THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL PRIVACY OF PROTECTED HEALTH INFORMATION POLICY

I. INTRODUCTION

The privacy and confidentiality of personal information, including personal health information is addressed in a variety of state and federal regulations and University of North Carolina at Chapel Hill ("UNC-Chapel Hill") policies. This policy addresses the specific privacy obligations required by the Health Insurance Portability and Accountability Act of 1996, as modified by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HIPAA").

HIPAA's requirements apply to records of individually identifiable health information in the control of health care clearing houses, health plans, and health care providers that transmit any health information electronically to carry out financial or administrative transactions related to health care or health insurance. The individually identifiable health information in these records is called Protected Health Information ("PHI").

At the UNC-Chapel Hill, some units function as health care providers covered by HIPAA. These units are designated as "covered University units" because HIPAA covers the maintenance and transmission of patient PHI (in all forms, not just electronic) from the unit to any other person or entity, including the flow of PHI from these units' records to functions other than health care treatment. This coverage includes the flow of PHI from these records into research studies.

The UNC-Chapel Hill recognizes its obligation to safeguard PHI against unauthorized use or disclosure. This policy describes the HIPAA requirements for protection of the privacy of PHI.

This policy is applicable to all members of UNC-Chapel Hill faculty, staff, fellows, volunteers, trainees, agents and students who work or train in University units that maintain PHI. Faculty and staff members found to have violated this policy will be subject to disciplinary action, up to and including dismissal, under the applicable disciplinary policy. Students will be subject to disciplinary action under the applicable student policies and procedures.

Definitions provided in Section II. further explain the scope of this policy and provide meaningful guidance regarding its application.

II. DEFINITIONS

A. Authorization:

An authorization is a written permission for a defined use and/or disclosure of an individual's PHI for purposes other than treatment, payment and health care operations. An authorization must contain specific elements and must be approved by (1) the applicable unit's health information management department or (2) in the absence of such internal department, by the

University's Privacy Officer or (3) by the UNC-Chapel Hill Institutional Review Board (IRB) for disclosure and use of PHI in UNC-Chapel Hill research.

B. Business Associate:
A business associate is an external (non-University affiliated) person or entity that performs certain functions, activities or services on behalf of a covered University unit, and under a written contract typically referred to as a Business Associate Agreement, when that function, activity, or service involves the use and/or disclosure of PHI.

C. Covered University Unit:
A covered University unit performs the functions of a health care provider, employs health care providers, and transmits health information in electronic or conventional form in association with any of the financial or administrative transactions listed in the HIPAA regulations.

D. De-identified PHI:
De-identified PHI is personal health information that does not identify an individual and with respect to which there is no reasonable basis that the information can be used to identify an individual. De-identified PHI is not individually identifiable health information subject to HIPAA protections.

To be "de-identified", the following identifiers of the individual and the individual's relatives, employers, and household members must be removed from the PHI:

1. Names;
2. All geographical subdivisions smaller than a State;
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission/discharge dates, date of death; and for persons over eighty-nine years of age all dates including year;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers & serial numbers & license plates;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locaters (URLS);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images;
18. Any other unique identifying number, characteristic, or code except for secure re-identification or data matching codes that are not derived from information about the individual.

E. Individually Identifiable Health Information:
Individually Identifiable Health Information is information that is a subset of health

information, including demographic information collected from an individual, and:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   a) That identifies the individual; or
   b) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

F. Marketing:

Marketing is a communication intended to encourage the purchase of products or services. Except where the covered University unit receives direct or indirect payment from or on behalf of a third party whose product or service is being described in exchange for making the communication, marketing does not include communications to the individual:

1. to provide refill reminders or otherwise communicate about a current prescription;
2. to describe a health-related product or service (or payment for same) provided by the covered University unit, including communications about entities participating in a provider network or health plan network;
3. relating to their own treatment; or
4. relating to the case management or care coordination or to direct or recommended alternative treatments, therapies, health care providers, or setting of care to that individual.

G. Minimum Necessary:

The "minimum necessary" standard applies when using or disclosing PHI or when requesting PHI from another covered University unit or external entity. A covered University unit must make reasonable efforts to limit access (both internally and externally) to PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request except when releasing PHI as follows:

1. disclosures to or requests by a health care provider for treatment purposes;
2. uses or disclosures to the individual about himself/herself;
3. uses or disclosures –pursuant to an authorization;
4. disclosures to the Secretary of Health and Human Services for compliance investigation purposes;
5. uses or disclosures required by law;
6. uses or disclosures required for compliance with applicable requirements of the HIPAA Privacy Rule; and
7. disclosures for research with waiver of authorization by an IRB or Privacy Board.

