HIPAA PRIVACY POLICY AND PROCEDURES FOR PROTECTED HEALTH INFORMATION

HILLSDALE COLLEGE HEALTH AND WELLNESS CENTER

Policy Preamble

This privacy policy ("**Policy**") is designed to address the Use and Disclosure of Protected Health Information (or "PHI") of the Hillsdale College Health and Wellness Center ("**Provider**"). This Policy is intended to fully comply with HIPAA. Any ambiguity within this Policy should be construed in a manner that permits the Provider to comply with the requirements of HIPAA, and take advantage of any potential exemptions.

No third party rights, including but not limited to rights of Business Associates, are intended to be created by this Policy. To the extent this Policy attempts to establish requirements and obligations above and beyond those required by HIPAA, the Policy shall be aspirational and shall not be binding upon the Provider. This Policy does not address requirements under other federal laws or under state laws. Nothing within this Policy should be construed as a contract and no vested rights are created by this Policy.

The Provider reserves the right to amend, change or terminate this Policy at any time, either prospectively or retroactively, without notice. This Policy will also change should it become necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of HIPAA. This Policy is designed to be implemented in conjunction with a set of comprehensive privacy procedures which are contained within a separate document, and any ambiguities between this Policy and those procedures should be harmonized consistent with the requirements of HIPAA.

HIPAA and the corresponding regulations restrict the Provider's ability to Use and Disclose PHI. It is the Provider's policy to comply fully with HIPAA's requirements. To that end, all Employees must comply with this Policy.

I. Responsibilities as Covered Entity

A. Privacy Official and Contact Person

The Provider will from time to time designate a person as the Privacy Official ("**Privacy Official**"). The Provider has the absolute discretion to designate or remove a Privacy Official at any time, either retroactively or prospectively. The Privacy Official will be responsible for the development and implementation of policies and procedures relating to privacy of PHI, including but not limited to this Policy and the Provider's Privacy Procedures. The Privacy Official will also serve as the contact person for individuals who have questions, concerns, or complaints about the privacy of their PHI or who would like further information about matters covered by the Provider's notice of privacy practices. If any questions arise as to the interpretation or implementation of this Policy, the Privacy Official shall have the authority to interpret the language of this Policy and determine the proper implementation of this Policy. The Privacy Official is responsible for ensuring that the Provider complies with the provisions of the HIPAA privacy rules regarding Business Associates, including the requirement that the Provider have a HIPAA compliant Business Associate agreement in place with all Business Associates (except Subcontractors). The Privacy Official shall also be responsible for monitoring compliance by all Business Associates (except Subcontractors) with the HIPAA privacy rules, this Policy, and the Provider's Privacy Procedures.

B. Employee Training

It is the Provider's policy to train or inform all Employees on this Policy and the Provider's Privacy Procedures as necessary and appropriate for the Employees to carry out their functions within the Provider. Some Employees may have more interaction with PHI than others, and consequently, some Employees may receive more extensive training than others. The Privacy Official is charged with developing training schedules and programs so that the applicable Employees receive the training necessary and appropriate to permit them to carry out their functions within the Provider in compliance with HIPAA. Training must be provided to each Employee by no later than the HIPAA compliance date for the Provider. Training must be provided to each new Employee within a reasonable time after the individual joins the workforce. Additionally, training must be provided to each Employee whose functions are affected by a material change in this Policy or the Provider's Privacy Procedures within a reasonable period of time after the material change becomes effective. All Employee training shall be documented.

C. Administrative, Technical, and Physical Safeguards and Firewall

The Provider will establish appropriate administrative, technical and physical safeguards to protect the privacy of PHI and to prevent PHI from intentionally or unintentionally being Used or Disclosed in violation of HIPAA's requirements. These safeguards will limit incidental Uses or Disclosure of PHI made pursuant to an otherwise permitted or required Use or Disclosure. Technical safeguards include limiting access to information by creating computer firewalls. Administrative safeguards include implementing procedures for Use and Disclosure of PHI. Physical safeguards include locking doors or filing cabinets. Firewalls will ensure that only authorized Employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary to perform their duties on behalf of the Provider and that they will not further Use or Disclose PHI in violation of the HIPAA privacy rules.

D. Privacy Notice

The Privacy Official is responsible for developing, maintaining, and providing individuals with an adequate notice of the Provider's privacy practices that describes in plain language: (1) the Uses and Disclosures of PHI that may be made by the Provider; (2) the individual's rights under the HIPAA privacy rules; (3) the Provider's legal duties with respect to the PHI; and (4) other detailed information as required by 45 C.F.R. §164.520. The privacy notice will also provide (1) a header; (2) a description of the Provider's complaint procedures; (3) the name (or title) and telephone number of the contact person (or office) for further information; (4) the effective date of the notice; and (5) all other information required or permitted by 45 C.F.R. §164.520.

The Privacy Official is responsible for determining which individuals are entitled to the notice of the Provider's privacy practices and ensuring compliance with the content and distribution requirements of 45 C.F.R. §164.520. Please note that an inmate does not have a right to a notice under 45 C.F.R. §164.520.

If the Provider has a Direct Treatment Relationship with an individual, then the Provider must (1) provide the notice (a) no later than the date of the first service delivery, including service delivered electronically, to such individual after the compliance date for the Provider, or (b) in an emergency Treatment situation, as soon as reasonably practicable after the emergency Treatment situation; (2) except in an emergency Treatment situation, make a good faith effort to obtain a written acknowledgement of receipt of the notice, and if not obtained, document its good faith efforts to obtain such acknowledgment and the reason why the acknowledgment was not obtained; (3) if the Provider maintains a physical service delivery site: (a) have the notice available at the service delivery site for individuals to request to take with them, and (b) post the notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the Provider to be able to read the notice; and (4) whenever the notice is revised, make the notice available upon request on or after the effective date of the revision and promptly comply with the distribution requirements of (3) above, if applicable.

If the Provider maintains a web site that provides information about the Provider's customer services or benefits, the notice must be prominently posted on the web site and be available electronically through the web site. The Provider must comply with the electronic delivery provisions of 45 C.F.R. §164.520(c)(3), as applicable.

The Provider reserves the right to amend, change or terminate the privacy notice at any time, either prospectively or retroactively (except as limited below), without notice. The privacy notice will also change should it become necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of HIPAA. The Provider must promptly revise and distribute the notice whenever there is a material change to the Uses or Disclosures, the individual's rights, the Provider's legal duties, or other privacy practices stated in the notice. Except when required by law, a material change to any term of the notice may not be implemented prior to the effective date of the notice in which such material change is reflected. The Privacy Official is responsible for determining when and if a change is "material" or required.

If the Provider participates in an organized health care arrangement, it may have a joint notice, provided that: (1) the covered entities participating in the organized health care arrangement agree to abide by the terms of the notice with respect to PHI created or received by the covered entity as part of its participation in the organized health care arrangement; (2) the joint notice meets the implementation specification of 45 C.F.R. §164.520(b), except that the statements required by that section may be altered to reflect the fact that the notice covers more than one covered entity and (i) describes with reasonable specificity the covered entities, or class of entities, to which the joint notice applies, (ii) describes with reasonable specificity the service delivery sites, or classes of service delivery sites, to which the joint notice applies, and (iii) if applicable, states that the covered entities participating in the organized health care arrangement will share PHI with each other, as necessary to carry out Treatment, Payment, or Health Care Operations relating to the organized health care arrangement; and (3) the covered entities included in the joint notice must provide the notice to individuals in accordance with the applicable implementation specifications of 45 C.F.R. §164.520(c).

The Provider must comply with the "Documentation" policies and procedures with respect to the privacy notice by retaining copies of the notices issued by the Provider and, if applicable, any written acknowledgments of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgment.

E. Complaints

The Privacy Official shall be the contact person for receiving complaints under HIPAA. The Privacy Official is responsible for creating a process for individuals to lodge complaints concerning this Policy, the Provider's Privacy Procedures, and for creating a system for handling such complaints. The Provider shall document all complaints received and any disposition thereof. A copy of the complaint procedure shall be provided to an individual upon request.

F. Sanctions for Violations of Privacy Policy

Sanctions for Using or Disclosing PHI in violation of this Policy or the Privacy Procedures will be imposed against Employees in accordance with the Provider's current discipline policy, up to and including termination. The Provider shall document any sanctions that are applied. However, this Section shall not apply to Employees with respect to individuals exercising their rights under the HIPAA privacy rules.

G. Mitigation of Inadvertent Disclosures of Protected Health Information

The Provider shall mitigate, to the extent practicable, any harmful effects that become known to it of a Use or

Disclosure of PHI in violation of this Policy, the Provider's Privacy Procedures, or the requirements of the HIPAA privacy rules. As a result, if an Employee or Business Associate becomes aware of an unauthorized Use or Disclosure of PHI, either by an Employee of the Provider or a Business Associate, the Employee or Business Associate shall immediately contact the Privacy Official or an officer of the Provider so that the appropriate steps to mitigate the harm to the individual can be taken.

H. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

The Provider shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights established or for the participation of any process provided for under the HIPAA privacy rules, filing a complaint, participating in an investigation, hearing, compliance review, or other proceeding, or opposing any improper practice under the HIPAA privacy rules (provided that the individual has a good faith belief that the practice opposed is unlawful and the manner of opposition is reasonable and does not involve a Disclosure of PHI in violation of the HIPAA privacy rules). No individual shall be required to waive his or her privacy or security rights under HIPAA as a condition of the provision of Treatment, Payment, enrollment in a health plan, or eligibility for benefits.

I. Documentation

The Provider's privacy policies and procedures shall be documented and maintained for at least six years unless state or federal law mandates a different time period. Policies and procedures must be changed as necessary and appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations) under HIPAA. Any changes to policies or procedures must be promptly documented. When the Provider changes a privacy practice that is stated in the notice of privacy practices and makes corresponding changes to its policies and procedures, the Provider may make the changes effective for PHI that is created or received prior to the effective date of the notice revision. Whenever there is a change in the law that necessitates a change in the Provider's policies and procedures, the Provider shall promptly document and implement the revised policy or procedure. If a change in law materially affects the content of the notice of privacy practices, the Provider must promptly make the appropriate revisions to the notice and distribute the revised notice. Such material change is effective only with respect to PHI created or received after the effective date of the notice, except when otherwise required by law. The Provider may change, at any time, a policy or procedure that does not materially affect the content of the notice of privacy practices provided that the policy or procedure, as revised, complies with the standards, requirements, and implementation specifications of the HIPAA privacy rules and is properly documented prior to the effective date of the change. The Provider shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights. The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form. Covered entities must maintain such documentation for at least six years from the date of its creation or the date when it last was in effect, whichever is later, unless state or federal law mandates a different time period. The Provider will also document personnel designations, training, any complaints received, the disposition of any complaints, and any sanctions applied.

The Provider must (1) maintain policies and procedures with regard to PHI in written or electronic form; (2) if a communication is required to be in writing, maintain a written or electronic copy of communication as documentation; (3) if an action, activity, or designation is required to be documented, maintain a written or electronic record of an action, activity or designation; and (4) maintain documentation sufficient to demonstrate that all notifications were made pursuant to the HIPAA privacy rules and that a Use or Disclosure did not constitute a Breach. Such documentation must be retained for six years from the date of its creation or the date when it last was in effect, whichever is later.

II. Policies on Use and Disclosure of PHI

A. Use and Disclosure In General

The Provider shall Use and Disclose PHI only as permitted under HIPAA. The Provider is permitted to Use or Disclose PHI incident to a Use or Disclosure otherwise permitted by the HIPAA privacy rules, provided that the Provider only abides by the "minimum necessary" standard and reasonably safeguards PHI to limit incidental Uses or Disclosures made pursuant to an otherwise permitted or required Use or Disclosure.

B. Employees Must Comply With Provider's Policy and Procedures

All Employees must comply with this Policy and the Provider's Privacy Procedures, which are set forth in a separate document.

C. Access to PHI Is Limited to Certain Employees

The Provider's functions, including creation and maintenance of its records, are carried out by Employees and by Business Associates of the Provider.

The Provider must identify Employees or classes of Employees, as appropriate, who need access to PHI to carry out their duties. For each such Employee or class of Employees, the Provider must identify the category or categories of PHI to which access is needed and any conditions appropriate to such access. The Provider must make reasonable efforts to limit the access of such Employees or classes of Employees to the category or categories of PHI to which access is needed and any conditions appropriate to such access.

Employees with this access may not Disclose PHI to Employees without the same access unless an authorization is in place or the Disclosure otherwise is in compliance with this Policy and the Provider's Privacy Procedures.

D. Permitted Uses and Disclosures

For Payment, Treatment, or Health Care Operations. Except with respect to Uses or Disclosures that require an authorization under 45 C.F.R. §164.508(a)(2) through (4) (related to psychotherapy notes, Marketing, and the sale of PHI), or that are prohibited under 45 C.F.R. §164.502(a)(5)(i) (related to the prohibition against Using or Disclosing PHI that is Genetic Information for underwriting purposes), the Provider may Use or Disclose PHI for Treatment, Payment, or Health Care Operations as set forth below, provided that such Use or Disclosure is consistent with other applicable requirements of the privacy rules.

Payment. The Provider may Use or Disclose PHI for its own Payment purposes and may Disclose PHI to another covered entity or a health care provider for the Payment activities of the entity that receives the information.

