POLICIES FOR PROTECTION OF THE PRIVACY

OF

PROTECTED HEALTH INFORMATION

Effective: November 1, 2014

Contents

Group Main Stream

POLICIES FOR PROTECTION OF THE PRIVACY OF PROTECTED HEALTH INFORMATION

I. INTRODUCTION

A. Purpose of These Privacy Policies

These Privacy Policies are intended to comply with the requirements of the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), regulations under HIPAA, and any applicable State law that is more stringent than the HIPAA requirements. They are designed to comply with the standards, implementation specifications, and other requirements of the HIPAA security, breach notification, and privacy regulations at 45 CFR Part 160 and Part 164.

These policies are designed to reasonably ensure the confidentiality, integrity, and availability of all electronic protected health information that Group Main Stream ("GMS"), creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under the HIPAA Privacy Rule, GMS's Privacy Policies, and applicable State law; and to ensure compliance with the HIPAA Security regulation by GMS's workforce.

In all instances, these Privacy Policies shall be interpreted and construed consistent with the requirements of HIPAA, its regulations, and any more stringent State law.

In the event of any conflict between a provision of these Privacy Policies and a requirement of HIPAA, a regulation under HIPAA, or a more stringent State law that HIPAA, HIPAA regulation, or State law requirement shall control.

B. Disclaimer

All of the policies and procedures contained or referred to in these Privacy Policies, or that may be added or otherwise established by GMS in the future, represent the policies established by GMS for the members of its workforce in relation to the particular subject addressed by the policy. It is the intention of GMS that these Privacy Policies be used by its employees, and other members of its workforce, in meeting their responsibilities to GMS. Violation of a policy can be the basis for discipline or termination of employment; however, because these Privacy Policies relate to the establishment and maintenance of high standards of performance, under no circumstances shall any policy or procedure be interpreted or construed as establishing a minimum standard, or any evidence of a minimum

standard, of the safety, due care, or any other obligation which may be owed by GMS, its employees, or its agents to another person.

II. PROTECTED HEALTH INFORMATION

A. What is "Protected Health Information?"

"Protected health information" is any health information maintained by GMS that is individually identifiable except employment records held by GMS in its role as an employer.

"Individually identifiable health information" means any health information, including demographic and genetic information, whether oral or recorded in any form or medium, including demographic information collected from an individual, that:

1. Is created or received by a health care provider, a health plan, employer, or health care clearinghouse;

2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and,

3. 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.

All health information maintained by GMS is individually identifiable unless and until it is de-identified as stated in Section II.B, below.

B. De-Identification of Health Information

1. De-Identification

Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

2. Requirements for De-Identification

Before any member of GMS's workforce treats any information as being de-identified, it must be submitted to the Privacy Officer. Whether or not health information has been de-identified will be determined by the Privacy Officer.

The Privacy Officer may find that health information has been de-identified only if one of the following two conditions are met:

a. Condition 1: Statistical and Scientific Principles

A person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(1) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject to the information; and,

(2) Documents the methods and results of the analysis that justify such determination. Such documentation shall be in accordance with the requirements stated in Section IV.N and Section IV.O of these Privacy Policies.

b. Condition 2: Removal of Identifiers

The following identifiers of the individual or of relatives, employers, or household members of the individual are removed and GMS does not 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:

(1) Names;

(2) All geographic subdivisions smaller than a State, including street addresses, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(a) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

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

(3) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date,

discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(4) Telephone numbers;

(5) Fax numbers;

(6) Electronic mail addresses;

(7) Social security numbers;

(8) Medical record numbers;

(9) Health plan beneficiary numbers;

(10) Account numbers;

(11) Certificate/license numbers;

(12) Vehicle identifiers and serial numbers, including license plate numbers;

(13) Device identifiers and serial numbers;

(14) Web Universal Resource Locators (URLs);

(15) Internet Protocol (IP) address numbers;

(16) Biometric identifiers, including finger and voice prints;

(17) Full face photographic images and any comparable images; and,

(18) Any other unique identifying number, characteristic, or code, except as permitted by Section II.B.3 of these Privacy Policies.

3. Requirements for Re-Identification

A code or other means of record identification may be assigned to allow information de-identified to be re-identified by GMS provided:

a. The code or other means of record identification shall not be derived from or related to information about the individual and

shall not otherwise be capable of being translated so as to identify the individual; and,

b. The code or other means of record identification shall not be used or disclosed for any other purpose and the mechanism for re-identification shall not be disclosed.

Whether or not information shall be coded for re-identification and be re-identified shall be determined by the Privacy Officer. If information is re-identified, the Privacy Officer shall oversee the process of doing so.

III. ELECTRONIC PROTECTED HEALTH INFORMATION

"Electronic Protected Health Information" is any protected health information maintained by GMS that is transmitted by electronic media or maintained in electronic media.

"Electronic Media" means:

(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."

IV. ADMINISTRATIVE POLICIES

A. Organizational Policies

1. Affiliated Covered Entity

GMS has elected to designate themselves as a single covered entity for purposes of the HIPAA Privacy and Security Rules. A written or electronic record of that election and designation shall be maintained by the Privacy Officer for six (6) years from the date of its creation or the date it is last in effect, whichever is later.

B. Designation of Privacy Official and Security Official

1. Designation of Privacy Official

GMS's Executive Director shall designate a privacy official who shall be responsible for the development, updating and implementation of GMS's privacy policies. That privacy official shall be called the "Privacy Officer" of GMS. The privacy official may be the same individual who is designated as the security official of GMS.

The Privacy Officer shall be assisted by a committee composed of *the Quality Assurance Manager, Director of HR, the Associate Director and the Executive Director*. This committee shall be known as the Privacy Committee and shall be responsible for assisting the Privacy Officer with developing, updating, and implementing GMS's Privacy Policies. However, final authority over and responsibility for GMS's compliance with the HIPAA Privacy and Breach Notification Rules shall rest with the Privacy Officer.

2. Designation of Security Official

GMS's Executive Director shall designate a security official who shall be responsible for the development, updating and implementation of GMS's security policies. That security official shall be called the "Security Officer" of GMS. The security official may be the same individual who is designated as the privacy official of GMS.

The Security Officer shall be assisted by a committee composed of *the Quality Assurance Manager, Director of HR, the Associate Director and the Executive Director* . This committee shall be known as the Security Committee and shall be responsible for assisting the Security Officer with developing, updating, and implementing GMS's security policies and procedures. However, final authority over and responsibility for GMS's compliance with the HIPAA Security Rule shall rest with the Security Officer.

3. Documentation

GMS's Executive Director shall maintain, or cause to be maintained, a written or electronic record of the designation of the Privacy Officer and of the Security Officer. Such record shall be maintained for six (6) years from the date of its creation or the date it is last in effect, whichever is later.

C. Designation of Other Persons

1. Person/Office to Receive Complaints

GMS's Executive Director shall designate a contact person or office who shall:

a. Be responsible for receiving complaints concerning GMS's privacy and breach notification policies and procedures, GMS's compliance with those policies and procedures, or GMS's compliance with the HIPAA Privacy and Breach Notification Rules pursuant to Section IV.H of these Privacy Policies; and,

b. Provide further information about matters covered by GMS's Notice of Privacy Practices.

2. Person/Office to Receive and Process Requests for Access

GMS's Executive Director shall designate a contact person or office who shall be responsible for receiving and processing individuals' requests for access to protected health information pursuant to Section VIII.B "Right of Access" of these policies.

3. Person/Office to Receive and Process Requests for Amendment, Correction, or Clarification

GMS's Executive Director shall designate a contact person or office who shall be responsible for receiving and processing individuals' requests for amendment, correction, or clarification of protected health information pursuant to Section VIII.C "Right to Request Amendment" of these policies.

4. Documentation.

GMS's Executive Director shall maintain, or cause to be maintained, a written or electronic record of the title of the person or office for each person or office designed under this Section IV.C. Such record shall be maintained for six (6) years from the date of its creation or the date it was last in effect, whichever is later.

D. Identification of Workforce Members' Access To Protected Health Information

Attached to these policies as Appendix A is an identification of those classes of

GMS's workforce who need access to protected health information to carry out their duties and, for each of those classes, the category or categories of protected health information to which access is needed and any conditions appropriate to that access. Failure of a member of the workforce to comply with that access or those conditions will result in disciplinary action up to and including termination of employment.

At least annually, the Privacy Officer shall cause a review of the identification and categories stated in Appendix A and make such changes to Appendix A as the Privacy Officer determines is necessary or desirable to keep Appendix A current.

E. Training of Workforce

All members of GMS's workforce shall be trained annually on GMS's privacy and breach notification policies and procedures with respect to protected health information as necessary and appropriate for the members of the workforce to carry out their functions within GMS.

New members of the workforce shall be trained within ninety (90) calendar days after the person joins the workforce. Each member of the workforce whose functions are affected by a material change in these Privacy Policies shall be trained within ninety (90) calendar days after the material change becomes effective.

Documentation of the training for each member of the workforce shall be kept in written or electronic form for six (6) years after the date of its creation or the date that person ceases to be a member of GMS's workforce, whichever is later.

F. Safeguards to Protect the Privacy of Protected Health Information

The safeguards for electronic protected health information are addressed in GMS's Security of Protected Health Information Policy.

At least annually, the Privacy Officer shall cause a review of the safeguards stated in GMS's Security of Protected Health Information Policy and make such changes as the Privacy Officer determines is necessary or desirable to keep GMS's Security of Protected Health Information Policy current.

G. Receipt of Notice of Amended Protected Health Information

Any member of GMS's workforce who is informed by another health care provider, health plan or a healthcare clearinghouse of an amendment to an individual's protected health information shall promptly inform the Privacy Officer of the amendment. The Privacy Officer shall cause the protected health information concerning that individual that is maintained by GMS to be amended as stated in Section VIII.C.4.a "Making the Amendment" of these policies.

H. Process for Individuals to Make Complaints

Individuals who desire to make a complaint against GMS concerning GMS's privacy and breach notification policies and procedures, its compliance with those policies and procedures, or the requirements of the HIPAA Privacy and Breach Notification Rules shall submit the complaint to *Matt Giesecke* in writing. Complaints shall be handled in accordance with applicable provisions of contracts between GMS and the State of Maine, as well as GMS's formal grievance policies and procedures, as applicable.

The *Director of Human Resources* shall investigate the complaint and respond to the individual in writing concerning his or her findings and what action, if any, GMS will take in response to the complaint.

The *Director of Human Resources* shall cause written documentation of each complaint and its disposition to be kept in written or electronic form for six (6) years after the date of its creation or the date when it was last in effect, whichever is later.

I. Sanctions

Except for actions that are covered by and meet the conditions of Section IV.K "Prohibition on Intimidating or Retaliatory Acts" of these Privacy Policies, any member of GMS's workforce who fails to comply with GMS's Privacy Policies and procedures or the requirements of the HIPAA Privacy, Breach Notification and Security Rules shall be subject to sanctions imposed through GMS's personnel discipline and discharge policies.

The *Director of Human Resources* shall cause written documentation of the sanctions that are applied, if any, to be kept in written or electronic form for six (6) years after the date of its creation or the date when it is last in effect, whichever is later.

J. Mitigation of Harmful Effect

If there is a use or disclosure of protected health information by a member of GMS's workforce or a GMS business associate in violation of GMS's privacy policies or the requirements of the HIPAA Privacy Rule or more stringent State law, the Privacy Officer shall mitigate, or cause to be mitigated, to the extent practicable, any harmful effect that is known to GMS.

K. Prohibition on Intimidating or Retaliatory Acts

Neither GMS nor any member of GMS's workforce may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against:

1. Individuals

Any individual for the exercise by the individual of any right under, or for participation by the individual in any process established by, these privacy, breach notification and security policies or the HIPAA regulations, including filing a complaint under the HIPAA Privacy Rule or under these policies.

2. Individuals and Others

Any individual or other person for:

a. Filing of a complaint with the Secretary of Health and Human Services under the Administrative Simplification provisions of HIPAA;

b. Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under the Administrative Simplification provisions of HIPAA; or

c. Opposing any act or practice made unlawful by the HIPAA regulations, 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 protected health information in violation of the HIPAA Privacy Rule.