H. Protected Health Information (PHI):

"Protected Health Information" or "PHI" is the term most commonly used in HIPAA to describe information protected from disclosure under the HIPAA privacy rules.

Protected Health Information is individually identifiable health information that is:

1. Transmitted by electronic media;
2. Maintained in electronic media; or
3. Transmitted or maintained in any other form or medium.

Protected Health Information excludes:

1. Education records covered by "FERPA";
2. Health care records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a healthcare provider and which are made or used only in connection with the treatment of the student, and are not available to anyone other than persons providing such treatment, except that such records can be reviewed by a physician or other appropriate professional of the student's choice. See 20 U.S.C. § 1232g(a)(4)(B)(iv);
3. Employment records even if they contain individually identifiable health information; or
4. Records regarding a person who has been deceased for more than 50 years.

I. Research:

Research is a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge. *Health care operations* studies are included in activities covered in consent for treatment, payment and health care operations and do not require authorization or waiver of authorization as research does. UNC-Chapel Hill quality assessment and improvement studies for outcomes evaluation and development of clinical guidelines are health care operations studies when they are applied to evaluation and assessment of UNC-Chapel Hill health care operations. Seek guidance from the UNC- Chapel Hill IRB when the scope or application of the health care operation study may be larger than UNC-Chapel Hill healthcare operations.

III. SCOPE

A. Applicability:

The policy applies to all units at The University of North Carolina at Chapel Hill that meet the definition of "covered University unit" in Section II. The University has further described its covered health care components in the ***"Statement on its Designation as a Hybrid Entity Under HIPAA".***

However, the UNC-Chapel Hill School of Medicine is not covered by this policy. The School of Medicine, its employees, students, and volunteers are covered under the "***Privacy and Confidentiality of Individually Identifiable Health Information Policy***" of the University of North Carolina Health Care System. This system includes UNC Hospitals, UNC Physicians & Associates, Rex HealthCare, and the clinical activities of the UNC School of Medicine.

HIPAA privacy requirements are focused on health information records maintained by health care providers, health care clearinghouses, and/or by health insurance plans. Although there are some units of the University that perform one or more covered functions, the University does not operate primarily as a health care provider or health insurance plan. For that reason, the University has determined that only those personal health information records maintained or transmitted in the provision of covered health care functions by units of the UNC- Chapel Hill, with the exception of the School of Medicine, shall be covered by this policy on "***Privacy of Protected Health Information Policy***".

Examples of personal health information records that are covered include appointment letters, medical charts, patient/client consents for treatment, and provider notes.

B. Exceptions to the HIPAA Privacy Requirements:
Statutory exceptions to HIPAA privacy requirements exist in limited and varied form. These may include court order, subpoena, or administrative procedures, as further defined below. If additional questions exist after reading this Policy, please consult the University's Office of University Counsel.

IV. PROCEDURE

Generally, PHI may not be used or disclosed except when at least one of the following conditions is true:

1. The individual who is the subject of the information has authorized the use or disclosure;
2. The individual who is the subject of the information has consented to the use and disclosure of their information for treatment, payment and health care operations purposes;
3. The disclosure is to the individual who is the subject of the PHI; and/or
4. The use or disclosure is required by federal or state law.

A. Notice of Privacy Practices:
After April 13, 2003, covered University units shall provide to each patient not later than the date of the first service delivery, including service transmitted electronically, a Notice of Privacy Practices ("NPP"). A copy of the NPP shall be posted by each covered University unit and copies shall be made available to patients upon request. Upon providing the copy of the NPP, each covered University unit must make a good faith effort to obtain a written acknowledgement of receipt by the patient and maintain the acknowledgement in the patient's medical record. If the patient refuses to acknowledge receipt of the NPP, each covered University unit must document such in the patient's medical record.

In the event of a material change to the uses or disclosures of PHI, individuals' rights, the covered University unit's legal duties, or other privacy practices stated in the NPP, each covered University unit shall promptly revise and distribute an updated NPP, post it in a clear and prominent location where it is reasonable to expect individuals seeking service to be able to read it, and have it available for individuals to request to take with them.

