



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 policies. This policy addresses the specific privacy obligations required by the Health Insurance Portability and Accountability Act of 1996, hereinafter referred to as “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” or “PHI”.

At the University of North Carolina-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 any patient or client 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 University of North Carolina at 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 will be provided in Section II. to further explain the scope of the policy and to provide meaningful guidance in 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 the covered unit when that function, activity, or service involves the use and/or disclosure of PHI.

C. Consent:

A HIPAA consent is written permission by the patient, client, or his/her representative for the covered university unit's use and/or disclosure of an individual's PHI for treatment, payment, and health care operations. This HIPAA consent is different from an informed consent for research participation.

D. Covered University Unit:

A covered University unit is either (1) a health plan that provides or pays the cost of medical care, or (2) a health care provider that transmits any health information in electronic or conventional form in association with any of the financial or administrative transactions listed in the HIPAA regulations.

E. De-identified PHI:

De-identified PHI is personal health information that is not individually identifiable because it meets the HIPAA criteria for de-identification.

The following identifiers of the individual and the individual's relatives, employers, and household members all must be absent from the PHI to designate it as "De-identified".

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. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers & serial numbers & license plates;
12. Device identifiers and serial numbers;
13. Web Universal Resource Locaters (URLS);
14. Internet Protocol (IP) address numbers;
15. Biometrical identifiers, including finger and voice prints;
16. Full face photographic images and any comparable images;
17. Any other unique identifying number, characteristic, or code except for secure reidentification or data matching codes that are not derived from information about the individual.

F. 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.

G. Marketing:

Marketing is communication intended to encourage the purchase or services. Marketing does not include communications to the individual: (1) to describe entities that participate in health care provider networks or health plans; (2) to describe products or services offered by a provider to include in a plan of benefits; (3) relating to their own treatment; (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.

H. 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) disclosures to the individual about himself/herself; (3) disclosures with authorization; (4) disclosures for research with waiver of authorization by an IRB or Privacy Board; or (5) disclosures approved by the University Privacy Officer.

I. 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. It is essentially the same definition as “Individually Identifiable Health Information” but also includes (1) the clarification that the form of the covered information is “whether oral or recorded in any form or medium” and (2) the additional clarification that some classes of information are exempted.

Protected Health Information is:

1. Information, including demographic information collected from an individual; and
2. Is oral or recorded in any form or medium; and
3. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

4. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
5. Identifies the individual; or there is a reasonable basis to believe the information can be used to identify the individual; and
6. Excludes:
 - (a) Education records covered by “FERPA”; or
 - (b) Employment records even if they contain individually identifiable health information; or
 - (c) 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 to 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)

J. 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 University of North Carolina at 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.

Except as authorized in this policy or other applicable University policies, all disclosures of PHI outside and within the University, other than for treatment, payment, or health care operations, must be processed through the applicable unit's health information management department, or, in the absence of such internal department, by the University's Privacy Officer. All uses and disclosures of PHI of any nature are subject to HIPAA, as well as this and other related University policies, and 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. A copy of the Notice of Privacy Practices shall be posted by each covered University unit and copies shall be made available to patients upon request. Upon providing the copy of the Notice of Privacy Practices, 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 Notice of Privacy Practices, document such in the patient's medical record.

B. Consent:

If possible, prior to providing care, covered University units shall obtain and retain from each patient, client or authorized representative a signed and dated general consent to use or disclose PHI to carry out treatment, payment, and health care operations.

C. Authorization:

To use or disclose PHI for any purpose other than treatment, payment and health care operations, a covered University unit must obtain from the patient, client, 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. Authorization is not required where waived by the IRB, or as further enumerated in Section VI. of this *Policy* or as further described in the covered University unit's release of information policy.

Other Uses and Disclosures:

1. **De-identified PHI** – as previously described in Section II.
2. **Marketing** – Marketing conducted by a face-to-face communication with an individual is allowed under HIPAA; however, other types of marketing activities using PHI require an

authorization. The applicable unit's marketing department must approve marketing activities in advance.

3. **Fundraising** – UNC-Chapel Hill may use, without authorization, demographic and date-of-service PHI in fundraising activities; however, all fundraising activities must be conducted through the applicable unit's institutionally related fundraising organization.
4. **Business Associates** – PHI may be used by and disclosed to a business associate of UNC-Chapel Hill under the procedures set forth under the *UNC-Chapel Hill Business Associate Policy*, including signing and complying with a Business Associate Agreement in a form approved by the University's Privacy Officer.
5. **Research** –
 - a. **With Authorization** – Use and 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 Research Board (IRB) grants a waiver of the requirement for authorization.
 - c. Other than with authorization or 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.

