National University of Health Sciences General Policies

Title: **HIPAA Privacy Rule Policy and Procedures**	Page **1** of **71**
Date Adopted: **02/01/18**	Date(s) Revised: 02/04/2025 Date(s) Reviewed: 09/29/2020
President	Date 02/04/25

I. Privacy Rule Policy

It is the policy of National University of Health Sciences (the "Covered Entity" or "NUHS") to protect any Protected Health Information (PHI) of Covered Entity patients and to abide by the Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and the federal rules that implement these two Acts. NUHS hereby elects status as a hybrid Covered Entity and designates the following units as subject to these policies and procedures:

II. Scope, Application, and Location of Policy

A. Scope: This HIPAA Privacy Rule Policy and Procedures (Policy) includes the procedures for Covered Entity workforce members to follow to protect PHI. Covered Entity does not employ health care providers who are mental health professionals, therefore the Privacy Rule's restrictions on the uses and disclosures of psychotherapy notes are inapplicable to Covered Entity.

B. Application: Covered Entity workforce members with access to PHI are required to adhere to this Policy. Covered Entity Business Associates must comply with the Privacy Rule as specified in their Business Associate Agreement with Covered Entity.

C. Location: Each location and Covered Entity Corporate Headquarters will keep copies of this Policy.

D. If you have any questions about this Policy, ask:

Theodore Johnson, Dean of Clinics, HIPAA Privacy Officer

200 E Roosevelt Rd
Lombard, IL 60148
tjohnson@nuhs.edu
630-889-6513

III. Training

All Covered Entity workforce members will receive training on HIPAA. Such training may be provided in-person or via electronic means. For new employees, HIPAA training must be completed within sixty (60) days of the employee's start date. The HIPAA Privacy Officer will keep training records for the previous six years of training.

IV. Printing and Copying of PHI

All workforce members must observe the following standards relating to the printing and copying of PHI. An individual's failure to follow these standards places Covered Entity at risk for accidentally disclosing PHI to an outside party.

A. Printers, copiers, and multifunction machines that print, copy, scan, fax, and/or email, which are used to print, copy, or fax PHI, should be in a secure, non-public location, where possible.

   i. If printers, copiers, and multifunction machines are located in a place accessible to the public, Covered Entity workforce members must promptly retrieve documents with PHI that are sent to a shared printer, copier, or multifunction machine.
   ii. Covered Entity may utilize "Secure Print" or similar features that hold a print or copy job until it is released by an authorized individual with the proper code, if permitted by the printers, copiers, or multifunction machines.
   iii. Where possible, employees and students that print PHI should direct their print jobs to machines in a non-public location.

B. Covered Entity workforce members must not copy PHI indiscriminately, leave PHI unattended, or leave PHI open to compromise.

V. Fax, Email, Mail, and SFTP Transmission of PHI

Covered Entity workforce members must observe the following standards relating to facsimile (fax), email, postal mail, and Secure File Transfer Protocols (SFTP) communications of PHI. Faxes are the preferred methods of sending PHI within Covered Entity.

A. PHI transmitted by fax, email, mail, or SFTP must be limited to the minimum necessary information requested.

B. Facsimiles (Faxes):

i. A fax cover sheet should be used to send faxes containing PHI.

ii. Staff members must make reasonable efforts to ensure that they send the fax transmission to the correct destination, including by:

a. Preprogramming frequently used numbers into the machine to prevent misdialing errors;

b. Confirming that the fax number to be used is in fact the correct number;

iii. For faxes sent for reasons other than the following reasons listed below, Covered Entity must maintain the fax cover sheet and the fax confirmation sheet or activity report with the patient's health records, so that such disclosure may be accounted for in accordance with Section XXI, Accounting of Disclosures of PHI.

a. To carry out treatment, payment, and health care operations;

b. To individuals requesting their own PHI;

c.. Incident to a use or disclosure otherwise permitted or required by the Privacy Rule;

d. Pursuant to an authorization;

e. To persons involved in the individual's care or other notification purposes;

f. For national security or intelligence purposes;

g. To correctional institutions or law enforcement officials;

h. As part of a limited data set; or

i. That occurred prior to the date that compliance with HIPAA Privacy Rule was required.

iv. Fax machines used to send and receive PHI should be located in secure areas not accessible to the general public.

C. Email:

i. Email of PHI from Covered Entity email address or Covered Entity computer to a non-Covered Entity email address or non-Covered Entity computer is prohibited unless:

a. the email is encrypted and the encryption key is not included in the email; or

b. the email is sent via a secure email system with encryption.

ii. Staff members must make reasonable efforts to ensure that they send the encrypted email to the correct email address, including by confirming that the address typed is accurate.

D. Postal Mail:

i. If PHI is sent via the United States Postal Service (USPS), the United Parcel Service (UPS), FedEx, or a similar postal mail or courier service, the letter or box containing the PHI should be securely taped to ensure that the envelope or box is closed and cannot be opened inadvertently.

ii. Postal mail services and courier services such as the USPS and UPS are not considered Business Associates under the Privacy Rule and no Business Associate Agreement is required with these entities.

E. Secure File Transfer Protocol (SFTP):

i. If a Business Associate or vendor requests that Covered Entity send PHI electronically, the responsible Covered Entity workforce member should contact Information Technology (IT) for support. IT can establish a SFTP to ensure that the file is encrypted in transit, which means the file will remain secure as it is sent from Covered Entity to the Business Associate or vendor.

VI. Disposal of PHI

Covered Entity workforce members must observe the following standards relating to disposal of documents with PHI. Following these standards[1] will reduce the risk that Covered Entity will accidentally disclose PHI to an outside party.

A. Covered Entity has a Business Associate Agreement with its shredding contractor to dispose of PHI. The shredding contractor will make scheduled visits to collect Covered Entity PHI. Covered Entity will save documentation of shredding performed by its shredding company.

B. Covered Entity has a SHRED ALL POLICY. Covered Entity will have containers for PHI to be shredded that will be:

[1] HHS, Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals, http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html

i. clearly marked for shredding.

C. Paper, film, or hard copies of PHI:

i. Paper, film, or hard copies of PHI that do not constitute patient medical records must be cross-shredded or destroyed to ensure that the PHI cannot be read or reconstructed.

ii. Paper with PHI, such as receipts with patient names and supplement identifier numbers, must be placed in a paper shred bin or appropriate container.

D. Covered Entity workforce members must not discard PHI that has not been shredded or destroyed in trash bins, dumpsters, recycle bins, or publicly accessible locations.

i. If a *patient* disposes of a receipt or a labeled prescription bottle on NUHS's premises (e.g., in a trash can, dumpster, etc.) after receiving a prescription from Covered Entity, the company is not responsible for shredding or destroying such receipts or prescription bottles.

E. It is the responsibility of all Covered Entity workforce members to ensure that PHI has been properly disposed.

F. Covered Entity managers are responsible for reviewing the disposal program and addressing any changes required due to the volume of shredding. The security of PHI must be maintained. Therefore, if the shredding piles become unmanageable, or if the volume of the shredding to be performed puts the PHI at risk for a breach, managers should call the Privacy Officer to request more frequent site visits by the shredding company.

G. Movement of electronic information systems and equipment with electronic PHI (ePHI), as well as disposal and re-use of such systems is addressed in Covered Entity HIPAA Security Rule Policies and Procedures.

VII. Notice of Privacy Practices for PHI

An individual has a right to adequate notice of the uses and disclosures of PHI that Covered Entity may make, and of the individual's rights and Covered Entity legal duties with respect to PHI. Covered Entity provides notice of the uses and disclosures of PHI that Covered Entity may make through its Notice of Privacy Practices (Notice).

A. Covered Entity is required to provide a Notice of Privacy Practices to all patients with whom it has a direct treatment relationship, and any other person who requests a copy. Covered Entity must:

   i. Provide the Notice to the individual no later than the date of the first service delivery, unless the situation requires emergency treatment or the individual is a prisoner (see below);

   ii. Make a good faith effort to obtain an initial written acknowledgment of the receipt of the Notice from the patient, by documenting the receipt of the Notice provided to the individual in the logs maintained at each Covered Entity location or on an acknowledgement form (see Appendix E);

   iii. If written acknowledgement of receipt of the Notice provided to the individual is not obtained, document good faith efforts to obtain the acknowledgment and the reason why the acknowledgment was not obtained (i.e., patient refused);

   iv. Have the Notice available at the physical service delivery site for individuals to request to take with them;

   v. Post the Notice in a clear and prominent location at all Covered Entity locations where it is reasonable to expect patients to be able to read the Notice, such as waiting rooms; and

   vi. Whenever the Notice is revised, make the Notice available upon request on or after the effective date of the revision.

B. Emergency Treatment Exception: If Covered Entity is providing health care to an individual in an emergency treatment situation where Covered Entity has a direct treatment relationship with the individual, Covered Entity does not have to provide the Notice at the time of the first service delivery. In an emergency treatment situation, Covered Entity must provide the Notice to the individual as soon as reasonably practicable after the emergency treatment situation.

C. Inmate Exception: An inmate receiving health care from Covered Entity does not have a right to receive a copy of the Notice.

D. Website:

   i. Covered Entity must post the Notice on its website and make the Notice available electronically through the website.

   ii. The Notice is posted online on the Covered Entity website, http://www.nuhs.edu/extras/docs/hipaa.pdf

iii. Individuals may still request a paper copy of the Notice from Covered Entity.

E. Revisions to the Notice: Covered Entity shall promptly revise and distribute or otherwise make available its Notice whenever there is a material change to the uses or disclosures, the individual's rights, Covered Entity legal duties, or other privacy practices stated in the Notice. Whenever the Notice is revised, Covered Entity will implement the Notice and make the Notice available on or after the effective date of the revision.

F. Retention of Prior Versions of the Notice: The HIPAA Privacy Officer must retain copies of the Notices issued by Covered Entity for six years from the date that the Notices were created or the date they were last in effect, whichever is later. Covered Entity must also maintain any written acknowledgments of receipt of the Notice or documentation of good faith efforts to obtain such written acknowledgment and the reason why the acknowledgment was not obtained (i.e., patient refused to sign).

G. Appendix E has a sample Notice of Privacy Practices Acknowledgment Form.

VIII. Minimum Necessary Use and Disclosure of PHI

All personnel within Covered Entity must observe the following standards relating to the use and disclosure of PHI. Personnel must not disclose PHI to an individual who does not have authorization to use, disclose, request, or access PHI.

A. Minimum Necessary Policy: Except as otherwise stated below, Covered Entity must make reasonable efforts to limit the PHI used, disclosed, or requested to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. If practicable, the PHI used, disclosed, or requested should be released in the form of a limited data set (see Section XVIII).

B. Exceptions to the Minimum Necessary Policy: The minimum necessary policy in (A), above, shall not apply to the use or disclosure of PHI if:

i. the disclosure is to a health care provider for treatment;

ii. the request is from a health care provider for treatment;

iii. the use or disclosure is made to the individual patient, including disclosures to the individual required under the accounting for disclosures and access provisions (see Sections XXI and XXIII);

iv. the use or disclosure is made pursuant to a valid Authorization for Release of Information;

v. the disclosure is made to the Secretary of the United States Department of Health and Human Services (HHS)[2];

vi. the use or disclosure is required by law[3];

vii. the use or disclosure is required for compliance with the requirements of the Privacy Rule; or

viii. the PHI has been de-identified (see Section XVII).