L. Prohibition on Waiver of Rights

No member of GMS's workforce may require an individual to waive the individual's rights under these privacy and breach notification policies or the HIPAA Privacy or Breach Notification Rules, or his or her right to file a complaint with the Secretary of HHS, as a condition for the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

M. Changes to Policies and Procedures

1. Changes in Law

The Privacy Officer shall promptly change these privacy and breach notification policies as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Privacy and Breach Notification Rules. The changed policy or procedure shall be promptly documented and implemented. If the change materially affects the content of GMS's Notice of Privacy Practices, the Privacy Officer shall promptly

make the appropriate revisions to the notice in accordance with Section VI.D "Revision of Notice of Privacy Practices" of these Privacy Policies.

The Security Officer shall promptly change these security policies and procedures as necessary and appropriate to comply with changes in the law, including changes in the HIPAA Security Rule, and to respond to environmental or operational changes. The changed policy or procedure shall be promptly documented and implemented.

2. Changes to Privacy Practices Stated In Notice of Privacy Practices

When GMS changes a privacy practice that is stated in its Notice of Privacy Practices and makes corresponding changes to GMS's policies, the change shall be effective for protected health information GMS created or received prior to the effective date of the notice revision provided:

a. The Privacy Officer ensures that the policy or procedure, as revised to reflect the change, complies with the HIPAA Privacy and Breach Notification Rules, as well as more stringent State law;

b. The Privacy Officer documents the policy or procedure, as revised, as stated in Section IV.N "Documentation" and Section IV.O "Period of Retention" of these Privacy Policies; and,

c. The Privacy Officer revises the Notice of Privacy Practices to state the changed practice and makes the revised notice available as stated in Section VI.B "Provision of Notice of Privacy Practices" of these Privacy Policies. The changed practice may not be implemented prior to the effective date of the revised Notice of Privacy Practices.

If these conditions are not met, then the change is effective only with respect to protected health information created or received after the effective date of the revised Notice of Privacy Practices.

3. Changes to Privacy Practices Not Stated In Notice of Privacy Practices

GMS may change, at any time, a privacy practice that does not materially affect the content of the Notice of Privacy Practices, provided:

a. The policy or procedure involved, as revised, complies with the HIPAA Privacy and Breach Notification Rules, as well as more stringent State law; and,

b. Prior to the effective date of the change, the policy or practice, as revised, is documented by *the Director of Human Resources,* by causing it to be kept in written or electronic form.

N. Documentation

The Privacy Officer shall take, or cause to be taken, each of the following actions:

a. Maintain these Privacy Policies and procedures in written or electronic form;

b. If a communication is required by these Privacy Policies and procedures, or by the HIPAA regulations, to be in writing, maintain that writing, or an electronic copy, as documentation;

c. If an action, activity, or designation is required by these Privacy Policies, or by the HIPAA regulations, to be documented, maintain a written or electronic record of that action, activity or designation.

O. Period of Retention

Documentation required by Section IV.N "Documentation," above, shall be retained for six (6) years from the date of its creation or the date when it last was in effect, whichever is later.

P. Maintenance of Psychotherapy Notes

Psychotherapy notes, if any are maintained by GMS, shall be maintained by the mental health professional who prepared the notes in a locked file in his or her office. A duplicate of the key to the locked file shall be retained by the Privacy Officer.

Upon termination of the mental health professional's employment, any psychotherapy notes maintained by him/her shall be destroyed, unless prohibited by other State or federal law.

Q. Business Associates

Prior to GMS disclosing any protected health information to a business associate or allowing a business associate to create or receive protected health information on its behalf, the Privacy Officer shall obtain satisfactory assurance from the business associate that the business associate will appropriately safeguard the protected health information disclosed to it or that it creates or receives on GMS's behalf. The satisfactory assurance shall be through a written contract with the business associate that contains at least all the provisions required by the HIPAA Privacy and Security Rules.

However, if the business associate is required by law to perform a function or activity on behalf of GMS or to provide a service described in the HIPAA Privacy Rule's definition of a business associate (see, Section XII.G, "Business Associate" of these Privacy Policies) to GMS, GMS may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements for business associates, provided:

1. GMS attempts in good faith to obtain satisfactory assurances, as stated above; and

2. If that attempt fails, *the Director of Human Resources* documents the attempt and the reasons that the assurances cannot be obtained.

Any contract of GMS where the other party, or one of the other parties, may be a business associate shall be submitted to the Privacy Officer for review for compliance with these Privacy Policies and the HIPAA Privacy Rule prior to being signed on behalf of GMS.

R. Reporting Violations

Each member of GMS's workforce must report any actual or possible violation of these Privacy Policies or the HIPAA Privacy, Breach Notification, or Security Rule, or more stringent State law to the Privacy Officer or the Security Officer as soon as he or she becomes aware of the actual or possible violation.

S. Questions Concerning HIPAA Compliance

If any member of GMS's workforce has a question concerning GMS's privacy or breach notification policies, the HIPAA Privacy or Breach Notification Rules, State law requirements, or their application to any situation, he or she should contact the Privacy Officer for guidance. If any member of GMS's workforce has a question concerning GMS's security policies, the HIPAA Security Rule, or its application to any situation, he or she should contact the Security Officer for guidance. Either the Privacy Officer or the Security Officer may contact legal counsel for legal advice as he or she believes is necessary or desirable.

T. Action by Designee

Whenever an action may be or is required to be taken under these Privacy Policies by the Privacy Officer, Security Officer, *the Director of Human Resources*, or any other member of GMS's workforce, the action may be taken by that person's designee.

V. GMS REQUESTS FOR PROTECTED HEALTH INFORMATION

A. Generally

When requesting protected health information from another health care provider, a health plan or a health care clearinghouse, a member of GMS's workforce must limit the request to that which is reasonably necessary to accomplish the purpose for which the request is made.

Except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the request, members of GMS's workforce may not request an entire medical record.

B. Routine and Recurring Requests

For a request that is made on a routine and recurring basis, the Privacy Officer shall from time to time develop and implement standard protocols that limit the protected health information requested to the amount that is reasonably necessary to accomplish the purpose for which the request is made. The protocols established by the Privacy Officer are set forth in Appendix C to these Privacy Policies.

C. Other Requests

Whenever any member of GMS's workforce desires to request protected health information from another provider, a health plan or a health care clearinghouse and the request is not one made pursuant to a protocol for routine and recurring requests, he or she shall first submit the request to the Privacy Officer for review and approval prior to the request being made. The Privacy Officer shall review the request on an individual basis using the following criteria to limit the request to the information reasonably necessary to accomplish the purpose for which the request is made:

The criteria to be applied are:

a. Whether or not the information requested is related to the purpose of the request.

b. Whether or not the information requested will assist in the accomplishment of the purpose of the request.

c. Whether or not the purpose of the request can be accomplished without the information requested.

d. Whether or not the purpose of the request can be met with information that is not protected health information.

VI. NOTICE OF PRIVACY PRACTICES

A. Form of Notice of Privacy Practices.

The Notice of Privacy Practices used by GMS shall be established from time to time by the Privacy Officer and shall meet the requirements of the HIPAA Privacy Rule.

B. Provision of Notice of Privacy Practices

1. To Each Individual

a. Generally

Except in an emergency treatment situation, GMS's Notice of Privacy Practices shall be provided to any individual who receives services or supports from GMS (except to an inmate of a correctional institution) no later than the date of the first service delivery by GMS and to other persons upon request. In an emergency treatment situation, GMS's Notice of Privacy Practices shall be provided as soon as reasonably practicable after the emergency treatment situation.

The Notice of Privacy Practices also shall be made available at GMS's office for individuals to request to take with them.

b. Via E-Mail

If the individual agrees and that agreement has not been withdrawn, the Notice of Privacy Practices will be provided to that individual by e-mail in lieu of physical delivery. The transmission of the Notice of Privacy Practices by e-mail will be accomplished by *Director of Human Resources*. If the e-mail transmission fails, a paper copy of the Notice of Privacy Practices will be provided to the individual. An individual who receives electronic notice may still obtain a paper copy of the notice upon request; his or her request should be submitted to *Director of Human Resources*.

2. Posting

GMS's Notice of Privacy Practices shall be prominently posted on *the Administrative Office Building Bulletin Board* at 1*5 Saunders Way, Suite 500-G, Westbrook, ME*.

3. Web Site

GMS's Notice of Privacy Practices shall be prominently posted on GMS's web site and made available electronically through the web site.

C. Obtaining Acknowledgment of Receipt of Notice of Privacy Practices

Except in an emergency treatment situation, the GMS staff member who provides GMS's Notice of Privacy Practices to an individual in conjunction with the date of first service delivery shall obtain a written acknowledgment of the individual's receipt of the Notice of Privacy Practices. The written acknowledgment shall be obtained *by signing a form of the notice* and *it shall be filed in the Consumer's personal folder*.

If the individual's written acknowledgment cannot be obtained, the staff member(s) who attempted to obtain it shall document their good faith efforts to obtain the acknowledgment and the reason why it was not obtained. That documentation shall *be documented in Therap* and *saved as a client specific T-Log under the To Do module.*

D. Revision of Notice of Privacy Practices

Whenever there is a material change to the uses or disclosures, the individual's rights, GMS's legal duties, or other privacy practices stated in the notice, the Privacy Officer shall cause the Notice of Privacy Practices to be promptly revised, made available on request and distributed.

Except when the material change is required by law, a material change to any term of the Notice of Privacy Practices shall not be implemented prior to the effective date of the Notice of Privacy Practices in which the material change is reflected.

E. Documentation

A copy of each Notice of Privacy Practices used by GMS and of each written acknowledgment of receipt of the notice or documentation of good faith efforts to obtain such acknowledgment shall be maintained by GMS in written or electronic form for six (6) years after the date the notice was last in effect, or any longer period required by law.

VII. USES AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

A. General Rule

Except as otherwise stated in this Section VII, GMS shall obtain the individual's

written authorization in accordance with these Privacy Policies, prior to using or disclosing protected health information concerning the individual.

B. Incidental Uses and Disclosures

A use or disclosure that is incidental to a use or disclosure that is otherwise permitted or required by these Privacy Policies or the HIPAA Privacy Rule is permissible provided: (1) the applicable requirements of Section VII.C "Use and Disclosure of Only the Minimum Necessary Information," below, are met; and, (2) reasonable safeguards have been applied to limit incidental uses or disclosures made pursuant to an otherwise permitted or required use or disclosure (see, Section IV.F, "Safeguards to Protect the Privacy of Protected Health Information").

C. Use and Disclosure of Only the Minimum Necessary Information

1. General Rule

Except as stated in Section VII.C.2, below, when using or disclosing protected health information, to the extent practical, members of GMS's workforce shall limit protected health information to the limited data set, or if needed, to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

2. Exceptions to Minimum Necessary Requirement

The preceding general rule concerning limiting use and disclosure of protected health information to the minimum necessary does not apply to:

a. Disclosures to a health care provider for treatment.

b. Uses or disclosures made to the individual.

c. Uses or disclosures made pursuant to a written authorization in accordance with these Privacy Policies.

d. Disclosures made to the Secretary of Health and Human Services in accordance with the HIPAA regulations.

e. Uses or disclosures that are required by law.

f. Uses or disclosures that are required for GMS's compliance with the HIPAA Privacy Rule.

3. Routine and Recurring Disclosures

For any type of disclosure that is made on a routine and recurring basis, the Privacy Officer shall from time to time develop and implement standard protocols that limit the protected health information requested to the amount that is reasonably necessary to accomplish the purpose for which the disclosure is made. The protocols established by the Privacy Officer are set forth in Appendix D to these Privacy Policies.

4. Other Disclosures

Any disclosures that are not covered by an established protocol, shall be reviewed by the Privacy Officer on an individual basis using the following criteria to limit the protected health information disclosed to the information reasonably necessary to accomplish the purpose for which disclosure is sought.

The criteria to be applied are:

a. Whether or not the information requested is reasonably related to the purpose of the request.

b. Whether or not the information requested will assist in the accomplishment of the purpose of the request.

c. Whether or not the purpose of the request can be accomplished without the information requested.

d. Whether or not the purpose of the request can be met with information that is not protected health information.

