

**The University of North Carolina at Chapel Hill**  
**Protocol for Responding to Breaches of Protected Health Information**

I. PURPOSE

In 2003, the United States Congress passed the Health Insurance Portability and Accountability Act (HIPAA). This legislation governs the protection of individually identifiable health information. In 2009, Congress imposed more rigorous requirements for the management of protected health information (PHI) through legislation titled the Health Information Technology for Economic and Clinical Health (HITECH) Act. Pursuant to HITECH, The University of North Carolina at Chapel Hill (University) is required to notify certain individuals and entities upon discovery of a potential Breach of PHI that is “unsecured.” In addition, the University is required to maintain records of Breaches and report them to the U.S. Secretary of Health and Human Services on an annual basis. This protocol sets forth the University process to comply with these requirements.

II. PROTOCOL FOR RESPONDING TO SUSPECTED OR ACTUAL BREACHES

A. Definitions

1. **Breach** – The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term “Breach” does not include:
  - a. Any unintentional acquisition, access, or use of PHI by an employee or individual acting with authorization if –
    - (i) such acquisition, access, or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or HIPAA Business Associate; and
    - (ii) such information is not further acquired, accessed, used, or disclosed by any person; or
  - b. any inadvertent disclosure from an individual who is otherwise authorized to access PHI at a facility operated by a covered entity or Business Associate to another similarly situated individual at the same facility; and
  - c. any such information received as a result of such disclosure is not further acquired, accessed, used, or disclosed without authorization by any person.
2. **Business Associate** – A Business Associate is a party with whom the Covered Entity or Unit enters into a contract in order to perform a service that the Covered Entity or Unit would otherwise perform for itself. Pursuant to HIPAA, the contract is called a “Business Associate Agreement” (BAA). The Business Associate “steps

into the shoes of the covered entity” with regard to its responsibility to protect PHI, including responsibility to report a Breach to the covered entity.

3. **Covered University Entity** – University unit that is designated by the HIPAA Privacy Officer as a “Covered Unit” under the University’s HIPAA Policy (<http://www.unc.edu/hipaa/index.htm>).
4. **Protected Health Information (“PHI”)** – Information that is created or received by a health care provider, health plan, employer, or health care clearinghouse that identifies an individual or provides a reasonable basis to believe the information can be used to identify the individual and that relates to:
  - a. the past, present, or future physical or mental health or condition of an individual;
  - b. the provision of health care to an individual; or
  - c. the past, present, or future payment for the provision of health care to an individual.
5. **Unsecured PHI** – PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals under standards issued by the U.S. Secretary of Health and Human Services as determined by the University’s Security Officer. Note that data contained in an “encrypted” format is deemed secured, even if lost or stolen.

## B. Breaches and Notification

The University is committed to the prevention of Breaches with respect to PHI, as defined above. Suspected Breaches of unsecured PHI will be reviewed and assessed by the HIPAA Privacy and/or Security Officer and other appropriate University units (including, for example, the Office of University Counsel, ITS Security, the Internal Audit Department and the Department of Public Safety). The purpose of the assessment will be to determine the likelihood of “harm” (pursuant to HIPAA) arising from the actual or suspected breach. The results of the assessment will be used to determine the actions to be taken in response to the actual or suspected Breach.

### 1. Internal Notification (for Assessment and Response)

Any University employee or student who becomes aware of a suspected or actual Breach must immediately notify his or her supervisor and one of the following officials: the HIPAA Privacy Officer, the HIPAA Security Officer, or the Office of University Counsel (for contact information, please go to: <http://www.unc.edu/hipaa/>).

### 2. Breach by Business Associate

In the event that a Business Associate becomes aware of a potential Breach, the Business Associate must immediately notify the office and official of the University

Covered Unit with whom the Business Associate contracted to perform the contracted service. The contacted University official must then immediately notify the HIPAA Privacy Officer, the HIPAA Security Officer, or the Office of University Counsel.