C. Workforce Access to PHI and Minimum Necessary Requirements for Uses and Disclosures of PHI and Requests for PHI: All persons who handle PHI in any manner are expected to know and abide by the following:

i. Access to PHI will be granted based on the individual's role and his/her need for PHI.

ii. In Appendix A, Covered Entity has identified:

a. Those persons or classes of persons in Covered Entity workforce who need access to PHI to carry out their duties; and

b. For each such person or class of persons, the category or categories of PHI to which access is needed (i.e., entire patient record), and any conditions that exist for access (i.e., role-based access).

iii. Covered Entity must make reasonable efforts to limit the access of such persons or classes of persons only to the amount of information needed to carry out the duties of that position.

iv. Covered Entity must limit any request for PHI to that which is reasonably necessary to accomplish the purpose for which the request is made, when requesting PHI from other covered entities.

v. Persons or categories of persons within Covered Entity with access to PHI shall refrain from discussing PHI with individuals who do not perform tasks or requests directly related to treatment, payment, or health care operations for the individual patient.

vi. Routine Disclosures and Requests: For disclosures of, and requests for, PHI that Covered Entity makes or receives on a routine and recurring basis, Covered Entity has established a standard protocol for limiting the PHI disclosed or requested to the minimum amount reasonably necessary to accomplish the purpose of the disclosure or request.

---

[2] 45 C.F.R. Part 160, Subpart C.
[3] 45 C.F.R. § 164.512(a).

vii. Non-Routine Disclosures and Requests: For disclosures of, and requests for, PHI that do not occur on a routine basis, Covered Entity workforce members may seek the advice of the HIPAA Privacy Officer, who may consult legal counsel, and who may review requests for disclosure on an individual basis and ensure the PHI disclosed or requested is reasonably necessary to accomplish the purpose for which disclosure is sought or for which the request is made.

viii. Covered Entity may rely, if such reliance is reasonable under the circumstances, on the belief that the PHI requested for disclosure is the minimum necessary for the stated purpose of the disclosure when:

a. The PHI is requested by another person previously approved for access to PHI;

b. The PHI is requested by a health care provider, health plan, or health care clearinghouse;

c. The PHI is requested by:

1. a professional who is a workforce member of Covered Entity; or

2. a professional who is a workforce member of a business associate that has entered into a Business Associate Agreement with Covered Entity, and the professional represents that the PHI requested is the minimum necessary for the stated purpose(s);

d. The PHI is requested by a person who provides documentation or representations that comply with the requirements for uses and disclosures for research purposes (see Section XVI);

e. The PHI is requested to comply with laws relating to workers' compensation (see D, below).

D. Disclosures for Workers' Compensation: Covered Entity may disclose PHI to comply with state workers' compensation laws and laws related to other similar programs, established by law, that provide benefits for work-related injuries or illness without regard to fault. Covered Entity may disclose PHI to comply with such workers' compensation laws without a written Authorization for Release of Information from the individual and without providing the individual an opportunity to agree or object to the disclosure of his/her PHI.

E. Requests for Uses or Disclosures of Entire Medical Record: Covered Entity must not use, disclose, or request an entire medical record unless the entire medical record is specifically justified as the amount that is reasonably necessary to

accomplish the purpose of the use, disclosure, or request. If needed, the HIPAA Privacy Officer can review requests for entire medical records in order to assure compliance with this Policy.

F. Disclosures to Family and Friends: Persons with authority to disclose PHI may only make disclosures to family and friends of the individual patient in accordance with Section X, Use and Disclosure of PHI to Family and Friends and for Notification Purposes.

G. Disclosures for Payment: The minimum necessary PHI shall be disclosed for payment functions. Workforce members of Covered Entity who handle PHI in the payment context shall refrain from publicizing patient diagnoses and PHI when possible on paper receipts, envelopes, and invoices.

IX. Use and Disclosure of PHI Based on an Individual's Authorization

The Privacy Rule permits certain uses and disclosures of PHI without an authorization for release of information, such as uses and disclosures of PHI for treatment, payment, and health care operations. Covered Entity workforce members may make other uses and disclosures of PHI only pursuant to a valid authorization for release of information. If Covered Entity is presented with a valid authorization for release of information, it may use and disclose PHI pursuant to such authorization.

A. Contents of the Authorization Form: In Appendix E, Covered Entity has created a version of an authorization for release of information form that is pre-populated with the information required by the Privacy Rule and a list of the information most likely to be requested by an individual. To use or disclose PHI pursuant to an authorization for release of information, Covered Entity must ensure that all of the required fields on the authorization form are completed by the individual or the individual's personal representative.

B. Copy to the Individual: If Covered Entity seeks an authorization from an individual for a use or disclosure of the individual's PHI, Covered Entity must provide a copy of the signed authorization to the individual.

C. Defective Authorizations: An authorization is defective and invalid if any of the following defects exist:

   i. the expiration date has passed or the expiration event (i.e., end of litigation) is known by Covered Entity to have occurred;

   ii. the authorization has not been filled out completely;

   iii. the authorization is known by Covered Entity to have been revoked;

iv. the authorization violates the compound authorization requirement or the requirements for conditioning authorizations; or

v. any material information in the authorization is known by Covered Entity to be false.

D. Compound Authorizations: Covered Entity Authorization for Release of Information has not been combined with any other document to create a compound authorization.

X. Use and Disclosure of PHI to Family and Friends and for Notification Purposes

The Privacy Rule permits Covered Entity to communicate with an individual's family, friends, or other persons who are involved in the individual's care when (1) the individual is present; (2) the individual is not present, incapacitated, in an emergency situation, deceased, in a disaster relief situation; or (3) the family member or other person is reasonably able to prevent or lessen a serious or imminent threat to the health or safety of the individual or others, pursuant to the requirements below. Disclosures of PHI to family members, friends, or other persons involved in the individual's care or payment for care are to be limited to the PHI directly relevant to the person's involvement in the patient's care or payment for care.

A. Uses and Disclosures when the Individual is Present: If the individual is present for, or otherwise available prior to, a use or disclosure and has the capacity to make health care decisions, Covered Entity may use or disclose PHI if it:

i. receives the individual's permission;

ii. provides the individual with the opportunity to object to the disclosure, and the individual does not express an objection; or

iii. reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to such disclosure.

iv. HHS example of (ii), above: "HIPAA permits a covered provider to communicate with a patient's family members, or others involved in the patient's care, to be on watch or ensure compliance with medication regimens." A Covered Entity workforce member should tell the patient that he/she plans to discuss the information with the patient's family member and give the patient an opportunity to object to the disclosure.

v. HHS example of (iii), above: "[S]ituations in which a family member or friend is invited by the patient and present in the treatment room with the patient and the provider when a disclosure is made."

B. Uses and Disclosures when the Individual is Not Present: 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, Covered Entity may, in the exercise of professional judgment, determine whether the disclosure is in the best interests of the individual.

   If Covered Entity determines that the disclosure is in the individual's best interest, Covered Entity may disclose only the PHI that is directly relevant to the person's involvement with the individual's health care or payment related to the individual's health care or needed for notification purposes.

   i. Incapacity: HHS examples of "incapacity" include unconscious patients and may include, depending on the circumstances, patients suffering from temporary psychosis or under the influence of drugs or alcohol.

   ii. Best Interests: Covered Entity may use professional judgment and its experience with common practice to make reasonable inferences of the individual's best interest in allowing a person to act on behalf of the individual patient who is not present to pick up medical supplies, filled prescriptions, or other similar forms of PHI.

C. Uses and Disclosures for the Purpose of Notifying Family or Others: Covered Entity may use or disclose PHI to notify, assist in the notification of, identify, or locate a family member, a personal representative of the individual, or another person responsible for the care of the individual.

   i. Covered Entity may disclose the individual's location, general condition, or death.

   ii. The use or disclosure of PHI must follow the other requirements for disclosures when the individual is present, when the individual is not present, when the individual is deceased, and when there is a disaster relief situation, as those requirements are stated in this Section X.

D. Uses and Disclosures when the Individual is Deceased:

   i. Covered Entity may disclose to a family member, other relative, close personal friend, or other person identified by the deceased who was 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.

   ii. Exception: Such disclosures are not permitted if the deceased previously expressed a preference and such preference is known to Covered Entity.

E. Uses and Disclosures for Disaster Relief Purposes: Covered Entity may use or disclose PHI to the Red Cross and other public or private entities authorized by law or by their charters to assist in disaster relief efforts.

i. Covered Entity uses and disclosures of PHI to the Red Cross and others must be for the purpose of coordinating with such entities the uses and disclosures of PHI to notify, or assist in notification of, a family member, personal representative, or other person responsible for the individual's care of the individual's location, general condition, or death.

ii. Covered Entity will follow the above requirements that apply to the uses and disclosures in a disaster relief situation to the extent that Covered Entity, in the exercise of professional judgment, determines that the requirements do not interfere with its ability to respond to the emergency circumstances.

F. Uses and Disclosures of PHI when there is a Serious and Imminent Threat to the Health or Safety of the Patient or Others and Family Members or Other Persons are in a Position to Lessen the Threat:

i. If Covered Entity believes in good faith that a use or disclosure of PHI is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, Covered Entity may use or disclose the PHI to the person(s) it believes are reasonably able to prevent or lessen the threat. The person(s) may be family members, other relatives, close personal friends, or other persons, provided that they are reasonably able to prevent or lessen the threat.

ii. HHS example: "[I]f a mental health professional has a patient who has made a credible threat to inflict serious and imminent bodily harm on one or more persons, HIPAA permits the mental health professional to alert the police, a parent or other family member, school administrators or campus police, and others who may be able to intervene to avert harm from the threat."

XI. Use and Disclosure of PHI to Personal Representatives

The Privacy Rule permits certain individuals with legal authority to act and to make decisions related to PHI on behalf of another person. For example, a father could sign an acknowledgment of receipt of the Covered Entity Notice of Privacy Practices on behalf of his minor child. If a person has the legal authority to act on behalf of an individual for purposes of making decisions related to health care, Covered Entity must treat the person as the personal representative for purposes of the Privacy Rule.

A. Deceased Individuals:

i. Covered Entity must treat an executor, administrator, or other person with authority to act on behalf of a deceased individual or the deceased's estate as

a personal representative with respect to PHI relevant to the personal representation of the deceased.

a. In Illinois, when (1) no executor, administrator, or agent exists; and (2) the deceased did not specifically object to the disclosure of his/her records in writing, the following individuals will be considered to be the personal representative of the deceased individual for purposes of the release of the deceased's health care records:

1. The surviving spouse, or, if none exists;
2. An adult son or daughter, a parent, or an adult brother or sister.

ii. Covered Entity is required to comply with the requirements of the HIPAA Privacy Rule with respect to the PHI of a deceased individual for a period of 50 years following the individual's death.

iii. Coroners and Medical Examiners: Covered Entity may disclose PHI about a decedent to a coroner or a medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.

iv. Funeral Directors: Covered Entity may disclose PHI about a decedent to a funeral director, as necessary for the funeral director to carry out his/her duties with respect to the deceased. Covered Entity may disclose PHI to funeral directors prior to, and in reasonable anticipation of, the individual's death if necessary for funeral directors to carry out their duties.

v. Organ, Eye, or Tissue Donation Purposes: Covered Entity 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.

B. Exception for Domestic Violence, Abuse, and Neglect: Covered Entity may elect not to treat a person as the personal representative of the individual if (i) and (ii), below, apply:

i. Covered Entity has a reasonable belief that:

a. The patient has been or may be subject to domestic violence, abuse, or neglect by the person who would otherwise be considered the personal representative of the individual; or

b. Treating the person as the personal representative could endanger the patient.

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

XII. Use and Disclosure of a Minor's PHI

Covered Entity is permitted to share patient information with a patient's personal representative. For "general treatment situations, a parent, guardian, or other person acting *in loco parentis* usually is the personal representative of the minor child."[4]

A. Unemancipated Minors:

i. An unemancipated minor is a child who is under the control or authority of his or her parents or guardians.

ii. If a parent, guardian, or other person acting *in loco parentis* has the legal authority to act on behalf of an unemancipated minor for the purposes of making decisions related to health care, Covered Entity must treat such parent, guardian, or other person acting *in loco parentis* as a personal representative. Such parent, guardian, or other person acting *in loco parentis* may act on the minor's behalf with respect to the PHI relevant to personal representation of the unemancipated minor.