- D. **Verification of Identity** – UNC-Chapel Hill covered University units will take reasonable steps to verify the identity and authority of individuals and entities requesting Protected Health Information under HIPAA. Such steps may include (without limitation) request for identification, alternate identifiers (e.g., verifying home address), and written authorizations. The identity and authority of a public official may be verified by agency badges, written authorizations on government letterhead, or other reasonable means or identification under the circumstances. Further guidance on verification of identification is available in 45 C.F.R. §164.514(h).

V. **PATIENT OR CLIENT OPT OUT OF USE OR DISCLOSURE OF PHI.**

PHI may be used or disclosed for the following purposes, if the patient, client or his/her authorized representative is informed in advance of the use or disclosure and has the opportunity to agree to or 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 (i) the patient's consent is obtained; (ii) the patient is provided with an opportunity to object and the patient does not object; (iii) 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 the disclosure is in the best interest of the patient, using professional judgment, and, if so, only the PHI which is directly relevant to the person's

involvement with the patient's health care may be disclosed. The University and/or 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.

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.

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 used 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. PATIENT OR CLIENT CONSENT, AUTHORIZATION, AGREEMENT NOT REQUIRED FOR USE OR DISCLOSURE OF PHI.

The following is a list of the types of uses and disclosures, which do not require consent, authorization or the opportunity to opt out. In each case, reference should be made to the applicable covered University unit's health information management policy.

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, as outlined in each covered University unit's release of information policies, 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, a subpoena, discovery request or other lawful process with certain assurances, as addressed in the covered University unit's health information release of information policies.

F. Law Enforcement Purposes:

PHI may be disclosed for law enforcement purposes to a law enforcement official under certain conditions, as addressed in the covered University unit's health information release of information policies.

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:

Without Authorization: PHI may be used in research without an individual's authorization if an IRB grants a waiver of the requirement for authorization. There are also four other research scenarios that require neither authorization nor waiver of authorization: (1) reviews preparatory to research; (2) research on decedent's information; (3) research using a "limited data set"; and (4) research using "deidentified" data.

- J. Threats to Health or Safety:**
PHI may be used or disclosed under certain circumstances if the University Privacy Officer believes in good faith that the use or disclosure is necessary to protect a person or the general 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 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 the 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 or to persons involved in the individual's care as allowed in Section V above;
 6. for national security or intelligence purposes;
 7. to correctional institutions or law enforcement officials;
 8. disclosures for research made in the form of de-identified data, a limited data set, or pursuant to an authorization; or;
 9. made prior to the compliance date.

Documentation including titles or departments responsible for providing accountings of disclosure must be retained for no less than six (6) years. Requests for accounting of disclosures should be referred to the Covered University Unit's Privacy Officer or University Privacy Officer.

- B. Right to amendment of PHI:**
The patient, client, or his/her authorized representative has the right to request that the covered University unit amend his/her PHI for as long as

the unit maintains the information. Requests for amendments should be referred to the applicable unit's health information management department or to the Covered University Unit's Privacy Officer or University Privacy Officer.

C. Right of access to PHI:

The patient, client, or his/her authorized representative has a right to request to inspect and receive a copy of his/her PHI that is used, in whole or in part, for as long as the covered University unit maintains the PHI, although in certain circumstances PHI generated in clinical research may be sheltered from disclosure until completion of the research study.

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

1. psychotherapy notes;
2. information compiled in anticipation of a criminal, civil or administrative action or proceeding; or
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.

D. Right to request additional privacy protection:

The patient, client, or his/her authorized representative has the right to request that the covered University unit restrict:

1. uses and disclosures for treatment, payment, and health care operations
2. disclosures permitted for involvement in the patient's care and for notifications purposes.

UNC-Chapel Hill is not required to agree to the restriction; however, if UNC-Chapel Hill agrees to the restriction, it must abide by it except in emergencies. The restriction must be properly documented and maintained for 6 years. Requests for restrictions should be referred to the applicable unit's health information management department or to the Covered University Unit's Privacy Officer or University Privacy Officer.

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

A patient, client, or his/her authorized representative has a right to complain about alleged violations of University policies and procedures regarding privacy and security of their PHI. A patient, client, or his/her authorized representative may file a complaint with the University Privacy

Officer or the Privacy Director for the applicable covered University unit. The University Privacy Officer will develop and maintain procedures regarding coordination, documentation and resolution of any such complaints.

F. 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 DHHS 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.

G. 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.

If any University employee or contractor 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 or contractor 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 a 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 are \$100 per incident, up to \$25,000 per person, per year. Federal criminal penalties range from \$50,000 to \$250,000 in fines and up to 10 years' imprisonment.