining Covered Entity's compliance with HIPAA. Business Associate shall provide Covered Entity with a copy of any PHI that Business Associate provides to the Secretary concurrently with providing such PHI to the Secretary.
- (G) HITECH Act: Business Associate and Covered Entity hereby agree that the provisions of HIPAA and the HITECH Act that apply to business associates and that are required to be incorporated by reference in a business associate agreement are incorporated into this Agreement as if set forth in this Agreement in their entirety and are effective as of the applicable effective date of each such provision. Business Associate hereby further agrees to comply with all requirements of HIPAA, the HITECH Act and each of their implementing regulations that are applicable to business associates commencing as of the applicable effective date of each such provision.
- (H) Reporting of Improper Use or Disclosure: Business Associate shall report to Covered Entity in writing within twenty-four (24) hours of any actual or suspected violations of this Agreement or any actual or suspected Breach of Unsecured PHI. An actual or suspected Breach shall be treated as discovered by Business Associate as of the first day on which such Breach is known to the Business Associate, its employees, officers or other agents, or, by exercising reasonable diligence, should have been known to Business Associate, its employees, officers or other agents. Business Associate's notification to Covered Entity, to the extent possible, shall include the identity of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, breached and be in substantially the same form as *Attachment A* hereto. Business Associate further agrees to fully cooperate in good faith with and to assist Covered Entity in complying with the requirements of HIPAA and the HITECH Act, including without limitation, the provision of written notices to affected Individuals following the discovery of a Breach of Unsecured PHI if requested by Covered Entity.
- (I) Mitigation: Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI or Unsecured PHI by Business Associate in violation of the requirements of this Agreement, HIPAA or the HITECH Act.
- (J) Availability of PHI: To the extent that the Parties mutually agree in writing that PHI is part of a Designated Record Set, and that such Designated Record Set (or a portion thereof) is to be maintained by Business Associate, as set forth and agreed to in *Attachment B*, Business Associate shall within ten (10) days after a written request from Covered Entity:
- (i) provide access, at the request of Covered Entity, and in the time and manner designated by Covered Entity, to such PHI to Covered Entity or,

as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR § 164.524; and

- (ii) make amendments to such PHI as directed or agreed to by Covered Entity in accordance with the requirements of 45 CFR § 164.526.
- (K) Accounting Rights: Business Associate shall document disclosures of PHI and information related to such disclosures and, within ten (10) days after Covered Entity's written request, shall provide to Covered Entity or to an Individual, in time and manner designated by Covered Entity, information collected in accordance with this Section, 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.

IV. COVERED ENTITY'S OBLIGATIONS

- (A) Notice: Covered Entity shall provide Business Associate with the notice of privacy practices that Covered Entity produces in accordance with 45 CFR § 164.520, as well as any subsequent changes to the Covered Entity's notice of privacy practices, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.
- (B) Changes in Access by Individual: Covered Entity shall provide Business Associate with any changes in, or revocation of, permission by an Individual to use or to disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.
- (C) Restrictions on Use and Disclosure of PHI: Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

V. TERMINATION

- (A) Term: The Term of this Agreement shall be effective as of the date set forth above and shall terminate when Business Associate ceases to perform the Services as set forth above; provided, however, that certain obligations shall survive termination of this Agreement as set forth in Sections V(C) and VI(F).
- (B) Termination for Cause: Covered Entity may immediately terminate this Agreement in the event that Business Associate breaches any provision of this Agreement. In its sole discretion, Covered Entity may permit Business Associate the ability to cure or to take substantial steps to cure such material breach to Covered Entity's satisfaction within thirty (30) days after receipt of written notice from Covered Entity. Covered Entity may additionally report any Breaches to the Secretary.

- (C) Termination of Business Arrangement: Upon termination of all Business Arrangements, either party may terminate this Agreement by providing written notice to the other party.
- (D) Obligations of Business Associate Upon Termination: Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity [or, if agreed to by Covered Entity, destroy] all PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business Associate shall retain no copies of PHI.
- (i) Upon termination of this Agreement for any reason, Business Associate, with respect to PHI received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:
- (1) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;
 - (2) Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the remaining PHI that the Business Associate still maintains in any form;
 - (3) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate retains the PHI;
 - (4) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out above, which applied prior to termination; and
 - (5) Return to Covered Entity [or, if agreed to by Covered Entity, destroy] the PHI retained by business associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.
- (E) Survival: The obligations of Business Associate under this Section shall survive the termination of this Agreement.

VI. MISCELLANEOUS

- (A) Amendment to Comply with Law: The Parties acknowledge that it may be necessary to amend this Agreement to comply with modifications to HIPAA, including but not limited to statutory or regulatory modifications or interpretations by a regulatory agency or court of competent jurisdiction. No later than sixty (60) days after the effective date of any such modifications, the Parties agree to use

good faith efforts to develop and execute any amendments to this Agreement as may be required for compliance with HIPAA.

- (B) Amendment: The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for compliance with the requirements of the HIPAA Rules and any other applicable law. This Agreement may be amended or modified only in writing signed by the Parties.
- (C) No Third Party Beneficiaries: Nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.
- (D) Governing Law: This Agreement shall be governed by and construed in accordance with HIPAA and its implementing administrative simplification regulations, the HITECH Act and its regulations, and the laws of the State of Georgia without regard to conflicts of law principles.
- (E) Paragraph Headings: The paragraph headings in this Agreement are for convenience only. They form no part of this Agreement and shall not affect its interpretations.
- (F) Indemnification: Business Associate shall indemnify and hold Covered Entity, and its employees, officers, directors, independent contractors, agents and representatives, harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards or other reasonable 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 of this Agreement by Business Associate, including without limitation, (1) expenses Covered Entity incurs in notifying affected Individuals of a Breach caused by Business Associate or its subcontractors or agents and (2) any penalties, sanctions, assessments, or charges incurred by Covered Entity resulting from Business Associate's failure to comply with the terms and conditions of Sections III(F) and III(G) of this Agreement. The obligations set forth in this Section VI(F) shall survive termination of this Agreement, regardless of the reasons for termination.
- (G) Entire Agreement: This Agreement in conjunction with the Business Arrangements and any attachments, exhibits and schedules of this Agreement and/or the Business Arrangements 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.

(Remainder of page intentionally left blank)

(Signature page follows)

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement by their duly authorized representatives to be effective as of the Effective Date.

COVERED ENTITY:

BUSINESS ASSOCIATE:

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Attachment A

Notification to Covered Entity about a Breach of Unsecured PHI

This notification is made pursuant to Section III(G) of the Business Associate Agreement (the “Agreement”) between _____ (“Covered Entity”) and _____ (“Business Associate”).

Business Associate hereby notifies Covered Entity that there has been an actual or suspected breach of unsecured protected health information (PHI) that Business Associate has used or has had access to under the terms of the Agreement (“Breach”).

I. Description of Breach: _____

II. Date of Breach (if known): _____

III. Date of the Discovery of Breach: _____

IV. Number of Individuals affected by Breach: _____

V. The types of unsecured PHI that were involved in Breach (such as the name, Social Security number, date of birth, home address, account number or disability code of the affected Individuals): _____

VI. Description of the steps Business Associate is taking to investigate Breach, mitigate losses, and to protect against any further Breaches: _____

VII. Contact information for Covered Entity and Affected Individuals to ask questions or learn additional information:

A. Name and Title: _____

B. Address: _____

C. E-mail address: _____

D. Telephone Number: _____

Attachment B

Identification of Designated Record Set

As contemplated in Section III(I), the Parties agree to the provision marked below:

- The PHI that Business Associate creates or receives from or on behalf of Covered Entity, or has access to, in the course of providing the Services constitutes a Designated Record Set (or a part thereof), and such Designated Record Set (or portion thereof) shall be maintained by Business Associate.