Health Care Operations. The Provider may Use or Disclose PHI for its own Health Care Operations. The Provider may Disclose PHI to another covered entity for Health Care Operations activities of the entity that receives the information, if each entity has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the Disclosure is for the purpose of (1) conducting quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. §3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting 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 learned under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; or (3) health care fraud and abuse detection or compliance. If the Provider participates in an organized health care arrangement, it may Disclose PHI about an individual to other participants in the organized health care arrangement for any Health Care Operations activities of the organized health care arrangement.

Treatment. The Provider may Use or Disclose PHI for its own Treatment and may Use or Disclose PHI for Treatment activities of a health care provider.

E. Mandatory Disclosures of PHI: to Individual and Health and Human Services

An individual's PHI must be Disclosed as required by HIPAA in the following situations: (1) the Disclosure is to the individual who is the subject of the information (see the policy for "Access to Protected Health Information and Request for Amendment" and "Accounting" that follow); and (2) the Disclosure is required by the Secretary to investigate or determine the Provider's compliance with HIPAA.

F. Disclosure to Personal Representatives

The Provider shall treat an a personal representative as the individual for purposes of the HIPAA privacy rules. The Provider requires documentation establishing that the person is a personal representative of the individual prior to Using or Disclosing any PHI of the individual.

If under applicable 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, the Provider must treat such person as a personal representative under the HIPAA privacy rules, with respect to PHI relevant to such personal representation.

If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decisions related to health care, the Provider must treat such person as a personal representative under the HIPAA privacy rules, with respect to PHI relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to PHI pertaining to a health care service if: (1) the minor consents to such health care service; no other consent to such health care service is required by 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; (2) 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 (3) a parent guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

Notwithstanding the previous paragraph: (1) If, and to the extent, permitted or required by an applicable provision of state or other law, including applicable case law, the Provider may Disclose, or provide access in accordance with 45 C.F.R. §164.524 to, PHI about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; (2) If, and to the extent, prohibited by an applicable provision of state or other law, including applicable case law, the Provider may not Disclose, or provide access in accordance with 45 C.F.R. §164.524 to, PHI about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and (3) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative and where there is no applicable access provision under state or other law, including case law, the Provider may provide or deny access under 45 C.F.R. §164.524 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.

If under applicable law an executor, administrator, or other person has authority to act on behalf of a deceased individual or of the individual's estate, the Provider must treat such person as a personal representative under the HIPAA privacy rules, with respect to PHI relevant to such personal representation.

Notwithstanding a state law or other requirement under HIPAA, the Provider may elect not to treat a person as the personal representative of an individual if: (1) the Provider 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 such person as the personal representative could endanger the individual; and (2) the Provider, 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.

G. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be Used or Disclosed in the following situations without an individual's written authorization or the opportunity for the individual to agree or object, when specific requirements are satisfied. The Provider's Privacy Procedures describe specific requirements that must be met before these types of Uses and Disclosures may be made. The requirements include prior approval of the Privacy Official. Permitted are: (1) Disclosures about victims of abuse, neglect or domestic violence; (2) Uses and Disclosures required by law; (3) Disclosures for judicial and administrative proceedings; (4) Disclosures for law enforcement purposes; (5) Uses and Disclosures for public health activities; (6) Uses and Disclosures for health oversight activities; (7) Uses and Disclosures about decedents; (8) Uses and Disclosures for cadaveric organ, eye or tissue donation purposes; (9) Uses and Disclosures for certain limited research purposes; (10) Uses and Disclosures to avert a serious threat to health or safety; (11) Uses and Disclosures for specialized government functions; and (12) Disclosures that relate to workers' compensation programs.

H. Disclosures of PHI Pursuant to an Authorization

PHI may be Disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the individual. All Uses and Disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization. An individual may revoke an authorization provided that the revocation is in writing, except to the extent that (1) the Provider has taken action in reliance thereon; or (2) if the authorization was obtained as a condition of obtaining insurance coverage, other law provides the insurer with the right to contest a claim under the policy or the policy itself. Authorizations are required for certain Uses and Disclosures related to psychotherapy notes, Marketing, and the sale of PHI.

Under certain circumstances, the Provider may Disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or Payment related to the individual's health care without a written authorization. Under certain circumstances, the Provider may Use or Disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death without a written authorization.

I. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when Using or Disclosing PHI or when requesting PHI from another covered entity, the Provider must make reasonable efforts to limit PHI to the "minimum necessary" to accomplish the intended

purpose of the Use, Disclosure, or request. The "minimum-necessary" standard does not apply to any of the following: (1) Disclosures to or requests by a health care provider for Treatment; (2) Uses or Disclosures made to the individual; (3) Uses or Disclosures made pursuant to a valid authorization; (4) Disclosures made to the Secretary; (5) Uses or Disclosures required by law; and (6) Uses or Disclosures required to comply with HIPAA.

The Provider shall be treated as being in compliance with the "minimum necessary" standard, with respect to the Use, Disclosure, or request of PHI, only if the Provider limits such PHI, to the extent practicable, to the Limited Data Set or, if needed by such entity, to the minimum necessary to accomplish the intended purpose of such Use, Disclosure, or request, respectively. In the case of the Disclosure of PHI, the Provider shall determine what constitutes the "minimum necessary" to accomplish the intended purpose of such Disclosure. The Provider shall keep itself informed of guidance issued by the Secretary with respect to what constitutes the "minimum necessary." Nothing regarding the "minimum necessary" standard shall be construed as affecting the Use, Disclosure, or request of PHI that has been de-identified.

Minimum Necessary Uses of PHI. The Privacy Official, on behalf of the Provider, shall identify and make reasonable efforts to limit access to PHI (1) to those Employees or classes of Employees, as appropriate, who need access to PHI to carryout their duties; and (2) for each such person or class of persons, to the category or categories of PHI to which access is needed and any conditions appropriate to such access.

Minimum Necessary When Disclosing PHI. The Provider, when disclosing PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI that is necessary to the requestor is Disclosed. For any type of Disclosure that is made on a routine and recurring basis, the Provider shall limit the PHI Disclosed to the amount reasonably necessary to achieve the purpose of the Disclosure. All Disclosures other than those made on a routine and recurring basis must be reviewed on an individual basis with the Privacy Official to ensure that the PHI Disclosed is limited to the information reasonably necessary to accomplish the purpose for which the Disclosure is sought.

Minimum Necessary When Requesting PHI. The Provider, when requesting PHI subject to the minimum necessary standard, shall take reasonable and appropriate steps to ensure that only the minimum amount of PHI necessary for the Provider is requested. The Provider shall limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting such information from other covered entities. For a request that is made on a routine and recurring basis, the Provider shall limit the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made. All requests other than those made on a routine and recurring basis must be reviewed on an individual basis with the Privacy Official to ensure that the PHI requested is limited to the information reasonably necessary to accomplish the purpose for which the request is made.

Limited Data Set Uses and Disclosures. Under limited circumstances, the Provider may Use or Disclose a Limited Data Set, if the Provider enters into a data use agreement with the Limited Data Set recipient. The Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with 45 C.F.R. §164.514(e) prior to Using or Disclosing a Limited Data Set.

J. Disclosures of PHI to Business Associates

The Provider may Disclose PHI to a Business Associate and may allow the Business Associate to create, receive, maintain, or transmit PHI on its behalf. However, prior to doing so, the Provider must first obtain satisfactory assurances from the Business Associate that it will appropriately safeguard the information. But, the Provider is not required to obtain such satisfactory assurances from a Business Associate that is a Subcontractor. The Provider shall document the Business Associate's satisfactory assurances through a written contract or other written agreement or arrangement with the Business Associate that meets the applicable

requirements of HIPAA (except with respect to Subcontractors). Before sharing PHI with outside consultants or contractors who meet the definition of a "Business Associate," Employees must contact the Privacy Official and verify that a Business Associate contract, which meets the applicable requirements of HIPAA, is in place. Before providing PHI to a Business Associate that is a Subcontractor, Employees must contact the Privacy Official to ensure all appropriate Business Associate contracts between the Provider's Business Associate and Subcontractor are in place.

The Provider shall require a Business Associate that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, Uses, or Discloses Unsecured PHI, following the discovery of a Breach of such information, to notify the Provider of such Breach. Such notice shall include the identification of each individual whose Unsecured PHI has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, or Disclosed during such Breach. The Business Associate shall also be required to provide the Provider with any other available information that the Provider is required to include in notification to the individual. A Breach shall be treated as discovered by a Business Associate as of the first day on which such Breach is known to such Business Associate, or by exercising reasonable diligence would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the Business Associate (determined in accordance with the federal common law of agency).

K. Disclosures of De-Identified Information

The Provider may Use PHI to create information that is not Individually Identifiable Health Information or Disclose PHI only to a Business Associate for such purpose, whether or not the De-identified Information is to be Used by the Provider. The Provider may freely Use and Disclose De-identified Information (which is not Individually Identifiable Health Information) in accordance with the HIPAA privacy rules. However, Disclosure of a code or other means of record identification designed to enable coded or otherwise De-identified Information to be re-identified constitutes Disclosure of PHI. Additionally, if De-identified Information is re-identified, the Provider may Use or Disclose such re-identified information only as permitted or required by the HIPAA privacy rules, this Policy, and the Privacy Procedures.

The Provider may assign a code or other means of record identification to allow information de-identified to be re-identified by the Provider if (1) the code or other means of record identification is not derived from or related to the information about the individual and is not otherwise capable of being translated so as to identify the individual; and (2) the Provider does not Use or Disclose the code or other means of record identification for any other purpose, and does not Disclose the mechanism for re-identification.

L. Notification of Breach of Unsecured PHI

The Provider, to the extent that it accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, Uses, or Discloses Unsecured PHI, shall, following the discovery of a Breach of Unsecured PHI, notify each individual whose Unsecured PHI has been, or is reasonably believed by the Provider to have been, accessed, acquired, Used, or Disclosed as a result of such Breach. A Breach shall be treated as discovered by the Provider as of the first day on which such Breach is known to the Provider, or by exercising reasonable diligence would have been known to the Provider. The Provider shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent of the Provider (determined in accordance with the federal common law of agency). Notice shall be provided by the Provider to prominent media outlets serving a State or jurisdiction, following the discovery of a Breach if the Unsecured PHI of more than 500 residents of such state or jurisdiction is, or is reasonably believed to have been, accessed, acquired, Used or Disclosed during such Breach. The Provider shall, following the discovery of a Breach of Unsecured

PHI, notify the Secretary.

M. Uses and Disclosures for Purposes of Marketing, Fundraising, the Sale of PHI, Psychotherapy Notes, and Facility Directories

Marketing. The Provider must obtain an authorization for any Use or Disclosure of PHI for Marketing, except if the communication is in the form of (1) a face-to-face communication made by the Provider to the individual; or (2) a promotional gift of nominal value provided by the Provider. If the Marketing involves Financial Remuneration to the Provider from a third party, the authorization must state that such remuneration is involved. The Provider shall consult with legal counsel or otherwise ensure compliance with 45 C.F.R. §164.508(a)(3) prior to Using or Disclosing PHI for any Marketing.

Fundraising. Under limited circumstances, the Provider may Use or Disclose certain PHI for fundraising purposes. The Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with 45 C.F.R. §164.514(f) prior to Using or Disclosing any PHI for fundraising purposes.

Sale of PHI. The Provider shall not sell PHI, except pursuant and in compliance with an authorization meeting the requirements of 45 C.F.R. §164.508(a)(4). The Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with 45 C.F.R. §164.502(a)(5)(ii) and 45 C.F.R. §164.508(a)(4) prior to selling PHI under all circumstances.

Psychotherapy Notes. The Provider must obtain an authorization for any Use or Disclosure of psychotherapy notes, except: (1) to carry out the following Treatment, Payment or Health Care Operations: (a) Use by the originator of the psychotherapy notes for Treatment, (b) Use or Disclosure by the Provider for 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 (c) Use or Disclosure by the Provider to defend itself in a legal action or other proceeding brought by the individual; and (2) a Use or Disclosure that is required by 45 C.F.R. §164.502(a)(2)(ii) (related to Disclosures required by the Secretary to investigate or determine the Provider's compliance with HIPAA) or permitted by 45 C.F.R. §164.512(a) (related to Uses and Disclosures required by law), 45 C.F.R. §164.512(d) (related to Uses and Disclosures for health oversight activities) with respect to the oversight of the originator of the psychotherapy notes, 45 C.F.R. §164.512(g)(1) (related to certain Disclosures about decedents to coroners and medical examiners), or 45 C.F.R. §164.512(j)(1)(i) (related to certain Uses and Disclosures necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public).

Use or Disclosure for Facility Directories. Except when an objection is expressed in accordance with this paragraph, the Provider may: (1) Use the following PHI to maintain a directory of individuals in its facility: the individual's name, the individual's location in the Provider's facility, the individual's condition described in general terms that does not communicate specific medical information about the individual, and the individual's religious affiliation; and (2) Use or Disclose for directory purposes such information: to members of the clergy, or, except for religious affiliation, to other persons who ask for the individual by name. The Provider must inform an individual of the PHI that it may include in a directory and the persons to whom it may Disclose such information (including Disclosures to clergy of information regarding religious affiliation) and provide the individual with the opportunity to restrict or prohibit some or all of the Uses or Disclosures permitted by this paragraph. However, in certain emergency circumstances, if the opportunity to object to the Uses or Disclosures described above cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, the Provider may Use or Disclose some or all of the PHI permitted above for the facility's directory, if such Disclosure is: (1) consistent with a prior expressed preference of the individual, if any, that is known to the Provider; and (2) in the individual's best interest as determined by the Provider, in the exercise of professional judgment. That being said, the Provider must inform the individual and provide an opportunity to object to Uses and Disclosures for directory purposes when it becomes practicable to

do so.