B. Authorization:
To use and/or disclose PHI for any purpose other than treatment, payment and health care operations, a covered University unit must obtain from the patient or authorized representative a signed and dated specific authorization, in a form approved or accepted by University's Privacy Officer or, for disclosure for use in a UNC-Chapel Hill research study, the authorization form approved by the UNC-Chapel Hill IRB. A covered University unit that obtains a signed authorization from a patient or his/her authorized representative must provide that individual with a copy.

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

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure;
3. The name or other specific identification of the person(s), or class of persons, to whom the covered University unit may make the requested use or disclosure;
4. A description of each purpose of the requested use or disclosure.
5. An expiration date or an expiration that relates to the individual or the purpose of the use or disclosure.
6. Signature of the individual and date. If the authorization is signed by a patient's authorized representative, a description of the representative's authority to act for the patient must also be provided.

Additionally, the authorization must contain statements that place the patient or his/her authorized representative on notice of the right to revoke his/her authorization, if there are any exceptions, and how to do it; when treatment, payment, enrollment or eligibility for benefits may be conditioned on signing the authorization; any consequences of not signing; and the potential for information disclosed to be re-disclosed by the recipient and no longer protected.

An authorization is not required where waived by the IRB, or as further enumerated in Section VI of this ***Policy***.

Other Uses and Disclosures:

1. **De-identified PHI** – De-identified PHI, as previously described in Section II, is not subject to HIPAA protections; therefore, no authorization is required for its use and/or disclosure.
2. **Marketing** – A covered University unit must obtain an individual's authorization for any use or disclosure of PHI for marketing, except in the following circumstances: a face-to-face encounter made by a covered University unit, or a marketing communication that concerns products or services of nominal value. Additionally, a covered University unit may make a marketing communication to an individual without authorization if it concerns health-related products and/or services of either the covered University unit or a third party if the communication identifies that the covered University unit is making the communication; clearly states whether the covered University unit has received or will receive direct or indirect payment for making the communication; and, except when the communication is included in a newsletter or similar type of general communication device distributed broadly, contains instructions describing how the individual may opt out of receiving such communications in the future.
3. **Fundraising** – UNC-Chapel Hill may use, without authorization, the following PHI for the purpose of raising funds: demographic information, dates of health care provided, department(s) of service, treating physician(s), outcome information, and health insurance status. Each fundraising solicitation will provide recipients a clear and conspicuous opportunity to elect not to receive any further fundraising communications. No covered University unit may condition treatment or payment on an individual's choice with respect to the receipt of fundraising communications.
4. **Business Associates** – A Business Associate may use or disclose PHI without authorization, but only as permitted or required by its Business Associate

Agreement with a covered University unit, or as otherwise required by law.

5. **Research –**
   a) **With Authorization** – Use and/or disclosure of PHI for research purposes generally requires the permission of the individual whose PHI will be used in research. Such permission must be in the form of an "authorization" as described above.
   b) **With Waiver of Authorization –** PHI may be used in research without an individual's authorization if a UNC- Chapel Hill Institutional Review Board or other Institutional Review Board (IRB) grants a waiver of the requirement for authorization.
   c) Other than with authorization or waiver of authorization –**Without Authorization or Waiver** – PHI may be used in certain research situations without an individual's authorization or an IRB waiver of authorization:
      i. Research use of a "Limited Data Set";
      ii. Research use of de-identified data;
      iii. Reviews preparatory to research; and
      iv. Research on decedent's information.

Verification of Identity – Prior to any disclosure of PHI, covered University units will verify both the identity of an individual requesting PHI and the authority of that individual to have access, if unknown, and will obtain any documentation, statements, or representations (oral or written) from the individual when required. The identity and authority of a public official may be verified by agency badges or other official credentials; written authorization on appropriate government letterhead; or, if the disclosure is to an individual acting on behalf of a public official, a written statement on appropriate government letterhead, or other evidence of documentation of agency, indicating the individual is acting under the government's authority. To verify the authority of the public official to request PHI, the covered University unit may rely on a written statement of the legal authority under which the PHI is requested, or if impracticable, an oral statement of the same. Covered University units may rely on the exercise of professional judgment and/or act on a good faith belief in making disclosures.

V. PATIENT MAY OPT OUT OF USE OR DISCLOSURE OF PHI.

PHI may be used or disclosed for the following purposes, if the patient or his/her authorized representative is informed in advance of the use or disclosure and has the opportunity to agree to, prohibit, or restrict, the use or disclosure:

A. Facility Directories:

Unless the patient objects, the following information can be used in the covered University unit's patient directory:

1. The patient's name;
2. The patient's location in the UNC Chapel Hill covered University unit;
3. The patient's condition described in general terms that do not give specific medical information about the patient (i.e. stable, critical, etc.); and
4. The patient's religious affiliation.

