UNIVERSITY STANDARD

Title

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL
STANDARD ON PRIVACY LIAISONS

Introduction

PURPOSE

To provide a framework that supports full HIPAA compliance for the University. Each Operating Unit with responsibility for Protected Health Information (PHI) must have a mechanism for obtaining information, understanding requirements, and maintaining compliance with HIPAA. This Standard describes the obligations of each Operating Unit and of the assigned Privacy Liaisons.

SCOPE OF APPLICABILITY

Heads and Privacy Liaisons of University Operating Units with responsibilities for the privacy and security of PHI, due to (a) the Operating Unit’s status as a designated Covered Unit of the University’s HIPAA hybrid entity (including those that would be either Covered Entities or act as internal Business Associates to a Covered Unit) or (b) Business Associate or Subcontractor status (as defined under HIPAA) of the Operating Unit with responsibility for the PHI of Covered Entities or Business Associates outside of the University.

Standard

University Operating Units with responsibility for management of PHI must provide to the University’s Designated HIPAA Privacy Officer/Chief Privacy Officer (CPO) a written designation of primary and secondary staff members to the role of Privacy Liaison.
Each Operating Unit that is designated as a Covered Unit of the University’s HIPAA hybrid entity, the School of Medicine, and any University Operating Unit with Business Associate or Subcontractor status with respect to PHI of Covered Entities or Business Associates outside of the University, must designate both a Primary Privacy Liaison and a Backup Privacy Liaison, and renew that designation as requested by the CPO.

Each individual so designated must: (a) understand the requirements of HIPAA regulations applicable to their Operating Unit, (b) have knowledge of the locations and uses of PHI within the Operating Unit, and (c) have a level of responsibility within the Operating Unit sufficient to perform privacy-related compliance activities involving a high degree of risk for the University and the Operating Unit.

Privacy Liaisons are responsible for managing privacy risk to information with the highest degree of sensitivity (PHI is classified as tier 3 in the University Information Classification Standard). Due to the critical and dynamic nature of each Privacy Liaison’s responsibilities, full participation in privacy activities is expected of Privacy Liaisons.

The CPO has final responsibility for coordination of Privacy Liaisons.

---

**Roles and Responsibilities**

**Operating Unit Head:** Appointment of Primary and Backup Privacy Liaisons. Ensuring Privacy Liaisons have support, training, and resources to fulfill responsibilities.

**Privacy Liaison (Note: Each Operating Unit will designate a “Primary Privacy Liaison” and a “Backup Privacy Liaison.” Both roles are referred to together in this Standard as a “Privacy Liaison”):** Attend all Privacy Liaison meetings (Primary or Backup should attend). Provide Privacy training, informational and compliance activities for the Operating Unit. The Privacy Liaison leads their Operating Unit’s investigation activities involving potential privacy breaches (in coordination with the Institutional Privacy Office and the CPO); manages the Operating Unit’s HIPAA-related policies and procedures; assures personnel have received applicable privacy training; serves as their Operating Unit's privacy point-of-contact; promotes privacy-awareness within the Operating Unit; and facilitates HIPAA risk assessment and remediation. Privacy Liaisons must maintain up-to-date knowledge of HIPAA and related requirements; provide guidance and
support to Operating Unit staff in performance of their data-management activities; and act as liaison for the Operating Unit with the Institutional Privacy Office.

Chief Privacy Officer: Confirm Privacy Liaison appointments; hold regular Privacy Liaison meetings as needed; provide guidance and support to Privacy Liaisons in performance of their required activities.

EXCEPTIONS

The CPO may make exceptions to requirements of this Standard to permit additional Privacy Liaisons from any University Operating Unit, waive the requirement for a Primary Privacy Liaison or a Backup Privacy Liaison for any Operating Unit, or other exceptions, as needed in the discretion of the CPO.

Definitions

**Business Associate**: A person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a HIPAA Covered Entity. Business Associate functions and activities include, but are not limited to: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business Associate services include but are not limited to: legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial. A member of a Covered Entity’s workforce is not a business associate.

**Covered Unit**: Officially designated health care components of the University, including Operating Units that would be either Covered Entities or act as internal Business Associates to a Covered Unit.

**HIPAA**: An acronym for the Health Insurance Portability and Accountability Act, a federal law that governs the use and disclosure of protected health information.

**Protected Health Information**: Individually identifiable 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 a subject; the provision of health care to a subject; or the past, present, or future payment for the provision of health care to a subject; and

a. That identifies the subject; or
b. With respect to which there is reasonable basis to believe the information can be used to identify the individual.

PHI can be:

a. Transmitted by electronic media;
b. Maintained in electronic media; or
c. Transmitted or maintained in any other form or medium.

PHI excludes individually identifiable information that is:

b. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);
c. In employment records held by a covered entity in its role as employer; and
d. Regarding a person who has been deceased for more than 50 years.

---

**Related Requirements**

**EXTERNAL REGULATIONS AND CONSEQUENCES**

HIPAA: [https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html)

**UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES**

HIPAA Policy

Information Classification
Retention Schedule

Designation of Covered Units document

Contact Information

PRIMARY CONTACT(S)

<table>
<thead>
<tr>
<th>Subject</th>
<th>Contact</th>
<th>Telephone</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy questions</td>
<td>ITS Policy Office</td>
<td>919-962-HELP</td>
<td><a href="mailto:Its_policy@unc.edu">Its_policy@unc.edu</a></td>
</tr>
<tr>
<td>Privacy activities</td>
<td>Institutional Privacy Office</td>
<td>919-962-HELP</td>
<td><a href="mailto:Privacy@unc.edu">Privacy@unc.edu</a></td>
</tr>
</tbody>
</table>

Important Dates

- Effective Date and title of Approver: September 6, 2017, Chief Privacy Officer
- Revision and Review Dates, Change notes, title of Reviewer or Approver: N/A

Approved by:

/S/

Micki Jernigan
Chief Privacy Officer

Date: September 6, 2017