5. Permitted Reliance

If the reliance is reasonable under the circumstances, members of GMS's workforce may rely on a requested disclosure as the minimum necessary for the stated purpose when:

a. Making disclosures to public officials that are permitted under Section VII.G "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" of these Privacy Policies, if the public official represents that the information is the minimum necessary for the stated purpose(s);

b. The information is requested by another covered entity;

c. The information is requested by a professional who is a member of GMS's workforce or a business associate of GMS for the purpose

of providing professional services to GMS, if the professional represents that the information requested is the minimum necessary for the stated purpose(s); or,

d. Documentation or representations that comply with the applicable requirements of Section VII.G.9 "Uses and Disclosures for Research Purposes" of these Privacy Policies have been provided by the person requesting the information for research purposes.

The basis for reliance under this Section VII.C.5 shall be documented by the Privacy Officer. That documentation shall be maintained in *the Director of HR's office*.

D. Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations

1. Uses of Information

GMS may use protected health information without the individual's authorization for its own treatment, payment, or health care operations.

2. Care Management and Coordination of Care

A GMS health care practitioner may disclose protected health information without the individual's authorization to a health care practitioner, health care facility, or payor or person engaged in the payment for health care for the purpose of care management or coordination of care. If an unauthorized disclosure is made under this Section VII.D.2, the health care practitioner making the disclosure shall make a reasonable effort to notify the individual or the authorized representative of the individual of the disclosure.

This Section VII.D.2 does not apply to psychotherapy notes.

3. Disclosures to Payors

Biographical and medical information may be disclosed to a commercial or governmental payor, or to another entity, for the purpose of determining reimbursement eligibility and receiving reimbursement for the care, treatment, education, training, or support of the individual.

E. Uses and Disclosures for Which an Authorization is Required

1. General Rule

Except as otherwise permitted or required by these Privacy Policies, GMS

will not use or disclose protected heath information without an authorization that is valid under this Section VII. When GMS obtains or receives a valid authorization for its use or disclosure of protected health information, GMS's use or disclosure must be consistent with that authorization.

2. Psychotherapy Notes

Notwithstanding any provision of these Privacy Policies, GMS will obtain an authorization for any use or disclosure of psychotherapy notes, except:

a. To carry out the following treatment, payment, or health care operations:

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

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

(3) Use by GMS to defend a legal action or other proceeding brought by the individual; and,

b. A use or disclosure that is:

(1) Required by Section VII.G.11 "Disclosure to the Secretary of Health and Human Services" of these Privacy Policies concerning "Disclosures to the Secretary of Health and Human Services";

(2) Permitted by Section VII.G.2 "Uses and Disclosures Required by Law" of these Privacy Policies concerning "Uses and Disclosures Required by Law";

(3) Permitted by Section VII.G.5 "Uses and Disclosures for Health Oversight Activities" of these Privacy Policies with respect to the oversight of the originator of the psychotherapy notes;

(4) Permitted by Section VII.G.8.b "Uses and Disclosures About Decedents" of these Privacy Policies concerning "Coroners and Medical Examiners"; or,

(5) Permitted by Section VII.G.10 "Serious and Imminent

Threat" of these Privacy Policies concerning "Serious and Imminent Threats."

3. Sale of Protected Health Information

Notwithstanding any provision of these Privacy Policies, GMS will obtain an authorization for any disclosure of protected health information for which the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the protected health information. Such authorization shall state that the disclosure will result in remuneration to GMS.

This does not apply, however, to disclosures of protected health information:

a. For public health purposes as stated in Sections VII.G.3 and VII.K of these Privacy Policies;

b. For research purposes as stated in Sections VII.G.9 and VII.K of these Privacy Policies, where the only remuneration received by GMS is a reasonable cost-based fee to cover the cost to prepare and transmit the protected health information for such purposes;

c. For treatment and payment purposes as stated in Section VII.D of these Privacy Policies;

d. For the sale, transfer, merger, or consolidation of all or part of GMS and for related due diligence as described in Section XII.L.6.d of the definition of health care operations of these Privacy Policies;

e. To or by a business associate for activities that the business associate undertakes on behalf of GMS pursuant to Section VII.G.12 of these Privacy Policies, and the only remuneration provided is by GMS to the business associate for the performance of such activities;

f. To an individual, when requested under Sections VIII.B or VIII.D of these Privacy Policies;

g. Required by law as permitted by Section VII.G.2 of these Privacy Policies; and,

h. Permitted by and in accordance with the applicable requirements of the HIPAA Privacy Rule, where the only remuneration received

by GMS is a reasonable, cost-based fee to cover the cost to prepare and transmit the protected health information for such purpose or a fee otherwise expressly permitted by law.

4. What is a Valid Authorization?

An authorization is valid if it contains all the elements required by Section VII.E.7 "Form of Authorization" of these Privacy Policies and it is not defective.

An authorization is defective if the document has any of the following defects:

a. The expiration date has passed or the expiration event is known by GMS to have occurred.

b. The authorization has not been filled out completely with respect to an element required to be included in the authorization;

c. The authorization is known by GMS to have been revoked;

d. The authorization lacks a required element (see, Section VII.E.7, "Form of Authorization") of these Privacy Policies;

e. The authorization violates the requirements concerning compound authorizations (see, Section VII.E.8, "Compound Authorizations") of these Privacy Policies;

f. The authorization violates the requirements concerning conditioning of authorizations (see, Section VII.E.6, "Prohibition on Conditioning of Authorizations") of these Privacy Policies; or,

g. If any material information in the authorization is known by GMS to be false.

If any member of GMS's workforce believes an authorization is defective for any reason, he or she should promptly report that fact and the basis for his or her belief to the Privacy Officer.

5. Maintaining an Authorization

All authorizations shall be delivered to *HR specialist, coordinators or managers of appropriate departments* who will *ensure* the *information is filed in the consumer's, business associate's or employee's file* .

6. Conditioning of Authorizations

a. General Rule

Except as stated in Section VII.E.6.b "Exceptions," below, GMS will not condition treatment or payment to an individual on the receipt of an authorization from that individual.

b. Exceptions

GMS may condition treatment or payment to an individual on the receipt of an authorization from that individual in the following situations:

(1) **Research.** GMS may condition the provision of research-related treatment on provision of an authorization for the use or disclosure of protected health information for such research.

(2) **Disclosure Is Sole Purpose.** GMS may condition the provision of health care that is solely for the purpose of creating protected health information for disclosure to a third party on provision of an authorization for the disclosure of the protected health information to that third party.

7. Form of Authorization

a. Required Elements - Generally

An authorization must contain at least 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 GMS may make the requested use or disclosure.

(4) A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual

initiates the authorization and does not, or elects not to, provide a statement of the purpose.

(5) An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure; provided, however, that no authorization may be effective for more than thirty (30) months.

(6) A statement of the individual's right to revoke the authorization in writing at any time and either:

(a) The exceptions to the right to revoke, together with a description of how the individual may revoke the authorization; or,

(b) To the extent that the information is stated in the Notice of Privacy Practices, a reference to that notice.

(7) A statement of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization by stating either:

(a) That the covered entity may not condition treatment, payment, enrollment or eligibility for benefits on whether the individual signs the authorization when the prohibition on conditioning of authorizations applies; or,

(b) The consequences to the individual of a refusal to sign the authorization when the Privacy Rule permits the entity to condition treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain the authorization.

(8) A statement that information used or disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer be protected by the Privacy Rule;

(9) Signature of the individual and date;

(10) If the authorization is signed by a personal representative of the individual, a description of that personal representative's authority to act for the individual;

(11) The statement regarding the disclosure of HIV information

described in Section VII.J.3 of these Privacy Policies.

b. Required Elements - Specific

The Privacy Rule requires certain things to be in the authorization if the authorization is for certain purposes.

(1) **Marketing.** If a disclosure for marketing involves direct or indirect financial remuneration to GMS from a third party, the authorization must state that such remuneration is involved. See, Section VII.H of these Privacy Policies.

(2) **Sale of Protected Health Information**. If the disclosure is in exchange for direct or indirect remuneration from or on behalf of the recipient of the protected health information, the authorization must state that the disclosure will result in remuneration to GMS. See, Section VII.E.3 of these Privacy Policies.

c. Additional Elements

An authorization may contain elements or information in addition to the elements stated in Section VII.E.7.a, above, concerning "Required Elements," provided those additional elements or information are not inconsistent with the elements required by this Section VII.E.

d. Plain Language

An authorization must be written in plain language.

e. Copy to Individual

If GMS seeks an authorization from an individual for use or disclosure of protected health information, GMS will provide the individual with a copy of the signed authorization, if requested.

8. Compound Authorizations

a. General Rule

Except as stated in Section VII.E.8.b, below, an authorization for use or disclosure of protected health information may not be combined with any other document to create a compound authorization.

b. Exceptions

Notwithstanding Section VII.E.8.a, above, an authorization for use or disclosure of protected health information may be combined with any other document to create a compound authorization in the following situations:

(1) An authorization for the use or disclosure of protected health information for a research study may be combined with any other type of written permission for the same or another research study. This exception includes combining an authorization for the use or disclosure of protected health information for a research study with another authorization for the same research study, with an authorization for the creation or maintenance of a research database or repository, or with consent to participate in the research. When GMS has conditioned the provision of research-related treatment on the provision of one of the authorizations, as permitted in exception (3), below, any compound authorization created under this exception must clearly differentiate between the conditioned and unconditioned components and provide the individual with an opportunity to opt in to the research activities described in the unconditional authorization.

(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;

(3) An authorization under this Section VII.E.8, other than an authorization for a use or disclosure of psychotherapy notes, may be combined with any other authorization under this Section VII.E.8, except when GMS has conditioned the provision of treatment or payment under Section VII.E.6.b "Exceptions" of these Privacy Policies on the provision of one of the authorizations. However, this prohibition does not apply to a compound authorization created in accordance with exception (1), above.

9. Revocation of an Authorization

An individual has the right to revoke an authorization in writing, except to the extent GMS has taken action in reliance thereon.

A written revocation should be submitted to *the appropriate department supervisor* who will cause the revocation to be *filed in the appropriate*

consumer/personnel/business associate folder.

10. Documentation

The *appropriate department supervisor* will document and retain any signed authorizations under this section in writing, or an electronic copy, for six (6) years from the date of its creation or the date when it was last in effect, whichever is later, or any longer period required by law.

F. Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object

1. General Rule

Members of GMS's workforce may use or disclose protected health information without the individual's written authorization for the purposes described in this Section VII.F provided:

a. The individual is informed orally or in writing in advance of the use or disclosure; and,

b. The individual has an opportunity to agree to or prohibit or restrict the disclosure in accordance with the requirements of this Section VII.F. The individual's agreement or objection may be oral or written.

2. Facility Directories

a. Except when an objection is expressed by the individual, GMS may use the following protected health information to maintain a directory of individuals in the facility:

(1) The individual's name;

(2) The individual's location in GMS'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. Opportunity to Object

The *department/program manager* will inform an individual of the protected health information that it may include in a directory and

provide the individual with the opportunity to restrict or prohibit some or all of the uses permitted by this Section VII.F.2. The *department/program manager* will document that opportunity and the agreement, restriction, or objection on the *Opportunity to Object form.*

c. Incapacity or Emergency Circumstance

If the *department supervisor* determines that the opportunity to object to uses for directory purposes cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, GMS will use some or all of the protected health information permitted by this Section VII.F.2, if the use is:

(1) Consistent with a prior expressed preference of the individual, if any, that is known to GMS; and,

(2) In the individual's best interest as determined by GMS, in the exercise of professional judgment.

Department supervisors will inform the individual and provide an opportunity to object to uses for directory purposes when it becomes practicable to do so.

Department supervisors will document the incapacity or emergency, how the use is consistent and in the individual's best interest on the *Opportunity to Object form*. *Department supervisor* will also document the provision of the opportunity to object later and whether or not the individual stated any objection or restriction.

3. Persons Involved in the Individual's Care; Notification

a. Condition and Status. Members of GMS's workforce may, if the individual has not expressly objected, disclose to an individual's spouse or next of kin, upon proper inquiry, protected health information relating to the physical condition or mental status of the individual.

b. Disclosure to Family; Caretakers. Members of GMS's workforce who are licensed mental health professionals providing care to an adult individual may use or disclose protected health information to notify a family member, another relative, a close personal friend, or to anyone identified by the individual, the individual's information that is directly relevant to the person's

involvement in the individual's care under the following circumstances:

(1) If the individual has capacity to make health care decisions and is either present or available prior to disclosure, the professional may disclose the information: (i) with the individual's consent, (ii) when the individual does not object in circumstances in which the individual has the opportunity to object, or (iii) when the professional may reasonably infer from the circumstances that the individual does not object.