III. Policies on Individual Rights

A. Access to Protected Health Information and Request for Amendment

HIPAA gives an individual the right of access to inspect and obtain a copy of his or her PHI that the Provider (or its Business Associates) maintains in Designated Record Sets, subject to limited exceptions. The Privacy Official may impose a reasonable cost-based fee for copies of documents containing PHI, consistent with the requirements of HIPAA.

HIPAA also gives an individual the right to have the Provider amend PHI or records about the individual in a Designated Record Set for as long as the PHI or record is maintained in the Designated Record Set. The Provider permits an individual to request that the Provider amend the PHI or record maintained in the Designated Record Set provided that the request is in writing and provides a reason to support a requested amendment.

The Provider may deny an individual's request for amendment, if it determines that the PHI or record that is the subject of the request: (1) was not created by the Provider (unless the individual provides a reasonable basis to believe that the originator of the PHI is no longer available to act on the requested amendment; (2) is not part of the Designated Record Set; (3) is not available for inspection pursuant to the individual's right to access; or (4) is accurate and complete.

B. Accounting

An individual has the right to receive an accounting of certain Disclosures made by the Provider of his or her own PHI. This right to an accounting extends to Disclosures made in the six years prior to the date on which the accounting is requested, other than Disclosures: (1) to carry out Treatment, Payment, or Health Care Operations; (2) to individuals about their own PHI; (3) incident to an otherwise permitted Use or Disclosure under the HIPAA privacy rules; (4) pursuant to an authorization; (5) for the facility's directory or to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes; (6) for other national security or intelligence purposes; (7) to correctional institutions or law enforcement officials; (8) as part of a Limited Data Set; or (9) that occurred prior to the HIPAA privacy rule compliance date for the Provider.

The Provider shall provide the individual with the accounting requested no later than 60 days after receipt of such request. If the Provider is unable to provide the accounting within 60 days, it may extend the time to provide the accounting by no more than 30 days, provided that it gives the individual a written statement (including the reason for the delay and the date the accounting will be provided) within the original 60-day period. The Provider must provide the individual with a written accounting that includes the Disclosures of PHI that occurred during the six years (or such shorter time period as requested) prior to the date of the request for an accounting, including Disclosures to or by Business Associates of the Provider, except as limited by the nine types of Disclosures above. The accounting for each Disclosure must include the date of the Disclosure, the name of the receiving party (and, if known, the address of the receiving party), a brief description of the PHI Disclosed, and a brief statement of the purpose of the Disclosure that reasonably informs the individual of the basis for the Disclosure (or a copy of the written request for Disclosure, if any). If a brief purpose statement is included in the accounting, it must be sufficient to reasonably inform the individual of the basis of the Disclosure. The first accounting to an individual in any 12-month period shall be provided free of charge. The Privacy Official may impose a reasonable cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period. For each subsequent request, the Provider shall inform the individual in advance of the fee and provide the individual with the opportunity to withdraw or modify the

request for a subsequent accounting in order to avoid or reduce the fee.

The Provider shall document and retain documentation for a period of six years for (1) the information required to be included in an accounting for Disclosures of PHI that are subject to the accounting; (2) the written accounting that is provided to the individual; and (3) the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

The Provider must temporarily suspend an individual's right to receive an accounting of Disclosures to a health oversight agency or law enforcement official for the time specified by such agency or official, if such agency or official provides the Provider 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 Provider must (1) document the statement, including the identity of the agency or official making the statement; (2) temporarily suspend the individual's right to an accounting of Disclosures subject to the statement; and (3) limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is submitted during that time.

If, during the period covered by the accounting, the Provider has made Disclosures of PHI for a particular research purpose in accordance with 45 C.F.R. §164.512(i) for 50 or more individuals, the accounting may provide certain information. The Privacy Official shall contact the Provider's legal counsel or ensure compliance with 45 C.F.R. §164.528(b)(4) prior to making an accounting of any such Disclosures.

If, during the period covered by the accounting, the Provider has made multiple Disclosures of PHI to the same person or entity for a single purpose of (1) demonstrating the Provider's compliance with the HIPAA privacy rules upon a request from the Secretary; or (2) a Disclosure under "Permissive Disclosures of PHI: for Legal and Public Policy Purposes", then the accounting may, with respect to such multiple disclosures, provide: (1) the date of the Disclosure, the name of the receiving party (and, if known, the address of the receiving party), a brief description of the PHI Disclosed, and a brief statement of the purpose of the Disclosure that reasonably informs the individual of the basis for the Disclosure (or a copy of the written request for Disclosure, if any); (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.

C. Request for Alternative Communication Means or Locations

Individuals may request, in writing, to receive communications regarding their PHI from the Provider by alternative means or at alternative locations. For example, individuals may ask to be called only at work rather than at home. Such requests may be accommodated, if in the sole discretion of the Provider, the requests are determined to be reasonable. The Privacy Official has responsibility for administering requests for confidential communications.

D. Request for Restrictions on Uses and Disclosures of Protected Health Information

An individual may request that the Provider restrict:

1. Uses or Disclosure of the individual's PHI to carryout Treatment, Payment, or Health Care Operations;
2. Disclosures to a family member, other relative, or a close personal friend of the individual, or another person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care in accordance with 45 C.F.R. §164.510(b)(2), (b)(3), or (b)(5);
3. Uses or Disclosures to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death in accordance with 45 C.F.R.

§164.510(b)(2), (b)(3), (b)(4), or (b)(5); and

4. Uses or Disclosures of PHI to a public or private entity authorized by law or its charter to assist in disaster relief efforts for the purpose of coordinating with such entities the Uses or Disclosures permitted by paragraph (3) above.

It is the Provider's policy to attempt to honor such requests if, in the sole discretion of the Provider, the requests are reasonable. The Privacy Official is charged with responsibility for administering requests for restrictions and is generally not required to agree to a restriction. However, the Provider must agree to the request of an individual to restrict Disclosure of PHI about the individual to a health plan if: (A) the Disclosure is for the purpose of carrying out Payment or Health Care Operations and is not otherwise required by law; and (b) the PHI 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 the covered entity in full (a "Required Restriction").

If the Provider agrees to a restriction, it may not Use or Disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment, the Provider may Use the restricted PHI, or may Disclose such information to a health care provider, to provide such treatment to the individual. However, if the restriction is Disclosed to a health care provider for emergency treatment, the Provider shall request that such health care provider not further Use or Disclose the information.

A restriction agreed to by the Provider is not effective to prevent Uses and/or Disclosures: related to an investigation by the Department of Health and Human Services to determine the Provider's compliance with HIPAA; required by law; for public health activities; related to victims of abuse; neglect or domestic violence; related to health oversight activities; related to judicial and administrative proceedings; related to law enforcement purposes; about decedents; for organ donations; for research purposes; to avert a serious threat to health or safety; for specialized government functions; and for workers compensation. The Employee shall contact the Privacy Official prior to Using or making any Disclosures on restricted PHI related to these subjects.

The Provider may terminate a restriction 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) the Provider informs the individual that it is terminating its agreement to a restriction, except that such termination is not effective for PHI restricted under a Required Restriction, and only effective with respect to PHI created or received after it has so informed the individual.

THIS SPACE IS INTENTIONALLY LEFT BLANK
PROCEDURES START ON THE NEXT PAGE

Procedures Preamble

This set of privacy procedures ("**Privacy Procedures**) is designed to specify the procedures required under HIPAA with respect to Uses and Disclosure of PHI of the Hillsdale College Health and Wellness Center ("**Provider**").

No third party rights, including but not limited to rights of Business Associates, are intended to be created by these Privacy Procedures. To the extent these Privacy Procedures attempt to establish requirements and obligations above and beyond those required by HIPAA, these Privacy Procedures shall be aspirational and shall not be binding upon the Provider. These Privacy Procedures do not address requirements under other federal laws or under state laws. Nothing within these Privacy Procedures should be construed as a contract and no vested rights are created by these Privacy Procedures.

The Provider reserves the right to amend, change or terminate these Privacy Procedures at any time, either prospectively or retroactively, without notice. These Privacy Procedures will also change should it become necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of HIPAA.

HIPAA and the corresponding regulations restrict the Provider's ability to Use and Disclose PHI. It is the Provider's policy to comply fully with HIPAA's requirements. These Privacy Procedures are intended to fully comply with HIPAA. To that end, all Employees must comply with these Privacy Procedures. Any ambiguity within these Privacy Procedures should be construed in a manner that permits the Provider to comply with the requirements of HIPAA, and take advantage of any potential exemptions. These Privacy Procedures are designed to be implemented in conjunction with a comprehensive privacy policy which is contained within a separate document, and any ambiguities between the Provider's Privacy Policy and these Privacy Procedures should be harmonized consistent with the requirements of HIPAA.

I. Procedures for Use and Disclosure of PHI

A. Use and Disclosure In General

The Provider will Use and Disclose PHI only as permitted under HIPAA. The Provider is permitted to Use or Disclose PHI incident to a Use or Disclosure otherwise permitted by the HIPAA privacy rules, provided that the Provider only abides by the "minimum necessary" standard and reasonably safeguards PHI to limit incidental Uses or Disclosures made pursuant to an otherwise permitted or required Use or Disclosure.

B. Employees Must Comply With Provider's Policy and Procedures

All Employees must comply with these Privacy Procedures and the Provider's Privacy Policy.

C. Access to PHI Is Limited to Certain Employees

All of the Provider's functions, including creation and maintenance of its records, are carried out by Employees and by Business Associates of the Provider.

The Provider must identify Employees or classes of Employees, as appropriate, who need access to PHI to carry out their duties. For each such Employee or class of Employees, the Provider must identify the category or categories of PHI to which access is needed and any conditions appropriate to such access. The Provider must make reasonable efforts to limit the access of such Employees or classes of Employees to the category or categories of PHI to which access is needed and any conditions appropriate to such access.

Employees with this access may not Disclose PHI to Employees without the same access unless an authorization is in place or the Disclosure otherwise is in compliance with these Privacy Procedures and the Provider's Privacy Policy. The Provider will from time to time designate one or more persons as the Privacy Official ("**Privacy Official**") who will have the duties and powers listed within the Provider's Privacy Policy. If any questions arise as to the interpretation or implementation of these Privacy Procedures, the Privacy Official shall have the authority to interpret the language of these Privacy Procedures and determine the proper implementation of these Privacy Procedures.

D. Permitted Uses and Disclosures of PHI

Uses and Disclosures for Payment, Treatment, or Health Care Operations. Except with respect to Uses and Disclosures that require an authorization under 45 C.F.R. §164.508(a)(2) through (4) (related to psychotherapy notes, Marketing, and the sale of PHI), or that are prohibited under 45 C.F.R §164.502(a)(5)(i) (related to the prohibition against Using or Disclosing PHI that is Genetic Information for underwriting purposes), the Provider may Use or Disclose PHI for Treatment, Payment, or Health Care Operations as set forth in this procedure, provided that such Use or Disclosure is consistent with other applicable requirements of the privacy rules.

- *Uses and Disclosures for Provider's Own Treatment Activities, Payment Activities, or Health Care Operations*. An Employee may Use or Disclose an individual's PHI to perform the Provider's own Treatment activities, Payment activities, or Health Care Operations.

    - Disclosures must comply with the "Minimum-Necessary" Standard.

    - If the Disclosure is not recurring, the Disclosure must be approved by the Privacy Official.

- *Disclosures for Another Entity's Payment Activities*. An Employee may Disclose PHI to another covered entity or health care provider for the Payment activities of the entity that receives the information. Disclosures may be made under the following procedures:

    - Disclosures must comply with the "Minimum-Necessary" Standard.

    - If the Disclosure is not recurring, the Disclosure must be approved by the Privacy Official.

- *Disclosures for a Health Care Provider's Treatment Activities.* An Employee may Disclose PHI to a health care provider for the Treatment activities of the health care provider.

    - If the Disclosure is not recurring, the Disclosure must be approved by the Privacy Official.

- *Disclosures for Certain Health Care Operations of the Receiving Entity*. An Employee may Disclose PHI to another covered entity for Health Care Operations activities of the entity that receives the information, if each entity has or had a relationship with the individual who is the subject of the PHI being requested, the PHI pertains to such relationship, and the Disclosure is for the purpose of (1) conducting quality assessment and improvement activities (including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalized knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. §3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting 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 professional, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learned under

supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; or (3) health care fraud and abuse detection or compliance. Such Disclosures are subject to the following:

- The Disclosure must be approved by the Privacy Official.
- Disclosures must comply with the "Minimum-Necessary" Standard.