B. Exception to Treating a Parent, Guardian, or Other Person Acting *In Loco Parentis* as an Unemancipated Minor's Personal Representative:

i. A minor has the authority to act as an individual. Parents, guardians, and other persons acting *in loco parentis* may not be a personal representative of an unemancipated minor in any of the three following situations:

a. The minor consents to a 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 the parent/guardian/person acting *in loco parentis* be treated as the personal representative;

b. The minor may lawfully obtain such health care service without the consent of a parent/guardian/person acting *in loco parentis*, and the minor, a court, or another person authorized by law provides consent for the minor to receive the health care service; or

c. A parent, guardian, or other person acting *in loco parentis* agrees to a confidential relationship between Covered Entity and the minor with respect to Covered Entity health care services.

---

[4] HHS Guidance Document, HIPAA Privacy Rule and Sharing Information Related to Mental Health, http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html.

ii. Example: State law permits a minor to obtain medical treatment without parental consent, and the minor consents to treatment. The minor's parent would not be the personal representative of the minor with respect to that medical treatment information.

iii. Illinois Law:

a. In Illinois, minors may consent to medical care and counseling for the diagnosis or treatment of sexually transmissible infections and for alcohol consumption, drug use, or alcohol and drug abuse by a member of the minor's family.

b. Minors under the age of 18 that are married, pregnant, or a parent may consent to medical and surgical procedures.

c. Minors that are victims of criminal sexual assault or criminal sexual abuse may consent to medical care or counseling related to the diagnosis or treatment of any disease or injury that results from the offense(s).

d. Minors twelve (12) years of age and older who may have come into contact with a sexually transmissible infection may consent to medical care and counseling related to the diagnosis or treatment of, or vaccination against, a sexually transmissible infection.

C. Access to or Denial of PHI to a Parent, Guardian, or Other Person Acting *In Loco Parentis* if the Parent, Guardian, or Other Person is Not the Minor's Personal Representative under (B), above

i. The HIPAA Privacy Rule defers to federal and state laws that expressly address the ability of a parent/guardian/person acting *in loco parentis* to obtain PHI of the minor. Therefore, Covered Entity may be permitted, required, or prohibited from disclosing PHI about the minor child to a parent/guardian/person acting *in loco parentis* even if the person is not the personal representative.

a. Example: Federal confidentiality laws and rules on federally-funded drug and alcohol abuse treatment programs may affect when parents, guardians, or other persons with the legal authority to act on behalf of the minor may be treated as the minor's personal representatives.

ii. Notwithstanding (B) above, if Illinois law or other law *permits or requires* Covered Entity to disclose or provide access to PHI in accordance with the Privacy Rule's access requirements, Covered Entity may disclose PHI or provide access to PHI about an unemancipated minor to a parent, guardian,

or other person acting *in loco parentis* to the extent permitted or required by state or other law.

iii. Notwithstanding (B) above, if Illinois law or other law *prohibits* Covered Entity from disclosing or providing access to PHI, Covered Entity is prohibited from disclosing or provide access to PHI about an unemancipated minor to a parent, guardian, or other person acting *in loco parentis*.

iv. Notwithstanding the above, if Illinois law or other law is *silent* and has no applicable access provision about the disclosure of a minor's PHI to a parent/guardian/person acting *in loco parentis*, Covered Entity may provide or deny access to PHI to a parent, guardian, or other person acting *in loco parentis* who is not the personal representative under (B) above, if:

a. the provision or denial of access is consistent with Illinois law or other law; and

b. the decision to provide or deny access is made by a licensed health care professional, in the exercise of professional judgment.

XIII. Use and Disclosure of PHI for Public Health and Safety Reasons

The Privacy Rule permits Covered Entity to make certain uses and disclosures of PHI to public health authorities, law enforcement officials, and others for public health or safety reasons, without the individual's written authorization for release of information and without providing the individual with an opportunity to agree or object. Covered Entity may disclose PHI without a patient's authorization for public health or safety reasons in the situations listed below.

A. Required by Law:

i. Covered Entity may use or disclose PHI to the extent that such use or disclosure is required by law and complies with and is limited to the relevant requirements of such law.

ii. Uses and disclosures required by law that involve reporting of victims of abuse, neglect, or domestic violence; law enforcement purposes; and judicial and administrative proceedings must comply with those particular Privacy Rule provisions in subsections C and E, below, and in Section XIV.

B. Public Health Activities:

i. Covered Entity is authorized to use and disclose PHI to public health authorities for public health activities and purposes, such as collecting and receiving 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.

ii. Covered Entity may use or disclose PHI for public health activities to a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect;

iii. Covered Entity workforce members may use or disclose PHI to a person subject to the jurisdiction of the Food and Drug Administration (FDA) with respect to FDA-regulated products (i.e., drugs and medical devices) or activities for which that person has responsibility, for the purpose of activities related to the quality, safety, or effectiveness of such FDA-regulated product or activity.

    a. For example, Covered Entity may disclose product defects or problems to a drug manufacturer, including problems with the use or labeling of a drug product.

iv. If Covered Entity is authorized by law to notify a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a disease or condition, Covered Entity may notify such person as necessary in the conduct of a public health intervention or investigation. Covered Entity workforce members must consult the HIPAA Privacy Officer prior to making this type of disclosure.

v. Covered Entity workforce members may use or disclose PHI to an employer, about an individual who is a member of the workforce of the employer if:

    a. Covered Entity 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 disclosed consists of findings concerning a work-related illness or injury or a workplace-related medical surveillance;

    c. The employer needs such findings in order to comply with certain occupational safety and health regulations (29 C.F.R. Parts 1904-1928 and 30 C.F.R. Parts 50-90) or under a state law with a similar purpose, to record such illness or injury or to carry out responsibilities for workplace medical surveillance; and

    d. Covered Entity 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 same 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.

vi. Covered Entity may use or disclose a student's or prospective student's proof of immunization to that student's or prospective student's school if:

a. the school is required by state or other law to have proof of immunization prior to admitting the individual; and

b. Covered Entity obtains and documents the agreement for disclosure from either:

1. a parent, guardian, or other person acting *in loco parentis* of the individual, if the individual is an unemancipated minor; or

2. the student or prospective student, if the individual is an adult or emancipated minor.

c. Covered Entity workforce members must document the agreement for disclosure, which may be oral, written, or electronic.

d. Covered Entity must keep the documentation for six years from the date of the agreement or the date when the agreement was last in effect, whichever is later.

C. Abuse, Neglect, or Domestic Violence:

i. Children: Covered Entity may disclose the PHI of an individual whom it reasonably believes to be a victim of abuse, neglect, or domestic violence to a public health authority (including a social service or protective services agency) that is authorized by law to receive reports of child abuse, neglect, or domestic violence.

ii. Adults: If Covered Entity reasonably believes that an adult patient has been a victim of abuse, neglect, or domestic violence, Covered Entity may disclose a patient's PHI to the government agency (including a social service or protective services agency) authorized by law to receive such information.

iii. Vulnerable Adults: If Covered Entity reasonably believes that a vulnerable adult is the subject of abuse, neglect, or exploitation, Covered Entity may disclose the patient's PHI to the appropriate government adult protective services provider or elder abuse agency.

iv. The disclosures of PHI in (i)-(iii), above, must be:

a. required by law and comply with and be limited to the requirements of the law; or

b. the individual must agree to the disclosure; or

c. the disclosure must be expressly authorized by law or regulation and:

1. Covered Entity, 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.

v. If Covered Entity makes a disclosure under the requirements for victims of abuse, neglect, or domestic violence, Covered Entity must promptly inform the individual that a report has been or will be made, except if:

a. Covered Entity, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or

b. Covered Entity would be informing a personal representative and:

1. Covered Entity reasonably believes the personal representative is responsible for the abuse, neglect, or other injury, and

2. that informing the personal representative would not be in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

D. Serious and Imminent Threats to the Health or Safety of a Person or the Public:

i. Covered Entity may, consistent with applicable law and standards of ethical conduct, use or disclose PHI if the healthcare component, in good faith, believes the use or disclosure:

a. is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

b. is to a person(s) reasonably able to prevent or lessen the threat, including the target of the threat.

ii. Covered Entity may, consistent with applicable law and standards of ethical conduct, use or disclose PHI if Covered Entity, in good faith, believes the use or disclosure is necessary for law enforcement authorities to identity or apprehend an individual:

a. Because of a statement by an individual admitting participation in a violent crime that Covered Entity reasonably believes may have caused serious physical harm to the victim; or

b. Where it appears from all the circumstances that the individual has escaped from a correctional institution or from lawful custody.

iii. A use or disclosure of PHI described in (ii)(a) (a statement by the individual admitting participation in a violent crime that Covered Entity reasonably believes may have caused serious physical harm to the victim) may not be made if:

a. Covered Entity learned of the information in the course of treatment to affect the propensity to commit criminal conduct, or counseling or therapy; or

b. Covered Entity learned of the information through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy.

iv. A disclosure made because Covered Entity, in good faith, believes the disclosure is necessary for law enforcement authorities to identify or apprehend an individual because of a statement by the individual admitting participation in a violent crime that may have caused serious physical harm to the victim must contain only that statement and the following information:

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

v. If Covered Entity uses or discloses PHI for the reasons in (i) or (ii) is presumed to have acted in good faith with regard to the beliefs described in (i) or (ii), if the belief is based on Covered Entity actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

E. Law Enforcement Officials: Covered Entity may disclose PHI for law enforcement purposes, to a law enforcement official, if certain conditions are met. Covered Entity may disclose PHI:

i. as required by law, to report certain wounds or other physical injuries;

ii. in compliance with, and as limited by the requirements of:

a. a court order, court-ordered warrant, 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:

1. the information sought is relevant and material to a legitimate law enforcement inquiry;

2. 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

3. de-identified information could not reasonably be used.

iii. in response to a law enforcement official's request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person, provided that Covered Entity may disclose only the following information:

a. Name and address;
b. Date and place of birth;
c. Social security number;
d. ABO blood type and rh factor;
e. Type of injury;
f. Date and time of treatment;
g. Date and time of death, if applicable; and

h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard of moustache), scars, and tattoos.
i. Except as permitted above, Covered Entity may not disclose for the purposes of identification or location any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples or analysis of body fluids or tissue.

iv. in response to a law enforcement official's request for such information about a person who is or is suspected to be a crime victim (other than for public health or abuse, neglect, or domestic violence-related disclosures discussed above), if;

a. the person agrees to the disclosure; or

b. if Covered Entity is unable to obtain the person's agreement, and

1. 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;

2. 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

3. the disclosure is in the best interests of the individual as determined by the covered entity, in the exercise of professional judgment.

v. to a law enforcement official regarding a person who has died, for the purpose of alerting law enforcement of the person's death, if Covered Entity has a suspicion that such death may have resulted from criminal conduct;

vi. to a law enforcement official regarding evidence of criminal conduct that occurred on the premises of Covered Entity; and

vii. to report a crime to a law enforcement official in an emergency, if Covered Entity is providing emergency care in response to a medical emergency other than an emergency on Covered Entity premises, if such disclosure appears necessary to alert law enforcement to:

a. the commission and nature of a crime;

b. the location of the crime or of victim(s) of the crime; and

c. the identity, description, and location of the perpetrator of such crime.

d. This permitted disclosure for reporting crimes in emergency situations does not apply if the health care provider believes that the medical emergency is the result of the abuse, neglect, or domestic violence of the individual in need of emergency care. The health care provider should follow the section on abuse, neglect, or domestic violence reports, above.