(2) The professional may disclose the information if in the professional's judgment it is in the individual's best interest to make the disclosure and the professional determines either that the individual lacks capacity to make health care decisions or an emergency precludes the individual from participating in the disclosure.

G. Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required

1. General Rules

To the extent permitted by this Section 1, an authorized member of GMS's workforce may use or disclose protected health information without the authorization of the individual or the opportunity of the individual to agree or object, in the situations described in this Section 1.

When GMS is required by any of these situations to inform the individual of a use or disclosure permitted by this Section VII.G, or when the individual may agree to, a use or disclosure permitted by this Section VII.G, VIII.A.1.d, GMS's information and the individual's agreement may be given orally. However, if given orally, the GMS workforce member involved shall document the giving of the information or the agreement by *electronic documentation*.

2. Uses and Disclosures Required by Law

a. Informing the Privacy Officer

Any member of GMS's workforce who receives a request, or who proposes, to use or disclose protected health information for a use or disclosure required by law must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then

oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Permitted Uses and Disclosures

GMS may use or disclose protected health information to the extent that the use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of the law.

GMS will meet the requirements of the following sections of these Privacy Policies, as applicable, for uses and disclosures required by law:

(1) Section VII.G.4 "Uses and Disclosures About Victims of Abuse, Neglect or Exploitation";

(2) Section VII.G.6 "Disclosures for Judicial and Administrative Proceedings"; and,

(3) Section VII.G.7 "Disclosures for Law Enforcement Purposes".

3. Uses and Disclosures for Public Health Activities

a. Informing the Privacy Officer

Any member of GMS's workforce who receives a request, or who proposes, to use or disclose protected health information for public health activities must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Permitted Disclosures

An authorized member of GMS's workforce may use and disclose protected health information for the public health activities and purposes described below:

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

including but not limited to, the reporting of disease, injury and vital events such as birth or death, and the conduct of public health surveillance, public health investigations, and public health interventions; or, at the direction of the public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; provided, however, that the use and disclosure relates to the statutory functions of the Maine Department of Health and Human Services;

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

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

4. Uses and Disclosures About Victims of Abuse, Neglect, or Exploitation

a. Delivery to Privacy Officer.

Any member of GMS's workforce who receives a request, or who proposes, to use or disclose protected health information about a victim of abuse, neglect, or exploitation must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. General Rule.

Except for reports of child abuse or neglect that are permitted by Section VII.G.3.b.(2) "Permitted Disclosures" of these Privacy Policies, an authorized member of GMS's workforce may disclose protected health information about an individual that workforce member reasonably believes to be a victim of abuse, neglect, or exploitation to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect or exploitation:

(1) To the extent the disclosure is required by law and the

disclosure complies with and is limited to the relevant requirements of that law;

(2) If the individual agrees to the disclosure; or,

(3) To the extent the disclosure is expressly authorized by statute or regulation and:

(a) The GMS workforce member, in the exercise of professional judgment, believes the disclosure is necessary to prevent serious harm to the individual or other potential victim; or,

(b) If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that:

i) The protected health information for which disclosure is sought is not intended to be used against the individual; and,

ii) An immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

c. Informing the Individual.

If a member of GMS's workforce makes a disclosure permitted by VII.G.4.b "General Rule," above, the d*epartment supervisor* shall promptly inform the individual that such a report has been or will be made, except if:

(1) The *department supervisor*, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

(2) The *department supervisor* would be informing a personal representative, and he or she reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing that person would not be in the best interests of the individual as determined by GMS, in the exercise of professional judgment.

5. Uses and Disclosures for Health Oversight Activities.

a. Delivery to Privacy Officer.

Any member of GMS's workforce who receives a request, or who proposes, to use or disclose protected health information for purposes of a health oversight activity must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. General Rule.

When required or permitted by law, an authorized member of GMS's workforce may disclose protected health information to a health oversight agency, *e.g*., state department of health, CMS, for oversight activities authorized by law, including: audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or other actions; or, other activities necessary for appropriate oversight of:

(1) The health care system;

(2) Government benefit programs for which health information is relevant to beneficiary eligibility;

(3) Entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or,

(4) Entities subject to civil rights laws for which health information is necessary for determining compliance.

c. Exception

For purposes of the disclosures permitted by Section VII.G.5.b "General Rule," above, a health oversight activity does not include an investigation or other activity in which the individual is the subject of the investigation or activity and such investigation or other activity does not arise out of and is not directly related to:

(1) The receipt of health care;

(2) A claim for public benefits related to health; or,

(3) Qualification for, or receipt of, public benefits or services when a patient's health is integral to the claim for public benefits or services.

d. Joint Activities or Investigations

Notwithstanding the exceptions stated in Section VII.G.5.c, above, if a health oversight activity or investigation is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not related to health, the joint activity or investigation is considered a health oversight activity for purposes of this section.

6. Disclosures for Judicial and Administrative Proceedings

a. Delivery to Privacy Officer

Any member of GMS's workforce who receives an order of a court or administrative tribunal or a subpoena, discovery request, or other lawful process must promptly deliver or otherwise communicate the document to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the disclosure for compliance with these Privacy Policies. The disclosure should not occur until it has been approved by the Privacy Officer.

b. General Rules

GMS will disclose protected health information in the course of any judicial or administrative proceeding in response to an order of a court, subject to any limitation in the Maine Rules of Evidence, Rule 503, and certain subpoenas provided GMS will disclose only the protected health information expressly authorized by the order or subpoena.

c. Not Limitation on Other Uses and Disclosures

The provisions of this section dealing with disclosures for judicial proceedings do not supersede other provisions of these Privacy Policies that otherwise permit or restrict uses or disclosures of protected health information.

7. Disclosures for Law Enforcement Purposes

a. Delivery to Privacy Officer

Any member of GMS's workforce who receives a request, or proposes, to disclose protected health information for law enforcement purposes must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Pursuant to Process and As Otherwise Required by Law

A direct support professional who is a member of GMS's workforce shall disclose protected health information for a law enforcement purpose to a law enforcement official:

(1) As required by law including laws that require the reporting of certain types of wounds or other physical injuries, except:

(a) For laws concerning a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect (see, Section VII.G.3.b.(2) "Permitted Disclosures" of these Privacy Policies); or,

(b) To the extent the disclosure is pursuant to a mandatory reporting law concerning reporting of abuse, neglect, or exploitation and the disclosure complies with and is limited to the relevant requirements of that law (see, Section VII.G.4.b.(1) of these Privacy Policies).

(2) In compliance with and as limited by relevant requirements of:

(a) A court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer;

(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:

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

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

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

(For verification of an administrative request see, Section VII.L.3, "Conditions on Disclosures" of these Privacy Policies.)

c. Limited Information for Identification and Location Purposes

Except for disclosures required by law as permitted by VII.G.7.b, above, an direct support professional who is a member of GMS's workforce shall disclose protected health information in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that:

(1) The licensed mental health professional shall disclose only the following information:

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

(2) Except as stated in (1), above, a licensed mental health professional who is a member of GMS's workforce may not disclose for the purposes of identification or location under this section any protected

health information related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

d. Victims of a Crime.

Except for disclosures required by law as permitted by VII.G.7.b, above, a direct support professional who is a member of GMS's workforce shall disclose protected health information in response to a law enforcement official's request for such information about an individual who is or is suspected to be a victim of a crime, other than disclosures that are subject to Section VII.G.7.b and Section VII.G.7.c, if:

(1) The individual agrees to the disclosure; or,

(2) GMS is unable to obtain the individual's agreement because of incapacity or other emergency circumstance provided that:

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

(b) The law enforcement official represents that immediate law enforcement activity that depends on the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure; and,

(c) The disclosure is in the best interests of the individual as determined by GMS, in the exercise of professional judgment.

e. Decedents

A member of GMS's workforce shall disclose protected health information about an individual who has died to a law enforcement official for the purpose of alerting law enforcement of the death of the individual if GMS has a suspicion that such death may have resulted from criminal conduct.

f. Crime on the Premises

A member of GMS's workforce shall disclose to a law enforcement official protected health information that he or she believes in good faith constitutes evidence of criminal conduct that occurred on the premises of GMS.

g. Reporting Crime in Emergencies

If GMS is providing emergency health care in response to a medical emergency, other than on the premises of GMS, a member of GMS's workforce shall disclose protected health information to a law enforcement official if such disclosure appears necessary to alert law enforcement to:

(1) The commission and nature of a crime;

(2) The location of such crime or of the victim(s) of such crime; and,

(3) The identity, description, and location of the perpetrator of the crime.

If a member of GMS's workforce believes the medical emergency is the result of abuse, neglect, or exploitation of the individual in need of emergency health care, the preceding does not apply and any disclosure to a law enforcement official for law enforcement purposes is subject to Section VII.G.7.c of these Privacy Policies.

8. Uses and Disclosures About Decedents

a. Delivery to Privacy Officer

Any member of GMS's workforce who receives a request, or proposes, to use or disclose protected health information to a coroner, medical examiner, or funeral director must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Coroners and Medical Examiners

Consistent with applicable law, an authorized member of GMS's

workforce may disclose protected health information to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

c. Funeral Directors

An authorized member of GMS's workforce may disclose protected health information to funeral directors consistent with applicable law, as necessary to carry out their duties with respect to the decedent. If necessary for funeral directors to carry out their duties, GMS may disclose the protected health information prior to, and in reasonable anticipation of, the individual's death.

9. Uses and Disclosures to Avert a Serious Threat to Health or Safety.

a. Delivery to Privacy Officer.

Any member of GMS's workforce who receives a request, or proposes, to use or disclose protected health information to avert a serious threat to health or safety must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the use or disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Permitted Uses and Disclosures.

A member of GMS's workforce shall, consistent with applicable law and standards of ethical conduct, use or disclose protected health information, if the member of GMS's workforce, in good faith, believes the use or disclosure:

(1) Is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and,

(2) Is to a person or persons reasonably able to prevent or minimize the threat, including the target of the threat.

11. Disclosure to the Secretary of Health and Human Services.

a. Delivery to Privacy Officer.

Any member of GMS's workforce who receives a request, or

proposes, to disclose protected health information to the Secretary of Health and Human Services must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the disclosure for compliance with these Privacy Policies. The use or disclosure should not occur until it has been approved by the Privacy Officer.

b. Permitted Disclosures.

Acting through its Privacy Officer, GMS will permit access by the Secretary of Health and Human Services during normal business hours to its facilities, books, records, accounts and other sources of information, including protected health information, that are pertinent to ascertaining compliance with the applicable requirements of HIPAA. If the Secretary of Health and Human Services determines that exigent circumstances exist, such as when documents may be hidden or destroyed, GMS will permit access by the Secretary of Health and Human Services at any time and without notice.

If any information required of GMS under this section is in the exclusive possession of any other agency, institution, or person and that other agency, institution or person fails or refuses to furnish the information, the Privacy Officer will so certify and set forth what efforts GMS has made to obtain the information.

12. Disclosures to Business Associates

a. Delivery to Privacy Officer.

Unless the use or disclosure has previously been approved by the Privacy Officer, any member of GMS's workforce who receives a request, or proposes, to disclose protected health information to a business associate of GMS must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the use or disclosure for compliance with these Privacy Policies. The use or disclosure may not occur until it has been approved by the Privacy Officer.

b. Permitted Disclosures.

Authorized members of GMS's workforce may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit

protected health information on GMS's behalf, if GMS has a written contract with the business associate that meets the requirements of the HIPAA Privacy Rule. However, such a written contract will not be required from a business associate that is a subcontractor of a business associate.

H. Uses and Disclosures for Marketing

1. General Rule

Except as stated in section VII.H.2, below, a member of GMS's workforce may not use or disclose protected health information for marketing without an authorization that meets the applicable requirements of this Section and of Section VII.E of these Privacy Policies.

If the marketing involves financial remuneration, as defined in Section VII.H.3.c of the definition of "marketing," to GMS from a third party, the authorization must state that such remuneration is involved.

Any use of protected health information for marketing without an authorization must be approved in advance by the Privacy Officer.

2. Exceptions

An authorization does not need to be obtained if GMS uses protected health information to make a marketing communication to an individual that is in the form of:

a. A face-to-face communication made by GMS to an individual; or,

b. A promotional gift of nominal value provided by GMS.