- *Disclosures to Organized Health Care Arrangement.* If the Provider participates in an organized health care arrangement, it may Disclose PHI about an individual to other participants in the organized health care arrangement for any Health Care Operations activities of the organized health care arrangement. Such Disclosures are subject to the following:

  - The Disclosure must be approved by the Privacy Official.
  - Disclosures must comply with the "Minimum-Necessary" Standard.

E. Mandatory Disclosures of PHI: to Individuals and Department of Health and Human Services

- *Request From Individual*. Upon receiving a request from an individual (or an individual's representative) for Disclosure of the individual's own PHI, the Employee must follow the procedure for "Individual's Right for Access".

- *Request from DHHS*. Upon receiving a request from a Department of Health and Human Services official for Disclosure of PHI to investigate or determine the Provider's compliance with HIPAA, the Employee must take the following steps:

  - Follow the procedures for verifying the identity of a public official set forth in "Verification of Identity of Those Requesting Protected Health Information."
  - Disclosures must be documented in accordance with the procedure for "Documentation."

F. Permissive Uses and Disclosures of PHI: As Required By Law for Legal and Public Policy Purposes

Procedure

- *Uses and Disclosures for Legal or Public Policy Purposes*. The Provider may Use or Disclose PHI without a written authorization of the individual, or the opportunity for the individual to agree or object if such Use or Disclosure falls within one of the categories described below under "Legal and Public Policy Uses and Disclosures Covered." An Employee who receives a request for a Use or Disclosure of an individual's PHI that appears to fall within one of the categories described below under "Legal and Public Policy Uses and Disclosures Covered" must contact the Privacy Official. Uses and Disclosures may be made under the following procedures:

  - The Use or Disclosure must be approved by the Privacy Official.
  - The Use or Disclosure must comply with the "Minimum-Necessary" Standard, except for Uses and Disclosures required by law.

- The Use or Disclosure must be documented in accordance with the procedure for "Documentation", unless otherwise provided below.

Legal and Public Policy Uses and Disclosures Covered

- *Uses and Disclosures required by law.* The Provider may Use or Disclose PHI to the extent that such Use or Disclosure is required by law and the Use or Disclosure complies with and is limited to the relevant requirements of such law.

- *Disclosures about victims of abuse, neglect or domestic violence*. Except for reports of child abuse or neglect, as addressed below, the Provider may Disclose PHI about an individual whom the Provider reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority, including a social service or protective services agency, authorized by law to receive reports of such abuse, neglect, or domestic violence:

    - To the extent the Disclosure is required by law and the Disclosure complies with and is limited to the relevant requirements of such law;

    - If the individual agrees to the Disclosure; or

    - To the extent the Disclosure is expressly authorized by statute or regulation and (1) the Provider, in the exercise of professional judgment, believes the Disclosure is necessary to prevent serious harm to the individual or other potential victims; or (2) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PHI for which the Disclosure is sought is not intended to be used against the individual and that 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.

    - If the Provider makes a Disclosure as permitted in this *Disclosures about victims of abuse, neglect or domestic violence* section, the Provider must promptly inform the individual that such a report has been or will be made, unless (1) the Provider, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or (2) the Provider would be informing a personal representative, and the Provider reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the individual as determined by the Provider, in the exercise of professional judgment. An Employee shall get approval from the Privacy Official prior to informing (or not informing) an individual.

- *For Judicial and Administrative Proceedings.* The Provider may Disclose PHI in the course of any judicial or administrative proceeding:

    - In response to an order of a court or administrative tribunal, provided that the Provider Discloses only the PHI expressly authorized by such order; or

    - In response to a subpoena, discovery request or other lawful process, not accompanied by a court or administrative tribunal order if the Provider receives satisfactory assurance from the party seeking the information that reasonable efforts have been made by such party to (1) ensure that the individual who is the subject of the PHI that has been requested has been given notice of the request; or (2) secure a qualified protective order. An Employee shall

contact the Privacy Official to determine whether the satisfactory assurances required have been obtained.

- *To a Law Enforcement Official for Law Enforcement Purposes.* The Provider may Disclose PHI for a law enforcement purpose to a law enforcement official under the following conditions:

  - Pursuant to a process and as otherwise required by law, but only (1) as required by law; (2) in compliance with and as limited by the relevant requirements of (a) a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer; (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 practicable in light of the purpose for which the information is sought, and (iii) it is not reasonably possible to Use De-identified Information.

  - In response to a law enforcement official's request for PHI for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. Such Disclosure must be limited to (1) name and address; (2) date and place of birth; (3) social security number; (4) ABO blood type and rh factor; (5) type of injury; (6) date and time of treatment; (7) date and time of death, if applicable; and (8) 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. Except as expressly permitted by HIPAA, the Provider may not Disclose for the purposes of identification or location any PHI related to an individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

  - In response to a law enforcement official's request for PHI about an individual who is or is suspected to be a victim of a crime if: (1) the individual agrees to Disclosure; or (2) if the Provider is unable to obtain the individual's agreement because of incapacity or other emergency circumstances and (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 upon 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 interest of the individual as determined by the Provider, in the exercise of professional judgment.

  - About a deceased individual to a law enforcement official for the purpose of alerting the law enforcement of the death of the individual if the Provider has suspicion that the individual's death may have resulted from criminal conduct.

  - Information to a law enforcement official that the Provider believes in good faith constitutes evidence of criminal conduct that occurred on the Provider's premises.

  - If providing emergency health care in response to a medical emergency, other than such emergency on the premises of the Provider, 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 such crime. If the Provider believes that the medical emergency described in the previous sentence is the result of abuse, neglect, or domestic violence of the

individual in need of emergency health care, the previous sentence does not apply and any Disclosure to a law enforcement official for law enforcement purposes is subject to the *Disclosures about victims of abuse, neglect or domestic violence* section above.

- *To Appropriate Public Health Authorities for Public Health Activities.* The Provider may Use or Disclose PHI for public health activities for certain purposes to (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, 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 a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority; (2) a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect; (3) a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to an FDA-regulated product or activity for which that person has responsibility, for the purpose of activities related to the quality, safety or effectiveness of such FDA-related product or activity (such as collecting or reporting adverse events, product defects or problems, or biological product deviations; tracking FDA-regulated products; enabling product recalls, repairs, or replacement, or lookback; or conducting post marketing surveillance); (4) 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 the Provider or public health authority is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation; (5) an employer, about an individual who is a member of the workforce of the employer, if (a) the Provider is a covered health care provider who provides health care to the individual at the request of the employer to conduct an evaluation relating to medical surveillance of the workplace, or to evaluate whether the individual has a work-related illness or injury; (b) the PHI that is Disclosed consists of findings concerning a work-related medical surveillance; (c) the employer needs such findings in order to comply with its obligations, under 29 CFR parts 1904 through 1928, 30 CFR parts 50 through 90, or under state law having a similar purpose, to record such illness or injury or to carry out responsibilities for work-place medical surveillance; and (d) the Provider provides written notice to the individual that PHI relating to the medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer by giving a copy of the notice to the individual at the time the health care is provided, or if the health care is provided on the work site of the employer, by posting the notice in a prominent place at the location where the health care is provided; and (6) a school, about an individual who is a student or prospective student of the school, if: (a) the PHI that is Disclosed is limited to proof of immunization; (b) the school is required by state or other law to have such proof of immunization prior to admitting the individual; and (c) the Provider obtains and documents the agreement to the Disclosure from either: (i) a parent, guardian, or other person acting in loco parentis of the individual, if the individual is an unemancipated minor, or (ii) the individual, if the individual is an adult or emancipated minor.

- *To a Health Oversight Agency for Health Oversight Activities.* The Provider may Disclose PHI to a health oversight agency for oversight activities authorized by law, including audits; civil, administrative, or criminal investigations; inspections; licensure or disciplinary actions; civil, administrative, or criminal proceedings or 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. 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. Nonetheless, 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.

- *To a Coroner or Medical Examiner and Funeral Directors About Decedents.* The Provider may Disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining the cause of death or other duties as authorized by law. The Provider may Disclose PHI to funeral directors, consistent with applicable law, as necessary to carry out their duties. If necessary for funeral directors to carry out their duties, the Provider may Disclose the PHI prior to, and in reasonable anticipation of, the individual's death.

- *For Cadaveric Organ, Eye or Tissue Donation Purposes.* The Provider may Use or Disclose PHI to organ procurement organizations or other entities engaged in the procurement, banking or transplantation of cadaveric organs, eyes or tissue for the purpose of facilitating organ, eye or tissue donation and transplantation.

- *For Certain Limited Research Purposes.* The Provider may Use or Disclose PHI for research regardless of the source of funding of the research, provided that (1) a waiver of the authorization required by HIPAA which includes certain requirements and contains certain information required by HIPAA has been approved by an appropriate institutional review or privacy board; (2) the Provider receives certain representations and information required by HIPAA from the researcher; (3) the Provider otherwise complies with the applicable requirements of 45 C.F.R. §164.512(i). The Employee shall contact the Privacy Official for approval of any Uses or Disclosures made for research purposes.

- *To Avert a Serious Threat to Health or Safety.* The Provider may, consistent with applicable law and standards of ethical conduct, Use or Disclose PHI, if the Provider, 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 is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or (2) is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the Provider reasonably believes may have caused serious physical harm to the victim, or where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody. A Disclosure which is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the Provider reasonably believes may have caused serious physical harm to the victim shall be strictly limited as required by the HIPAA privacy rules by the Privacy Official. A Use or Disclosure which is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by an individual admitting participation in a violent crime that the Provider reasonably believes may have caused serious physical harm to the victim may not be made if the information is learned by the Provider (1) in the course of treatment to affect the propensity to commit the criminal conduct that is the basis for the Disclosure, or counseling or therapy; or (2) through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.

- *For Specialized Government Functions.* The Provider may Use and Disclose PHI of individuals who are armed forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission if certain requirements are met. The Provider may Use and Disclose the PHI of individuals who are foreign military personnel to their appropriate military authority if certain requirements are met. The Provider may also Use or Disclose PHI to authorized federal officials for the conduct of (1) certain national security, intelligence, and counter-intelligence activities; (2) protective services to the President of the United States, other officials and foreign heads of state; and (3) correctional institutional and other law enforcement custodial situations. An Employee shall contact the Privacy Official for further information prior to Using or Disclosing PHI for these purposes. A Disclosure

made for certain national security and intelligence activities or to correctional institutional and other law enforcement custodial situations does not need to be documented in accordance with the procedure for "Documentation."

- *For Workers' Compensation Programs.* The Provider may Disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault.

G. Disclosures of PHI Pursuant to an Authorization

Disclosure Pursuant to Individual Authorization. Except as otherwise permitted or required by HIPAA, the Provider may not Use or Disclose PHI without a valid authorization. Any requested Disclosure to a third party (i.e., not the individual to whom the PHI pertains) that does not fall within one of the categories for which Disclosure is permitted or required under these Privacy Procedures may be made pursuant to an individual authorization. If a Use or Disclosure pursuant to an authorization is requested, the following procedures should be followed:

- Follow the procedures for verifying the identity of the individual (or individual's representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Verify that the authorization form is valid. Valid authorization forms are those that are written in plain language and contain at least the following elements:

    - Are properly signed and dated by the individual or the individual's representative. If the authorization is signed by a personal representative of the individual, a description of such representative's authority to act for the individual must also be provided;

    - An expiration date or an expiration event that relates to the individual or the purpose of the Use or Disclosure. The expiration date of the authorization form must be a specific date (such as July 1, 2003) or a specific time period (e.g., one year from the date of signature), or an event directly relevant to the individual or the purpose of the Use or Disclosure (e.g., for the duration of the individual's treatment). The statement "end of the research study," "none," or similar language is sufficient if the authorization is for a Use or Disclosure of PHI for research, including the creation and maintenance of a research database or research repository;

    - A description of the information to be Used or Disclosed that identifies the information in a specific and meaningful fashion;

    - The name or other specific identification of the person(s), or class of persons, authorized to make the requested Use or Disclosure;

    - The name or other specific identification of the person(s), or class of persons, to whom the Provider may make the requested Use or Disclosure;

    - 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;

- Contain a statement regarding the individual's right to revoke the authorization in writing (including any exceptions to the right to revoke) and a description of how the individual may revoke the authorization;

- Contain a statement indicating that (1) the Provider may not condition Treatment, Payment, or enrollment or eligibility for benefits on whether the individual signs the authorization; or (2) the consequences to the individual of a refusal to sign an authorization when the Provider can condition Treatment, enrollment in the health plan, or eligibility for benefits on failure to obtain such authorization;

- Contain a statement regarding the possibility for a subsequent re-Disclosure by the recipient of the information Disclosed pursuant to the authorization; and

- If the authorization is related to a Use or Disclosure of PHI for Marketing, and if the Marketing involves Financial Remuneration to the Provider from a third party, the authorization must state that such remuneration is involved.

- If the authorization is for any Disclosure of PHI which is a sale of PHI, the authorization must state that the Disclosure will result in remuneration to the Provider. Contact the Privacy Official upon receipt of any authorization related to the sale of PHI.

- Verify that the authorization is not defective. An authorization is invalid, if the document submitted has any of the following defects:

    - The expiration date has passed or the expiration event is known by the Provider to have occurred.

    - The authorization has not been filled out completely, with respect to an element described above, if applicable.

    - The authorization is known by the Provider to have been revoked.