F. Specialized Government Functions:

i. Covered Entity may disclose an individual's PHI to authorized federal officials for the conduct of military and veteran's activities if the appropriate military authority has published a notice in the Federal Register,[5] as well as for intelligence, counter-intelligence, and national security activities authorized by law.

ii. Covered Entity may also disclose an individual's PHI to authorized federal officials to protect the President of the United States, other authorized officials, or foreign heads of state, or to conduct investigations authorized by law.

iii. Covered Entity may disclose to a correctional institution or a law enforcement official having lawful custody of an inmate or other individual, the PHI of such inmate or individual, if the correctional institution or law enforcement official represents that such PHI is necessary for:

a. the provision of health care to such individuals;

b. the health and safety of such individuals or other inmates;

c. the health and safety of the officers or employees of or others at the correctional institution;

d. the health and safety of such individuals and officers or other persons responsible for the transporting of inmates or their transfer from one institution, facility, or setting to another;

e. law enforcement on the premises of the correctional institution; or

f. the administration and maintenance of the safety, security, and good order of the correctional institution.

g. This provision does not apply if the individual is no longer an inmate when released on parole, probation, supervised release, or otherwise is no longer in lawful custody.

[5] Available online at www.federalregister.gov.

XIV. Use and Disclosure of PHI for Judicial and Administrative Proceedings

Covered Entity may receive court orders or subpoenas for PHI. Typically, subpoenas for PHI are accompanied by a "qualified protective order" or a "HIPAA order."

A. Definition: A "qualified protective order" is defined as an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

   i. prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which such information was requested; and

   ii. requires the return to Covered Entity or destruction or the PHI (including all copies made) at the end of the litigation or proceeding.

B. If Covered Entity receives a subpoena or discovery request for PHI, the HIPAA Privacy Officer may consult legal counsel to ensure that the subpoena or discovery requests complies with the requirements below.

   i. Court Order or Order of Administrative Tribunal: If Covered Entity receives a court order, or an order of an administrative tribunal, it may disclose only the PHI expressly authorized by such order.

   ii. Subpoena, Discovery Request, or Other Lawful Process: If Covered Entity receives a subpoena, discovery request, or other lawful process that is not accompanied by a court order or an order of an administrative tribunal, Covered Entity may disclose PHI if:

      a. Covered Entity receives satisfactory assurances (as described in (C), below) from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual whose PHI has been requested has been given notice of the request; or

      b. Covered Entity receives satisfactory assurances (as described in (D), below) from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order (also called a HIPAA order).

C. Satisfactory Assurances for Notice: In order to meet the requirements for "satisfactory assurances" in (B)(ii)(a), above, Covered Entity must receive a written statement and accompanying documentation demonstrating that:

   i. the party requesting PHI has made a good faith attempt to provide written notice to the individual (or, if the individual's location is unknown, to mail a notice to the individual's last known address);

ii. the notice included sufficient information about the litigation or proceeding in which the PHI is requested to permit the individual to raise an objection to the court or administrative tribunal; and

iii. the time for the individual to raise objections to the court or administrative tribunal has elapsed; and

a. no objections were filed; or

b. all objections filed by the individual have been resolved by the court or administrative tribunal and the disclosures being sought are consistent with such resolution.

D. Satisfactory Assurances for Qualified Protective Order (aka "HIPAA Order"): In order to meet the requirements for "satisfactory assurances" in (B)(ii)(b), above, Covered Entity must receive from the party seeking PHI a written statement and accompanying documentation demonstrating that:

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

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

E. If Satisfactory Assurances are Not Received: Covered Entity may disclose PHI in response to a subpoena, discovery request, or other lawful process, without receiving satisfactory assurances as described above in (C) or (D), if Covered Entity makes reasonable efforts to provide notice to the individual sufficient to meet the requirements of (D) or if Covered Entity seeks a qualified protective order sufficient to meet the requirements of (D).

XV. Use and Disclosure of PHI to Business Associates

A. Covered Entity has a written contract called a Business Associate Agreement that complies with the requirements of the Privacy Rule. Covered Entity will use this Business Associate Agreement if it permits a vendor or contractor to create, receive, maintain, or transmit PHI on its behalf. The Business Associate Agreement with Covered Entity may be a stand-alone Business Associate Agreement or an exhibit to the larger contract between the business associate and Covered Entity.

B. For example, if Covered Entity were to provide a vendor or contractor with PHI for claims processing, data analysis, utilization review, quality assurance, patient safety activities, benefit management, billing, data aggregation, auditing,

accounting, financial, legal, or consulting services, Covered Entity would enter into a Business Associate Agreement with such vendor or contractor.

XVI. Use and Disclosure of PHI for Research

A. Definition: Research is defined as "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge."[6]

B. Generally, Covered Entity must receive a valid, signed authorization for release of information from an individual for the use or disclosure of PHI for research purposes.

   i. The researcher must provide Covered Entity with authorizations for the release of PHI that comply with 45 C.F.R. § 164.508.

   ii. The signed authorizations for release of PHI also must comply with Section IX, Use and Disclosure of PHI Based on an Individual's Authorization, except that the expiration date or event on the authorization may state "none" or "end of research study," or use similar language.

C. Covered Entity may use or disclose PHI for research without an authorization for release of PHI in the following instances, provided that the procedures below are followed for each situation:

   i. pursuant to institutional review board (IRB) approval of an alteration to, or waiver of, authorization;

   ii. pursuant to written representations from a researcher seeking PHI preparatory to research;

   iii. pursuant to the written representations required for research on the PHI of individuals that are deceased for less than 50 years; or

   iv. pursuant to Section XVII, De-identification of PHI and Section XVIII, Use and Disclosure of Limited Data Sets.

D. Institutional Review Board Waiver of Authorization: Covered Entity must receive documentation of approval by an appropriate IRB of an alteration to, or full or partial waiver of, the individual authorization required for the use or disclosure of PHI.

---

[6] 45 C.F.R. § 164.501.

i. For a use or disclosure to be permitted based on documentation of the IRB's approval, the researcher must provide the following information to Covered Entity:

   a. The name of the IRB and contact information for the IRB Chair;

   b. The date on which the alteration or waiver of authorization was approved;

   c. The signature of the IRB Chair (or other IRB member designated by the chair) on the alteration or waiver of authorization;

   d. A statement that the IRB has determined that the alteration or waiver satisfies these criteria:

      1. The use or disclosure of PHI involves no more than a minimal risk to the privacy of individuals, based on at least these three elements:

         A. An adequate plan to protect the identifiers from improper use and disclosure;

         B. An adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is required by law; and

         C. Adequate written assurances that the PHI will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research study, or for other research for which the use or disclosure of PHI would be permitted by the HIPAA Privacy Rule.

      2. The research could not practicably be conducted without the waiver or alteration; and

      3. The research could not practicably be conducted without access to and use of the PHI;

   e. A brief description of the PHI for which use or access has been determined to be necessary by the IRB, pursuant to the above statement that the research could not practicably be conducted without access to and use of the PHI; and

   f. A statement that the alteration or waiver of authorization has been reviewed and approved by the IRB under either normal or expedited review procedures under the requirements of the "Common Rule" (also known as the Federal Policy for the Protection of Human Subjects).

E. Preparatory to Research: Covered Entity must receive the following written representations from the researcher:

i. The use or disclosure of PHI is sought solely to review PHI as necessary to prepare a research protocol or for similar purposes preparatory to research;

ii. No PHI will be removed from Covered Entity location where it is being reviewed by the researcher in the course of the review;

iii. The PHI for which use or access is sought is necessary for the research purposes; and

iv. If the researcher is taking notes, no identifying information may be copied.

F. Decedents: Covered Entity should follow the HHS guidance entitled "Health Information of Deceased Individuals."[7]

i. Individuals Deceased for Less than 50 Years: Covered Entity must receive the following written representations from the researcher:

a. The use or disclosure sought is solely for research on the PHI of decedents;

b. The PHI for which use or disclosure is sought is necessary for research purposes; and

c. Documentation of the death(s) of the individual(s).

ii. Individuals Deceased for More than 50 Years: Covered Entity may use or disclose the individually identifiable health information of individuals who have been deceased for more than 50 years without regard to the HIPAA Privacy Rule because the individually identifiable information of such decedents is not considered PHI.

XVII. De-identification of PHI

Generally, PHI is individually identifiable health information transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. If health information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual, then the information is not individually identifiable health information and is not PHI. Therefore, if individually identifiable health information is de-identified, the de-identified data is not PHI and is not subject to the HIPAA Privacy Rule.

---

[7] HHS, Health Information of Deceased Individuals (Sept. 19, 2013), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/decedents.html.

A. PHI must be de-identified prior to disclosure to individuals who are not authorized by the Privacy Rule to receive PHI.

B. Whenever possible, PHI should be de-identified prior to the use of such information for quality assurance monitoring, internal audits, and similar activities or functions.

C. To meet the de-identification requirements, Covered Entity may determine that health information is not individually identifiable health information in accordance with the HHS guidance document on de-identification and pursuant to one of the two procedures: the "Expert Determination Method" or the "Safe Harbor Method."[8] Covered Entity should refer to the HHS guidance document for questions and answers on the de-identification standard.

D. Expert Determination Method: Under the expert determination method, Covered Entity may determine that health information is not individually identifiable health information only if a person with appropriate knowledge of and experience with generally accepted scientific principles and methods for rendering information not individually identifiable applying such principles and methods:

   i. 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.

E. Safe Harbor Method Involving the Removal of Specific Identifiers and the Absence of Actual Knowledge by Covered Entity:

   i. Under the safe harbor method, Covered Entity may determine that health information is not individually identifiable health information only if:

      a. the identifiers (listed below) of the individual, or of relatives, employers, or household members of the individual, are removed; and

      b. Covered Entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

---

[8] 45 C.F.R. § 164.514(b); United States Department of Health and Human Services (HHS), Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, (Nov. 26, 2012), http://www.hhs.gov/ocr/privacy/ hipaa/understanding/coveredentities/De-identification/hhs_deid_ guidance.pdf.

ii. The identifiers of the individual, or of relatives, employers, or household members of the individual, which must be removed are:

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:
    1. the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people (i.e., 606--); and
    2. if 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. E-mail addresses;
g. Social security numbers;
h. Medical record numbers (including prescription numbers);
i. Health plan beneficiary numbers;
j. Account numbers (including Covered Entity Advantage 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, unless the code meets the following criteria:
    1. Covered Entity may assign a code or other means of record identification to allow information de-identified under this policy to be re-identified by Covered Entity.
    2. The code or other means of record identification must not be derived from or related to information about the individual (i.e., birth date and year) and must not be capable of being translated so as to identify the individual.
    3. Covered Entity must not use or disclose the code or other means of record identification for any other purpose.
    4. Covered Entity must not disclose the mechanism for re-identification.

XVIII. Use and Disclosure of Limited Data Sets

Covered Entity may receive requests to disclose limited data sets. Covered Entity may also apply to receive limited data sets from other entities. In order to use or disclose a limited data set, a data use agreement must be created. Covered Entity may use or disclose a limited data set, pursuant to a data use agreement and the procedures below, only for the purposes of research, public health, or health care operations.

A. Definition: A limited data set is PHI that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual:
   i. names;
   ii. postal address information, other than town or city, state, and zip code;
   iii. telephone numbers;
   iv. fax numbers;
   v. electronic mail addresses;
   vi. social security numbers;
   vii. medical record numbers; (including prescription numbers)
   viii. health plan beneficiary numbers;
   ix. account numbers;
   x. certificate/license numbers;
   xi. vehicle identifiers and serial numbers, including license plate numbers;
   xii. device identifiers and serial numbers;
   xiii. web universal resource locators (URLs);
   xiv. internet protocol (IP) address numbers;
   xv. biometric identifiers, including finger and voice prints; and
   xvi. full face photographic images and any comparable images.