- The PHI that Business Associate creates or receives from or on behalf of Covered Entity, or has access to, in the course of providing the Services DOES NOT constitute a Designated Record Set (or a part thereof), and NO such Designated Record Set (or portion thereof) shall be maintained by Business Associate.

BUSINESS ASSOCIATE SUBCONTRACTOR AGREEMENT

This Business Associate Subcontractor Agreement (this “Agreement”) is made as of _____, 2013, (the “Effective Date”), and is entered into between _____ (“Business Associate”) and [Subcontractor Name] (“Subcontractor”), (individually a “Party” and collectively the “Parties”) and supersedes and amends any prior business associate agreement, and any amendments thereto between the Parties.

RECITALS

WHEREAS, Business Associate will provide services for certain clients (such clients hereinafter collectively referred to as “Covered Entities”) that may require Business Associate to access, create and use individually identifiable protected health information (“PHI”) that is protected by state and/or federal law;

WHEREAS, pursuant to the Health Insurance Portability and Accountability Act of 1996 and its implementing administrative simplification regulations (45 CFR §§ 160-164) (“HIPAA”) as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act and its implementing regulations, as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5) (the “HITECH Act”), Covered Entities are required to enter into Business Associate Agreements with Business Associate (the “BA Agreements”);

WHEREAS, pursuant to the BA Agreements, Business Associate has agreed to ensure that its agents, including subcontractors, to whom it provides PHI agree to the same restrictions and conditions that apply to Business Associate pursuant to the BA Agreements with respect to PHI;

WHEREAS, Business Associate and Subcontractor have entered into an offsite records storage agreement (the “Records Agreement”) contemporaneously with the execution of this Agreement; and

WHEREAS, Business Associates are requiring Subcontractor to enter into this Agreement because Subcontractor and its employees may access paper and/or electronic records containing PHI in carrying out its obligations pursuant to the Records Agreement.

NOW THEREFORE, in consideration of the foregoing recitals and the mutual covenants contained herein, the Parties, intending to be legally bound, agree as follows:

1. **Definitions. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms defined in HIPAA, as amended. Effect of Agreement. The Parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Parties to comply with HIPAA.**

2. Subcontractor Obligations.

2.1 Permitted Uses and Disclosures. Except as otherwise limited in this Agreement, subcontractor may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Business Associate as specified in the Records Agreement, provided that such use or disclosure would not violate HIPAA if made by Business Associate or Covered Entities or as required or permitted by applicable law, rule, regulation, or regulatory agency or by any accrediting or credentialing organization to whom a Party is required to disclose such PHI. In addition, Subcontractor may:

(a) use PHI, if necessary, for the proper management and administration of Subcontractor or to carry out the legal responsibilities of Subcontractor; or

(b) disclose PHI, if necessary, if the following requirements are met:

(i) the disclosure is required by law; or

(ii) Subcontractor 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 purpose for which it was disclosed to the person, and the person notifies Subcontractor of any instances of which it is aware in which the confidentiality of the PHI has been breached.

2.2 Restrictions. Subcontractor shall not use or disclose PHI for any other purpose not described herein.

2.3 Subcontractor Employees. Subcontractor shall ensure that its employees to whom it provides PHI agree to the same restrictions and conditions that apply to Subcontractor pursuant to this Agreement with respect to PHI and Electronic PHI. Appropriate Safeguards; Security. Subcontractor shall implement appropriate and commercially reasonable safeguards to prevent use or disclosure of PHI other than as permitted in this Agreement. Effective as of the date Business Associate is required to comply with 45 C.F.R. Part 164 Subpart C, Subcontractor shall implement Administrative, Physical and Technical Safeguards that reasonably and appropriately protect the Integrity, Availability, and Confidentiality of Electronic PHI. Subcontractor shall report to Business Associate in writing within twenty-four (24) hours of any Security Incident of which it becomes aware.

2.5 Government Access to Records. Subcontractor shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Subcontractor on behalf of, Business Associate available to the Secretary of the Department of Health and Human Services for purposes of determining Business Associate's compliance with HIPAA. Subcontractor shall provide Business Associate with a copy of any PHI that Subcontractor provides to the Secretary concurrently with providing such PHI to the Secretary.

2.6 HITECH Act. Business Associate and Subcontractor hereby agree that the provisions of HIPAA and the HITECH Act that apply to business associates and that are required to be incorporated by reference in a business associate agreement are incorporated into this

Agreement as if set forth in this Agreement in their entirety and are effective as of the applicable effective date of each such provision. Subcontractor hereby further agrees to comply with all requirements of HIPAA, the HITECH Act and each of their implementing regulations that are applicable to business associates commencing as of the applicable effective date of each such provision.

2.7 Reporting of Improper Use or Disclosure. Subcontractor shall report to Business Associate in writing within twenty-four (24) hours of any actual or suspected violations of this Agreement or any actual or suspected Breach of Unsecured PHI. An actual or suspected Breach shall be treated as discovered by Subcontractor as of the first day on which such Breach is known to the Subcontractor, its employees, officers or other agents, or, by exercising reasonable diligence, should have been known to Subcontractor, its employees, officers or other agents. Subcontractor's notification to Business Associate, to the extent possible, shall include the identity of each Individual whose Unsecured PHI has been, or is reasonably believed to have been, breached and be in substantially the same form as **Attachment A** hereto. Subcontractor further agrees to fully cooperate in good faith with and to assist Business Associate in complying with the requirements of HIPAA and the HITECH Act.

2.8 Mitigation. Subcontractor shall mitigate, to the extent practicable, any harmful effect that is known to Subcontractor of a use or disclosure of PHI or Unsecured PHI by Subcontractor in violation of the requirements of this Agreement, HIPAA or the HITECH Act.

2.9 Availability of PHI. To the extent that the Parties mutually agree in writing that PHI is part of a Designated Record Set, and that such Designated Record Set (or a portion thereof) is to be maintained by Subcontractor, as set forth and agreed to in **Attachment B**, Subcontractor shall within ten (10) days after a written request from Business Associate:

(a) provide access, at the request of Business Associate, and in the time and manner designated by Business Associate, to such PHI to Business Associate or, as directed by Business Associate, to an Individual in order to meet the requirements under 45 CFR § 164.524; and

(b) make amendments to such PHI as directed or agreed to by Business Associate in accordance with the requirements of 45 CFR § 164.526.

2.10 Accounting Rights. Subcontractor shall document disclosures of PHI and information related to such disclosures and, within ten (10) days after Business Associate's written request, shall provide to Business Associate or to an Individual, in time and manner designated by Business Associate, information collected in accordance with this Section, as would be required for Business Associate to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR § 164.528.

3. Termination.

3.1 Term. The Term of this Agreement shall be effective as of the date set forth above and shall terminate when Subcontractor ceases to perform the services as set forth in the

Records Agreement; provided, however, that certain obligations shall survive termination of this Agreement as set forth in Sections 3.3 and 4.6.

3.2 Termination for Cause. Business Associate may immediately terminate this Agreement in the event that Subcontractor breaches any provision of this Agreement. In its sole discretion, Business Associate may permit Subcontractor the ability to cure or to take substantial steps to cure such material breach to Business Associate's satisfaction within thirty (30) days after receipt of written notice from Business Associate. Business Associate may additionally report any Breaches to the Secretary.