    - The authorization violates the HIPAA privacy rules related to compound authorizations. An authorization for Use or Disclosure of PHI may not be combined with any other document to create a compound authorization except under limited circumstances, as authorized under 45 C.F.R. §164.508(b)(3). Contact the Privacy Official prior to approving a compound authorization.

    - The authorization violates the HIPAA privacy rules related to the prohibition on the conditioning of authorizations, if applicable. The Provider may not condition the provision to an individual of Treatment, Payment, enrollment in the health plan, or eligibility for benefits on the provision of an authorization, except under limited circumstances, as set forth in 45 C.F.R. §164.508(b)(4). Contact the Privacy Official prior to approving an authorization with such conditional language.

    - Any material information in the authorization is known by the Provider to be false.

- All Uses and Disclosures made pursuant to a valid authorization must be consistent with the terms and conditions of the authorization. Verify that all Uses and Disclosures made pursuant to the valid authorization are consistent with the terms and conditions of the authorization.

- Provide the individual with a copy of the signed authorization.

- All signed authorizations, and revocations of valid authorizations must be documented in accordance with the procedure for "Documentation."

H. Disclosure of PHI to Business Associates

Use and Disclosure of PHI by Business Associate. The Provider may Disclose PHI to a Business Associate and may allow a Business Associate to create, receive, maintain, or transmit PHI on its behalf, if the Provider obtains satisfactory assurance that the Business Associate will appropriately safeguard the information. However, the Provider is not required to obtain such satisfactory assurances from a Business Associate that is a Subcontractor. All Uses and Disclosures by a Business Associate must be made in accordance with a valid Business Associate agreement (except with respect to Subcontractors). Before providing PHI to a Business Associate, Employees must contact the Privacy Official and verify that a Business Associate contract, which meets the applicable requirements of HIPAA, is in place. Before providing PHI to a Business Associate that is a Subcontractor, Employees must contact the Privacy Official to ensure all appropriate Business Associate contracts between the Provider's Business Associate and Subcontractor are in place. The following additional procedures must be satisfied:

- Disclosures must be consistent with the terms of the Business Associate contract.

- Disclosures must comply with the "Minimum-Necessary" Standard.

- Each non-recurring Disclosure must be approved by the Privacy Official.

- Disclosures must be documented in accordance with the procedure for "Documentation."

Notification of Breach of Unsecured PHI by Business Associate. The Business Associate contract must require a Business Associate that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, Uses, or Discloses Unsecured PHI to notify the Provider of a Breach of Unsecured PHI following the discovery of a Breach of Unsecured PHI. A Breach shall be treated as discovered by a Business Associate as of the first day on which such Breach is known to such Business Associate or, by exercising reasonable diligence, would have been known to the Business Associate. A Business Associate shall be deemed to have knowledge of a Breach if the Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is an employee, officer, or other agent of the Business Associate (determined in accordance with the federal common law of agency). Notification shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a Breach by the Business Associate involved. The notification by a Business Associate must include the following:

- Identification of each individual whose Unsecured PHI information has been, or is reasonably believed by the Business Associate to have been, accessed, acquired, Used, or Disclosed during the Breach

- A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

- A description of the types of Unsecured PHI 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).

- Any steps individuals should take to protect themselves from potential harm resulting from the

Breach.

- A brief description of what the Business Associate is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches.

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

- Any other available information that the Provider is required to include in its notification to the individual.

- Exception. If a law enforcement official states to the Provider or a Business Associate that a notification, notice, or posting required by the Breach Notification Rules would impede a criminal investigation or cause damage to national security, the Provider or Business Associate shall:

  - If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice or posting for the time period specified by the official; or

  - If the statement is made orally, document the statement, including the identity of the official making the statement, and delay notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during this time.

- Breaches and notifications of Breaches must be documented in accordance with the procedure for "Documentation."

I. Requests for Disclosure of PHI From Spouses, Family Members, and Friends

The Provider will not Disclose PHI to family and friends of an individual except as required or permitted by HIPAA. Generally, an authorization is required before another party, including spouse, family member or friend, will be able to access an individual's PHI.

- If an Employee receives a request for Disclosure of an individual's PHI from a spouse, family member, or personal friend of an individual, and the spouse, family member, or personal friend is either: (1) the parent of the individual and the individual is an unemancipated minor child; or (2) the personal representative of the individual, then follow the procedure for "Verification of Identity of Those Requesting Protected Health Information."

- Once the identity of a parent or personal representative is verified, then follow the procedure for "Individual's Request for Access."

- All other requests from spouses, family members, and friends must be authorized by the individual whose PHI is involved either pursuant to a valid authorization (see the procedures for "Disclosures of PHI Pursuant to Individual Authorization") or in accordance with the following paragraph.

The Provider may Disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual, the PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. The Provider may Use or Disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the individual, or another person responsible for the care of the individual of the individual's location, general condition, or death. Such Uses and Disclosures must be in accordance with the following, as applicable: (1) If the individual is present for, or otherwise available prior to a Use or

Disclosure permitted by this paragraph and has the capacity to make health care decisions, the Provider may Use or Disclose the PHI if it (a) obtains the individual's agreement, (b) provides the individual with the opportunity to object to the Disclosure, and the individual does not express an objection, or (c) reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the Disclosure; (2) If the individual is not present, or the opportunity to agree or object to the Use or Disclosure cannot practicably be provided because of the individual's incapacity or an emergency circumstance, the Provider may, in the exercise of professional judgment, determine whether the Disclosure is in the best interests of the individual and, if so, Disclose only the PHI that is directly relevant to the person's involvement with the individual's care or payment related to the individual's health care or needed for notification purposes; (3) The Provider may Use or Disclose PHI to a public or privacy entity authorized by law or by its charter to assist in disaster relief efforts to make certain notification of the individual's location, general condition, or death; or (4) If the individual is deceased, the Provider may Disclose to a family member, other relative, or a close personal friend of the individual, or any other person identified by the individual who were involved in the individual's care or payment for health care prior to the individual's death, PHI of the individual that is relevant to such person's involvement, unless doing so is inconsistent with any prior expressed preference of the individual that is known to the Provider.

J. Disclosures of De-Identified Information

- Obtain approval from Privacy Official for the Disclosure. The Privacy Official will verify that the information is de-identified.

- The Provider may freely Use and Disclose De-identified Information. De-identified Information is not PHI.

K. Verification of Identity of Those Requesting Protected Health Information.

In General. Except for certain Disclosures related to an involvement with an individual's care and certain notification purposes, prior to any Disclosure permitted by these Privacy Procedures and the Provider's Privacy Policy, the Provider must (1) verify the identity of a person requesting PHI and the authority of any such person to have access to PHI, if the identity of any such authority of such person is not known to the Provider; and (2) obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of the Disclosure under the HIPAA privacy rules. If a Disclosure is conditioned by the HIPAA privacy rules on particular documentation, statements, or representations from the person requesting the PHI, the Provider may rely, if such reliance is reasonable under the circumstances, on documentation, statements or representations that, on their face, meet the applicable requirements. With respect to Disclosures permitted by law pursuant to an administrative request, the administrative subpoena or similar process or by a written statement that, on its face, demonstrates that the applicable requirements have been met. With respect to certain Disclosures related to research purposes, the Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with the privacy rules (including 45 C.F.R. §164.512(i), §164.514, and §164.524(a)(2)(iii)) to determine whether the verification requirements have been met.

Verifying Identity and Authority of Requesting Party. Employees must take steps to verify the identity of individuals who request access to PHI. They must also verify the authority of any person to have access to PHI, if the identity or authority of such person is not known. Separate procedures are set forth below for verifying the identity and authority, depending on whether the request is made by the individual, a parent seeking access to the PHI of his or her unemancipated minor child, a personal representative, or a public official seeking access.

- *Request Made by Individual.* When an individual requests access to his or her own PHI, the following steps should be followed:

    - Request a form of identification from the individual. Employees may rely on a valid driver's license, passport or other photo identification issued by a government agency.

    - Verify that the identification matches the identity of the individual requesting access to the PHI. If you have any doubts as to the validity or authenticity of the identification provided or the identity of the individual requesting access to the PHI, contact the Privacy Official.

    - Make a copy of the identification provided by the individual and file it with the individual's Designated Record Set.

    - If the individual requests PHI over the telephone, the Employee must verify the identity of the individual from at least three identifying sources (e.g., social security number, employee number, address, home telephone number, etc).

- *Request Made by Parent Seeking PHI of Unemancipated Minor Child.* When a parent requests access to the PHI of the parent's unemancipated minor child, the following steps should be followed:

    - Seek verification of the person's relationship with the child. Such verification may take the form of confirming enrollment of the child in the parent's plan as a dependent. If relevant state law forbids access, then access will not be permitted. Contact with Privacy Official upon any request by a parent for access to the PHI of the parent's emancipated minor child.

    - If under applicable law a parent, guardian, or other person acting in loco parentis has authority to act on behalf of an individual who is an unemancipated minor in making decision related to health care, the Provider must treat such person as a personal representative under the HIPAA privacy rules, with respect to PHI relevant to such personal representation, except that such person may not be a personal representative of an unemancipated minor, and the minor has the authority to act as an individual, with respect to PHI pertaining to a health care service if: (1) the minor consents to such health care service; no other consent to such health care service is required by 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; (2) 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 (3) a parent guardian, or other person acting in loco parentis assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

      Notwithstanding the previous paragraph: (1) If, and to the extent, permitted or required by an applicable provision of state or other law, including applicable case law, the Provider may Disclose, or provide access in accordance with 45 C.F.R. §164.524 to, PHI about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; (2) If, and to the extent, prohibited by an applicable provision of state or other law, including applicable case law, the Provider may not Disclose, or provide access in accordance with 45 C.F.R. §524 to, PHI about an unemancipated minor to a parent, guardian, or other person acting in loco parentis; and (3) Where the parent, guardian, or other person acting in loco parentis, is not the personal representative and where there is no applicable access provision under state or other law, including case law, the Provider may provide or deny access under 45 C.F.R.

§164.524 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.

Contact the Privacy Official if a parent requests access to an unemancipated minor child's PHI in any of these situations.

- *Request Made by Personal Representative.* When a personal representative requests access to an individual's PHI, the following steps should be followed:

  - Require a copy of a valid health care power of attorney or other documentation establishing that the person is the personal representative of the individual. If there are any questions about the validity of the document, seek review by the Privacy Official.

  - Make a copy of the documentation provided and file it with the individual's Designated Record Set.

  - Notwithstanding a state law or other requirement under HIPAA, the Provider may elect not to treat a person as the personal representative of an individual if: (1) the Provider 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 such person as the personal representative could endanger the individual; and (2) the Provider, 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. Contact the Privacy Official if you believe the Provider may need to exercise this right.

- *Request Made by Public Official.* If a public official (or person acting on behalf of a public official) requests access to PHI, and if the request is for one of the purposes set forth above in "Mandatory Disclosures of PHI: to Individuals and Department of Health and Human Services" or "Permissive Uses and Disclosures of PHI: As Required By Law for Legal and Public Policy Purposes", the following steps should be followed to verify the official's identity and authority:

  - If the request is made in person, request presentation of an agency identification badge, other official credentials, or other proof of government status. Make a copy of the identification provided and file it with the individual's Designated Record Set.

  - If the request is in writing, verify that the request is on the appropriate government letterhead;

  - If the request is made by a person purporting to act on behalf of a public official, request a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of 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.

  - Request a written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority. If the 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, contact the legal department of the Provider or retain outside counsel for additional guidance.

- Obtain approval for the Disclosure from the Privacy Official.

- When making certain Disclosures of PHI related an involvement with an individual's care and certain notification purposes, the Privacy Official shall exercise professional judgment in making such Disclosure to ensure compliance with the HIPAA privacy rules. When making certain Disclosures of PHI to avert a serious threat to health or safety, the Privacy Official shall only make a Disclosure based upon a good faith belief that Disclosure is in compliance with the HIPAA privacy rules.

- Disclosures must be documented in accordance with the procedure for "Documentation."

L. Complying With the "Minimum-Necessary" Standard

Procedures for Uses

- The Privacy Official (or an Employee at the Privacy Official's direction) shall create and maintain a file of Employees or classes of Employees who need access to PHI to carryout their duties, the categories of PHI to which access is needed, and any conditions appropriate to such access.

- Do not Use an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the Use.

Procedures for Disclosures

- Routine and Recurring Disclosures. The Privacy Official (or an Employee at the Privacy Official's direction) shall create and maintain a file of routine and recurring Disclosures which identifies the types of PHI to be Disclosed, the types of person who may receive the PHI, the conditions that would apply to such access, and the standards for Disclosure to routinely-hired types of Business Associates. The Privacy Official shall also create a policy for each specific recurring Disclosure that limits the PHI Disclosed to the amount reasonably necessary to achieve the purpose of the Disclosure.

- For all other requests for Disclosures of PHI, contact the Privacy Official, who will (1) ensure that the PHI Disclosed is limited to the information reasonably necessary to accomplish the purpose for which the Disclosure is sought, and (2) review the requests for Disclosure on an individual basis in accordance with such criteria.