3. "Marketing" Defined

a. Generally

Except as stated in b, below, marketing means to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

b. Exceptions

Marketing does not include a communication made:

(1) To provide refill reminders or otherwise communicate

about a drug or biologic that is currently being prescribed for the individual, only if any financial remuneration received by GMS in exchange for making the communication is reasonably related to GMS's cost of making the communication.

(2) For the following treatment and health care operations purposes, except where GMS received financial remuneration in exchange for making the communication:

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

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

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

c. As used in this definition of marketing, "financial remuneration" means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

I. Uses and Disclosures for Fundraising

1. General Rule

Provided the conditions stated in Section VII.I.2 "Fundraising Requirements," below, are met, an authorized member of GMS's workforce may use, or disclose to a business associate, the following protected health information for the purpose of raising funds for its own

benefit, without an authorization meeting the requirements of Section VII.E "Uses and Disclosures for Which an Authorization is Required" of these Privacy Policies:

a. Demographic information relating to an individual;

b. Dates of health care provided to an individual;

c. Department of service information;

d. Treating physician;

e. Outcome information; and,

f. Health insurance status.

Any use of protected health information for the purpose of raising funds for GMS's benefit without an authorization must be approved in advance by the Privacy Officer.

2. Fundraising Requirements

a. Notice of Privacy Practices

GMS will not use or disclose protected health information for fundraising purposes unless a statement is included in its Notice of Privacy Practices stating that GMS may contact the individual to raise funds for GMS and the individual has a right to opt out of receiving such communications.

b. Right to Opt Out

With each fundraising communication sent to an individual, GMS will provide the individual with a clear and conspicuous opportunity to elect not to receive any further fundraising communications. The method for an individual to elect not to receive any further fundraising communications may not cause the individual to incur an undue burden or more than a nominal cost.

c. No Conditioning of Treatment or Payment

GMS will not condition treatment or payment on the individual's choice with respect to the receipt of fundraising communications.

d. Cessation of Fundraising Communications to an Individual

GMS will not make fundraising communications to an individual where the individual has elected not to receive such communications.

e. Right to Opt In

With the Privacy Officer's approval, GMS may provide an individual who has elected not to receive further fundraising communications with a method to opt back in to receive such communications.

J. Special Rules for HIV Information. GMS and its authorized workforce members will not disclose any information regarding an individual's HIV test results or HIV status except as specifically authorized or required below.

1. Privacy Officer. Unless the disclosure has previously been approved by the Privacy Officer, any member of GMS's workforce who receives a request, or proposes, to disclose any protected health information containing HIV information must promptly deliver or otherwise communicate the request or proposal to the Privacy Officer prior to the disclosure being made. The Privacy Officer will then oversee the disclosure for compliance with these Privacy Policies. The disclosure may not occur until it has been approved by the Privacy Officer.

2. Specific Authorization Required. If an individual's written authorization for the disclosure of the individual's records does not *specifically authorize the disclosure of HIV information*, only those portions of the individual's records that do not contain HIV infection status information may be disclosed pursuant to the individual's authorization. *A general authorization to disclose all of the individual's records is not legally sufficient to authorize the disclosure of an individual's HIV information.*

3. Mandatory Notice of Risks of Disclosure. Individuals authorizing the disclosure of records containing HIV infection status information will be informed of the potential implications of authorizing the disclosure of HIV information prior to the disclosure, and such risks will be disclosed and documented either in the individual's record or on the individual's authorization form by the member of GMS's workforce making the disclosure.

4. Disclosures of HIV Test Results. The results of an individual's HIV test are confidential and GMS will only disclose such information to:

a. The individual;

b. Anyone designated by the individual in writing. When a

individual has authorized disclosure of HIV test results to GMS, GMS may make the individual's HIV test results available only to other GMS health care providers working directly with the individual and only for the purpose of providing direct medical or dental patient care to the individual;

c. The Maine Department of Health and Human Services ("DHHS"), a laboratory certified and approved by DHHS, or a health care provider, blood bank, blood center or plasma center, for a research-related purpose, so long as the disclosure of the test results does not reveal the identity of the individual and the individual's identity cannot be retrieved by the researcher;

d. Persons employed or designated by DHHS who are responsible for the treatment or care of the individual;

e. The Maine Bureau of Health as necessary to carry out the Bureau of Health's statutory duties, provided that such disclosure is required by law; or

f. Persons authorized by a court order to receive the test results.

5. Disclosures of Records Containing HIV Information. Records maintained by GMS that contain information concerning an individual's HIV infection status, including HIV test results, will be afforded heightened confidentiality and will only be disclosed to:

a. The individual;

b. Persons designated and specifically authorized by the individual in writing to receive portions of the individual's medical record containing information revealing the individual's HIV infection status;

c. Authorized employees and designees of DHHS involved in legal proceedings held pursuant to Maine communicable disease laws;

d. Authorized persons involved in adult protective proceedings, including the Maine DHHS and the Attorney General's Office;

e. Authorized persons involved in child protective proceedings, including the Maine DHHS and the Attorney General's Office;

f. Authorized persons involved in involuntary hospitalization proceedings;

g. To designated persons pursuant to a court order upon a showing of good cause and in accordance with Rule 503 of the Maine Rules of Evidence, provided such court order limits the use and disclosure of the records and provides sanctions for misuse of the records or sets forth other methods for ensuring the confidentiality of the records;

h. Duly authorized utilization review committees. If such committee is outside of GMS and the disclosure will identify the individual, the disclosure must be otherwise permitted by law;

i. Duly authorized peer review organizations. If such organization is outside of GMS and the disclosure will identify the individual, the disclosure must be otherwise permitted by law; or

j. Qualified personnel conducting scientific research, management audits, financial audits or program evaluations, so long as (i) disclosures to such entities are permitted by law, and (ii) such entities do not identify, directly or indirectly, any individual in any report of the entity's activities and do not otherwise disclose the identities of any patients tested for HIV.

6. Disclosures of HIV/AIDS-Related Health Information of Patients Whose Behavior Exposes Third Parties to Risks of Infection. In the event that a GMS health care provider has a good faith, reasonable basis to believe that an individual's behavior intentionally or negligently places a third party at serious health risk of exposure to HIV/AIDS, the health care provider is authorized to report the provider's concerns about the risk of exposure of a communicable disease the individual poses to a third party to the Maine Bureau of Public Health. The Bureau of Public Health is authorized to take any appropriate preventive action deemed necessary to protect the health and safety of third parties at risk, including notification of such third parties of their risk of exposure. The health care provider is authorized to cooperate with the Bureau of Public Health in the course of the Bureau's taking preventive action in the case.

K. Limited Data Set

1. General Rule

GMS may use or disclose a limited data set that meets of the requirements of Section VII.K.3 "Limited Data Set Defined," below, if GMS enters into a "data use agreement" with the limited data set recipient. Prior to GMS using or disclosing any protected health information as part of a "limited data set," both the limited data set and the data use agreement must be approved by the Privacy Officer as meeting the requirements of this

Section VII.K.

2. Permitted Uses

a. A limited data set may be used and disclosed only for the purposes of research, public health, or health care operations; provided, however, such use or disclosure is otherwise permitted by these Privacy Policies.

b. GMS may use protected health information to create a limited data set or disclose protected health information to a business associate of GMS for that purpose, whether or not the limited data set is to be used by GMS.

3. "Limited Data Set" Defined

A "limited data set" is protected health information 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 Resources 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.

4. Data Use Agreement

A data use agreement between GMS and the limited data set recipient must:

a. Establish the permitted uses and disclosures of the limited data set by the limited data set recipient consistent with the permitted uses

stated above. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the requirements of these policies or the HIPAA Privacy Rule if done by GMS;

b. Establish who is permitted to use or receive the limited data set; and,

c. Provide that the limited data set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3) Report to the covered entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

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

(5) Not identify the information or contact the individuals.

5. Compliance

If GMS knows of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the data use agreement, GMS will take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful:

a. Discontinue disclosure of protected health information to the recipient; and,

b. Report the problem to the Secretary of Health and Human Services.

L. Verification of Identity and Authority

1. General Rule

Prior to any disclosure of protected health information, the authorized member of GMS's workforce who is making the disclosure must:

a. Except with respect to disclosures under Section VII.F, "Uses and Disclosures Requiring an Opportunity for the Individual to Agree or to Object" of these Privacy Policies, verify the identity of a person requesting protected health information and the authority of that person to have access to protected health information under these Privacy Policies, if the identity of that person is not known to GMS; and,

b. Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under these Privacy Policies.

2. Personal Representatives

Unless the person and his or her authority is known to GMS, the authorized member of GMS's workforce who is making a disclosure to an individual's personal representative shall verify the person's identity by way of a government issued document with a picture (*e.g.*, a driver's license, passport) and verify the person's authority (*e.g.*, requiring a copy of a power of attorney or guardianship order, asking questions to establish relationship to a child.)

3. Conditions on Disclosures

If a disclosure is conditioned by these Privacy Policies on particular documentation, statements, or representations form the person requesting the protected health information, the authorized member of GMS's workforce who is making the disclosure may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

In this regard:

a. The conditions in Section VII.G.7.b.(2)(c) under "Disclosures for Law Enforcement Purposes" of these Privacy Policies may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

b. The documentation required by Section VII.G.9.b.(1), "Board Approval of a Waiver of Authorization" of these Privacy Policies, may be satisfied by one or more written statements provided that

each is appropriately dated and signed in accordance with the HIPAA Privacy Rule, 45 CFR §164.512(i)(2)(i)&(v).

4. Identity of Public Officials

GMS may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of a public official:

a. If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

b. If the request is made in writing, the request is on the appropriate government letterhead; or,

c. If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of the agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

5. Authority of Public Officials

GMS may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of protected health information is to a public official or a person acting on behalf of a public official:

a. A written statement of the legal authority under which the information is requested, or, if a written statement would be impractical, an oral statement of such legal authority;

b. If a request is made pursuant to legal process, warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

6. Exercise of Professional Judgment

The verification requirements of this section are met if a member of GMS's workforce relies on the exercise of professional judgment in making a use or disclosure in accordance with Section VII.F, "Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object" of these Privacy Policies or acts on a good faith belief in making a

disclosure in accordance with Section VII.G.10, "Uses or Disclosures to Avert a Serious Threat to Health or Safety" of these Privacy Policies.

VIII. RIGHTS OF INDIVIDUALS

A. Right to Request Privacy Protection

1. Restriction of Uses and Disclosures

a. Generally.

GMS will permit an individual to request that GMS restrict:

(1) Uses and disclosures of protected health information about the individual to carry out treatment, payment or health care operations; and,

(2) Disclosures permitted under Section VII.F.3, "Persons Involved in the Individual's Care; Notification" of these Privacy Policies, for involvement in the individual's care and notification purposes.

b. Agreement to Restriction

With one exception, whether or not GMS will agree to the restriction will be determined by *the department supervisor*. The exception is that GMS will always agree to a request of an individual to restrict disclosures of protected health information about the individual 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 protected health information pertains solely to a health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid GMS in full.

If a restriction is agreed to, a written or electronic record of that restriction shall be retained by GMS for six years from the date of its creation or the date when it was last in effect, whichever is later, or any longer period required by law.

c. If GMS Agrees to a Restriction

If GMS agrees to a restriction, the protected health information shall not be used or disclosed in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted protected health information is needed to provide the emergency treatment, the restricted protected health information may be used by GMS, or may be disclosed by an authorized member of GMS's workforce to a health care provider, to provide such treatment to the individual. However, such disclosure must otherwise be allowed by these Privacy Policies. If the information is disclosed to a health care provider for emergency treatment, the member of GMS's workforce making the disclosure shall request that health care provider not further use or disclose the information.

d. Limitations

A restriction agreed to by GMS under this Section VIII.A.1 is not effective to prevent uses or disclosures:

(a) To the individual when requested by the individual pursuant to the individual's right of access to the information (see, Section VIII.B, "Right of Access" of these Privacy Policies);

(b) For facility directories pursuant to Section VII.F.2, "Facility Directories" of these Privacy Policies; or,

(c) When the use or disclosure does not require an authorization or opportunity to agree or object is not required (see, Section VII.G, "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Disagree is Not Required" of these Privacy Policies).

e. Termination of Restriction

GMS may terminate a restriction under this Section VIII.A.1, if:

(1) The individual agrees to or requests the termination in writing;

(2) The individual orally agrees to the termination and the oral agreement is documented; or,

(3) GMS informs the individual that it is terminating its agreement to the restriction, except that such termination is:

(a) Not effective for protected health information restricted under the exception stated in Section VIII.A.1.b "Agreement to Restriction," above; and,

(b) Only effective with respect to protected health information created or received after GMS has so informed the individual.