3.3 Return or Destruction of PHI. Upon termination, if feasible, Subcontractor shall return or destroy all PHI received from, or created or received by Subcontractor on behalf of, Business Associate that Subcontractor still maintains in any form and shall retain no copies of such information. Prior to doing so, Subcontractor further agrees to recover any PHI in the possession of its subcontractors or agents. If it is infeasible to return or destroy PHI, Subcontractor shall provide to Business Associate notification of the conditions that make return or destruction of PHI infeasible. Subcontractor shall continue to extend the protections of this Agreement to such PHI, and limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

3.4 Termination of Records Agreement. Upon termination of the Records Agreement, either party may terminate this Agreement by providing written notice to the other party.

4. Miscellaneous.

4.1 Amendment to Comply with Law. The Parties acknowledge that it may be necessary to amend this Agreement to comply with modifications to HIPAA, including but not limited to statutory or regulatory modifications or interpretations by a regulatory agency or court of competent jurisdiction. No later than sixty (60) days after the effective date of any such modifications, the Parties agree to use good faith efforts to develop and execute any amendments to this Agreement as may be required for compliance with HIPAA.

4.2 Amendment. This Agreement may be amended or modified only in writing signed by the Parties.

4.3 No Third Party Beneficiaries. Except as provided in Section 5.6 below, nothing expressed or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Business Associate, Subcontractor and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

4.4 Governing Law. This Agreement shall be governed by and construed in accordance with HIPAA and its implementing administrative simplification regulations, the HITECH Act and its regulations, and the laws of the State of Georgia without regard to conflicts of law principles.

4.5 Paragraph Headings. The paragraph headings in this Agreement are for convenience only. They form no part of this Agreement and shall not affect its interpretations.

4.6 Indemnification. Subcontractor shall indemnify and hold Business Associate, each Covered Entity, and each of their respective employees, partners, members, independent contractors, agents and representatives (collectively the “Indemnified Persons”), harmless from and against all claims, liabilities, judgments, fines, assessments, penalties, awards or other reasonable 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 of this Agreement by Subcontractor, including without limitation, (a) expenses the Indemnified Persons directly or indirectly incur in notifying affected Individuals of a Breach caused by Subcontractor or its employees or agents and (b) any penalties, sanctions, assessments, or charges incurred by the Indemnified Persons resulting from Subcontractor’s failure to comply with the terms and conditions of Sections 2.5 and 2.7 of this Agreement. The obligations set forth in this Section 4.6 shall survive termination of this Agreement, regardless of the reasons for termination.

4.7 Entire Agreement. This Agreement in conjunction with the Records Agreement and any attachments, exhibits and schedules of this Agreement and/or the Records 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.

IN WITNESS WHEREOF, the Parties hereto have executed this Agreement by their duly authorized representatives to be effective as of the Effective Date.

SUBCONTRACTOR:

BUSINESS ASSOCIATE:

[SUBCONTRACTOR NAME]

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Attachment A

Notification to Business Associate about a Breach of Unsecured PHI

This notification is made pursuant to Section 3.7 of the Business Associate Subcontractor Agreement (the “Agreement”) between [Subcontractor Name] (“Subcontractor”) and _____ (“Business Associate”).

Subcontractor hereby notifies Business Associate that there has been an actual or suspected breach of unsecured protected health information (PHI) that Subcontractor has used or has had access to under the terms of the Agreement (“Breach”).

Description of Breach: _____

Date of Breach (if known): _____

Date of the Discovery of Breach: _____

Number of Individuals affected by Breach:

The types of unsecured PHI that were involved in Breach (such as the name, Social Security number, date of birth, home address, account number or disability code of the affected Individuals): _____

Description of the steps Subcontractor is taking to investigate Breach, mitigate losses, and to protect against any further Breaches: _____

Contact information for Business Associate and Affected Individuals to ask questions or learn additional information:

Attachment B

Identification of Designated Record Set

As contemplated in Section 2.9, the Parties agree to the provision marked below:

- The PHI that Subcontractor creates or receives from or on behalf of Business Associate, or has access to, in the course of providing the Services constitutes a Designated Record Set (or a part thereof), and such Designated Record Set (or portion thereof) shall be maintained by Subcontractor.

- The PHI that Subcontractor creates or receives from or on behalf of Business Associate, or has access to, in the course of providing the Services DOES NOT constitute a Designated Record Set (or a part thereof), and NO such Designated Record Set (or portion thereof) shall be maintained by Subcontractor.

Policy 14.1(4) and 18.2 (b)

INFORMATION SYSTEM ACTIVITY REVIEW

Policy:

Center shall conduct a regular organizational review of activity on its systems containing electronic private health information (EPHI) and otherwise act to determine if this information is being used or disclosed in an inappropriate manner.

Procedures:

- 1) The Security Officer will review audit logs, access reports, security incident reports, and identity theft Red Flag reports on a (monthly/weekly) basis.
- 2) The Security Officer will immediately act to correct any threat or potential threat to the security of Center's EPHI discovered as a result of this review.
- 3) Georgia Mountains Health Services will monitor and control access to computers and other electronic devices containing or accessing EPHI so that only the appropriate personnel can use these.
- 4) Georgia Mountains Health Services will monitor and control access to EPHI itself through the continual use of unique passwords and key cards and tokens.



Policy 14.2

ASSIGNED SECURITY RESPONSIBILITY

Designated Security Officer: Rhonda Patterson, IT Manager

By signing below, I hereby accept the position of Security Officer for Georgia Mountains Health Services. I understand that with my acceptance of this position, I am accepting additional duties and responsibilities,* including, but not limited to:

- 1) Perform and document an information security risk analysis.
- 2) Provide guidance and assistance in identifying, implementing, and maintaining organization-wide information security policies and procedures that comply with the Final Security Rule.
- 3) Provide direct training and oversight to all employees, contractors, alliance, or other third parties with information security clearance on the information security policies and procedures.
- 4) Initiate activities to create information security awareness within the organization.
- 5) Serve as the information security liaison to administration and staff.
- 6) Review all security-related activity, assist with security-related planning, and act as a liaison to information technology professionals.
- 7) Monitor compliance with the security policies and procedures.
- 8) Oversee the Identity Theft Prevention Program.

Accepted: _____ Date: _____

Print name: _____

*[The above duties can also be added to the Security Officer's official job description, if one exists.]



SECURITY INCIDENT POLICIES AND PROCEDURES

Policy:

A security incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. Georgia Mountains Health Services shall address all known or suspected security incidents involving Center's electronic private health information (EPHI) and will try to lessen, to the extent possible, their harmful effects.

Procedures:

- 1) All staff members will be informed as to who Center's Security Officer is and what constitutes a security incident.
- 2) Any staff member of Georgia Mountains Health Services who learns that a security incident has taken place, is taking place, or will probably take place shall report this to Center's Security Officer, either orally or in writing, immediately.
- 3) Georgia Mountains Health Services shall immediately respond to all security incidents and work quickly to mitigate any damage resulting from same.
- 4) If criminal activity is indicated, the Security Officer shall contact law enforcement authorities.
- 5) The Security Officer will oversee an investigation into each and every security incident to determine its cause.
- 6) The Security Officer will work with staff and/or information technology professionals to correct the problem causing the security incident or allowing it to occur.
- 7) The Security Officer will complete a Security Incident Report identifying the security incident and documenting the response to, and investigation and outcome of same.