This directory information may be disclosed to:

1. Members of the clergy; and/or

2. Except for religious affiliation, to other persons who ask for the patient by name.

B. Family Members/Friends:

When the requirements of subsections 1 and 2 below are met, a covered University unit may (i) use or disclose to a family member, other relative, or close personal friend of the patient, or any other person identified by the patient, PHI directly relevant to such person's involvement with the patient's care or related payment; and (ii) use or disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the patient, or another person responsible for the care of the patient, of the patient's location, general condition, or death.

1. If the patient is present at the time of or prior to the use or disclosure and has the capacity to make decisions, the use or disclosure may be made if
   a) the patient's consent is obtained;
   b) the patient is provided with an opportunity to object and the patient does not object;
   c) it is reasonably inferred from the circumstances, using professional judgment, that the individual does not object to the disclosure.
2. If the patient is not present at the time of or prior to the use or disclosure, or the opportunity to object to the use or disclosure cannot practicably be provided due to the patient's incapacity, or in an emergency, the use or disclosure may be made if, using professional judgment, the disclosure is in the best interest of the patient. Only the PHI which is directly relevant to the person's involvement with the patient's health care may be disclosed. The covered University unit may use professional judgment and experience with common practice to make reasonable inferences regarding the patient's best interest in allowing a person to act on behalf of the patient to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of PHI, unless otherwise restricted by state law.

   The University and/or covered University unit may use or disclose PHI to a public or private entity authorized by law or its charter to assist in disaster relief efforts, for the purpose of coordinating with such entities the uses or disclosures permitted above. The requirements listed above apply to the extent that it is determined, using professional judgment, the requirements do not interfere with the ability to respond to the emergency circumstances.

   If the individual is deceased, a covered University unit may disclose relevant PHI to a family member, other relative, or a close personal friend of the individual, or any other person identified previously by the deceased individual who was involved in the individual's care or payment for health care prior to the individual's death, unless doing so is inconsistent with the individual's prior expressed preference that is known to the covered University unit.

   At the first point of contact with the patient or the legal representative, he/she must be informed of the proposed use and disclosure of this information, and of his/her right to prohibit or to restrict any of these used or disclosures. If the opportunity to prohibit or restrict any of these uses or disclosures cannot be provided to a patient due to incapacity or emergency, the information may be used or disclosed if the disclosure is consistent with a prior expressed preference by the patient, if any, that is known to the covered University unit, and the disclosure is determined, in the exercise of professional judgment, to be in the best interest of the patient. Under such circumstances, the patient must be informed and then allowed then allowed to prohibit or restrict such uses and

disclosures when it becomes practicable to do so.

VI. AUTHORIZATION NOT REQUIRED FOR USE AND/OR DISCLOSURE OF PHI

The following is a list of the types of uses and/or disclosures, which do not require consent, authorization or the opportunity to opt out. Notice of these is provided in designated units' Notices of Privacy Practices.

A. Disclosure required by law:
PHI may be used or disclosed if and to the extent required by law.

B. Public health activities:
PHI may be used or disclosed to a public health authority that is authorized by law to collect or receive such information for preventing or controlling disease, injury or disability, including public health issues, vital records, child or adult abuse or neglect; adverse food or drug events, and investigations of work-related illnesses or injuries as required under law.

C. Victims of abuse, neglect, or domestic violence:
PHI may be used or disclosed to a government authority, including a social service or protected service agency, which is investigating a report of abuse, neglect or domestic violence to the extent the disclosure is required or permitted by law.

D. Health oversight activities:
With certain exceptions, PHI may be used or disclosed to a health oversight agency for oversight activities authorized by law, including audits, civil, administrative or criminal investigations or proceedings, inspections, licensure or disciplinary actions, or other activities for oversight of the University or other government benefit or regulatory programs (i.e. JCAHO).

E. Judicial and Administrative Proceedings:
PHI may be disclosed in the course of a judicial or administrative proceeding in response to an order of a court or administrative tribunal, or a HIPAA compliant subpoena, discovery request or other lawful process.

F. Law Enforcement Purposes:
PHI may be disclosed for law enforcement purposes to comply with laws that require the reporting of certain types of wounds or physical injuries.