- The Provider may rely, if such reliance is reasonable under the circumstances, on a requested Disclosure as the minimum necessary for the stated purpose when: (1) making Disclosures to public officials that are permitted under the HIPAA privacy rules, if the public official represents that the information requested is the minimum necessary for the stated purposes; (2) the information is requested by another covered entity; (3) the information is requested by a professional who is a member of its workforce or is a Business Associate of the Provider for the purpose of providing professional services to the Provider, if the professional represents that the information requested is the minimum necessary for the stated purposes; or (4) documentation or representations that comply with the applicable requirements of the HIPAA privacy rules have been provided by a person requesting the information for research purposes.

- Do not Disclose an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonably necessary to accomplish the purpose of the Disclosure.

Procedures for Requests

- Routine and Recurring Requests. The Privacy Official (or an Employee at the Privacy Official's direction) shall create and maintain a file of routine and recurring requests which identifies the information that is necessary for the purpose of the requested Disclosure and create a policy that limits the PHI requested to the amount reasonably necessary to accomplish the purpose for which the request is made.

- For all other requests for PHI, contact the Privacy Official, who will (1) ensure that the PHI requested is limited to the information reasonably necessary to accomplish the purpose for which the request is made and (2) review requests for Disclosure on an individual basis in accordance with such criteria.

- Do not request an entire medical record, except when the entire medical record is specifically justified as the amount that is reasonable necessary to accomplish the purpose of the request.

Exceptions

- The "minimum-necessary" standard does not apply to any of the following:

    - Disclosures to or requests by a health care provider for Treatment;
    - Uses or Disclosures made to the individual;
    - Uses or Disclosures made pursuant to a valid authorization;
    - Disclosures made to the Secretary;
    - Uses or Disclosures required by law; and
    - Uses or Disclosures required to comply with HIPAA.

Procedures for Limited Data Set Uses and Disclosures.

- Under limited circumstances, the Provider may Use or Disclose a Limited Data Set, if the Provider enters into a data use agreement with the Limited Data Set recipient. An Employee shall contact the Privacy Official prior to Using or Disclosing such information. The Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with 45 C.F.R. §164.514(e) prior to Using or Disclosing a Limited Data Set.

M. Documentation

Documentation. Employees shall maintain copies of all of the following items for a period of at least six years (unless state or federal law mandates a different time period) from the date the documents were created or were last in effect, whichever is later:

- "Notices of Privacy Practices" that are issued;

- Copies of policies and procedures;

- Individual authorizations;

- When Disclosures of certain PHI are made:

    - the date of the Disclosure;

- the name of the entity or persons who received the PHI and, if known, the address of such entity or person;
- a brief description of the PHI Disclosed;
- a brief statement of the purpose of the Disclosure;

- Breaches of Unsecured PHI and notices related to any such Breaches;

- All sanctions that are applied to Employees who fail to comply with these Privacy Procedures, the Provider's Privacy Policy, or the HIPAA privacy rules.

- All complaints received and the disposition thereof; and

- Any other documentation required under these Privacy Procedures, the Provider's Privacy Policy, or the HIPAA privacy rules.

Note: The retention requirement only applies to documentation required by HIPAA. It does not apply to all medical or business records. An Employee shall contact the Privacy Official if he or she has any questions regarding whether a document needs to be retained.

N. Mitigation of Inadvertent Disclosures of PHI

Mitigation: Reporting Required. HIPAA requires that the Provider mitigate, to the extent practicable, any harmful effects that become known to it of a Use or Disclosure of PHI in violation of these Privacy Procedures, the Provider's Privacy Policy, or the requirements of the HIPAA privacy rules. As a result, if you become aware of an unauthorized Use or Disclosure of PHI, either by an Employee of Provider or a Business Associate, immediately contact the Privacy Official or an officer of the Provider so that the appropriate steps to mitigate the harm to the individual can be taken.

O. Notification of Breach of Unsecured PHI

Individual Notice. The Provider, to the extent that it accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, Uses, or Discloses Unsecured PHI, shall, following the discovery of a Breach of Unsecured PHI, notify each individual whose Unsecured PHI has been, or is reasonably believed by the Provider to have been, accessed, acquired, Used, or Disclosed as a result of such Breach. A Breach shall be treated as discovered by the Provider as of the first day on which such Breach is known to the Provider, or by exercising reasonable diligence would have been known to the Provider. The Provider shall be deemed to have knowledge of a Breach if such Breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the Breach, who is a workforce member or agent of the Provider (determined in accordance with the federal common law of agency). Notification shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a Breach. Notice to an individual with respect to a Breach shall be provided promptly in the following form:

- Written notification by first-class mail to the individual (or the next of kin of the individual or personal representative if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if the individual agrees 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.

- In the case in which there is insufficient, or out-of-date contact information that precludes written (or electronic) notification to the individual, a substitute form of notice reasonably calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is

insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual.

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

- In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (1) be in the form of either a conspicuous posting for a period of 90 days on the home page of the website of the Provider involved, or 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 phone number that remains active for at least 90 days where an individual can learn whether the individual's Unsecured PHI may be included in the Breach.

- In any case deemed by the Provider to require urgency because of possible imminent misuse of Unsecured PHI, the Provider, in addition to notice provided above, may provide information to individuals by telephone or other means, as appropriate, in addition to the written (or electronic) notice.

- Regardless of the method by which notice is provided to individuals, notice of a Breach shall be written in plain language and include, to the extent possible, the following:

  - A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

  - A description of the types of Unsecured PHI 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).

  - Any steps individuals should take to protect themselves from potential harm resulting from the Breach.

  - A brief description of what the Provider is doing to investigate the Breach, to mitigate harm to the individuals, and to protect against any further Breaches.

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

Media Notice. Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a Breach if Unsecured PHI of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, Used, or Disclosed during such Breach. Notice shall be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a Breach. Notice of a Breach shall be written in plain language and include, to the extent possible, the following:

- A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known.

- A description of the types of Unsecured PHI 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).

- Any steps individuals should take to protect themselves from potential harm resulting from the Breach.

- A brief description of what the Provider is doing to investigate the Breach, to mitigate harm to individuals, and to protect against any further Breaches.

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

Secretary Notice. Notice shall, following the discovery of a Breach of Unsecured PHI be provided to the Secretary by the Provider. If the Breach was with respect to 500 or more individuals then such notice must be provided contemporaneously with the notice required to the individual and in the manner specified on the Department of Health and Human Services ("**HHS**") website. If the Breach was with respect to less than 500 individuals, the Provider shall maintain a log or other documentation of such Breaches and, not later than 60 days after the end of the calendar year, provide the notification for Breaches discovered during the preceding calendar year in the manner specified on the HHS website.

Exception. If a law enforcement official states to the Provider or a Business Associate that a notification, notice, or posting required under the Breach Notification Rules would impede a criminal investigation or cause damage to national security, the Provider or Business Associate shall:

- If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice or posting for the time period specified by the official; or
- If the statement is made orally, document the statement, including the identity of the official making the statement, and delay notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement is submitted during this time.

Documentation. Breaches and notifications of Breaches must be documented in accordance with the procedure for "Documentation."

P. Uses and Disclosures for Purposes of Marketing, Fundraising, the Sale of PHI, Psychotherapy Notes, and Facility Directories

Use or Disclosure for Purposes of Marketing. Except after consultation with the Provider's legal counsel or other assurance that the Provider is in compliance with 45 C.F.R. §164.508(a)(3), and unless an authorization from the individual (as discussed in "Disclosures of PHI Pursuant to an Authorization") has been received, the communication is made face-to-face by the Employee (on behalf of the Provider) to the individual, or the communication is in the form of a promotional gift of nominal value provided by the Provider, an Employee may not Use or Disclose PHI for Marketing. If the Marketing involves Financial Remuneration to the Provider from a third party, the authorization must state that such remuneration is involved.

- If an Employee receives a valid individual authorization (as discussed in "Disclosures of PHI Pursuant to an Authorization"), the following procedures must be followed prior to Using or Disclosing the individual's PHI for Marketing:

  - The Disclosure must be approved by the Privacy Official.

  - The Disclosure must comply with the "Minimum-Necessary" Standard.

- The Disclosure must be documented in accordance with the procedure for "Documentation."

- *Questions?* Any Employee who is unsure as to whether a task he or she is asked to perform is considered Marketing should contact the Privacy Official.

Use or Disclosure for Purposes of Fundraising. Under limited circumstances, the Provider may Use or Disclose certain PHI for fundraising purposes. If an Employee receives a request to Use or Disclose PHI for fundraising purposes, the Employee shall contact the Privacy Official. The Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with 45 C.F.R. §164.514(f) prior to Using or Disclosing any PHI for fundraising purposes.

- Any Disclosure must be documented in accordance with the procedure for "Documentation."

Sale of PHI. The Provider shall not sell PHI, except pursuant and in compliance with an authorization meeting the requirements of 45 C.F.R. §164.508(a)(4). If an Employee is requested to sell PHI, the Employee shall contact the Privacy Official. The Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with 45 C.F.R. §164.502(a)(5)(ii) and 45 C.F.R. §164.508(a)(4) prior to selling PHI under all circumstances.

- Any Disclosure (and the related authorization) must be documented in accordance with the procedure for "Documentation."

Psychotherapy Notes. The Provider must obtain an authorization for any Use or Disclosure of psychotherapy notes, except: (1) to carry out the following Treatment, Payment or Health Care Operations: (a) Use by the originator of the psychotherapy notes for Treatment, (b) Use or Disclosure by the Provider for 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 (c) Use or Disclosure by the Provider to defend itself in a legal action or other proceeding brought by the individual; and (2) a Use or Disclosure that is required by 45 C.F.R. §164.502(a)(2)(ii) (related to Disclosures required by the Secretary to investigate or determine the Provider's compliance with HIPAA) or permitted by 45 C.F.R. §164.512(a) (related to Uses and Disclosures required by law), 45 C.F.R. §164.512(d) (related to Uses and Disclosures for health oversight activities) with respect to the oversight of the originator of the psychotherapy notes), 45 C.F.R. §164.512(g)(1) (related to certain Disclosures about decedents to coroners and medical examiners), or 45 C.F.R. §164.512(j)(1)(i) (related to certain Uses and Disclosures necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public). If an Employee receives a request to Use or Disclose of psychotherapy notes, the Employee shall contact the Privacy Official. The Privacy Official shall contact the Provider's legal counsel or otherwise ensure compliance with 45 C.F.R. §164.508 prior to Using or Disclosing any psychotherapy notes.

- Any Disclosure (and the related authorization if required) must be documented in accordance with the procedure for "Documentation."

Use or Disclosure for Facility Directories. Except when an objection is expressed in accordance with this paragraph, the Provider may: (1) Use the following PHI to maintain a directory of individuals in its facility: the individual's name, the individual's location in the Provider's facility, the individual's condition described in general terms that does not communicate specific medical information about the individual, and the individual's religious affiliation; and (2) Use or Disclose for directory purposes such information: to members of the clergy, or, except for religious affiliation, to other persons who ask for the individual by name. The Provider must inform an individual of the PHI that it may include in a directory and the persons to whom it may Disclose such information (including Disclosures to clergy of information regarding religious affiliation) and provide the

individual with the opportunity to restrict or prohibit some or all of the Uses or Disclosures permitted by this paragraph. However, in certain emergency circumstances, if the opportunity to object to the Uses or Disclosures described above cannot practicably be provided because of the individual's incapacity or an emergency treatment circumstance, the Provider may Use or Disclose some or all of the PHI permitted above for the facility's directory, if such Disclosure is: (1) consistent with a prior expressed preference of the individual, if any, that is known to the Provider; and (2) in the individual's best interest as determined by the Provider, in the exercise of professional judgment. That being said, the Provider must inform the individual and provide an opportunity to object to Uses and Disclosures for directory purposes when it becomes practicable to do so.

- All evidence that an individual has been informed that certain of his or her PHI may be included in the facility directory, and/or of an individual's objection or restriction on such Use or Disclosure must be documented in accordance with the procedure for "Documentation."

II. Procedures for Complying With Individual Rights

Individual Rights: HIPAA generally gives individuals the right to access and obtain copies of PHI that the Provider or its Business Associates maintains in Designated Record Sets. HIPAA also generally provides that individuals may request to have their PHI amended, and that they are entitled to an accounting of certain types of Disclosures.

A. Individual's Request for Access

Request From Individual, Parent of Unemancipated Minor Child, or Personal Representative. Upon receiving a request from an individual (or from an unemancipated minor's parent or an individual's personal representative) for Disclosure of an individual's PHI, the Employee must take the following steps:

- Have the individual (or an unemancipated minor's parent or an individual's personal representative) submit a request in writing, unless such requirement is expressly waived by the Privacy Official.

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Review the Disclosure request to determine whether the PHI requested is held in the individual's Designated Record Set. See the Privacy Official if it appears that the requested information is not held in the individual's Designated Record Set. ***No request for access may be denied without approval from the Privacy Official.***

- Review the Disclosure request to determine whether an exception to the Disclosure requirement might exist; for example, Disclosure may be denied for requests to access psychotherapy notes, information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding, certain other limited clinical information, certain requests by inmates, certain information compiled during research when the individual has agreed to denial of access, certain information contained in records subject to the Privacy Act or obtained under a promise of confidentiality, and certain other Disclosures that are determined by a licensed health care professional to be reasonably likely to endanger the life or physical safety of the individual or another person or cause substantial harm to the individual or another person. See the Privacy Official if there is any question about whether one of these exceptions applies and 45 CFR §164.524 for full details regarding potential exceptions. ***No request for access may be denied without approval of the Privacy Official.***

- Respond to the request for access no later than 30 days after receipt of the request. If the Provider is unable to take an action (either granting or denying the request in whole or in part) within the 30 day period, the Provider may extend the time for such actions by no more than 30 days, provided that: (A) the Provider, within the 30 day period, provides the individual with a written statement of the reasons for the delay and the date by which the Provider will complete its action on the request; and (B) the Provider may have only one such extension of time for action on a request for access. If applicable, arrange with the individual for a convenient time and place to inspect or obtain a copy of the PHI, or mail the copy of the PHI at the individual's request. You 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 the Provider to transmit the copy of PHI directly to another person designated by the individual, the Provider must provide the copy to the person designated by the individual. The individual's request must be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of PHI.