Policy 14.3 and 18.3

Georgia Mountains Health Services

SECURITY INCIDENT REPORT

Date _____ Time _____ Reported by _____
 employee patient/family member other

Category:

- Impermissible disclosure of EPHI
- Lack of physical safeguards protecting EPHI
- Inappropriate accessing of EPHI
- Identity Theft Red Flag
- Other

Describe events as reported:

Immediate response:

Date investigation begun:

Describe fact finding and person involved:

Final summary and response:

Signature of person reporting: _____ Title: _____



Policy 14.4

CONTINGENCY PLAN

Emergency Mode Operation Plan

- 1) Any staff member detecting an emergency should immediately report it to the Security Officer or the Privacy Officer.
- 2) The Security Officer will determine the extent and seriousness of the emergency and initiate the Disaster Recovery Plan, if appropriate.
- 3) The Security Officer will determine whether additional equipment and supplies are needed and notify vendors if immediate delivery of these is necessary to bring Georgia Mountains Health Services to an operational level.
- 4) If needed, the Security Officer will set up a temporary office site with telephone and computer equipment and coordinate moving equipment and support personnel to the alternate site.
- 5) If needed, the Security Officer will supervise the retrieval of the backed-up EPHI onto the computer equipment at the temporary office site. Critical applications that must work in order to continue operations while in emergency mode are electronic medical and dental records. These systems contain the most critical information and should receive the highest priority in data restoration.
- 6) As soon as the hardware is up and running at Center's regular offices, the Security Officer will supervise the loading of software and restoration of the backed-up EPHI.



Policy 14.8

WORKFORCE SECURITY POLICIES AND PROCEDURES

Policy:

Georgia Mountains Health shall ensure that all staff members have appropriate access to electronic private health information (EPHI) according to their job function and responsibilities.

Procedures:

- 1) Potential new employees will be screened prior to hiring via reference checks.
- 2) The Security Officer shall grant access to the computers and programs containing EPHI to new staff members upon their beginning employment with Georgia Mountains Health Services. Such access will be granted in the form of unique username(s) and password(s) to allow each staff member to access those screens necessary to perform their specific job function for Georgia Mountains Health Services.
- 3) The Security Officer will document the level of access granted to each staff member and the reasons such access is necessary.
- 4) If the status or job functions of any staff member changes, the Security Officer will review that staff member's access to determine if it remains appropriate. If such a staff member's access is no longer adequate, the Security Officer will expand access as necessary. If a staff member no longer needs access to certain programs or screens, the Security Officer will diminish that staff member's access to correspond with his or her new duties.
- 5) The Security Officer will maintain a current log of the assignment of usernames to staff members.
- 6) All staff members of Georgia Mountains Health Services will be trained as to the importance of keeping EPHI secure and will be required to sign a Confidentiality Agreement regarding EPHI as a condition of continued employment with Georgia Mountains Health Services.
- 7) The Security Officer will ensure that a staff member's username(s) and password(s) have been deleted from the system so as to prohibit access to EPHI within 24 hours of the termination of that staff member's employment, whatever the reason for such termination.
- 8) If the Security Officer is not the person terminating a staff member's employment, the Security Officer will be notified of that termination immediately.
- 9) The Security Officer or other designated staff member(s) will supervise outside maintenance and vendor personnel who are working in Georgia Mountains Health Services' facility during office hours when staff members are logged into programs containing EPHI.

User IDs and Passwords Policy and Procedures

PURPOSE

It is the policy of the Georgia Mountains Health Services that only authorized Information System Users will be allowed to access the electronic information systems. Individual job descriptions, duties, and responsibilities of the employee will be used to determine the level of access for each authorized system/network user.

SCOPE

This policy applies to all business associates, partners, vendors, and staff of Georgia Mountains Health Services that have been issued User IDs for access to the information system and network of all managed sites and services of the organization.

POLICY

This policy is in place to aid in the protection of confidential or private information. It is the duty of all Georgia Mountains Health Services users to take steps appropriate to aid in this protection. The policy is broken down into the following components:

- Only authorized, approved users are provided access to Georgia Mountains Health Services computer systems.
- All users must complete an IT security training session BEFORE access to any system is granted/authorized.
- Authorized system users will only receive access to Protective Health Information as outlined in their respective role or job duties.
- All computer system users must adhere to the security policies implemented by Georgia Mountains Health Services. Copies of these policies are available through the Georgia Mountains Health Services internal exchange server.
- Information and data entered into Georgia Mountains Health Services supported systems is the property of Georgia Mountains Health Services and must be protected in accordance with Georgia Mountains Health Services policies.
- The system User ID and password is to be used exclusively by the assigned staff member. Neither the User ID nor password should be shared by any other person, including other staff members. It is the duty of the authorized staff member to take the steps necessary to protect Georgia Mountains Health Services systems.
- The IT Department will maintain a listing of all assigned logins. This listing WILL NOT include any user password.
- User IDs will be disabled or deleted immediately upon notification of employee separation by the Human Resources department to the IT Help Desk. Terminated staff should not attempt to access Georgia Mountains Health Services equipment or systems.
- Georgia Mountains Health Services IT staff will perform User Login audits at least twice annually or as needed.
- Any User ID found to be shared or used by anyone other than the assigned user will be disabled. Formal disciplinary actions may be taken for this violation.

RESPONSIBILITIES/ROLES

Overall responsibility for ensuring satisfactory implementation of Information Security falls on many levels of staff:

- **IT Manager**– to ensure the appropriate information security policies are developed and enforced. Also, to work with clinical and administrative team members to create a secure yet workable information system environment.

- **Compliance Manager**-to monitor, address, and report any breach in protected health information.
- **Support Staff** – to follow and enforce information security policies as well as use every opportunity to train staff at large.
- **Human Resources Department** – to timely notify the IT department of staff terminations.
- **Managers/Supervisors** – to request only the minimal access level needed for the staff member to effectively perform his/her job.
- **ALL Staff** – to alert the IT Department of any concerns or issues that arise.

PROCEDURE

Upon completion of Information System Management training session provided as a part of New Employee Orientation, the staff member is eligible to be assigned a unique User ID and password.

- To request a user login account:
 1. The Human Resources Coordinator or Office Manager/Supervisor must submit an IT work order request through the IT Help Desk for the requested account(s) access.
 2. The IT Manager or System Administer will create the staff's User ID and password.
 3. An initial password is created for the staff member but the system will require that the staff member change the password on the first successful sign-on/login.
 4. Login information will be provided to the staff member.
- Removing/Deleting/Inactivating logins:
The IT Department will immediately remove/delete/inactivate user IDs upon notification by the Human Resources Department. Additionally periodic (quarterly) audits will be performed comparing an active staff listing (generated from our personnel system) to authorized system logins/User IDs.

COVERED SERVICES

The following are sites or services, administered by the IT Department, that require unique, individual logins:

- Network, E-mail and Internet services
- Web Portal
- SunRx 340B
- Greenway Success EHS
- Georgia Registry of Immunization Transactions (GRITS)

GENERAL GUIDELINES

The following guidelines should be observed to protect confidential information:

- Users should not share their User ID and/or password with other staff members.
- Passwords should be changed every ninety (90) days.
- If you forget your password, or believe someone is using your login, create an IT Help Desk ticket immediately.
- When creating a password:
 - Refrain from using words found in the dictionary.
 - Use a combination of letters and numbers.
 - Create a password at least 6 characters in length.
 - DO NOT write down your password on paper.

- Select or create a password that is easy to remember but difficult for others to guess.

INFORMATION ACCESS GUIDELINES

Access to information, sites and/or services is limited by the job duties or role of the requesting user. It is the goal to provide users with the minimal amount of access required to complete their assigned tasks.

Types of Information

The following table outlines examples of the general types of information that is compiled as a part of a patient record. Most, if not all, of this information is stored in an electronic format.