2. Restriction on Means and Location of Communications

a. Generally

GMS shall permit individuals to request and, subject to the conditions stated below, shall accommodate reasonable requests by individuals to receive communications of protected health information from GMS by alternative means or at alternative locations.

The request by the individual to receive communications by alternative means or at alternative locations must be in writing.

b. Conditions

GMS's accommodation of such requests shall be conditioned on:

(a) When appropriate, information as to how payment, if any, will be handled; and,

(b) Specification by the individual of an alternative address or other method of contact.

GMS shall not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.

B. Right of Access

1. Generally

An individual shall have a right of access to inspect and obtain a copy of protected health information about the individual for as long as the protected health information is maintained in that record set.

2. Request for Access

The individual's request for access must be submitted in writing or orally

to the *QA Manager or appropriate department supervisor*.

3. Action on Request for Access

a. Time Limits for Action

The *QA Manager or department supervisor* shall act on a request for access no later than one (1) business day after GMS's receipt of the request.

4. Providing Access

a. Access

GMS shall provide the access requested by the individual, including inspection and obtaining a copy, or both, of the protected health information about the individual in designated record sets. If the same protected health information that is the subject of a request for access is maintained in more than one designated record set or at more than one location, the protected health information will only be produced once in response to a request for access.

b. Form and Format

The protected health information will be provided to the individual in the form or format requested by the individual, if it is readily producible in that form or format. If it is not readily producible in that form or format, it shall be provided in a readable hard copy form or such other form and format as agreed to by GMS and the individual.

c. If in Electronic Format

If the protected health information that is the subject of a request or access is maintained in one or more designated record sets electronically and if the individual requests an electronic copy of such information, GMS will provide the individual with access to the protected health information in the electronic form and format required by the individual if it is readily producible in that form and format. If it is not readily producible in that form and format, GMS will provide it in electronic form and format as agreed to by GMS and the individual.

d. Summary In Lieu of Access

The individual may be provided a summary of the protected health information requested, in lieu of providing access to the protected health information, or may be provided an explanation of the protected health information to which access has been provided, if:

(1) The individual agrees in advance to such a summary or explanation; and,

(2) The individual agrees in advance to the fees imposed, if any, by GMS for such summary or explanation.

e. Time and Manner of Access

Access shall be provided in a timely manner as stated in Section VIII.B.3.a, "Action on Request for Access", of these Privacy Policies, including arranging with the individual for a convenient time and place to inspect or obtain a copy of the protected health information, or mailing the copy to the individual at the individual's request. The *QA Manager or department supervisor* may discuss the scope, format and other aspects of the request for access with the individual as necessary to facilitate the timely provision of access.

If an individual's request for access directs GMS to transmit the copy of protected health information directly to another person designated by the individual, GMS will provide the copy to the person designated by the individual provided the individual's request is in writing, signed by the individual and clearly identifies the designated person and where to send the copy of the protected health information.

f. Fees

If the individual requests a copy of the protected health information, or agrees to a summary or explanation of such information, GMS shall impose charges as set forth in Appendix E to these Privacy Policies.

5. Documentation

The Privacy Officer shall maintain, or cause to be maintained, documentation of:

a. The designated record sets that are subject to access by individuals; and,

b. The titles of the persons or offices responsible for receiving and processing request for access by individuals.

The documentation shall be maintained by GMS in written or electronic form for six years after the date of its creation or the date when it was last in effect, whichever is later, or any longer period required by law.

C. Right to Request Amendment, Correction, or Clarification

1. Generally

An individual shall have a right to have GMS amend protected health information or a record about the individual in a designated record set for as long as the protected health information is maintained in the designated record set.

2. Request for Amendment, Correction, or Clarification

The individual's request for amendment, correction, or clarification must be submitted in writing to the *Director of Human Resources* and must state in the written request a reason to support the requested amendment. Individuals shall be informed in advance of these requirements in GMS's Notice of Privacy Practices.

3. Action on Request

a. Time Limits for Action

The *Director of Human Resources* shall act on a request for amendment, correction, or clarification no later than sixty (60) calendar days after GMS's receipt of the request.

If the *Director of Human Resources* is unable to take an action on the request within that sixty (60) day period, the *Executive Director* may extend the time for the action by no more than thirty (30) calendar days, provided:

(1) Within that sixty (60) day period, the *Director of Human Resources* shall provide the individual with a written statement of the reason(s) for the delay and the date by which GMS will complete its action on the request; and,

(2) Only one such extension shall be permitted on a request for amendment.

b. Inform Individual of Action on Request

The *Director of Human Resources* shall inform the individual of the acceptance of the request and add to the information the statement amending, correcting, or clarifying the information requested in accordance with Section VIII.C.4.a, below, of these Privacy Policies. The *Director of Human Resources* shall not delete any portion of the individual's information.

4. Accepting the Amendment, Correction, or Clarification

a. Making the Amendment, Correction, or Clarification

The *Director of Human Resources* shall make the appropriate amendment, correction, or clarification to the protected health information or record that is the subject of the request by, at a minimum, identifying the records in the designated record set that are affected by the amendment, correction, or clarification and appending or otherwise providing a link to the location of the amendment.

b. Informing the Individual

The *Director of Human Resources* shall inform the individual as stated in Section VIII.C.3.b, "Inform Individual of Action on Request" of these Privacy Policies, that the amendment, correction, or clarification has been accepted and obtain the individual's identification of and agreement to have GMS notify the relevant persons with the amendment, correction, or clarification needs to be shared in accordance with Section VIII.C.4.c, below.

c. Informing Others

The *Director of Human Resources* shall make a reasonable effort to inform and provide the amendment, correction, or clarification within a reasonable time to:

(1) Persons identified by the individual as having received protected health information about the individual and needing amendment, correction, or clarification;

(2) Persons, including GMS business associates, that GMS knows have the protected health information that is the subject of the amendment, correction, or clarification and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

5. Responding to the Amendment, Correction, or Clarification

An authorized member of GMS's workforce may add to the individual's protected health information a statement in response to the submitted amendment, correction, or clarification. The *Director of Human Resources* shall provide a copy of such statement to the individual.

6. Documentation

The Privacy Officer shall maintain documentation of the titles of the persons or offices responsible for receiving and processing requests for amendment, correction, or clarification. The documentation shall be maintained by GMS in written or electronic form for six (6) years after the date the notice was last in effect, or any longer period required by law.

D. Right to an Accounting of Disclosures

1. Right to Accounting

a. General Rule

Except as stated in VIII.D.1.b, "Exceptions" or VIII.D.1.c "Suspension of Right for Certain Disclosures," below, an individual shall have a right to receive an accounting of disclosures of protected health information made by GMS in the six (6) years prior to the date on which the accounting is requested or for such shorter period as the individual may request.

b. Exceptions

The right to an accounting of disclosures does not apply to the following types of disclosures:

(1) To carry out treatment, payment and health care operations as provided in Section VII.D, "Uses and Disclosures to Carry Out Treatment, Payment and Health Care Operations" of these Privacy Policies;

(2) To individuals of protected health information about them;

(3) Incident to a use or disclosure otherwise permitted or required by these Privacy Policies as provided in Section VII.B "Incidental Uses and Disclosures" of these Privacy Policies;

(4) Pursuant to an authorization as provided in Section VII.E "Uses and Disclosures for Which an Authorization is Required" of these Privacy Policies;

(5) For the facility's directory or to persons involved in the individual's care or other notification purposes as provided in Section VII.F "Uses and Disclosures Requiring an Opportunity for the Individual to Agree or Object" of these Privacy Policies;

(6) For national security or intelligence purposes;

(7) To correctional institutions or law enforcement officials having lawful custody of an individual;

(8) As part of a limited data set in accordance with Section VII.K "Limited Data Set" of these Privacy Policies;

c. Suspension of Right for Certain Disclosures

An individual's right to receive an accounting of disclosures to a health oversight agency (see, Section VII.G.5) "Uses and Disclosures for Health Oversight Activities" of these Privacy Policies or to a law enforcement official (see, Section VII.G.7) "Disclosures for Law Enforcement Purposes" of these Privacy Policies) shall be temporarily suspended for the time specified by the agency or official, if the agency or official provides GMS with a written statement that such an accounting to the individual would be reasonably likely to impede the agency's activities and specifying the time for which such a suspension is required.

If the agency or official statement is made orally, the *Director of Human Resources* shall:

(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) calendar days from the date of the oral statement, unless a written statement as described above is submitted during that time.

2. Content of the Accounting

The written accounting provided to the individual shall meet the following requirements:

a. Content

Except as otherwise stated in Section VIII.D.1.b, "Exceptions" of these Privacy Policies, the accounting must include the disclosures of protected health information that occurred during the period the individual requests up to a maximum of six (6) years prior to the date of the request, including disclosures to or by business associates of GMS.

b. Information

Except as stated in Section VIII.D.2.c, "Multiple Disclosures for a Single Purpose" or Section VIII.D.2.d "Disclosures for Particular Research" of these Privacy Policies, the accounting must include for each disclosure:

(1) The date of the disclosure;

(2) The name of the entity or person who received the protected health information and, if known, the address of such entity or person;

(3) A brief description of the protected health information disclosed; and,

(4) 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:

(a) A copy of a written request for disclosure by the Secretary of Health and Human Services under Section VII.G.11, "Disclosure to the Secretary of Health and Human Services" of these Privacy Policies, if any; or,

(b) A copy of a written request for disclosure under Section VII.G, "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" of these Privacy Policies, if any.

c. Multiple Disclosures for a Single Purpose

If, during the period covered by the accounting, GMS has made multiple disclosures of protected health information to the same person or entity for a single purpose under Section VII.G.11, "Disclosure to the Secretary of Health and Human Services" or Section VII.G, "Uses and Disclosures for which an Authorization or an Opportunity to Agree or Object is Not Required" of these Privacy Policies, the accounting may, with respect to such multiple disclosures, provide:

(1) The information required by Section VIII.D.2.b of these Privacy Policies, for the first disclosure during the accounting period;

(2) The frequency, periodicity, or number of the disclosures made during the accounting period; and,

(3) The date of the last such disclosure during the accounting period.

d. Disclosures for Particular Research

If during the period covered by the accounting, GMS has made disclosures of protected information for a particular research purpose in accordance with Section VII.G.9 "Uses and Disclosures for Research Purposes" of these Privacy Policies for 50 or more individuals, the accounting may, with respect to the disclosures for which the protected health information about the individual may have been included, provide:

(1) The name of the protocol or other research activity;

(2) A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular records;

(3) A brief description of the type of protected health information that was disclosed;

(4) The date or period of time during which such disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;

(5) The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and,

(6) A statement that the protected health information of the individual may or may not have been disclosed for a particular protocol or other research activity.

If GMS provides an accounting for research disclosures in accordance with this Section VIII.D.2.d, "Disclosures for Particular Research," and if it is reasonably likely that the protected health information of the individual was disclosed for that research protocol or activity, GMS shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

3. Provision of the Accounting

a. Time Limit to Provide the Accounting

The *Director of Human Resources* shall act on a request for an accounting no later than sixty (60) calendar days after GMS's receipt of the request.

Within that sixty (60) day period, the *Director of Human Resources* shall:

(1) Provide the individual with the accounting requested; or,

(2) If the *Director of Human Resources* is unable to take an action on the request within that sixty (60) day period, the *Executive Director* may extend the time for the action by no more than thirty (30) calendar days, provided:

(a) Within that sixty (60) day period, the *Director of Human Resources* shall provide the individual with a written statement of the reason(s) for the delay and the date by which GMS will provide the accounting; and,

(b) Only one such extension shall be permitted on a request for amendment.

b. Fee for Accounting

The first accounting to an individual in any twelve (12) month period will be provided to the individual without charge. For each subsequent request for an accounting by the same individual within the twelve (12) month period shall be as stated in Appendix F to these Privacy Policies; before charging the fee, however, the

Director of Human Resources shall notify the individual in advance of the fee and provide the individual an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

c. Documentation

The Privacy Officer shall document and retain the following:

(1) The information required to be included in an accounting under Section VIII.D.2, "Content of the Accounting" of these Privacy Policies, for disclosures of protected health 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 of offices responsible for receiving and processing requests for an accounting by individuals.