B. Requirement for Data Use Agreement for Uses or Disclosures of Limited Data Sets: Covered Entity may use or disclose a limited data set if Covered Entity enters into a data use agreement with the limited data set recipient that meets the requirements for data use agreements outlined below. Disclosures of a limited data set are exempt from Section XXI, Accounting of Disclosures of PHI.

C. Permitted Uses or Disclosures:

   i. Covered Entity may use or disclose a limited data set only for the purposes of research, public health, or health care operations.

   ii. Covered Entity may use or disclose a limited data set if it obtains satisfactory assurances, in the form of a data use agreement that meets the requirements in (E), below, that the limited data set recipient will only use and disclose the PHI for limited purposes.

D. Creation of Limited Data Sets: Covered Entity may use PHI to create a limited data set, or disclose PHI only to a business associate for purposes of creating a limited data set, whether or not the limited data set is to be used by Covered Entity.

E. Data Use Agreement Requirements: A data use agreement between Covered Entity and the limited data set recipient must:

i. establish the permitted uses and disclosures of such information by the limited data set recipient, consistent with the listed permitted purposes above. The data use agreement may not authorize the limited data set recipient to use or further disclose the information in a manner that would violate the HIPAA Privacy Rule if the further use or disclosure was instead done by Covered Entity;

ii. establish who is permitted to use or receive the limited data set; and

iii. provide that the limited data set recipient will:

a. not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

b. use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

c. report to Covered Entity any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

d. ensure that any agents, including subcontractors, to whom it provides the limited data set agree to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and

e. not identify the information or contact the individuals.

F. Creation and Maintenance of Data Use Agreements: Data use agreements will be created and maintained by the HIPAA Privacy Officer.

G. Compliance:

i. If Covered Entity knows of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the data use agreement, Covered Entity must take the following actions:

a. notify the HIPAA Privacy Officer,

b. take reasonable steps to cure the breach or end the violation, as applicable, and

c. if such steps were unsuccessful:

1. discontinue disclosure of PHI to the recipient; and

2. report the problem to the HIPAA Privacy Officer, who must report the problem to the HHS Secretary.

ii. If Covered Entity is the recipient of a limited data set, it must adhere to the data use agreement.

XIX. Mitigation after an Improper Use or Disclosure of PHI

Covered Entity should take steps to mitigate the risk to the individual who has had his/her PHI used or disclosed other than as permitted by the HIPAA Privacy Rule. If the risk to the individual has been mitigated, and Covered Entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment, the improper acquisition, access, use, or disclosure may not constitute a breach.

Mitigation measures that Covered Entity may take include, but are not limited to, the following:

A. Taking operational and procedural corrective measures to remedy violations;

B. Implementing additional administrative, technical, and physical safeguards to secure and protect PHI;

C. Re-training employees as necessary;

D. Taking employment actions to reprimand or discipline employees as necessary, up to and including termination;

E. Addressing problems with business associates (per the provisions of the Business Associate Agreement) once Covered Entity is aware of a breach of the agreement;

F. Creating new HIPAA policies, as appropriate; and

G. Incorporating mitigating solutions into Covered Entity HIPAA policies and procedures, as appropriate.

XX. Discipline and Sanctions for Improper Use or Disclosure of PHI

Covered Entity must apply appropriate sanctions against workforce members who fail to comply with this Policy.

A. Workforce members may be subject to discipline, up to and including termination, depending on the severity of a workforce member's failure to comply with this Policy. Workforce members are similarly subject to discipline for violations of any provision of HIPAA, HITECH, or the federal rules that implement those laws.

B. The HIPAA Privacy Officer will document disciplinary actions taken as a result of a violation of this Policy. See sample documentation log in Appendix B. Documentation of discipline or sanctions must be maintained for six years.

XXI. Accounting of Disclosures of PHI

As stated in Covered Entity Notice of Privacy Practices, individuals have the right to receive a report of the certain disclosures of PHI. Individuals should complete the form in Appendix E (page 48). Covered Entity should complete the Appendix E form on page 49.

A. Right to an Accounting of Disclosures: An individual has the right to receive an accounting of PHI made by Covered Entity in the six years prior to the date on which the accounting is requested. An individual may request an accounting of disclosures for a period of time less than six years from the date of the request.

B. Accounting of Disclosures: Covered Entity must account for disclosures of PHI for the six years prior (or such shorter time period at the request of the individual), except for disclosures:

   i. To carry out treatment, payment, and health care operations;

   ii. To individuals requesting their own PHI;

   iii. Incident to a use or disclosure otherwise permitted or required by the Privacy Rule;

   iv. Pursuant to an authorization;

   v. To persons involved in the individual's care or other notification purposes;

   vi. For national security or intelligence purposes;

   vii. To correctional institutions or law enforcement officials; or

   viii. As part of a limited data set;

   ix. That occurred prior to the date that compliance with HIPAA Privacy Rule was required.

C. Temporary Suspension of an Individual's Right to Receive an Accounting:

   i. Pursuant to written statement: Covered Entity 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 Covered Entity 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.

ii. Pursuant to oral statement: If the agency or official statement described above is made orally, Covered Entity must:

a. document the statement, including the identity of the agency or official making the statement;

b. temporarily suspend the individual's right to an accounting of disclosures subject to the statement; and

c. limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement, as described in (i), is submitted during that time.

D. Content of the Accounting of Disclosures: Except as provided below for multiple disclosures and disclosures for a particular research purpose, Covered Entity must provide the individual with a written accounting of disclosures that must include:

i. The disclosures of PHI that occurred in the six years (or such shorter time period at the request of the individual) prior to the date of the request for an accounting, including disclosures to or by business associates of Covered Entity;

ii. The date of the disclosure;

iii. The name of the entity or person who received PHI and, if known, the address of such entity or person;

iv. A brief description of the PHI disclosed; and

v. A brief statement of the purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or, in place of such a statement, if applicable, a copy of a written request for a disclosure:

a. required by the HHS Secretary under 45 C.F.R. Part 160, subpart C, to investigate or determine Covered Entity' compliance with the HIPAA Privacy Rule; or

b. for which an authorization or opportunity to agree or object is not required.

E. Multiple Disclosures: If, during the time period of the accounting, Covered Entity has made multiple disclosures of PHI to the same person or entity for a single purpose under the requirement for disclosures to the HHS Secretary or when an authorization or opportunity to agree or object was not required, the accounting may, with respect to multiple disclosures, provide:

i. The information required under (D), above, for the first disclosure during the accounting period;

ii. The frequency, periodicity, or number of the disclosures made during the accounting period; and

iii. The date of the last such disclosure during the accounting period.

F. Accounting for Research Disclosures:

i. If, during the time period of the accounting, Covered Entity has made disclosures of PHI for a particular research purpose as permitted under 45 C.F.R. § 164.512(i) for 50 or more individuals, the accounting may provide the following for disclosures for which the individual's PHI may have been included:

a. The name of the protocol or other research activity;

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

c. A brief description of the type of PHI that was disclosed;

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

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

f. A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or other research activity.

ii. If Covered Entity provides an accounting for research disclosures, and if it is reasonably likely that the individual's PHI was disclosed for such research protocol or activity, Covered Entity shall assist the individual (at his/her request) in contacting the entity that sponsored the research and the researcher.

G. Time Limits for Responding to Requests: Covered Entity must act on the individual's request for an accounting, no later than 60 days after receipt of such a request, as follows:

i. Provide the individual with the accounting requested; or

ii. If Covered Entity is unable to provide the accounting within the 60 days, Covered Entity may extend the time to provide the accounting by no more than 30 days, provided that:

a. Covered Entity, within the time limit of 60 days, provides the individual with a written statement of the reasons for the delay and the date by which Covered Entity will provide the accounting; and

b. Covered Entity may have only one such extension of time for action on a request for an accounting.

H. Fees for Accounting:

i. First Request in 12-Month Period: Covered Entity must provide the first accounting to an individual in any 12-month period without charge.

ii. Subsequent Requests: Covered Entity may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, provided that Covered Entity informs the individual in advance of the fee and provides the individual with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

I. Documentation of Accounting Requests: Covered Entity must document, and retain for six years:

i. The information required in (D) above for the disclosures that are subject to an accounting;

ii. The written accounting that is provided to the individual; and

iii. That the HIPAA Privacy Officer is responsible for receiving and processing requests for an accounting of disclosures. This is also documented in Covered Entity Notice of Privacy Practices.

XXII. Requests for Restricting Uses and Disclosures and for Confidential Communications

Individuals may seek restrictions on how their PHI is used and disclosed and where their communications may be sent or received.

A. Permitted Restrictions: Covered Entity must permit an individual to request that Covered Entity restrict:

   i. Uses and disclosures of PHI about the individual to carry out treatment, payment, or health care operations.

   ii. Disclosures for involvement in the individual's care and notification purposes, as outlined in Section X, Use and Disclosure of PHI to Family and Friends and for Notification Purposes.

   iii. Individual should make such requests on the form in Appendix E (pages 57-58); Covered Entity should document its response on the form on page 59.

B. Documentation: If Covered Entity agrees to a restriction on uses or disclosures of PHI, Covered Entity must document the restriction in the individual's electronic medical record and/or other files maintained on the individual.

C. Restrictions Related to Out-of-Pocket Payments in Full: Covered Entity is required to agree to a restriction that meets the following criteria:

   i. the individual requests that Covered Entity restrict the disclosure of PHI about the individual to a health plan;

   ii. the disclosure is for the purpose of carrying out payment or health care operations (not treatment) and is not otherwise required by law; and

   iii. 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 Covered Entity in full.

D. Exceptions for Certain Uses and Disclosures: A restriction agreed to by Covered Entity is not effective to prevent:

   i. uses and disclosures required by the HHS Secretary under 45 C.F.R. Part 160, Subpart C, to investigate or determine Covered Entity compliance with the HIPAA Privacy Rule; and

   ii. uses and disclosures for which an individual's authorization or opportunity to agree or object is not required.

E. Exception for Emergency Treatment: If Covered Entity agrees to a restriction on uses and disclosures of PHI, Covered Entity may not use or disclose PHI in violation of such restriction, unless the individual who requested the restriction is in need of emergency treatment and the restricted PHI is needed to provide the emergency treatment.

i. In such a situation, Covered Entity may use the restricted PHI itself or may disclose such restricted PHI to a health care provider to provide such treatment to the individual.

ii. If the restricted PHI is disclosed to another health care provider for emergency treatment under such a situation, Covered Entity must request that the health care provider not further use or disclose the PHI.

F. Termination of a Restriction: Covered Entity may end a restriction if:

i. the individual agrees to or requests the termination of the restriction in writing;

ii. the individual orally agrees to the termination and the individual's oral agreement of the termination of the restriction is documented by Covered Entity; or

iii. Covered Entity informs the individual that it is terminating its agreement to the restriction.

a. Covered Entity termination of the restriction will be effective only with respect to the PHI that Covered Entity created or received after Covered Entity informed the individual that it was terminating its agreement to the restriction.

b. Covered Entity may not terminate a restriction related to out-of-pocket payments in full that meet the criteria for restrictions of PHI in (C), above.

G. Requests for Confidential Communications at Alternate Locations:

i. Covered Entity must permit individuals to request and must accommodate reasonable requests by individuals to receive communications of PHI from the covered health care provider by alternative means or at alternate locations (e.g., work phone number, relative's address).

ii. Covered Entity 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.

iii. Covered Entity may require the individual to make a request for a confidential communication in writing. Individuals should make such requests on the form in Appendix E (page 60); Covered Entity should document its response on the form on page 61.

iv. Covered Entity may condition the provision of a reasonable accommodation on:

a. when appropriate, information as to how payment, if any, will be handled; and

b. specifications of an alternative address or other method of contact.