Demographics	Payor	Complaint/Concern	Diagnosis	Clinical Notes	Sensitive
Name, Address, Date of Birth, Sex, Telephone Number	Insurer, Policy Number, Group Number, Insured's Name	Reason for visit, chief complaint	Diagnosis	Treatment Plan, Observational Notes, Orders	Behavioral Health, Family Planning, HIV/AIDS status

General Information Access EHS

The following table outlines the “general” access guidelines used when granting system/data access. Please note that these guidelines are conditioned by the actual job duties of the individual staff member.

	Demographics	Payor	Complaint/Concern	Diagnosis	Clinical Notes	Sensitive
Front Desk	Yes	Yes	Yes	No	No	No
Clinical Staff	Yes	Yes	Yes	Yes	Yes	Conditional
Provider Staff	Yes	Yes	Yes	Yes	Yes	Yes
Billing Department	Yes	Yes	Yes	Yes	No	No
Audit/Utilization Review	Yes	Yes	Yes	Yes	Yes	No
Third Party Access	Yes	Yes	No	Yes	No	No

Conditional: Only as it applies to direct patient care. Examples include Behavioral Health services, Family Planning services, HIV, or other protected types of information.

VIOLATION REPORTING

Any suspected use of your User ID and/or password by others should be immediately reported to the IT Department.

The IT Department can be reached by:

- Work order submitted at helpdesk@gamtnhealth.org
- Telephone at (706) 946-5603
- Fax at (706) 374-7628



Policy 14.8/16.1

Password Log

All password logs will be maintained by the IT Manager/Security Officer.



INFORMATION ACCESS MANAGEMENT: CLEARINGHOUSE FUNCTION

By my signature below, I certify that the required implementation specification “Isolating Health Care Clearinghouse Functions,” located at § 164.308(a)(4)(ii)(A) of the Final Security Rule, does not apply to Georgia Mountains Health Services, as same does not function as a clearinghouse for any larger health care organization.

Signed: _____

Date: _____

Title: _____



Policy 14.9(2)

ACCESS ESTABLISHMENT POLICIES AND PROCEDURES

Policies:

Authorized access to electronic private health information (EPHI) shall be established by allowing use of Georgia Mountains Health Services computers and issuing each user a unique username and password by which to open and manipulate certain of Center's software programs.

Should any staff member's duties change such that he/she requires access to more, less, or different EPHI than in his/her prior position, his/her access will be modified accordingly.

Procedures:

- 1) Georgia Mountains Health Services provides PCs for its staff members' use in accessing the minimum amount of EPHI necessary for each staff member to perform his/her specific duties.
- 2) Unique usernames and passwords will be assigned to each staff member. These are to be kept confidential and are not to be shared with anyone. Each username and password will only gain entry to those programs which the user to whom they are assigned has been authorized to access.
- 3) Any staff member who learns of password-sharing for any reason should immediately notify the Security Officer. Staff members who (a) participate in password-sharing or (b) fail to report knowledge of password-sharing are subject to sanctions up to and including termination of employment.
- 4) Users must log off programs when leaving a PC unattended for a substantial period of time (for example, when going to lunch). All users must log off PCs before leaving for the day.
- 5) If a staff member's duties change such that different access to EPHI is required, the Security Officer will make sure that person's access to the Center's programs is modified to correspond with the new duties.
- 6) If a staff member's employment is terminated, his/her username(s) and password(s) will be deleted upon leaving Georgia Mountains Health Services.
- 7) All changes to staff members' access will be documented in the Center's Level of Access Log and/or Password Log.



Policy 14.10(2)

PROCEDURES FOR PROTECTION FROM MALICIOUS SOFTWARE

Procedures:

- 1) To protect our patients' EPHI from being damaged or destroyed by a computer virus, staff must never bring in software, diskettes and CDs from home and put them in Georgia Mountains Health Services' PCs. Please do not do this, even if you think it is safe.
- 2) No one should ever download anything off of the Internet unless it is checked and authorized by the Security Officer. Computer viruses and "worms" can completely wipe out patient information. Any unauthorized software or games should be promptly removed. The Security Officer will periodically check PCs to make sure they do not contain unauthorized programs.
- 3) Virus protection software is installed and will be kept reasonably current to protect against new computer viruses.



Policy 14.10(3)

LOG-IN MONITORING PROCEDURES

Procedures:

- 1) Each staff member has been assigned a unique username and password. If a user unsuccessfully tries to log into one of Georgia Mountains Health Services' programs three times, that username will be locked out and the unsuccessful log-in attempt reported to the Security Officer.
- 2) The Security Officer will regularly review software reports of attempted unsuccessful log-ins and investigate as necessary.



Policy 14.10(4)

PASSWORD MANAGEMENT PROCEDURES

Policy:

All staff members have been assigned unique usernames and passwords to access Georgia Mountains Health Services' computer systems. These must be kept confidential and not shared with anyone, as disclosure of usernames and passwords can put our patients' EPHI in danger of being compromised.

Procedures:

- 1) The Security Officer or his/her designee will assign each staff member a personal username and password(s) that cannot be easily guessed. This assignment will be documented in Center's Password Log.
- 2) A staff member's password(s) will afford him/her access to only those computer programs necessary to complete the duties that come with his/her particular position with Georgia Mountains Health Services.
- 3) All staff members must guard the confidentiality of their usernames and passwords. If a staff member – either intentionally or negligently – allows someone else to access, alter or disclose our patients' EPHI, that staff member will be held responsible for any improper action taken. Any person having knowledge of the misuse of usernames and passwords, or who has been given a username and password that has not been officially assigned to him/her, should report this to the Security Officer immediately.
- 4) Any time the Security Officer has reason to believe that one or more assigned usernames and passwords at Georgia Mountains Health Services has been compromised, he/she will delete those usernames and passwords from the system and assign new ones.
- 5) To further protect our patients' EPHI, the Security Officer will periodically assign replacement usernames and passwords to all staff and delete the old ones.



Policy 14.11(2)

Application and Data Criticality Log

Application and critical data logs will be maintained by IT Manager/Security Officer.



Policy 15.1

WORKSTATION USE POLICIES AND PROCEDURES

Policy:

Physical access to EPHI will be restricted to authorized personnel.

Procedures:

- 1) Only authorized staff members may use Georgia Mountains Health Services' PCs and/or view EPHI.
- 2) PC monitors will be positioned where they cannot be viewed by casual observers. In instances where this is not possible, privacy screens will be employed or screen savers will be set to come up after 60 seconds of inactivity.
- 3) Visitors outside the waiting area will be escorted or monitored at all times.
- 4) Visitors will not be allowed to use Georgia Mountains Health Services' PCs for any reason.
- 5) All staff members must log off when leaving their workstation for an extended period of time (i.e., to go to lunch).
- 6) All staff members must log off when leaving for the day.



Policy 15.3

DEVICE AND MEDIA CONTROLS POLICIES AND PROCEDURES

PURPOSE

This policy provides the guidelines used by Georgia Mountains Health regarding removable media including its use, accounting, and destruction procedures. The use of removable media creates a risk of loss or compromise of Personal Health Information or confidential information. This policy has been developed to minimize that risk of loss.

SCOPE

This policy governs the use of removable media by anyone gaining access to Georgia Mountains Health network services or equipment.