The documentation shall be maintained by GMS in written or electronic form for six years after the date of its creation or the date when it was last in effect, whichever is later, or any longer period required by law.

IX. PERSONAL REPRESENTATIVES

A. General Rule

Except as otherwise stated or permitted in these Privacy Policies, GMS will treat a personal representative as the individual for purposes of these Privacy Policies.

B. Adults and Emancipated Minors

If, under State law, a person has authority to act on behalf of an individual who is an adult or an emancipated minor in making decisions related to health care, GMS will treat such person as a personal representative with respect to protected health information relevant to such personal representative.

C. Unemancipated Minors

1. General Rule

If, under State 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, GMS

will treat such person as a personal representative with respect to protected health information relevant to such personal representative.

Notwithstanding the general rule stated above, a person will not be treated as a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to protected health information pertaining to health care services, if:

a. The minor consents to such health care service; no other consent to such health care services is required by State law, regardless of whether the consent of another person has also been obtained; and, the minor has not requested that such person be treated as the personal representative.

b. 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; or,

c. A parent, guardian, or other person acting *in loco parentis* assents to an agreement of confidentiality between GMS and the minor with respect to such health care service.

2. Exception.

Notwithstanding the preceding paragraph "1. General Rule:"

a. If, and to the extent, permitted or required by an applicable provision of State or other law, including applicable case law, a covered entity may disclose, or provide access in accordance with Section VIII.B "Right of Access" of these Privacy Policies to protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*;

b. If, and to the extent, prohibited by an applicable provision of State or other law, including applicable case law, GMS may not disclose, or provide access in accordance with Section VIII.B "Right of Access" of these Privacy Policies to, protected health information about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*; and,

c. Where the parent, guardian, or other person acting *in loco parentis*, is not the personal representative under subparagraphs IX.C.1.a, IX.C.1.b and IX.C.1.c of this Section IX.C "Unemancipated Minors" of these Privacy Policies and where there is no applicable access provision under State or other law, including case law,

GMS may provide access under Section VIII.B "Right of Access" of these Privacy Policies to a parent, guardian, or other person acting *in loco parentis*, if such action is consistent with State or other applicable law, provided that such decision must be made by a licensed health care professional, in the exercise of professional judgment.

D. Deceased Individuals.

If under State law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, GMS will treat that person as a personal representative under these Privacy Policies with respect to protected health information relevant to such personal representation.

E. Abuse, Neglect, Endangerment Situations

Notwithstanding anything in State law or these Privacy Policies to the contrary, GMS may elect not to treat a person as the personal representative of an individual if:

1. GMS has a reasonable belief that:

    a. The individual has been or may be subjected to domestic violence, abuse, or neglect by such person; or,

    b. Treating that person as the personal representative could endanger the individual; and

2. GMS, in the exercise of professional judgment, decides that it is not in the best interest of the individual to treat the person as the individual's personal representative.

X. HIPAA BREACH NOTIFICATION

A. Generally

Following discovery of a breach of unsecured protected health information, GMS's Privacy Officer shall notify each individual whose unsecured protected health information has been or is reasonably believed by the Privacy Officer to have been, accessed, acquired, used, or disclosed as a result of that breach. Such notification shall be as stated in this Section X.

B. Determining Whether a Breach Occurred

Unless the breach falls within the exceptions stated in subparagraphs 1, 2, or 3, of the definition of "breach", an acquisition, access, use, or disclosure of protected

health information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Security Officer or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;

2. The unauthorized person who used the protected health information or to whom the disclosure was made;

3. Whether the protected health information was actually acquired or viewed; and,

4. The extent to which the risk to the protected health information has been mitigated.

C. When a Breach is Considered to be "Discovered"

A breach shall be considered to be "discovered" as of the first day on which the breach is known to GMS, or, by exercising reasonable diligence would have been known to GMS. GMS shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of GMS.

D. Time of Notification

The notification to affected individuals shall be provided without unreasonable delay and in no case later than sixty (60) calendar days after discovery of the breach.

E. Content of Notification

The notification to affected individuals shall be written in plain language and include to the extent possible:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

2. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

3. Any steps individuals should take to protect themselves from potential harm resulting from the breach;

4. A brief description of what GMS is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and,

5. Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free number, an e-mail address, Web site, or postal address.

Generally, the notice should avoid including any sensitive material, such as the individual's actual social security number or credit card number.

As appropriate for the individuals to whom notice is given, reasonable steps shall be taken to have the notification translated into languages that are frequently encountered by GMS and as may be necessary to ensure effective communication with individuals with disabilities.

F. Methods of Notification

1. Written Notice

The notification to affected individuals shall be by first class mail to the individual at the last known address of the individual, or, if the individual has agreed to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as information is available.

If GMS knows the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first class mail to either the next of kin or the personal representative is permitted. It may be provided in one or more mailings as information is available.

2. Substitute Notice

a. Generally. If there is insufficient or out-of-date contact information that precludes written notification to the individual, a substitute form of notice, which is reasonably calculated to reach the individual, will be used. However, substitute notice will not be made if the insufficient or out-of-date contact information precludes written notice to the next of kin or personal representative.

b. If Fewer Than 10 Individuals. If there are fewer than ten (10)

individuals to receive substitute notice, the substitute notice may be provided by an alternate form of written notice, telephone, or other means.

c. If 10 or More Individuals. If there are ten (10) or more individuals to receive substitute notice, then the substitute notice must:

(1) Be in the form of either: (a) a conspicuous posting for a period of ninety (90) days on the home page of the Web site of GMS; or, (b) a conspicuous notice in major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and,

(2) Include a toll-free telephone number that remains active for at least ninety (90) days where an individual can learn whether the individual's unsecured PHI may be included in the breach.

3. Additional Notice in Urgent Situations

If the Privacy Officer deems the situation to require urgency because of possible imminent misuse of unsecured protected health information, GMS may provide information to individuals by telephone or other means, as appropriate, in addition to the written notice stated above.

G. Notification to the Media

If a breach of unsecured protected health information involves more than five hundred (500) residents of a State or other jurisdiction, GMS shall notify prominent media outlets serving that State or jurisdiction of the breach. This notice will be provided without unreasonable delay and in no case later than sixty (60) calendar days after discovery of the breach. To the extent possible, the notification shall meet the requirements stated in paragraph X.E, "Content of Notification," for its content.

H. Notification to the Secretary of Health and Human Services

Following discovery of a breach, the Privacy Officer shall notify the Secretary of Health and Human Services as stated below.

1. Breaches involving five hundred (500) or more individuals. If the If a breach involves five hundred (500) or more individuals, with one exception, GMS will provide the Secretary of Health and Human Services with notice of the breach contemporaneously with its notice to the affected individuals. The notice will include the same information that is provided

to affected individuals and will be provided to the Secretary of Health and Human Services in the manner specified on the Health and Human Services Web site. The exception is when there is a law enforcement delay pursuant to Section X.J, "Law Enforcement Delay" of these Privacy Policies.

2. **Breaches involving less than five hundred (500) individuals.** If a breach involves less than five hundred (500) individuals, the Privacy Officer will maintain a log or other documentation of such breaches and, no later than sixty (60) days after the end of each calendar year, provide the Secretary of Health and Human Services with notice of breaches discovered during the preceding calendar year in the manner specified on the Department of Health and Human Services Web site. This log will be kept for six years. The reporting of a breach under this Section X.H.2 may be delayed when there is a law enforcement delay pursuant to Section X.J, "Law Enforcement Delay" of these Privacy Policies.

I. Notification from a Business Associate

When notification is received from a business associate of GMS of its discovery of a breach of unsecured protected health information, the Privacy Officer shall give notice to affected individuals in accordance with this Section X of these Privacy Policies. Provided, however, if the agreement between GMS and the business associate permits, the Privacy Officer may require the business associate to give such notice.

J. Law Enforcement Delay

Notwithstanding anything in this Section X "HIPAA Breach Notification" to the contrary, if a law enforcement official states to GMS that a notification, notice, or posting required by this Section X "Breach Notification" would impede a criminal investigation or cause damage to national security, the Privacy Officer shall:

1. If the statement of the law enforcement official is in writing and specifies how long of a delay is required, delay the notification, notice, or posting for the time period specified in the writing; or,

2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily but no longer than 30 days from the date of the statement, unless a written statement as described in subparagraph 1, above, is submitted during that time.

Any member of the workforce of GMS who is contacted by a law enforcement official in this regard shall immediately refer the official to the Privacy Officer.

XI. MAINE PERSONAL DATA BREACH NOTIFICATION

A. Definitions. For purposes of this Section XI, the following terms have the following meanings:

1. "Personal Information": An individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or data elements are not encrypted or redacted:

a. Social Security Number;

b. Driver's license number;

c. State identification number;

d. Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords;

e. Account passwords or personal information numbers or other access codes; or

f. Any of the above data elements when not in connection with the individual's first name, or first initial, and last name, if the information, if compromised, would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised.

2. "Breach of the Security of a System" (or "Security Breach"): The unauthorized acquisition, release or use of an individual's computerized data that includes Personal Information that compromises the security, confidentiality or integrity of Personal Information of the individual maintained by GMS. The good faith acquisition, release or use of Personal Information by a workforce member or agent of GMS on behalf of GMS is not a Security Breach if the Personal Information is not used for or subject to further unauthorized disclosure to another person.

B. Reporting Suspected Security Breaches. If a member of GMS's workforce discovers or is notified that a suspected Security Breach of computerized data has occurred, the workforce member shall immediately notify the Security Officer or Privacy Officer. In the event that either the Security Officer or Privacy Officer discovers or is notified of a suspected Security Breach, he or she shall immediately notify the other Officer of the suspected Security Breach to coordinate an investigation of the incident in accordance with their respective roles and responsibilities.

C. Investigating Suspected Security Breaches. The Security Officer shall be responsible for ensuring that a reasonable and prompt good faith investigation is conducted to determine whether a Security Breach has occurred, and the likelihood that Personal Information has been or will be misused as a result of the Security Breach.

1. No Security Breach Found. In the event that the Security Officer concludes that a Security Breach either did not occur, did not involve Personal Information, or did not involve the misuse or reasonably possible misuse of Personal Information, no notice is required to be provided under this Policy.

2. Security Breach Found. In the event that the Security Officer concludes that a Security Breach did occur and involved Personal Information that either has been misused or is reasonably possible to be misused, the Security Officer shall notify the Privacy Officer who shall in turn provide the mandatory notifications required by this Section XI.

D. Mandatory Notifications

1. Notification of Persons Affected by Security Breach. Subject to the legitimate needs of law enforcement described in Section XI.D.4, and any delay consistent with measures being taken by GMS to determine the scope of the Security Breach and to restore the reasonable integrity, security and confidentiality of data in the breached computer system, GMS shall, as expediently as possible and without unreasonable delay, give notice of the Security Breach and risk to personal information to all persons whose Personal Information is determined to have been misused or is reasonably possible to be misused.

2. Notification of State Regulators of Security Breach. Whenever notice of a Security Breach is required to be sent to an individual under this Section XI, GMS shall also notify (i) the Maine Attorney General's Office of the Security Breach, and (ii) the appropriate state regulators within the Maine Department of Professional and Financial Regulation if the person responsible for the Security Breach is regulated by that Department.

3. Notification of Consumer Reporting Agencies. If the Privacy Officer determines that the Security Breach requires notification to more than 1,000 people, GMS shall also report the Security Breach without unreasonable delay to consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. Such notice shall include:

a. The date of the Security Breach;

b. An estimate of the number of people affected by the Security Breach, if known; and

c. The actual or anticipated date that persons affected by the Security Breach were or will be notified.

4. Delays in Notification Requested by Law Enforcement. After completion of the internal investigation described in Section XI.C, any notice required to be provided under this Section XI may be delayed for no longer than seven (7) business days upon request from law enforcement, or for a shorter time provided that the requesting law enforcement agency determines that the notification will not compromise a criminal investigation.

XII. DEFINITIONS

As used in these Privacy Policies, the following terms and phrases shall have the following meanings.