- If the request for access is granted, in whole or in part, inform the individual of the acceptance of the request and provide the access requested, including inspection or obtaining a copy, or both, of the PHI about him or her in Designated Record Sets. If the same PHI that is the subject of a request for access is maintained in more than one Designated Record Set or at more than one location, you need only produce the PHI once in response to a request for access. Provide the individual with access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form and format as agreed to by the Provider and the individual. Notwithstanding the previous sentence of this paragraph, if the PHI that is the subject of a request for access is maintained in one or more Designated Record Sets electronically and if the individual requests an electronic copy of such information, the Provider must provide the individual with access to the PHI in the electronic form and format requested by the individual, if it is readily producible in such form and format; or, if not, in a readable electronic form and format as agreed to by the Provider and the individual.

- If the request is denied, in whole or in part, provide the individual with a written denial. To the extent possible, provide the individual access to any other PHI requested, after excluding the PHI as to which there is a ground to deny access to. The denial notice must be timely provided, be written in plain language and contain:

    - The basis for the denial;
    - a statement of the individual's right to request a review of the denial, including a description of how the individual may exercise such review rights, if applicable; and
    - a description (including the name, or title, and telephone number of the contact person or office designated) of how the individual may file a complaint concerning the denial to the Provider or the Secretary pursuant to the "Complaint Procedures" .

- If the Provider does not maintain the PHI that is the subject of the individual's request for access, but the Provider knows where the requested information is maintained, inform the individual where to direct his or her request for access. All notices of denial must be prepared or approved by the Privacy Official.

- If access is denied because it relates to Disclosures that are determined by a licensed health care professional to be reasonably likely to endanger the life or physical safety of the individual or another person to cause substantial harm to the individual or another person, the individual must be given the right to have such denial reviewed by a licensed health care professional who is designated by the Provider to act as a reviewing official and who did not participate in the original decision to

deny. Ensure that the designated reviewing official determines, within a reasonable period of time, whether or not to deny the access requested. Promptly provide written notice to the individual of the determination of the designated reviewing official and take other action as may be required to carryout the designated reviewing official's determination.

- Individuals (except for inmates) have the right to receive a copy by mail or by e-mail or can come in and pick up a copy. Individuals (including inmates) also have the right to come in and inspect the information.

- If the individual has requested a summary of the PHI requested, in lieu of providing, or in addition to, providing access to the PHI, prepare such summary of the information requested and make it available to the individual in the form or format requested by the individual. Advise the individual in advance of any fee that will be imposed for such summary and obtain the individual's consent to such fee.

  When copies of information are provided to an individual or the individual requests a summary, the Employee providing such information may collect a reasonable cost-based fee, provided that the fee includes only the cost of (i) labor for copying the PHI requested by the individual, whether in paper or electronic form; (ii) supplies for creating the paper copy or electronic media if the individual requests that the electronic copy be provided on portable media; (iii) postage, when the individual has requested the copy, or the summary or explanation, be mailed; and (iv) preparing an explanation or summary of PHI, if agreed to by the individual.

- The schedule of fees for providing copies of information shall be periodically set by the Privacy Official. Before fees may be collected for the preparation of a summary, the fees must be agreed to in advance by the individual. The Privacy Official shall have the discretion to expressly waive such fee under this section.

- Disclosures, Designated Record Sets that are subject to access by individuals, and the titles of the persons or offices responsible for receiving and processing requests for access by individuals must be documented in accordance with the procedure "Documentation."

B. Individual's Request for Amendment

Request From Individual, Parent of Unemancipated Minor Child, or Personal Representative. Upon receiving a written request from an individual (or an unemancipated minor's parent or an individual's personal representative) for amendment of an individual's PHI held in a Designated Record Set, the Employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- Review the request to determine whether the PHI or record that is subject to the request was created by the Provider, and if not, whether the individual making the request has provided a reasonable basis to believe that the originator of the PHI is no longer available on the requested amendment. See the Privacy Official if it appears that the requested information was not created by the Provider and if the individual making the request has not provided a reasonable basis to believe that the originator of the PHI is no longer available on the requested amendment. ***No request for amendment may be denied without approval from the Privacy Official***.

- Review the Disclosure requests to determine whether the PHI at issue is held in the individual's Designated Record Set. See the Privacy Official if it appears that the requested information is not held in the individual's Designated Record Set. ***No request for amendment may be denied without approval from the Privacy Official***.

- Review the request for amendment to determine whether the information would be accessible under HIPAA's right to access (see the access procedures above). See the Privacy Official if there is any question about whether the information is not subject to HIPAA's right to access. ***No request for amendment may be denied without approval from the Privacy Official***.

- Review the request for amendment to determine whether the amendment is appropriate - that is, determine whether the information in the Designated Record Set is accurate and complete without the amendment. See the Privacy Official if it appears that the Designated Record Set is accurate and complete without amendment. ***No request for amendment may be denied without approval from the Privacy Official***.

- Respond to the request no later than 60 days after receipt of the request by informing the individual in writing that the amendment will be made or that the request is denied. If the determination cannot be made within the 60-day period, the deadline may be extended once for no more than 30 days by providing a written statement to the individual within the original 60-day period setting forth the reasons for the delay and the date by which the Provider will complete its action on the request.

- When a requested amendment is accepted (in whole or in part), make the appropriate amendment to the PHI or record that is the subject of the request for amendment by, at a minimum, identifying the records in the Designated Record Set that are affected by the amendment and attaching or otherwise providing a link to the location of the amendment. Provide timely appropriate notice that the amendment is accepted to the individual and obtain the individual's identification of an agreement to have the Provider notify the relevant persons with which the amendment needs to be shared. Inform and provide the amendment within a reasonable time to: (1) persons identified by the individual as having received PHI about the individual and needing amendment; and (2) persons, including Business Associates, that the Provider knows has the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

- When an amendment request is denied (in whole or in part), the following procedures apply:

    - All notices of denial must be prepared or approved by the Privacy Official and be in plain language. A denial notice must contain (1) the basis for the denial; (2) information about the individual's right to submit a written statement disagreeing with the denial and how to file such a statement; (3) an explanation that the individual may (if he or she does not file a statement of disagreement) request that the Provider provide the individual's request for amendment and its denial be included in future Disclosures of the PHI that is the subject of the amendment; and (4) a description of how the individual may file a complaint concerning the denial to the Provider or the Secretary pursuant to the "Complaint Procedures" .

    - If, following the denial, the individual files a statement of disagreement, contact the Privacy Official to determine whether the Provider should prepare a written rebuttal to the individual's statement of disagreement. Prepare the written rebuttal, if applicable, and provide a copy of the rebuttal to the individual who submitted the statement of disagreement.

- Identify the record or PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment; the denial notice of the request; the individual's statement of disagreement, if any; and the Provider's rebuttal/response to such statement of disagreement, if any, to the Designated Record Set. If a statement of disagreement has been submitted by the individual, include the above materials with any subsequent Disclosure of the record to which the request for amendment relates. If the individual has not submitted a written statement of disagreement, include the individual's request for amendment and its denial with any subsequent Disclosure of the PHI only if the individual has requested such action. When a subsequent Disclosure is made using a standard transaction that does not permit the additional material to be included with the Disclosure, separately transmit the material, as applicable, to the recipient of the standard transaction.

- If the Provider is informed of an amendment to an individual's PHI by another covered entity, amend the PHI in the Designated Record Set in accordance with the procedures set forth above.

- The Provider must document the titles of persons or offices responsible for receiving and processing requests for amendments by individuals and retain the documentation in accordance with the procedures for "Documentation."

C. Processing Requests for an Accounting of Disclosures of Protected Health Information

Request From Individual, Parent of Unemancipated Minor Child, or Personal Representative. Upon receiving a request from an individual (or an unemancipated minor's parent or an individual's personal representative) for an accounting of Disclosures, the Employee must take the following steps:

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- The first accounting provided to an individual in any 12-month period shall be provided free of charge. If the individual requesting the accounting has already received one accounting within the 12-month period immediately preceding the date of receipt of the current request, the Employee shall be required to collect a reasonable cost-based fee from the individual to prepare the subsequent accounting. The schedule of fees for providing this type of accounting shall be periodically set by the Privacy Official. If a fee is required, the Provider shall notify the individual in advance of providing the accounting and provide the individual with an opportunity to withdraw or modify the request for an accounting in order to avoid or reduce the fee. The Privacy Official shall have the discretion to expressly waive such fee under this section.

- Respond to the request for an accounting no later than 60 days after receipt of such request by providing the accounting (as described in more detail below), or informing the individual that there have been no Disclosures that must be included in an accounting (see the list of exceptions to the accounting requirement below). If the accounting cannot be provided within the 60-day period, the deadline to provide the accounting may be extended once by no more than 30 days by providing a written statement to the individual within the original 60-day period which includes the reasons for the extension and the date by which the accounting will be provided.

- The accounting must include Disclosures (but not Uses) of the requesting individual's PHI made by the Provider and any of its Business Associates during the period requested by the individual up to

six years prior to the date of which the accounting is requested. The accounting will not include Disclosures that occurred before the compliance date of the HIPAA privacy rules as they directly related to the Provider. The accounting does not have to include Disclosures made:

- to carry out Treatment, Payment and Health Care Operations;
- to the individual about his or her own PHI;
- incident to an otherwise permitted Use or Disclosure under the HIPAA privacy rules;
- pursuant to an individual authorization;
- for the facility's directory or to persons involved in the individual's care or payment for the individual's care or for certain other notification purposes;
- for specific national security or intelligence purposes;
- to correctional institutions or law enforcement officials; and
- as part of a Limited Data Set.

- If any Business Associate of the Provider has the authority to Disclose the individual's PHI, then the Provider shall make reasonable efforts to contact the Business Associate to obtain an accounting of the Business Associate's Disclosures.

- The accounting must include the following information for each Disclosure of the individual's PHI:

  - the date of the Disclosure;
  - the name (and if known, the address) of the entity or person to whom the information was Disclosed;
  - a brief description of the PHI Disclosed; and
  - a brief statement explaining the purpose for the Disclosure that reasonably informs the individual of the basis for the Disclosure. The statement of purpose may be accomplished by providing a copy of the written request for Disclosure, when applicable.

- If the Provider has received a temporary suspension statement from a health oversight agency or a law enforcement official indicating that notice to the individual of Disclosures of PHI would be reasonably likely to impede the agency's activities, Disclosure may not be required. If an Employee received such a statement, either orally or in writing, the Employee must contact the Privacy Official for more guidance.

- If, during the period covered by the accounting, the Provider has made Disclosures of PHI for a particular research purpose in accordance with 45 C.F.R. §164.512(i) for 50 or more individuals, the accounting may provide certain information. The Privacy Official shall contact the Provider's legal counsel or ensure compliance with 45 C.F.R. §164.528(b)(4) prior to making an accounting of any such Disclosures.

- If, during the period covered by the accounting, the Provider has made multiple Disclosures of PHI to the same person or entity for a single purpose of (1) demonstrating the Provider's compliance with the HIPAA privacy rules upon a request from the Secretary; or (2) a Disclosure under "Permissive Disclosures of PHI: for Legal and Public Policy Purposes", then the accounting may, with respect to such multiple disclosures, provide: (1) the date of the Disclosure, the name of the receiving party (and, if known, the address of the receiving party), a brief description of the PHI Disclosed, and a brief statement of the purpose of the Disclosure that reasonably informs the individual of the basis for the Disclosure (or a copy of the written request for Disclosure, if any); (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. An Employee shall contact the Privacy Official

prior to providing an accounting with multiple Disclosures.

- Accountings must be documented in accordance with the procedure for "Documentation" and shall include
    - the information required to be included in an accounting for Disclosures of PHI that is subject to the accounting;
    - the written accounting that is provided to the individual; and
    - the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals.

D. Processing Requests for Confidential Communications

Request From Individual, Parent of Unemancipated Minor Child, or Personal Representative. Upon receiving a request from an individual (or an unemancipated minor's parent or an individual's personal representative) to receive communications of PHI from the Provider by alternative means or at alternative locations, the Employee must take the following steps:

- Have the individual (or an unemancipated minor's parent or an individual's personal representative) submit a request in writing, unless such requirement is expressly waived by the Privacy Official.
- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."
- Determine whether the request specifies an alternate address or other method of contact for the individual.
- The Employee will take preliminary steps to honor Disclosure requests, if they are reasonable. Such requests may be ultimately denied or terminated if the Privacy Official subsequently determines that such requests cannot be honored because they are unreasonable. The Privacy Official shall have the final authority to determine whether a request is reasonable and whether to grant or deny a request. The Privacy Official may condition the provision of a reasonable accommodation on: (1) when appropriate, information as to how payment, if any, will be handled; and (2) specifications of an alternative address or other method of contact. The Privacy Official may not require an explanation from the individual as to the basis for the request as a condition of providing communications on a confidential basis.
- If a request will not be accommodated, the Employee must contact the individual in person, in writing, or by telephone to explain why the request will not be accommodated.
- All confidential communication requests that are approved will be tracked and the Privacy Official (or an Employee at the Privacy Official's direction) shall create and maintain a file of confidential communication requests.
- Requests and their dispositions must be documented in accordance with the procedure for "Documentation."