Examples of removable media include, but are not limited to:

- Memory cards or memory sticks
- External Hard Drives
- Smart Phones
- Laptops, notebooks, netbooks
- iPods, iPads, MP3 Players
- Magnetic Tapes or Cartridges
- Flash or thumb drives
- Diskettes (Floppy, Zip, Jaz)
- CDs or DVDs
- Printers, copiers, and fax machines

POLICY

The following guidelines should be followed to comply with this policy:

- The use of removable media for business purposes must be approved by your supervisor and the Georgia Mountains Health IT department. **NOTE: Be prepared to provide the information to justify the stated need for the media device. Devices must be protected and passwords must be shared with the IT Manager and Administrative Support Staff.**
- Extreme care should be used when copying any PHI or other confidential information to removable media.
- Information and data produced or created by any individual, contractor, or vendor employed by Georgia Mountains Health is the property of Georgia Mountains Health Services, Inc.
- Release or sharing of unapproved, confidential information is a violation of Georgia Mountains Health policy. Any violation of this policy may be turned over to the Human Resources department or law enforcement.
- Loss, theft, or damage of removable media must be immediately reported to the IT Manager, Compliance Manager, and/or the CEO.


- If you are transferred to a different position, any removable media assigned to you must be returned to the IT department. If your new position requires, the removable media will be re-assigned.
- Removable media is not to be shared with co-workers.
- The removable media/device is issued for business use only.

PROCEDURE

Request to use removable media

1. A request for removable media use must be made to the IT Manager. The request must contain the reason for the need and the approval of your supervisor.
2. The requesting staff member must sign and acknowledge the *Removable Media and Data Device Usage Agreement* form.
3. A copy of the form is maintained on file in the IT Department.
4. The IT Department will review all authorizations on an annual basis and may require that staff assigned removable media produce the device for verification and that updated acknowledgement forms are completed.

Use of removable media

- All removable media devices, including any cell phone used to access the organization's network, must be password protected.
- Users are required to enable the lock screen function on every computer upon leaving the workstation. The function is enabled by holding down the Windows logo key  and the L key simultaneously. CTRL, ALT, Delete will unlock the screen.
- User must take appropriate steps to prevent disclosure of sensitive data.
- It is the responsibility of the user to store removable data devices in a secure location at all times.
- It is the responsibility of the user to immediately notify the IT Manager or the Compliance Manager if a mobile data device is lost or stolen.

Disposal/Destruction of removable media

- All destruction/disposal of electronic protected health information (PHI) media will be done in accordance with federal and state law, state policy and following Georgia Mountains Health written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- Records involved in any open investigation, audit or litigation should not be destroyed/disposed. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
- Records or other documents containing PHI scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of protected health information is complete. This means that this material should be stored in secure containers (not in wastebaskets, boxes, recycle bins, etc.) and secure locations until the time of destruction/disposal.
- Contracts between Georgia Mountains Health and its business associates will provide that, upon termination of the contract, the business associate will promptly return or

destroy/dispose of all protected health information. The destruction of PHI by the Business Associate will be documented in writing and sent to the Georgia Mountains Health. This accounting should include:

- Date of destruction/disposal.
 - Method of destruction/disposal.
 - Description of the destroyed/disposed record series or medium.
 - Inclusive dates covered.
 - A statement that the protected health information records were destroyed/disposed of in the normal course of business.
 - The signatures of the individuals supervising and witnessing the destruction/disposal.
- If such return or destruction/disposal is not feasible, the contract will limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
 - A record of all case files containing protected health information that are destroyed or disposed will be made and retained permanently by Georgia Mountains Health. Permanent retention is required because the records of destruction/disposal may become necessary to demonstrate that the protected health information records were destroyed/disposed of in the regular course of business.
 - Records of destruction/disposal should include:
 - Date of destruction/disposal.
 - Method of destruction/disposal.
 - Specify the time that will elapse between acquisition and destruction/disposal of data/media.
 - Description of the destroyed/disposed record series or medium.
 - Inclusive dates covered.
 - A statement that the protected health information records were destroyed/disposed of in the normal course of business.
 - The signatures of the individuals supervising and witnessing the destruction/ disposal.
 - Establish safeguards against breaches in confidentiality.
 - Indemnify Georgia Mountains Health from loss due to unauthorized disclosure.
 - Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.
 - Provide proof of destruction/disposal.
 - Consumer information media will be destroyed/disposed of using a method that ensures the consumer information cannot be recovered or reconstructed.
 - Methods of destruction/disposal may be reassessed annually by the IT Manager and/or the Compliance Manager, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

VIOLATION REPORTING

Any observed/suspected violation of this policy, or any suspected loss or breach should be **immediately** reported to the IT Manager, Compliance Manager and/or the CEO.

- Rhonda Patterson, IT Manager
Email: rpatterson@gamtnhealth.org
Office: 706-946-5603
Cell: 706-455-0591

- Karen Driskill, Compliance Manager
Email: kdriskill@gamtnhealth.org
Office: 706-946-5605
Cell: 706-889-8241
- Steven Miracle, CEO
Email: smiracle@gamtnhealth.org
Office: 706-946-5610
Cell: 706-455-3044

DEFINITIONS

Personal Health Information (PHI) – Individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

REVISION HISTORY

June 13, 2017



Removable Media and Data Device

USAGE POLICY AGREEMENT

This policy governs the use of removable media and data devices that are issued to individuals for corporate use. Examples of removable media include, but are not limited to:

- Memory cards or memory sticks
- External Hard Drives
- Smart Phones
- Laptops, notebooks, netbooks, iPads
- Magnetic Tapes or Cartridges
- Flash or thumb drives
- CDs or DVDs
- Printers, copiers, and fax machines

The data device being issued to you is the property of Georgia Mountains Health Services, Inc. It is being issued to you as a tool to aid you in completing your work assignments. You are expected to take reasonable care of the equipment in order to prevent loss, misuse or damage. The device must be password protected and enhanced security settings must be enabled.

You are responsible for any loss, misuse, theft or damage. Loss or damage due to negligence or misuse of the device will result in a deduction from your paycheck equal to cost for repair or replacement. **YOU MUST REPORT LOSS OR DAMAGE IMMEDIATELY TO THE IT DEPARTMENT AT (706) 455-0591 OR BY E-MAIL TO rpatterson@gamtnhealth.org**

If you misplace your device, call or e-mail the IT Manager or Compliance Officer **immediately** in order to have service temporarily suspended and passwords reset. Failure to notify the organization may make you responsible for additional charges.

Do not share your device with patients or coworkers. You will be held responsible for any mishandling or breach of confidentiality as a result of misuse.

If you leave your present position, you must turn in the device and all accompanying equipment to your supervisor or the IT Department. You will be required to pay the full replacement cost of any item not returned.

PLEASE FOLLOW THESE BASIC GUIDELINES:

- **The data device is issued for business purposes** - Personal use should be kept to a minimum.
- **Do not use the device while driving.** To make or receive emails, be sure to be safely stopped before using any device.

Additional software cannot be added to the device. This includes services such as instant messaging, games, or other applications without IT approval. You will be held financially responsible for any such actions including any charges related to the service or processing fees imposed.

Please note some mobile devices are GPS enabled and movement of these assets may be tracked without notice.

You are required to report any questionable emails which might contain malware or viruses on the device assigned to you.

This is to certify that I have read and understand the **Data Device Usage Policy** and I agree to abide by the policy as a condition of my employment with Georgia Mountains Health Services, Inc.

Furthermore, I understand that by assuming custody of the device, I assume responsibility for use thereof and will reimburse Georgia Mountains Health Services, Inc in case of theft or damage. Any questions regarding this agreement should be addressed to the CEO, IT Manager, or Compliance Officer.