A. Access

"Access" means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

B. Administrative Safeguards

"Administrative safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of GMS's workforce in relation to the protection of that information.

C. Authentication

"Authentication" means the corroboration that a person is the one claimed.

D. Authorized Member of GMS's Workforce

"Authorized member of GMS's workforce" means a member of GMS's workforce who has been authorized to take the action involved by: (a) his or her job description; (b) a protocol established by the Privacy Officer or Security Officer; or, (c) by the Privacy Officer or Security Officer.

E. Availability

"Availability" means the property that data or information is accessible and useable upon demand by an authorized person.

F. Breach

"Breach" means the acquisition, access, use or disclosure of protected health information in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the protected health information. Provided, however, breach does not include:

1. Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of GMS or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted by the HIPAA Privacy Rule.

2. Any inadvertent disclosure by a person who is authorized to access protected health information at GMS or business associate to another person authorized to access protected health information at the same GMS or business associate, or organized health care arrangement in which GMS participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule.

3. A disclosure of protected health information where GMS or a business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

G. Business Associate

Option 1

"Business associate" means:

1. Except as provided in paragraph (4) of this definition, business associate means, with respect to GMS, a person who:

    a. On behalf of GMS, but other than in the capacity of a member of GMS's workforce, creates, receives, maintains, or transmits protected health information for a function or activity regulated by the HIPAA regulations, including claims processing or administration, data analysis, processing or administration,

utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing, or

b. Provides, other than in the capacity of a member of GMS's workforce, legal, actuarial, accounting, consulting, data aggregation (as defined in the Privacy Rule), management, administrative, accreditation, or financial services to or for GMS, where the provision of the service involves the disclosure of protected health information from GMS to the person.

2. A covered entity may be a business associate of another covered entity.

3. Business associate includes:

a. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to GMS and that requires access on a routine basis to such protected health information.

b. A person that offers a personal health record to one or more individuals on behalf of GMS.

c. A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a business associate.

4. Business associate does not include:

a. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

b. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO) with respect to a group health plan) to the plan sponsor, to the extent that requirements of HIPAA apply and are met.

c. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

Option 2

"Business associate" means:

1. Except as provided in paragraph (4) of this definition, business associate means, with respect to GMS, a person who:

    a. On behalf of GMS or of an organized health care arrangement in which GMS participates, but other than in the capacity of a member of the GMS's or that arrangement's workforce, creates, receives, maintains, or transmits protected health information for a function or activity regulated by the HIPAA regulations, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing, or

    b. Provides, other than in the capacity of a member of GMS's workforce, legal, actuarial, accounting, consulting, data aggregation (as defined in the Privacy Rule), management, administrative, accreditation, or financial services to or for GMS or the organized health care arrangement in which GMS participates, where the provision of the service involves the disclosure of protected health information from GMS or that arrangement to the person.

2. A covered entity may be a business associate of another covered entity.

3. *Business associate* includes:

    a. A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to GMS and that requires access on a routine basis to such protected health information.

    b. A person that offers a personal health record to one or more individuals on behalf of GMS.

    c. A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of a business associate.

4. *Business associate* does not include:

    a. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

    b. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO) with respect to a group

health plan) to the plan sponsor, to the extent that requirements of HIPAA apply and are met.

c. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

d. A covered entity participating in an organized health care arrangement that performs a function or activity as described in paragraph (1)(a) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(b) of this definition to or for such organized health care arrangement by virtue of such activities.

H. Covered Entity

"Covered entity" means a health plan, a health care clearinghouse, or a health care provider that is covered by the HIPAA Privacy Rule.

I. Designated Record Set

"Designated record set" means a group of records maintained by or for GMS that is:

1. The medical records and billing records about individuals maintained by or for GMS;

2. The enrollment, payment, claims adjudication, and case or medical management record systems maintained for a health plan; or,

3. Used, in whole or in part, by or for GMS to make decisions about individuals.

For purposes of this definition, the term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for GMS.

J. Disclosure

"Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside GMS.

K. Health Care

"Health care" means care, services, or supplies related to the health of an individual.

"Health care" includes, but is not limited to, the following:

1. 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,

2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

L. Health Care Operations

"Health care operations" means any of the following activities of GMS to the extent that the activities are related to covered functions:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

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

3. Except as prohibited for genetic information, underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided the requirements of the HIPAA Privacy Rule concerning uses and disclosures for underwriting and related purposes are met, if applicable, see, *45 CFR §164.514(g)*.

4. Conducting or arranging for medical review, legal services, and auditing

functions, including fraud and abuse detection and compliance programs;

5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and,

6. Business management and general administrative activities of GMS, including, but not limited to:

    a. Management activities relating to implementation of and compliance with the requirements of these Privacy Policies and the HIPAA Privacy Rule;

    b. Customer service;

    c. Resolution of internal grievances;

    d. The sale, transfer, merger, or consolidation of all or part of GMS with another covered entity, or an entity, that following such activity, will become a covered entity and due diligence related to such activity; and,

    e. Consistent with the applicable requirements of Section II.B, "De-Identification of Health Information", creating de-identified health information or a limited data set, and fundraising for the benefit of GMS.

M. Health Oversight Agency

"Health oversight agency" means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

"Health oversight agency" includes the employees or agents of such a public agency or its contractors or persons or entities to whom it has granted authority.

N. HIPAA Breach Notification Rule

"HIPAA Breach Notification Rule" means 45 CFR Subpart D, as amended from time to time.

O. HIPAA Privacy Rule

"HIPAA Privacy Rule" means 45 CFR Subpart E, as amended from time to time.

P. HIPAA Security Rule

"HIPAA Security Rule" means 45 CFR Subpart C, as amended from time to time.

Q. Information System

"Information system" means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

R. Inmate

"Inmate" means a person incarcerated in or otherwise confined to a correctional institution.

S. Integrity

Integrity" means the property that data or information have not been altered or destroyed in an unauthorized manner.

T. Law Enforcement Official

Law enforcement official" means an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

(1) Investigate or conduct an official inquiry into a potential violation of law; or,

(2) Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

U. Password

"Password" means confidential authentication information composed of a string of characters.

V. Payment

"Payment" means the activities undertaken by GMS to obtain reimbursement for the provision of health care that relate to the individual for whom health care is provided.

"Payment" includes but is not limited to:

1. Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts) and adjudication or subrogation of health benefit claims;

2. Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance) and related health care data processing;

3. Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

4. Utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and,

5. Disclosure to consumer reporting agencies of any of the following protected health information relating to collection of premiums or reimbursement:

    Name and address;

    Date of birth;

    Social security number;

    Payment history;

    Account number; or

    Name and address of GMS.

W. Physical Safeguards

"Physical safeguards" are physical measures, policies, and procedures to protect GMS's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

X. Privacy Officer

"Privacy Officer" is the member of GMS's workforce who has been designated, pursuant to the HIPAA Privacy Rule, with responsibility for ensuring GMS's compliance with the HIPAA Privacy Rule.

Y. Psychotherapy Notes

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

Z. Secretary of Health and Human Services

"Secretary of Health and Human Services" means the Secretary of the United States Department of Health and Human Services or any other officer or employee of that Department to whom the authority involved has been delegated.

AA. Security Officer

"Security Officer" is the member as GMS's workforce who has been designated, pursuant to the HIPAA Security Rule, with responsibility for the development, updating and implementation of GMS's security policies.

BB. Security or Security Measures

"Security or Security Measures" encompass all of the administrative, physical, and technical safeguards in an information system.

CC. Technical Safeguards

"Technical safeguards" means the technology and the policy and procedures for its use that protect electronic protected health information and control access to it.

DD. These Privacy Policies

"These Privacy Policies" means these Privacy Policies adopted by GMS concerning the protection of the privacy of protected health information.

EE. Treatment

"Treatment" means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

FF. Unsecured Protected Health Information

"Unsecured protected health information" means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services (the "Secretary of Health and Human Services") through guidance issued by the Secretary of Health and Human Services on the Health and Human Services Web site.

GG. Use

"Use" means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of that information within GMS.

HH. Workforce

"Workforce" means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for GMS, is under the direct control of GMS, whether or not they are paid by GMS.

APPENDIX A

Identification of Workforce Members' Access To Protected Health Information.

(1)	Executive Director:	The Executive Director must have access to all protected health information maintained by GMS. There are no conditions applicable to that access.
(2)	Finance Manager:	The Chief Financial Officer must have access to any and all financial information concerning individuals served or supported by GMS. There are no conditions applicable to that access.
(3)	Registered Nurse:	A Registered Nurse must have access to all clinical information of individuals to whom she/he is providing services. There are no conditions applicable to that access.
(4)	Direct Support Staff: Directors Sr. & Program Manager Quality Assurance Manager Case Manager	Direct Support Staff must have access to all health/clinical information of individuals whom she/he supports. There are no conditions applicable to that access. She/he must have access to billing information concerning an individual if the Billing Staff must discuss billing matters concerning that individual with the Direct Support Staff.
(5)	Billing Staff:	The Billing Staff must have access to all billing and payment information concerning the individual. There are no conditions applicable to that access. Billing Staff must have access to health/clinical information concerning the individual to the extent necessary to bill for services provided to the individual.
(6)	HR Specialist:	The HR Specialist must have access to the names of all individuals and of their personal representatives. There are no conditions applicable to that access.
(7)	Facilities Manager:	The Maintenance Staff does not need access to any protected health information concerning any individual of GMS.

APPENDIX B

Safeguards to Protect the Privacy of Protected Health Information

(1) Computers.

(a) All computers must have screen savers that activate after five minutes of inactivity. The screen saver must require the employee's password to be de-activated.

(b) All employees must change their passwords at least every month.

(c) No protected health information may be removed from the office on computer disk without the prior approval of the Privacy Officer. When removal is permitted by the Privacy Officer, the disk shall be encrypted and password protected.

(2) Trash.

All trash that contains protected health information must be placed in the designated receptacles to be shredded. The designated receptacles shall be located only in office rooms that can be locked when the office is closed.

(3) Files.

(a) During the workday, files containing protected health information shall remain in the appropriate file drawers except when being used. When being used, the person who removes the file shall place a red file divider at the location of the file in the file drawers indicating that the file is with that person. At the end of the work day, all files containing protected health information shall be returned to the appropriate file drawers.

(b) When the office is closed, all file drawers containing protected health information shall be locked.

(c) Any files being transported in a motor vehicle outside of the office, shall be transported in the trunk of the vehicle. If the vehicle does not have a truck, files shall be transported in a locked container which does not identify the contents as individuals' files.

(4) Faxes.

(a) Received Faxes.

The *Director of Human Resources* shall remove all received faxes from the fax machine promptly upon the faxes' receipt and deliver the fax to the intended recipient. If delivery

cannot be accomplished immediately, the *Director of Human Resources* shall maintain the faxes in a confidential file until delivery is accomplished.

At the end of the workday, the *Director of Human Resources* shall remove all paper from the fax machine.

(b) Sending Faxes.

All faxes must be sent with a fully completed cover sheet. The fax number to which the material is being faxed double checked before being sent.

APPENDIX C

Protocols for Routine and Recurring Requests by GMS

(1) Requests for Information When Receiving a Referral.

The information requested should be limited to the individual's name, address, telephone number, diagnosis, present condition, and the services required.

(2) Requests for Information to Verify Insurance Coverage.

The information requested should be limited to the individual's name, address, telephone number, diagnosis, present condition, the services required, insurance identification numbers, and, for group insurance, the name of the person who holds the coverage.

APPENDIX D

Protocols for Routine and Recurring Disclosures

(1) Disclosure for Reimbursement.

The information disclosed should be limited to the individual's name, address, social security number (or other applicable identification number), and the services for which reimbursement is requested.

APPENDIX E

Fees for Copies of Protected Health Information

Fees for copies of protected health insurance may not be more than the actual cost of reproduction. In no event may such fees for paper copies exceed $5 for the first page and $.45 for each additional page up to a maximum of $250 for an entire treatment record or medical report. In no event may such fees for electronic copies exceed $150, and costs may not include a retrieval fee or the costs of new technology, maintenance of the electronic record system, data access, or storage infrastructure.

APPENDIX F

Fees for Accounting

For the first accounting in a twelve (12) month period - No Charge.

For the second or greater accounting in a twelve (12) month period - $ _____.

APPENDIX G

ASSESSMENTS