E. Processing Requests for Restrictions on Uses and Disclosures of Protected Health Information

Request From Individual, Parent of Unemancipated Minor Child, or Personal Representative. Upon receiving a request from an individual (or an emancipated minor's parent or an individual's personal representative) for restrictions on access to an individual's PHI, the Employee must take the following steps:

- Have the individual (or an unemancipated minor's parent or an individual's personal representative) submit a request in writing, unless such requirement is expressly waived by the Privacy Official.

- Follow the procedures for verifying the identity of the individual (or parent or personal representative) set forth in "Verification of Identity of Those Requesting Protected Health Information."

- The Employee should take preliminary steps to honor requests that are reasonable. Such requests may be ultimately denied or terminated if the Privacy Official subsequently determines that such requests cannot be honored. The Privacy Official shall have the final authority to determine whether a request is reasonable.

- The Employee must agree to the request of an individual to restrict Disclosure of PHI about the individual to a health plan if: (A) the Disclosure is for the purpose of carrying out Payment or Health Care Operations and is not otherwise required by law; and (b) the PHI 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 the covered entity in full (a "Required Restriction").

- If a request will not be accommodated, the Employee must contact the individual in person, in writing, or by telephone to explain why the request cannot be accommodated.

- All requests for limitations on Use or Disclosure of PHI that are approved will be tracked and the Privacy Official (or an Employee at the Privacy Official's direction) shall create and maintain a file of agreed-to restriction requests.

- Once a restriction is agreed to, the Employee may not Use or Disclose PHI in violation of such restriction, except that, if the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency Treatment, the Provider may Use the restricted PHI, or may Disclose such information to a health care provider, to provide such Treatment to the individual. However, if the restriction is Disclosed to a health care provider for emergency Treatment, the Provider shall request that such health care provider not further Use or Disclose the information. The Employee must obtain consent from the Privacy Official prior to Using or Disclosing PHI in violation of any restriction.

- A restriction agreed to by the Provider is not effective to prevent Uses and/or Disclosures: related to an investigation by the Department of Health and Human Services to determine the Provider's compliance with HIPAA; required by law; for public health activities; related to victims of abuse; neglect or domestic violence; related to health oversight activities; related to judicial and administrative proceedings; related to law enforcement purposes; about decedents; for organ donations; for research purposes; to avert a serious threat to health or safety; for specialized government functions; and for workers compensation. The Employee shall contact the Privacy Official prior to Using or making any Disclosures on restricted PHI related to these subjects. The Employee shall contact the Privacy Official prior to making any Disclosures on restricted PHI related to these subjects.

- All Business Associates that may have access to the individual's PHI must be notified of any agreed-to restrictions. The Provider shall make reasonable efforts to identify and notify the Business Associate that apply to an specific agreed-to restriction request.

- An Employee shall terminate a restriction (1) if 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) the Privacy Official informs the individual that it the Provider is terminating its agreement to a restriction, except that such termination is not effective for PHI restricted under a Required Restriction, and only effective with respect to PHI created or received after it has so informed the individual.

- Requests and their dispositions must be documented in accordance with the procedure for "Documentation."

Definitions

The following general definitions are applicable to the Privacy Policy and Procedures for Protected Health Information:

"Breach" generally means the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the privacy rules which compromises the security or privacy of the PHI. Except as provided in the following sentence, an acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the privacy rules is presumed to be a Breach unless the Provider or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the PHI involved, including the types of identifiers and likelihood of re-identification;
- The unauthorized person who uses the PHI or to whom the Disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

However, Breach shall not include:

- Any unintentional acquisition, access, or Use of PHI by a workforce member or person acting under the authority of the Provider or 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 under the privacy rules; or

- Any inadvertent Disclosure by a person who is authorized to access PHI at the Provider or Business Associate to another person authorized to access PHI at the Provider or same Business Associate, or organized health care arrangement in which the Provider participates, and the information received as a result of such Disclosure is not further used or disclosed in a manner not permitted under the privacy rules; or

- A Disclosure of PHI where the Provider or 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.

"**Breach Notification Rules**" shall mean the Standards and Implementation Specifications for Notification in the Case of Breach of Unsecured Protected Health Information under 45 C.F.R. Part 160 and Part 164, Subparts A and D, and as may be amended from time to time.

"**Business Associate**" generally is, with respect to the Provider, a person who:

- on behalf of the Provider, or of an organized health care arrangement in which the Provider participates, but other than in the capacity of a member of the workforce of the Provider or arrangement, creates, receives, maintains, or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or

- provides, other than in the capacity of a member of the workforce of the Provider, legal, accounting, actuarial, consulting, data aggregation, management, administrative,

accreditation, or financial services to or for the Provider, or to or for an organized health care arrangement in which the Provider participates, where the provision of the service involves the Disclosure of PHI from the Provider or arrangement, or from another Business Associate of the Provider or arrangement, to the person.

The Provider may be a Business Associate of another covered entity. Business Associate includes: (1) a health information organization, E-prescribing gateway, or other person that provides data transmission services with respect to PHI to the Provider and that requires access on a routine basis to such PHI; (2) a person that offers a personal health record to one or more individuals on behalf of the Provider; and (3) a Subcontractor that creates, receives, maintains, or transmits PHI on behalf of the Business Associate. Business Associate does not include: (1) a health care provider, with respect to Disclosure by the Provider to the health care provider concerning the treatment of an individual; (2) a plan sponsor, with respect to Disclosure 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 the requirements of 45 C.F.R. §164.504(f) apply and are met; (3) 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 PHI for such purposes, to the extent such activities are authorized by law; or a covered entity participating in an organized health care arrangement that performs a function or activity as described above in this definition to or for such organized health care arrangement by virtue of such activities or services.

"**De-identified Information**" is 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. There are two ways a covered entity can determine that information is de-identified: (1) if a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (i) 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 a subject of the information, and (ii) documents the methods and results of the analysis that justify such determination; or (2) (i) the following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (a) names, (b) all geographic subdivisions smaller than a state, including street address, 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: (i) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and (ii) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000, (c) 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, (d) telephone numbers, (e) fax numbers, (f) electronic mail addresses, (g) social security numbers, (h) medical record numbers, (i) health plan beneficiary numbers, (j) account numbers, (k) certificate/license numbers, (l) vehicle identifiers and serial numbers, including license plate numbers, (m) device identifiers and serial numbers, (n) web universal resource locators (URLs), (o) internet protocol (IP) address numbers, (p) biometric identifiers, including finger and voice prints, (q) full face photographic images and any comparable images, and (r) any other unique identifying number, characteristic, or code except as permitted by the HIPAA privacy rules with respect to re-identification; and (ii) the Provider does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is the subject of the information.

"**Designated Record Set**" means a group of records maintained by or for the Provider that includes: (1) the medical records and billing records about individuals maintained by or for the Provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) other group of records used, in whole or in part, by or for the Provider to make decisions about an individual. The term "record" for this purpose means any item collection, or grouping of information that

includes PHI and is maintained, collected, used, or disseminated by or for the Provider.

"Direct Treatment Relationship" means a Treatment relationship between an individual and a health care provider that is not an Indirect Treatment Relationship.

"**Disclosure**" is defined as the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information (i.e., the Provider or Business Associate of the Provider).

"**Employee**", means the Provider's workforce. As used in this definition, the term "workforce" includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Provider, is under the direct control of the Provider, whether or not they are paid by the Provider. The term "Employee" includes all of these types of workers.

"**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.

"Genetic Information" means, subject to the next two sentences of this definition, with respect to an individual, information about: (i) the individual's Genetic Tests; (ii) the Genetic Tests of family members of the individual; (iii) the manifestation of a disease or disorder in family members of such individual; or (iv) any request for, or receipt of, Genetic Services, or participation in clinical research which includes Genetic Services, by the individual of any family member of the individual. Any reference in HIPAA to genetic information concerning an individual or family member of an individual shall include the genetic information of: (i) a fetus carried by the individual or family member who is a pregnant woman; and (ii) any embryo legally held by an individual or family member utilizing an assisted reproductive technology. Genetic information excludes information about the sex or age or any individual.

"**Genetic Services**" means (1) a Genetic Test; (2) genetic counseling (including obtaining, interpreting, or assessing Genetic Information); or (3) genetic education.

"**Genetic Test**" means an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, if the analysis detects genotypes, mutations, or chromosomal changes. Genetic Test does not include an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition.

"Health Care Operations" means any of the following activities of the Provider 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 generalized knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. §3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting 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 learned 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 under §164.502(a)(5)(i) (related to the prohibition against Using or Disclosing PHI that is Genetic Information for underwriting purposes), 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 that the applicable requirements of

the HIPAA privacy rules are met (if applicable); (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 relating 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 the Provider, including but not limited to (a) management activities relating to implementation of and compliance with the requirements of the HIPAA privacy rules, (b) customer services, including the provision of data analysis for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer, (c) resolution of internal grievances, (d) the sale, transfer, merger, or consolidation of all or part of the Provider 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 HIPAA privacy rules, creating De-identified Health Information or a Limited Data Set, and fundraising for the benefit of the Provider.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as amended by the HITECH Act, and as may otherwise be amended from time to time, and their implementing regulations ("**HIPAA**"). References in the Privacy Policy and Procedures for Protected Health Information to any HIPAA section shall include any comparable or succeeding provisions of any legislation which amends, supplements, or replaces the section.

"**HITECH Act**" means Subtitle D of the Health Information Technology for Economic and Clinical Health Act as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, and as may be amended from time to time.

"**HMO**" means a federally qualified health maintenance organization (HMO), an organization recognized as an HMO under state law, or a similar organization regulated for solvency under state law in the same manner and to the same extent as such an HMO.

"Indirect Treatment Relationship" means a relationship between an individual and a health care provider in which: (1) the health care provider delivers health care to the individual based on the orders of another health care provider; and (2) the health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

"**Individually Identifiable Health Information**" is information that is a subset of health information, including demographic information collected from an individual, and: (a) is created or received by a health care provider, a health clearinghouse, a health plan, or an employer; and (b) (1) relates to (i) the past, present or future physical or mental health condition of an individual; (ii) the provision of health care to an individual; or (iii) the past, present or future payment for the provision of health care to an individual; and (2) 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.

"**Limited Data Set**" is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (1) names; (2) postal address information, other than town or city, State, and zip code; (3) telephone numbers; (4) fax numbers; (5) electronic mail addresses; (6) social security numbers; (7) medical record numbers; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license numbers; (11) vehicle identifiers and serial numbers, including license plate numbers; (12) device identifiers and serial numbers; (13) web universal resource locators; (14) internet protocol address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

"**Marketing**" means, except as provided below in this definition, to make a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. 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 the Provider in exchange for making the communication is reasonably related to the Provider's cost of making the communication; or (2) for the following Treatment and Health Care Operations purposes, except where the Provider receives Financial Remuneration in exchange for making the communication: (a) for Treatment of an individual by a health care provider, including case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; (b) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the covered entity making the communication, 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.

"Payment" means (1) the activities undertaken by (a) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan (except as prohibited under 45 C.F.R. §164.502(a)(5)(i), which relates to the prohibition against Using or Disclosing PHI that is Genetic Information for underwriting purposes), or (b) a health care provider or health plan to obtain or provide reimbursement for the provision of health care; and (2) the activities relate to the individual to whom health care is provided, including but not limited to (a) eligibility or coverage determinations (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims; (b) risk adjusting amounts due based on enrollee health status and demographic characteristics; (c) billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess loss insurance) and related health care data processing; (d) review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges; (e) utilization review activities, including precertification and preauthorization of services, concurrent and retrospective review of services; and (f) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address, date of birth, social security number, payment history, account number, and name and address of the health care provider and/or plan.

"**Protected Health Information**" or "**PHI**" means Individually Identifiable Health Information, except as provided below in this definition, that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes Individually Identifiable Health Information (1) in education records covered by the Family Educational Rights and Privacy Act, as amended (20 U.S.C. 1232g), (2) in records described at 20 U.S.C. 1232g(a)(4)(B)(iv), (3) in employment records held by the Provider in its role as employer, and (4) regarding a person who has been deceased for more than 50 years.

"**Secretary**" means the Secretary of the Department of Health and Human Services.

"**Subcontractor**" means a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

"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.

"**Unsecured PHI**" currently means PHI that is not secured through encryption, destruction, or the use of a technology or methodology that renders PHI unusable, unreadable, or indecipherable to unauthorized persons as specified by the Secretary of the Department of Health and Human Services (the "**Secretary**") in guidance.

"**Use**" means, with respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within the entity that maintains such information (i.e., the Provider or a Business Associate of the Provider).