It is also necessary to report lost or stolen personal devices which are used to access work emails and electronic PHI. Should you leave your present position with Georgia Mountains Health Services, all work related accounts and logins will be immediately terminated.

Personal devices are not allowed to be connected to the organization’s wireless internet. Streaming of music or videos is not permitted on any device that is connected to Georgia Mountains Health’s secured WIFI.

Requesting Staff Member:

Printed Name

Signature

____/____/____
Date

Issuing IT Department Signature

____/____/____
Date

**** IT Department Use ONLY ****					
Equipment Issued:					
Manufacturer		Model		Serial Number	
Equipment (list accessories seperately)		Issued by	Date Issued	Returned to	Date Returned

Return Information (IT Department Use ONLY):

____/____/____
Date Returned

Returned By (Staff Name)

ID Tag#

Received By

Document any known problems with condition of equipment:



Policy 15.3

IT Equipment Tracking Log

All IT equipment will be tracked from acquisition to destruction by IT Manager. No equipment shall be moved without approval from the IT Manager. Staff should utilize the *IT Movement of Property* form to request a relocation of equipment.

The IT Manager/Security Office will maintain an IT Equipment Tracking Log.



MOVEMENT OF PROPERTY

To be completed in all instances where equipment is removed from a station/location

DETAILS OF PERSON REQUESTING TO REMOVE/MOVE EQUIPMENT

Name _____ Contact number _____

FULL DESCRIPTION OF EQUIPMENT INCLUDING ANY RELEVANT SERIAL NUMBERS

CURRENT LOCATION OF EQUIPMENT (circle one)

Blue Ridge Medical Ellijay Dental DaltonChatsworth Dahlonega Administration

DESTINATION OF EQUIPMENT

DATE OF MOVEMENT

____ / ____ / ____

Tag# _____

Room Number _____

DETAILS OF PERSON GIVING AUTHORITY FOR MOVEMENT

Name _____ **Position** _____

Contact Number(s) _____

SIGNATURE

Date ____ / ____ / ____

COMMENTS (i.e. mode of transport etc)

The original copy of this form must kept on file on site and a copy submitted to IT dept.



Policy 15.4

FACILITY ACCESS CONTROLS

Policy:

Georgia Mountains Health Services strives to control physical access to its offices. Staff members are expected to safeguard our patients' EPHI by helping keep visitors out of unauthorized areas.

Procedures:

- 1) The rear door of Georgia Mountains Health Services will remain locked at all times. All staff members are provided a key to this door, and propping the door open is never allowed.
- 2) The visitors' entry opens into the waiting area. This door will be unlocked during the hours in which Georgia Mountains Health Services is seeing patients. Visitors in the waiting area will be monitored by staff members in reception. Staff members in reception are located where they can see the waiting area and control access to the rest of the facility.
- 3) The receptionist will unlock the visitors' entry door when she arrives each morning and lock it when she leaves for the day. The last staff member to leave for the day will arm the security alarm system. The first staff member to arrive in the morning will disarm it.
- 4) Every staff member is allowed in every part of the facility and may access any piece of equipment, though, depending on his/her job function, he/she may not have the passwords needed to access certain computer applications.
- 5) Computer monitors are positioned so as to prevent visitors from seeing other persons' EPHI. Visitors to Georgia Mountains Health Services are to be escorted or monitored at all times so as to prevent them from accessing or seeing any EPHI except their own.
- 6) All staff members must log off before leaving for the day to prevent facility maintenance and cleaning personnel from unnecessarily accessing or seeing EPHI after hours.
- 7) In the event of an emergency, the Security Officer will notify vendors and other repair personnel of needed service, supplies and/or equipment. The Security Officer will ensure that vendors and other repair personnel have access to EPHI in support of restoration of lost data, if necessary. The Security Officer or his/her designee will monitor such outside personnel while they have this temporary access. All staff members will continue to have routine access to EPHI as under normal conditions.
- 8) The Security Officer will record any security-related repairs or modifications to the facility in Georgia Mountains Health Services' Maintenance Log.



Information Systems Audits

Policy 16.2

All information systems audits will be maintained by the IT Manager/Security Officer.



Policy 16.4(2) and 16.6

ENCRYPTION AND DECRYPTION/ TRANSMISSION SECURITY

All of Georgia Mountains Health Services' electronic protected health information is contained on secured local, cloud based, and data center servers. Electronic health records are not stored on any portable devices such as laptops or smart phones. Access to the Georgia Mountains Health Services' EPHI is limited to those staff members who have been assigned a personal username and password because that access is necessary for them to perform their specific job functions. Staff members must log in using their username and password in order to gain access to applications containing EPHI.

The only electronic transmissions involving EPHI sent by Georgia Mountains Health are insurance claims sent via Greenway Success EHS software. It is the understanding of the Center that this software encrypts and decrypts these transmissions so as to adequately protect the EPHI contained therein. Therefore, Georgia Mountains Health Services does not believe it needs to employ encryption and decryption itself.

Georgia Mountains Health does not routinely e-mail EPHI, but if we ever do, we will inform our patients that we will communicate with them via e-mail only after the patient signs a statement that he/she understands that e-mail is not secure, may be intercepted, and the patient's privacy breached.



Policy 16.5

INTEGRITY OF EPHI POLICIES AND PROCEDURES

Policy:

Georgia Mountains Health Services will take steps to protect its patients' Electronic Personal Health Information from improper alteration or destruction.

Procedures:

- 1) Passwords will be necessary to access those applications containing EPHI.
- 2) Through unique usernames and passwords, staff members will be granted access only to that EPHI necessary to perform their specific job functions.
- 3) Virus protection will be employed and updated as needed on all PCs.
- 4) Firewall protection will be employed to protect against unauthorized access.
- 5) Physicians' electronic notes are locked and dated at creation so that changes cannot be made without authorization from the software administrator.



Policy 18.3

Examples of Identity Theft Red Flags

Identity theft is an increasing problem in our society. In the course of receiving medical care, patients may need to provide information that could place them at risk for identity theft. Red flags are patterns or activities that could indicate identity theft, and federal regulations now require many health care providers to recognize and respond to red flags. Georgia Mountains Health Services is currently exempt from Red Flag regulations. However, detailed attention to information and documents collected from patients is vitally important to detect and prevent identity theft.

The examples provided in this document can serve as a guide for the types of events or activities that may constitute Red Flags for identity theft. Because methods of identity theft and identity theft detection are continually evolving, no list can be considered comprehensive. The World Privacy Forum maintains a regularly updated collection of materials and news about medical identity theft, including detailed FAQs, reports, public comments, speeches, and other materials at:

<http://www.worldprivacyforum.org/medicalidentitytheft.html>

GENERAL EXAMPLES (applicable to any creditor)

Suspicious Documents:

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
3. Other information on the identification is not consistent with information provided by the patient or client presenting the identification.
4. Other information on the identification is not consistent with readily accessible information that is on file with the Center, such as a signature on forms or recent proof of income.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against external information such as Social Security statements or other sources of income verification.
2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the patient.
3. Personal identifying information provided is of a type commonly associated with fraudulent activity. For example:
 - a. The address on an application is fictitious, a mail drop, or a prison; or
 - b. The phone number is invalid, or is associated with a pager or answering service.
4. The SSN provided is the same as that submitted by other persons in the electronic health system.
5. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
6. Personal identifying information provided is not consistent with personal identifying information that is on file in the electronic medical record.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Center

The Center is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

EXAMPLES SPECIFIC TO HEALTHCARE PROVIDERS

1. A complaint or question from a patient based on the patient's receipt of:
 - a. A bill for another individual
 - b. A bill for a product or service that the patient denies receiving
 - c. A bill from a health care provider that the patient never patronized, or
 - d. A notice of insurance benefits (or Explanation of Benefits) for health services never received.
2. Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.
3. A complaint or question from a patient about the receipt of a collection notice from a bill collector.