XXIII. Access and Denial of an Individual's Request for PHI

A. An individual has a right to inspect and obtain a copy, at his/her expense, of the PHI about the individual in a designated record set, for as long as the PHI is maintained in the designated record set, except for:

i. information compiled in reasonable anticipation of, or for use in, civil, criminal, or administration actions or proceedings; and

ii. PHI maintained by Covered Entity that is subject to the Clinical Laboratory Improvements Amendments Act of 1988, to the extent the provision of access would be prohibited by law, or exempt from that Act, under 42 C.F.R. § 493.3(a)(2).

B. Access of PHI:

i. If Covered Entity does not maintain the PHI that is the subject of the patient's request for access, and Covered Entity knows where the requested information is maintained, Covered Entity must inform the individual where to direct the request for access.

ii. The individual must make the request in writing. Covered Entity may supply the individual with the "Request for Access to Protected Health Information" form located in Appendix E (pages 50-51).

iii. Covered Entity must act on a request for access no later than 30 days after receipt of the request. Covered Entity shall:

a. Make the information available, in full or in part, for examination; or

b. Inform the authorized requester if the information does not exist, cannot be found, or is not yet complete. Upon completion or location of the information, Covered Entity must notify the individual.

c. The response to the request for access may be made on the "Response to Request for Access to Protected Health Information" form located in Appendix E (pages 52-53).

iv. If access is granted, in whole or in part, Covered Entity must comply with the following requirements:

a. Covered Entity must provide the individual access to his/her PHI in the designated record set, including inspection or receiving a copy, or both. 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, Covered Entity need only produce the PHI once in response to a request for access.

b. Covered Entity must provide the individual with access to the PHI in the form or format requested by the patient, if readily producible in such form or format; or if not, in a readable hard copy form or such other form or format as agreed to by both parties.

c. Covered Entity may provide the individual with a summary of the PHI requested, in lieu of providing access to the PHI, or may provide an explanation of the PHI to which access has been provided, if:

1. The individual agrees in advance to such a summary or explanation; and

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

d. Covered Entity must provide the access as requested by the individual in a timely manner, including arranging with the patient for a convenient time and place to inspect or receive a copy of the PHI, or mailing a copy of the PHI at the individual's request. Covered Entity 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.

e. If the individual requests a copy of the PHI or agrees to a summary or explanation of such information, Covered Entity may impose a reasonable, cost-based fee.

f. If the individual cannot pay the above fees, Covered Entity may offer the individual the right to inspect his/her designated record set at a time convenient for Covered Entity.

C. Denial of PHI

i. Covered Entity may deny an individual's request without providing an opportunity for review when:

a. One of the exceptions listed in (A) above applies;

b. Covered Entity is acting under the direction of a correctional institution and the inmate's request to obtain a copy of PHI would jeopardize the health, safety, or rehabilitation of the inmate or of other inmates, or the safety of any officer, employee, or other person at the correctional institution, or a person responsible for transporting the inmate;

c. The individual agreed to a temporary denial of access to PHI created or obtained by Covered Entity in the course of research that includes treatment when the individual consented to participate in the research, Covered Entity informed the individual that the right of access will be reinstated upon completion of the research, and the research is in progress;

d. The PHI is contained in records that are subject to the Privacy Act of 1974, 5 U.S.C. §552a, and the denial of access meets the requirements of that law; or

e. The PHI was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

ii. Covered Entity may also deny an individual access for other reasons, provided that the individual is given a right to have such denials reviewed under the following circumstances:

a. A licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person;

b. The PHI makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to such other person; or

c. The request for access is made by the individual's personal representative and a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.

iii. If access is denied on a ground permitted above, the individual has the right to have the denial reviewed by the HIPAA Privacy Officer. Covered Entity must provide or deny access in accordance with the determination of the reviewing official.

iv. If Covered Entity denies access, in whole or in part, to PHI, Covered Entity must comply with the following requirements:

a. Covered Entity must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI to which Covered Entity denied access.

b. Covered Entity must provide a timely, written denial to the individual, in plain language and containing:

1. The basis for the denial;

2. If applicable, a statement of the individual's review rights, including a description of how the patient may exercise such review rights; and

3. A description of how the individual may complain to Covered Entity pursuant to the Privacy Complaint Policy in Section XXV.

4. If the individual has requested a review of a denial, Covered Entity must promptly refer the request to the HIPAA Privacy Officer. The HIPAA Privacy Officer must determine, within a reasonable period of time, whether or not to deny the access requested based on the standards discussed above. Covered Entity must promptly provide written notice to the patient of the findings of the HIPAA Privacy Officer and take other action as required to carry out the HIPAA Privacy Officer's determination.

D. Designated Record Sets Maintained by Covered Entity:

i. A designated record set is defined as a group of records that is maintained by or for Covered Entity that is:

a. medical and billing records about individuals maintained by or for Covered Entity;

b. the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or

c. used, in whole or in part, by or for Covered Entity to make decisions about individuals.

ii. Covered Entity maintains patient PHI in the following designated record sets:

a. See Appendix D.

iii. Covered Entity maintains other sets of records regarding its workforce members that do not include patient PHI, including: See Appendix D.

E. Documentation: The HIPAA Privacy Officer or his designee(s) is responsible for receiving and processing requests for access by individuals and retaining documentation for six years from the date of the request for access.

XXIV. Requests to Amend PHI

An individual may request an amendment of certain information maintained by Covered Entity. Individuals should make their requests and Covered Entity should document its response on the form in Appendix E.

A. Right to Amend: An individual has the right to have Covered Entity amend PHI or a record about the individual in a designated record set for as long as the PHI is maintained in the designated record set.

B. Denial of Amendment Request: Covered Entity may deny the individual's request for amendment (see F, below), if Covered Entity determines that the PHI or record that is the subject of the request:

i. Was not created by Covered Entity, 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;

ii. Is not part of the designated record set;

iii. Would not be available for inspection under Section XXIII, Access and Denial of an Individual's Request for PHI; or

iv. Is accurate and complete.

C. Individual's Request for Amendment:

i. The individual must make the request to amend PHI in writing with a reason to support a requested amendment.

ii. Covered Entity has notified individuals in its Notice of Privacy Practices that requests for an amendment of your PHI should be made in writing to the HIPAA Privacy Officer.

D. Timely Action: Covered Entity must act on the individual's request for an amendment no later than 60 days after receipt of such a request. If Covered

Entity is unable to act on the amendment within the required 60 day time limit, Covered Entity may extend the time for such action by no more than 30 days, provided that:

i. Covered Entity provides the individual with a written statement of the reasons for the delay and the date by which action on the request will be completed by Covered Entity; and

ii. Covered Entity may have only one such extension of time for action on a request for an amendment.

E. If the requested amendment is granted, in whole or in part:

i. Covered Entity must 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 appending or otherwise providing a link to the location of an amendment.

ii. Covered Entity must inform the individual in a timely manner that the amendment is accepted and obtain the individual's identification of an agreement to have Covered Entity notify the relevant persons with which the amendment needs to be shared.

iii. Covered Entity must make reasonable efforts to inform and provide the amendment within a reasonable time, to:

a. Persons identified by the individual as having received PHI about the individual and needing the amendment; and

b. Persons, including business associates, that Covered Entity knows have the PHI that is the subject of the amendment and that may have relied, or could foreseeably rely, on such information to the detriment of the individual.

F. If the requested amendment is denied, in whole or in part:

i. Covered Entity must provide the individual with a timely, written denial. The denial must use plain language and must contain:

a. The basis for the denial, in accordance with (B), above;

b. The individual's right to submit a written statement disagreeing with the denial and how the individual may file such a statement;

c. A statement that, if the individual does not submit a statement of disagreement, the individual may request that Covered Entity provide the

individual's request for amendment and the denial with any future disclosures of the PHI that is the subject of the amendment; and

d. A description of how the individual may complain to Covered Entity or the HHS Secretary, in accordance with the Section XXV, Privacy Complaint Policy. The description must include the Privacy Officer's name or title and the telephone number of the Privacy Officer or the HIPAA hotline.

ii. Covered Entity must permit the individual to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. Covered Entity may reasonably limit the length of a statement of disagreement.

iii. Covered Entity may prepare a written rebuttal to the individual's statement of disagreement. Whenever such a rebuttal is prepared, a copy of the rebuttal must be provided to the individual who submitted the statement of disagreement.

G. Documentation: The HIPAA Privacy Officer or his designee(s) is responsible for receiving and processing requests for amendments by individuals and retaining documentation for six years from the date of the amendment.

XXV. Privacy Complaint Policy

A. A person who believes Covered Entity or business associate is not complying with the HIPAA Privacy Rule may file a complaint with the HHS Secretary or Covered Entity HIPAA Privacy Officer.

B. If a customer makes a privacy-related complaint or complains about Covered Entity handling of PHI, the complaint must be forwarded to the HIPAA Privacy Officer.

i. The Privacy Officer shall document the complaint and its resolution and retain the records for a minimum of six years. See Appendix C for a sample complaint log.

ii. The Privacy Officer shall investigate the alleged privacy violations.

iii. The Privacy Officer shall suggest corrective actions and make reasonable efforts to mitigate the situation, to the extent practicable.

iv. If applicable, the Privacy Officer shall follow Covered Entity HIPAA Protected Health Information Breach Investigation and Notification Policy and Procedures.

C. If applicable, Covered Entity may discipline its workforce member(s), pursuant to Section XX, Discipline and Sanctions for Improper Use or Disclosure of PHI.

XXVI. Non-Retaliation Policy

A. All Covered Entity employees are allowed to freely discuss and raise questions to the HIPAA Privacy Officer, supervisors, or the appropriate personnel about situations they feel are in violation of federal, state, or local law or regulations; this Policy; or other Covered Entity HIPAA policies.

B. Covered Entity shall not require an individual to waive his or her rights under federal health privacy, enforcement, or breach regulations as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits from Covered Entity.

C. Covered Entity shall not intimidate, threaten, coerce, harass, discriminate against, or take any other retaliatory action against any individual or other person for:

   i. exercising, or attempting to exercise, his or her rights under the HIPAA Privacy Rule;

   ii. filing a complaint, report, or incident report regarding the privacy and/or confidentiality of PHI;

   iii. testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing regarding the privacy and/or confidentiality of PHI;

   iv. opposing any act or practice made unlawful by the federal health privacy, security, and breach regulations, provided the:

      a. individual or person has a good faith belief that the practice opposed is unlawful,

      b. the manner of opposition is reasonable, and

      c. the manner of opposition does not involve a disclosure of PHI in violation of the HIPAA Privacy Rule;

   v. otherwise participating in compliance efforts with the HIPAA Privacy Rule.

D. Workforce members of Covered Entity shall immediately report, in good faith, to the HIPAA Privacy Officer or Covered Entity management:

   i. any knowledge of a violation of federal health privacy laws or the HIPAA Privacy Rule;

ii. any knowledge of a violation of this Policy or Covered Entity HIPAA policies; or

iii. any knowledge of a violation of this Policy on non-retaliation and non-waiver of rights.

E. If the HIPAA Privacy Officer or Covered Entity receives information that this Policy may have been violated, the report of retaliation shall be investigated promptly by the HIPAA Privacy Officer.

F. Covered Entity workforce members who violate this Policy must be sanctioned in accordance with Section XX, Discipline and Sanctions for Improper Use or Disclosure of PHI.

XXVII. Effective Date

Covered Entity HIPAA Privacy Rule Policy and Procedures shall become effective February 1, 2018.

XXVIII. Revisions

A. Frequency of Revisions: This Policy may be changed at any time.

B. Necessity of Revisions: This Policy, and any measures implemented under it, shall be reviewed and modified as needed. This Policy will be updated to reflect changes in federal law, regulations, or HHS guidance.

C. Documentation of Revisions: Revisions to this Policy must be documented.

D. Maintenance of Prior Versions of Policy: The HIPAA Privacy Officer must keep the previous version of the Policy for six years from the date the Policy was last in effect.