G. Decedents:
PHI regarding decedents may be disclosed to coroners, medical examiners and funeral directors if necessary to carry out the duties of their positions.

H. Cadaveric organ, eye, or tissue donation:
PHI may be disclosed to organ procurement, banking or transplantation organizations to facilitate organ, eye or tissue donation and transplantation.

I. Research:
PHI may be used and/or disclosed for research pursuant to a waiver of authorization from the IRB, or for the following:

1. reviews preparatory to research;

2. research on decedent's information;
3. research using a "limited data set"; and
4. research using "de-identified" data.

J. Threats to Health or Safety:
PHI may be used or disclosed under certain circumstances to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.

K. Specialized Government Functions:
PHI may be used or disclosed for specialized government functions such as military and veterans activities, security and intelligence activities, protective services for officials, medical suitability, and to correctional institutions.

L. Workers' Compensation:
PHI may be used or disclosed to the extent required to comply with worker's compensation and similar programs.

VII. SPECIFIC PATIENT RIGHTS

A. Right to accounting of disclosures:
A patient has the right to receive an accounting of disclosures of PHI made by covered University units in the six (6) years prior to the request, except for disclosures:

1. for payment, treatment and health care operations;
2. to the individual patient;
3. incident to a use or disclosure otherwise permitted by HIPAA;
4. pursuant to an authorization;
5. for the entity's directory, to persons involved in the individual's care, or for other purposes described in Section VI above;
6. for national security or intelligence purposes;
7. to correctional institutions or law enforcement officials; or
8. disclosures for research made in the form of de-identified data, a limited data set, or pursuant to an authorization.

B. Right to amendment of PHI:
The patient or his/her authorized representative has the right to request that the covered University unit amend his/her PHI contained in clinical, billing and other records used to make decisions about the patient.

Requests for amendments must be in writing and must explain the reason(s) for amendment. The covered University unit may deny a request in the following circumstances:

1. the information was not created by the covered University unit (unless the patient is able to prove the creator of the information is no longer available to amend the record);
2. the information is not part of the records used to make decisions about the patient;
3. the covered University unit believes the information is correct and complete; or
4. the patient does not have the right to see and copy the particular record, as described in Section VII C.

C. Right to an explanation of any denial:

The covered University unit will explain any denial in writing and describe a patient's rights to give the covered University unit a written statement disagreeing with the denial. If the covered University unit accepts a patient's request to amend, that unit will make reasonable efforts to inform others of the amendment, including Business Associates, as necessary or appropriate, and persons the patient names who have received PHI about him/her and who need the amendment.

D. Right to request different means of communications:

The patient or his/her authorized representative has a right to request how and where a covered University unit contacts him/her about PHI. The request must be in writing. The covered University unit must accommodate reasonable requests, but, when appropriate, may condition that accommodation on the patient or his/her authorized representative providing the covered University unit with an alternative address or other method of contact, as well as information regarding how payment, if any, will be handled.

E. Right of access to PHI:

The patient or his/her authorized representative has a right to request to see and receive a copy of his/her PHI contained in clinical, billing or other records used to make decisions about the patient. The patient or his/her authorized representative has the right to receive a copy of PHI in its original electronic version if possible or, if not possible, in another electronic format to which the patient and the covered University unit mutually agree. The covered University unit may charge related fees, and instead of providing a full copy, may provide a summary or explanation of the patient's PHI, if the patient agrees in advance to the form and cost.

The patient or his/her authorized representative does not have the automatic right to access the following:

1. psychotherapy notes;
2. information compiled in anticipation of, or for use in, a criminal, civil or administrative action or proceeding;
3. PHI that is maintained by an entity that is subject to Clinical Laboratory Improvement Amendments (CLIA), to the extent provisions of access would be prohibited by law, or exempted from CLIA;
4. PHI created or obtained in the course of research that includes treatment, provided the patient or his/her authorized representative agreed to the denial of access to the patient's PHI during the research period when the patient (or his/her authorized representative on his/her behalf) consented to participate in the research;
5. PHI that is contained in records that are subject to the Privacy Act, 5 U.S.C. § 552a, if the denial of access under the Privacy Act would meet the requirements of that law;
6. PHI 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 that information.

A covered University unit may deny a patient or his/her authorized representative access to PHI in certain circumstances, provided that the patient or his/her authorized representative is given a right to have such denials reviewed by a health care professional designated by the covered University unit to act as a reviewing official and who did not participate in the original decision to deny access. The covered University unit must provide or deny access in

accordance with the reviewing official's determination. The following circumstances are reviewable grounds for denial:

1. a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person;
2. the PHI makes reference to another (unless the 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
3. 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.