4. A patient or insurance company report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.
5. A complaint or question from a patient about information added to a credit report by a health care provider or insurer.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.
8. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.



Policy 18.5

Identity Theft Alerts

If medical identity theft is suspected, staff must notify the Compliance Manager or the Chief Financial Officer. An “Identity Theft alert” should be placed in a victim's health care records to warn providers, insurers, and consumers of potential fraudulent activity in the past or present.



Policy 18.5

Identity Theft File Extraction¹

If fraud or medical identity theft can be substantiated, the victim's file is purged of all information that was entered as a result of the fraudulent activity, and is left with a brief cross-reference and explanation of the deletion.

In the operation of medical identity theft, sometimes fraudulent information may be added to a pre-existing health file. In other cases, the contents of an entire health file may refer only to the thief's health conditions, but under the victim's name and other identifying information. In either case, the fraudulent activity has the end result of having the potential to introduce errors into the file of the victim. Many times the errors entered into a victim's file resulting from activities of a medical identity thief can be medically significant. This is one of the core harms of medical identity theft.

In a file extraction, if the thief is an unknown individual, the fraudulent information is completely removed from the victim's file and held separately so there is no danger of mistreatment due to factual error in the file. That separate file is the Jane or John Doe file. The victim's file and the extracted file are then cross-referenced, allowing for a retraceable data trail for any audits. If the thief is a known individual, the victim's file can undergo the same kind of data extraction. The only difference is that the provider will have a name to file the purged file information under.

¹Source: Robert Gellman and Pam Dixon. Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers. World Privacy Forum, 2008. <http://www.worldprivacyforum.org>



Policy 20

SAMPLE LETTER OF BREACH NOIFICATION

[Date]

BY U.S. MAIL

[Name]

[Address Here]

[City, State Zip Code]

Dear [Name of Patient]:

We are writing to inform you about an information security situation that could potentially affect you and to share with you the steps we have taken to address it.

We discovered on [Insert the date the breach was discovered] that [Insert a brief, objective description of what happened, including the date of the breach.]

The personal health information involved includes [insert a description of the types of unsecured protected health information that were involved in the breach, such as full name, SSN, date of birth, gender, home address, account number, diagnosis, disability code, or other types of information. If appropriate, describe the information that was not involved, such as credit card numbers, bank account numbers, etc.]

We assure you that we are committed to safeguarding your sensitive personal information and have taken steps to fortify the protective measures that were already in place. As soon as this breach of information was discovered, Georgia Mountains Health Services [insert a description of what was done.] [NOTE: Ensure that the description of how the incident was handled does not include any privileged information, i.e. we called our lawyers, had legal counsel order an investigation, produced a report, etc.]. Since the incident, we have [insert a description of what has been done to prevent a future breach].

[OPTIONAL] In addition, to help ensure that this information is not used inappropriately, we have made arrangements to offer you a free one-year membership to [insert name of credit monitoring company]. [Insert a brief description of how the monitoring works]. To take advantage of this offer, [describe the steps for the patient to initiate the monitoring].

While we are uncertain whether your personal information was actually obtained during the unauthorized access, we want to urge you to take actions to minimize your potential risk of identity theft. You may want to consider taking the following steps:

- Call the toll-free numbers of any one of the three major credit bureaus (below) to place a fraud alert on your credit report. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report.
 - Equifax: 1-800-525-6285; www.equifax.com
 - Experian: 1-888-397-3742; www.experian.com
 - TransUnion: 1-800-680-7289; www.transunion.com
- Order your credit reports. By establishing the fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.
- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.
- You can also place a “credit freeze” on your credit file so that no credit reports can be released without your approval. All bureaus charge a fee for this service.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. Georgia Mountains Health apologizes for the stress and inconvenience this situation has caused you.

If you have any questions or require assistance regarding the loss of your personal information, please contact us at *[insert local or toll-free number]*. An associate will be available to answer your call Monday through Friday from 8:30 a.m. to 5:00 p.m. If you would prefer, you may contact us by regular mail at 165 Blue Ridge Overlook, Blue Ridge, GA 30513.

[OPTIONAL] We have also established a section on our Website with updated information and links to Websites that offer information on what to do if your personal information has been compromised.

Sincerely,

Georgia Mountains Health Services



Identification of Breach and Activation of Notification

Policy 20

All incidents of breach or suspected breach of protected health information must be reported to the Privacy Officer. The Privacy Officer will follow the guidelines below.

The guidelines are intended to assist in identifying the appropriate steps to take when a breach of unsecured PHI occurs. The following questions will guide you through a breach of PHI and ensure that you meet the requisite Rule requirements.

Step 1. Was there a breach of unsecured PHI?

- a) Determine whether the use or disclosure of PHI violates the HIPAA Privacy Rule.
 - i) It is not a violation if the information was de-identified.
 - ii) It is not a violation if information disclosed for treatment, payment or operations.
 - iii) Consult with legal counsel if you need advice concerning whether a breach has occurred.
- b) Was the PHI “unsecured”?
 - i) Was the information unreadable, undecipherable through technology?
 - ii) Was the PHI secured through the use of a technology or methodology specified in guidance from HHS?
 - iii) Was the PHI a Limited Data Set that excludes zip codes and dates of birth?

Step 2. Did the use or disclosure compromise the security and privacy of PHI?

- a) Does the use or disclosure of PHI pose a significant risk of financial, reputation or other harm to the individual?
 - i) How many people affected?
 - ii) What type of information was disclosed?
 - (1) Financial information?
 - (2) Sensitive health information?

- iii) To whom was the PHI disclosed?
 - (1) A coworker?
 - (2) A business associate?
- iv) Why did the disclosure occur?
 - (1) Unintentional?
 - (2) Curiosity?
 - (3) Intentional (i.e., theft, sales)?
- v) Who is the patient?
 - (1) Celebrity or Government Official?
 - (2) Mentally ill patients?
 - (3) Minors?

Step 3. Was the breach unintentional, inadvertent, or otherwise excluded from the breach notification requirements?

- a) Was the breach unintentional or acquired by a staff member acting in good faith within the scope of his or her authority?
- b) Was the breach limited to that one staff member?
- c) Was the breach limited to two authorized persons?
- d) Was the disclosure to a person who would not reasonably have been able to mentally or physically retain the unsecured PHI?

Step 4. Determine who to notify.

- a) The following individuals **must** be notified:
 - i) Individual.
 - ii) Media, if 500 or more individuals residing in the same state or jurisdiction are affected.
 - iii) HHS.
- b) The following individuals and entities **may** be notified:
 - i) Notify vendors and business associates of breach.
 - ii) Notify the entity's insurance carrier if necessary.

iii) Notify counsel if necessary.

Step 5. Determine time-frame for notification.

- a) Determine the date of discovery.
- b) Calendar the appropriate deadlines:
 - i) Provider must deliver the breach notification without unreasonable delay, but no later than sixty (60) days after the date of discovery of the breach.
 - ii) If the provider has insufficient contact information for ten (10) or more individuals, then the provider has ninety (90) days to post the notification on its website.
 - iii) If 500 or more individuals affected by the breach, then the provider must notify the media without unreasonable delay, and at the same time, notify HHS.
 - iv) If less than 500 individuals are affected, the provider must keep a log of the breaches and submit to HHS within sixty (60) days of the end of the calendar year.