Appendix A. Workforce Access to PHI

A. NUHS has identified the following persons or classes of persons in the NUHS workforce who need access to PHI to carry out their duties.

Name	Position
Theodore Johnson	Dean of Clinics
Bambi Jackson	Administrative Assistant, Deans of Clinic and Research
Anna Jurik	DC Clinician -IL
Tari Reinke	DC Clinician -IL
Sonia Joubert	DC Clinician -IL
Andrew Serlin	DC Clinician -IL
Frank Frydrych	DC Clinician -IL - locum tenens
Stephanie Durocher	DC Clinician -FL
Addison Ozakyol	DC Clinician - FL -
Brett Martin	Faculty Practice - IL
Carlos Guadagno	Faculty Practice - FL
Jennifer Green	ND Chief Clinician
Patricia Coe	ND Clinician; Massage Supervisor; Faculty Practice - IL
Fraser Smith	ND Assistant Dean, locum tenens
Gregory Cramer	Dean of Research
Judy Pocius	Research Coordinator
Jocelyn Faydenko	Research Instructor

Vacant	Research Assistant
Vacant	Clinical Research Fellow
Hyundo Kim	AHM Assistant Dean
Nakiesha Pearson	DC – Assistant Dean

David Mayer	AHM Chief Clinician
Sarah Montesa	AHM Clinician
Zhanxiang Wang	AHM Clinician ; Faculty Practice
Jennifer Gantzer	Faculty Practice - FL
Jodi Perrin	Faculty Practice - IL
Yihyun Kwon	AHM Clinician - locum tenens
William Bogar	Chair, Diagnostic Imaging
Yuri Korvatko	Diagnostic Imaging, instructor
Ayla Osborn	Diagnostic Imaging Resident
Lorae Kornaus	Comptroller

Shirley Raychel	Florida Clinic
Agnielis Amezquita-Pizzaro	Lombard Clinic
Mary Harris-Adams	Lombard Clinic
Micah Lavendar	Florida Clinic
Kathleen Van Dussen	Florida Clinic
Contrice Tyler	Lombard Clinic Temp

B. Each class of persons listed above receives HIPAA training from NUHS.

C

Appendix B. Discipline Log

Name of Workforce Member	Date and Type of Incident	Type of Discipline	Date of Discipline
Example: John Doe	*12/1/14; failure to lock doors upon going home for the evening*	*Formal written reprimand; probation for 90 days*	*12/7/14*

Appendix C. Complaint Log

NUHS is required to provide a process for individuals to make complaints concerning NUHS policies and procedures required by HIPAA and HITECH and its compliance with such policies and procedures or the HIPAA and HITECH requirements.

#	Date	Location	Description of Complaint	Disposition of Complaint
Exam -ple	*12/1/14*		*Customer Jane Doe complained that the reception area is not private enough and that you can overhear conversations with the clinician.*	
1				
2				
3				
4				
5				
6				
7				
8				
9				

Appendix D. Designation of HIPAA Officials and Record Sets

I. Documentation:

The HIPAA Privacy Officer will keep documentation of the designations below for six years from the date of the designation or the date when the designation was last in effect, whichever is later.

II. Designation of Privacy Official:

On November 1, 2017, NUHS designated Theodore Johnson as the HIPAA Privacy Officer who is responsible for the development and implementation of this Policy and the policies and procedures required by the Privacy Rule. Theodore Johnson may consult with legal counsel as needed to develop, modify, and implement this Policy and the HIPAA Privacy Rule's required policies and procedures.

III. Designation of Contact Person or Office for Receiving Complaints:

Theodore Johnson, Dean of Clinics, HIPAA Privacy Officer
200 East Roosevelt Rd.
Lombard, Illinois 60148
tjohnson@nuhs.edu
(630)889-6513

IV. Designation of Security Official:

On June 1, 2017, NUHS designated Ron Mensching, Vice President of Business Services, as the security official who is responsible for the development and implementation of the policies and procedures required by the HIPAA Security Standards for the Protection of Electronic Protected Health Information.

Ron Mensching, Vice President for Business Services, HIPAA Security Officer
National University of Health Sciences
200 E. Roosevelt Rd.
Lombard, Illinois 60148
(630) 889-6606

Appendix E. Forms

1. Notice of Privacy Practices Acknowledgment
2. Authorization for Release of Protected Health Information
3. Request for an Accounting of Certain Disclosures of Protected Health Information
4. Response to Request for Accounting
5. Request for Access to Protected Health Information (2 pages)
6. Response to Request for Access to Protected Health Information (2 pages)
7. Request for Amendment of Protected Health Information (2 pages)
8. Response to Request for an Amendment
9. Request for Restriction on Use or Disclosure of Protected Health Information (2 pages)
10. Response to Request for Restriction
11. Request for Confidential Communications
12. Response to Request for Confidential Communications

NUHS Notice of Privacy Practices Acknowledgment

I have been presented with National University of Health Sciences' Notice of Privacy Practices.

Signature of Patient or Personal Representative Date

Acuse de Recibo

Por medio de la presente hago constar que he recibido una copia de la Notificación de las Prácticas de Privacidad de NUHS.

Firma del Paciente o Representante Personal Fecha

Patient Refused to Sign

Patient refused to sign acknowledgment.

Signature of NUHS Representative Title Date

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

Individual's Name:	**Date of Birth:**
Street Address:	**City, State and Zip:**
Telephone Number: **Circle One: Work Home Mobile**	

I authorize the use and disclosure of my protected health information as described below:

1. The following organization and its workforce members are authorized to make the requested use or disclosure:
   Any NUHS location.

2. NUHS is authorized to use or disclose my protected health information to the following person(s) or organization(s):

_____
Name of Organization or Person Telephone Number Fax Number

_____
Address

_____
City State Zip

3. The protected health information that may be used and disclosed is as follows:

___ Billing History ___ Prescription Records ___ Counseling Notes ___ Vaccination Records

___ Specialty ___ Entire Medical Record ___ Records for the following dates: _____

___ Other instructions: _____

4. I understand that if I indicate below, this information may include the following:

___ Sexually Transmissible Infection Results or Treatment ___ HIV/AIDS Results or Treatment ___ Mental Health Treatment

___ Alcohol Treatment ___ Drug Treatment/Evaluation ___ Domestic Violence History

5. These records shall be used for the purpose of: _____
   (For example, litigation, taxes, or individual request.)

6. Date or event on which this authorization expires: _____

7. I understand that:
   - I have the right to revoke this authorization in writing at any time by sending written notification to:
     HIPAA Privacy Officer, National University of Health Sciences, 200 E Roosevelt Rd, Lombard, IL 60148.
   - Revoking this authorization shall have no effect on disclosures made before the withdrawal of the authorization.
   - NUHS may not condition treatment, payment, enrollment or eligibility for benefits on this authorization or my refusal to sign such authorization.
   - I may ask for a copy of this authorization.
   - The information disclosed pursuant to the authorization may be subject to redisclosure by the recipient and no longer protected by federal privacy rules.

8. Signature of Individual: _____ Date: _____

9. If this request is by a personal representative, complete the following:

Personal Representative's Name: _____

Description of Authority to Act on Individual's Behalf (i.e., parent/guardian): _____

REQUEST FOR AN ACCOUNTING OF CERTAIN DISCLOSURES OF PROTECTED HEALTH INFORMATION

I. INDIVIDUAL DATA

Individual's Name:	**Date of Birth:**
Street Address:	**City, State and Zip:**
Telephone Number: **Circle One: Work Home Mobile**	

II. NATURE OF REQUEST FOR AN ACCOUNTING

I hereby request to receive an accounting of all disclosures made of my protected health information for reasons other than those expressly excluded from this accounting requirement by the HIPAA Privacy Rule.

CHECK ONE:

☐ All disclosures (that are not excluded) made during the six (6) year period prior to the date of this request.

☐ All disclosures (that are not excluded) made during the following time period:

_____.

III. CONDITIONS GOVERNING THE REQUEST FOR AN ACCOUNTING

A. Under the HIPAA Privacy Rule, National University of Health Sciences ("NUHS") and its Business Associates are required to provide an accounting of certain disclosures of protected health information to individuals who request the accounting. However, the HIPAA Privacy Rule does not require NUHS to account for the following disclosures:

1. Disclosures made prior to the compliance date for HIPAA Privacy Rule;
2. Disclosures made for purposes of carrying out treatment, payment, or health care operations;
3. Disclosures made to the individual regarding his/her protected health information;
4. Incidental disclosures made pursuant to the HIPAA Privacy Rule;
5. Disclosures made pursuant to an authorization;
6. Disclosures made to persons involved in the individual's care or other notification purposes provided in the HIPAA Privacy Rule;
7. Disclosures for national security or intelligence purposes;
8. Disclosures made to correctional institutions or law enforcement; and
9. Disclosures made as part of limited data set.

B. NUHS may temporarily suspend the individual's right to receive an accounting of disclosures NUHS has made to a health oversight agency or a law enforcement official, if the agency or official has informed NUHS that such an accounting would be reasonably likely to impede the activities of such agency or official.

C. The individual is entitled to one free accounting for each twelve (12) month period. For any additional accounting requested within the same twelve (12) month period, NUHS may charge a reasonable fee for copy costs and mailing fees. If NUHS changes a fee, the individual will receive an estimate of such cost prior to receiving the accounting. If the individual chooses not to pay such costs, the request will be deemed cancelled.

Signature:_____

Date:_____

If this request is by a personal representative on behalf of the individual, complete the following:

Personal Representative's Name:_____

Description of Authority to Act on Individual's Behalf (i.e., parent/guardian):

RESPONSE TO REQUEST FOR ACCOUNTING

Individual's Name: _____

Date request for accounting received: _____

Accounting period from _____ to _____

If NUHS cannot provide the accounting within 60 days, date extension notice sent on: _____

Response date promised in extension notice (maximum 30 day extension): _____

Reason for extension:

_____

_____

If requested accounting is the second or greater accounting requested within the same twelve (12) month period, complete the following:

Date estimated charge communicated to individual:_____

Date individual: ☐ accepted charge ☐ rejected charge _____

Date accounting sent to individual: _____

Request For Accounting Is Suspended:

☐ Individual's right to receive an accounting of disclosures made to a health oversight agency or law enforcement official is temporarily suspended pursuant to the written notification received by NUHS from the agency or official. The suspension period expires on:_____.

Request For Accounting Is Denied:

The request for accounting is denied for the following reason(s):

- ☐ Disclosures made prior to the compliance date for HIPAA Privacy Rule;
- ☐ Disclosures made for purposes of carrying out treatment, payment or health care operations;
- ☐ Incidental disclosures made pursuant to the HIPAA Privacy Rule;
- ☐ Disclosures made pursuant to an authorization;
- ☐ Disclosures made to persons involved in the individual's care or other notification purposes provided in the HIPAA Privacy Rule;
- ☐ Disclosures made for national security or intelligence purposes;
- ☐ Disclosures made to correctional institutions or law enforcement officials; and/or
- ☐ Disclosures made as part of a limited data set.

The individual was notified of the denial on: _____

Signature of NUHS Representative:_____

Title:_____ Date:_____

REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

I. INDIVIDUAL DATA

Individual's Name:	**Date of Birth:**
Street Address:	**City, State and Zip:**
Telephone Number: **Circle One: Work Home Mobile**	

II. NATURE OF REQUEST FOR ACCESS

A. I wish: ☐ To inspect ☐ To have a copy of the following protected health information:

☐ My medical records ☐ My prescription records

☐ My billing and payment records ☐ My immunization records

☐ Any other protected health information used by NUHS to make medical decisions about me
Please describe.