F. Right to request restrictions on uses and disclosures of PHI:

The patient or his/her authorized representative has the right to request that the covered University unit restrict the use and disclosure of PHI about the patient. The covered University unit is not required to agree to the request in most circumstances. When the covered University unit does agree to a request, in certain situations the restrictions may not be followed. Such situations include emergency treatment, disclosures to the Secretary of the Department of Health and Human Services, and uses and disclosures described in Section VI above. The covered University unit must agree to a patient's request to restrict disclosure of PHI which pertains solely to a health care item or service for which the patient, or another or that patient's behalf, paid in full out of pocket, if such a disclosure is to a health plan for the purpose of payment or health care operations.

G. Right to Complain about Privacy and Security Policies and Procedures:

A patient or his/her authorized representative has a right to complain about alleged violations of HIPAA and/or UNC-Chapel Hill's HIPAA policies, and /or procedures regarding privacy and security of their PHI. A patient, or his/her authorized representative may file a complaint with the University Privacy Officer, send a written complaint to the United States Secretary of the Department of Health and Human Services, or lodge a complaint via the Ethics Hotline.

The University Privacy Officer will develop and maintain procedures regarding coordination, documentation and resolution of any such complaints.

H. Refraining from Intimidating or Retaliatory Acts:

Neither the University nor any of its employees, students, trainees, volunteers, agents, or contractors may intimidate, threaten, coerce, discriminate against, or take any other retaliatory action against:

1. any individual for exercising his/her rights under this policy or HIPAA regulations, or participating in any process established by this policy or HIPAA regulations, including filing a complaint; or
2. any individual or entity for filing a complaint with the Secretary of the Department of Health and Human Services under HIPAA; or testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under any section of HIPAA or opposing any act or practice which is unlawful under HIPAA, as long as the individual or

entity has a good faith belief that the practice is unlawful, and the manner of opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.

I. Waiver of Rights:
The University will not require an individual to waive his/her rights under this policy or HIPAA as a condition of treatment, payment, enrollment in a health plan, and/or eligibility for benefits.

VIII. PHYSICAL AND ELECTRONIC SECURITY OF PHI

HIPAA requires physical and electronic security to maintain the privacy of PHI. This requirement includes limiting physical and electronic access to PHI through all forms, such as written, spoken, pictorial, recorded electronically, or printed. See security requirements contained in the UNC-Chapel Hill ***Information Security Policy***.

IX. BREACHES OF PRIVACY OR SECURITY

Under HIPAA, a breach is the impermissible acquisition, access, use or disclosure of PHI which compromises the security or privacy of unsecured PHI. Unsecured PHI is PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by the Secretary of the Department of Health and Human Services, including but not limited to encryption of electronic PHI and shredding, clearing or purging media containing PHI.

Except in limited circumstances, impermissible acquisition, access, use or disclosure of unsecured PHI is presumed to be a breach under HIPAA, unless the covered University unit (or Business Associate, as applicable) demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following four factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom it was disclosed;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

A covered University unit shall, following the discovery of a breach of unsecured PHI, notify each individual whose unsecured PHI has been, or is reasonably believed by the covered University unit to have been, acquired, accessed, used or disclosed as a result of the breach without unreasonable delay, but in no case later than 60 calendar days following the discovery of the breach. In some circumstances, the covered University unit must also notify the media, the state Attorney General, and the Secretary of the Department of Health and Human Services.

If any University employee , contractor or student becomes aware of an actual or alleged breach of this policy or any related departmental policies, or any other actual or alleged breach of required privacy or security of PHI, the employee, contractor or student is required to report the actual or alleged breach to the University Privacy Officer or Security Officer. UNC- Chapel Hill will mitigate, to the extent practicable, any known harmful effect of an impermissible use or disclosure of PHI in violation of this or any similar policies and procedures, or other applicable requirements of HIPAA. Any UNC-Chapel Hill employee or student who is found to be in violation of any part of this policy is subject to disciplinary action, up to and including dismissal in accordance with established University policies.

X. PENALTIES

UNC-Chapel Hill and its employees or students who violate HIPAA may be subject to both civil and criminal penalties under HIPAA regulations. Civil monetary penalties range from $100 to $1,500,000 per violation. Federal criminal penalties range from $50,000 to $250,000 in fines and up to 10 years' imprisonment.