_____

_____

___

B. I wish to receive a copy of the requested protected health information in the following format:

☐ Photocopies ☐ Electronic Format ☐ Email (if you would like to receive your information via email, you understand that NUHS will transmit the copies to you via a network that is not encrypted and there is some risk that the information in the email could be read by a third party)

C. In lieu of inspecting or obtaining a copy of my protected health information, I would prefer to receive the requested information in the form of a summary prepared by NUHS at an additional cost to me, if I agree to such cost.

☐ Yes ☐ No

D. In addition to inspecting and/or obtaining a copy of my protected health information, I request that NUHS prepare an explanation of the requested protected health information at an additional cost to me, if I agree to such cost.

☐ Yes ☐ No

I want you to mail copies of the requested information to the following address (I understand that NUHS will charge me for the postage):

_____

—

III. CONDITIONS GOVERNING THE REQUEST FOR ACCESS

A. Under the HIPAA Privacy Rule, NUHS and its Business Associates are required to permit an individual to inspect and obtain a copy of his/her protected health information that NUHS or its Business Associates maintain in a "designated record set." Under the HIPAA Privacy Rule, a designated record set is a group of records maintained by NUHS and its Business Associates that are the medical records and billing records about individuals maintained by or for NUHS and its Business Associates and any other records that may be used to make health care decisions about individuals.

B. The individual is not, however, entitled to inspect or obtain a copy of any information compiled in anticipation of or for use in any civil, criminal, or administrative proceeding and certain other records, even if such records are in a designated record set. Additionally, NUHS may deny requests for access as permitted by the HIPAA Privacy Rule.

C. The individual will be charged a fee for any copies made and a postage charge if copies are to be mailed to the individual. NUHS will calculate the charge of the individual's request and notify the individual of the amount due before NUHS processes the request. If the individual chooses not to pay the charge, the request for access will be considered cancelled. There is no charge to the individual to inspect his/her records on NUHS's premises.

Signature: _____

Date: _____

If this request is by a personal representative on behalf of the individual, complete the following:

Personal Representative's Name: _____

Description of Authority to Act on Individual's Behalf (i.e., parent/guardian): _____

RESPONSE TO REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

Individual's Name: _____

Date request for access received: _____

Date appropriate NUHS units and business associate(s) were directed to search for requested records:

_____

Extension notice sent on: _____

Response date promised in extension notice: _____

Reason for extension: _____

_____

Review of Request for Access:

The request for access has been reviewed by NUHS and is: ☐ Accepted ☐ Denied

Denial of Request for Access:

☐ Protected health information is not part of the designated record set.

☐ The requested information is not maintained by NUHS or its Business Associate(s).

☐ Federal law forbids making the requested information available to the individual for inspection.

☐ The requested information has been compiled for a legal proceeding in which NUHS is involved.

☐ The requested information was obtained from someone other than a health care provider under promise of confidentiality and access would be reasonably likely to reveal the source of the information.

☐ The requested information is temporarily unavailable because the individual is a research participant.

☐ Other (specify):_____

If denied, the denial is for one of the following *reviewable* reasons for denial:

☐ A licensed health care provider has determined that access to the requested information is reasonably likely to endanger the life or physical safety of the individual or others.

☐ A licensed health care provider has determined that the requested information identifies a third person who is not a health care provider and that substantial harm is a reasonably likely to occur if access to the information is granted.

☐ A licensed health care provider has determined that access to the requested information by the individual's personal representative is reasonably likely to cause substantial harm to the individual or others.

RESPONSE TO REQUEST FOR ACCESS TO PROTECTED HEALTH INFORMATION

Individual's Name: _____

Review of a Denial of Request for Access:

Individual requested a review of NUHS denial of access on: _____

A licensed health care professional examined the individual's request for review of a denial of access on:

_____

Result of the review is attached. ☐ Yes ☐ No

Request for Access Granted:

Access granted on_____ and notice of granted request for access sent to individual.

☐ Records inspected: _____

☐ Copies supplied: _____

Charges: $_____

Date paid:_____

Summary or explanation provided: _____

Charges: $_____

Paid:_____

Signature of NUHS Representative: _____

Title:_____

Date: _____

REQUEST FOR AMENDMENT OF PROTECTED HEALTH INFORMATION

I. INDIVIDUAL DATA

Individual's Name:	**Date of Birth:**
Street Address:	**City, State and Zip:**
Telephone Number:	**Circle One: Work Home Mobile**

II. NATURE OF REQUEST FOR AMENDMENT

A. I request NUHS to amend the following protected health information:

_____

_____

B. I request this amendment for the following reason(s):

_____

_____

C. The information should be amended as follows:

_____

_____

D. I want NUHS to notify the following persons who may have received my protected health information in the past of any amendment to my protected health information:

_____

_____

E. I agree that NUHS may provide my amended protected health information to the following Business Associates:
(1) Business Associates to whom NUHS has provided the protected health information that is the subject of the amendment request, and
(2) Business Associates from whom NUHS has received the protected health information that is the subject of the amendment request.

☐ Yes ☐ No

III. CONDITIONS GOVERNING THE REQUEST FOR AN AMENDMENT

A. Under the HIPAA Privacy Rule, NUHS and its Business Associates are required to permit an individual to request an amendment of his/her protected health information that he/she believes is inaccurate or incomplete.

REQUEST FOR AMENDMENT OF PROTECTED HEALTH INFORMATION

Individual's Name_____

B. NUHS may deny an individual's request if the protected health information:

1. Is not part of a designated record set (Under the HIPAA Privacy Rule, a designated record set is a group of records maintained by NUHS and its Business Associates that are the medical records and billing records about individuals maintained by or for NUHS and any other record that may be used to make health care decisions about individuals.);
2. Was not created by NUHS or its Business Associate(s);
3. Is complete and accurate;
4. Was compiled in anticipation of or for use in any civil, criminal, or administrative action or proceeding involving NUHS; or
5. Is not subject to disclosure to the individual under the Clinical Laboratory Improvements Amendments of 1988.

Signature: _____

Date: _____

If this request is by a personal representative on behalf of the individual, complete the following:

Personal Representative's Name: _____

Description of Authority to Act on Individual's Behalf (i.e., parent/guardian):

_____

RESPONSE TO REQUEST FOR AN AMENDMENT

Individual's Name: _____

Date request for amendment received: _____

If extension is needed, complete the following:

Extension notice sent on: _____

Response date promised in extension notice: _____

Reason given for extension:

_____

_____

Review of Request for Amendment

The request for correction or amendment has been: ☐ Accepted ☐ Denied

Request for Amendment Is Accepted

Date the individual notified of the acceptance of the request: _____

Date the persons or entities identified by the individual to receive the amendment protected health information were notified of the amendment: _____

Request for Amendment is Denied

The request for amendment was denied for the following reasons:

☐ The protected health information was not created by NUHS or its Business Associate(s).

☐ The protected health information is not part of a designated record set.

☐ The protected health information is accurate and complete.

☐ The protected health information is compiled in anticipation of or for use in any civil, criminal, or administrative action or proceeding in which NUHS is involved.

☐ The protected health information is not subject to disclosure under the Clinical Laboratory Improvements Amendments of 1988.

The individual was notified of the denial on: _____

Signature of NUHS Representative: _____

Title: _____ Date: _____

REQUEST FOR RESTRICTIONS ON USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION

I. INDIVIDUAL DATA

Individual's Name:	**Date of Birth:**
Street Address:	**City, State and Zip:**
Telephone Number:	**Circle One: Work Home Mobile**

II. NATURE OF REQUESTED RESTRICTION

I request NUHS or its Business Associate(s) to restrict the use and/or disclosure of the following protected health information:

☐ Restrict uses and/or disclosures of protected health information for purposes of payment or health care operation in the following manner:

_____

_____

_____

☐ Restrict disclosures to a family member, relative, or close personal friend who is involved with my health care. Please specify individual(s) to whom this restriction applies:

_____

_____

_____

☐ Restrict disclosures to a health plan for the purpose of carrying out payment or health care operations. Please specify the health plan and the health care item or service for which the individual, or person other than the individual's health plan, has paid NUHS out-of-pocket in full.

_____

_____

_____

_____

III. CONDITIONS GOVERNING THE REQUEST FOR RESTRICTIONS

A. Under the HIPAA Privacy Rule, NUHS and its Business Associate(s) are not required to agree to requests for restrictions unless the disclosure is for the purpose of carrying out payment or health care operations and is otherwise not required by law; and the protected health information pertains solely to health care item or service for which the individual, or person other than the health plan on behalf of the individual, has paid NUHS in full.

B. If NUHS or its Business Associate(s) agrees to the requested restriction (whether in its entirety or in part), then the restriction is in effect until one of the following events occurs:

1. You agree to, or request in writing, that the restriction be terminated; or
2. NUHS or its Business Associate(s) notify you of NUHS's (or its Business Associate's) termination of the agreement to restrict the uses and/or disclosures of protected health information.

C. If you agree to the termination of a restriction, then your protected health information will no longer be subject to the restriction. If NUHS or a Business Associate terminates the agreement to restrict, then the termination is effective only with respect to information created or received after the date of notice of the termination of the restriction.

D. You understand that if NUHS or its Business Associate(s) have agreed to a request for restriction, restricted protected health information still may be disclosed to provide emergency treatment, but that NUHS and its Business Associate(s) will not further use or disclose restricted protected health information for any other purpose.

E. You understand that you still have a right to access protected health information as allowed under the HIPAA Privacy Rule and any other applicable law.

F. You understand that you may receive an accounting of certain disclosures of protected health information as explained in the NUHS Notice of Privacy Practices.

G. You understand that restricted protected health information may still be disclosed for the purposes as stated in the Notice of Privacy Practices.

Individual Signature :_____

Date:_____

RESPONSE TO REQUEST FOR RESTRICTION

Individual's Name: _____

The request for restriction is: ☐ Accepted ☐ Denied

*If request is accepted *in part,* describe the restriction to be implemented:

_____

_____

_____

_____

_____

_____

Date restriction becomes effective: _____

Signature of NHS Representative:_____

Title:_____

Date:_____

REQUEST FOR CONFIDENTIAL COMMUNICATIONS

I. INDIVIDUAL DATA

Individual's Name:	**Date of Birth:**
Street Address:	**City, State and Zip:**

Telephone Number: **Circle One:** **Work** **Home** **Mobile**

II. NATURE OF REQUESTED RESTRICTION

I request NUHS or its Business Associate(s) communicate with me regarding my protected health information by the following alternative means or at the following alternative locations.

☐ At a telephone number other than my home number.

The telephone number at which I should be contacted at is: _____.

This telephone number is: ☐ Work ☐ Mobile ☐ Other (specify) _____

☐ At a mailing address other than my home mailing address.

The mailing address at which I should be contacted is:

_____
_____
_____.

☐ Through my e-mail address, rather than my home address. If you would like to receive your information via email, you understand that NUHS will transmit the copies to you via a network that is not encrypted and there is some risk that the information in the email could be read by a third party.

My e-mail address for purposes of contacting me is:

_____.

☐ Other. Please specify: _____
_____
_____.

III. CONDITIONS GOVERNING THE REQUEST FOR CONFIDENTIAL COMMUNICATIONS

Under the HIPAA Privacy Rule, NUHS and its Business Associate(s) are required to honor only *reasonable* Requests for Confidential Communications. NUHS and its Business Associate(s) may condition granting the request for reasonable accommodation upon the following:

A. Individual providing information concerning how payments will be handled; and

B. Individual specifying an alternative address or other method of contact.

Individual Signature: _____ Date: _____

RESPONSE TO REQUEST FOR CONFIDENTIAL COMMUNICATIONS

Individual's Name: _____

The request confidential communications has been reviewed by NUHS and is:

☐ Accepted ☐ Denied

*If request is accepted in part, describe the confidential communications to be implemented:

_____

_____

_____

Date confidential communication becomes effective: _____

Signature of NUHS Representative: _____

Title: _____

Date: _____