### 3. External Notification

#### a. Required Notification to Affected Individuals

In the case of a Breach of unsecured PHI that is discovered by the University, and which Breach is determined by the University to present a significant risk of harm, the University shall notify each individual whose unsecured PHI has been or is reasonably believed to have been accessed, acquired or disclosed as a result of the Breach. Without unreasonable delay, but in no case later than 60 calendar days after discovery of a Breach, the University, through the appropriate office, shall take the following actions:

- (i) Notify affected individuals (or next of kin if deceased) in writing via first class mail at the last known address of the affected individual (or via electronic communication if so indicated by the individual as the preferred method of communication) of the following information:
  - a) A brief description of the Breach including date of the Breach and date of discovery;
  - b) A description of the types of PHI that were involved in the Breach; note, that if Social Security numbers are contained in a breached data set, notification shall be in compliance with the requirements of the North Carolina Identity Theft Protection Act ([http://www.unc.edu/campus/policies/breach\\_protocol.html](http://www.unc.edu/campus/policies/breach_protocol.html));
  - c) Steps that individuals should take to protect themselves from potential harm resulting from the Breach;
  - d) A brief description of University's remedial measures in response to the Breach including investigations, mitigation of losses and protection against further Breaches; and
  - e) Contact information for the University or its designated agent, including, as appropriate, a toll-free telephone number, e-mail address, website, or postal address where individuals can obtain additional information and make inquiries.
- (ii) If there is insufficient or up-to-date contact information precluding direct written communication to an individual, then a substitute form of notice shall be provided.

If there is insufficient or out-of-date contact information of ten (10) or more individuals, the University shall provide a toll-free telephone number where individuals can learn if they have been affected by the Breach by:

- a) Posting a notice of the Breach on the University's website as specified by the U.S. Department of Health and Human Services; or
- b) Placing a notice in major print or broadcast media in geographic areas where the affected individuals are likely to reside.

(iii) If the University's HIPAA Privacy Officer or the Office of University Counsel deems that a Breach notification is urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other means is permitted, as appropriate.

b. Required Notification to Media

Notice of a Breach shall be provided to prominent media outlets serving a state, if the unsecured PHI of more than 500 residents of such state has been or is reasonably believed to have been accessed, acquired, or disclosed as a result of a Breach.

c. Required Recordkeeping and Notification to the U.S. Secretary of Health and Human Services

Notice shall be provided to the Secretary of unsecured PHI that has been acquired or disclosed in a Breach.

- (i) If the Breach involved the data of 500 or more individuals, the University's HIPAA Privacy Officer or Office of University Counsel shall provide such notice immediately.
- (ii) Breaches that involve the data of fewer than 500 individuals will be maintained in a log and submitted annually to the Secretary.

4. Delayed Notification

Notice shall be delayed if law enforcement informs the University that disclosure of a Breach would impede a criminal investigation or jeopardize national security. A request for delayed notification must be made in writing or documented contemporaneously by the University in writing, including the name of the law enforcement officer making the request and the officer's agency engaged in the investigation. The required notice shall be provided without unreasonable delay after the law enforcement agency communicates to the University its determination that notice will no longer impede the investigation or jeopardize national or homeland security.

### III. INSTITUTIONAL ACTIONS

At least annually, the University's HIPAA Steering Committee will review all incidents of suspected or actual security breaches and may make recommendations to the Chancellor for institutional improvements.

#### IV. ADDITIONAL UNIVERSITY POLICIES AND RESOURCES

##### A. Policies

A Breach of PHI may invoke additional federal and State laws as well as University Policies and Procedures. The following may also be applicable or informative:

- UNC-Chapel Hill HIPAA Implementation (general):  
<http://www.unc.edu/hipaa/>
- Information Security Policy:  
[http://www.unc.edu/hipaa/policies/Information\\_Security.pdf](http://www.unc.edu/hipaa/policies/Information_Security.pdf)
- HIPAA “Minimum Necessary” Policy:  
[http://www.unc.edu/hipaa/policies/Minimum\\_Necessary.pdf](http://www.unc.edu/hipaa/policies/Minimum_Necessary.pdf)
- Payment Card Industry Standards:  
[http://www.unc.edu/finance/controller/fc/pcd\\_manual.pdf](http://www.unc.edu/finance/controller/fc/pcd_manual.pdf)
- Protocol for Responding to Security Breaches of Certain Identifying Information  
[http://www.unc.edu/campus/policies/breach\\_protocol.html](http://www.unc.edu/campus/policies/breach_protocol.html)
- UNC-Chapel Hill Identity Theft Prevention Program  
<http://www.unc.edu/depts/legal/UCPPD/>
- Reporting of Misuse of State Property:  
[http://www.unc.edu/finance/controller/fc/report\\_misuse.pdf](http://www.unc.edu/finance/controller/fc/report_misuse.pdf)
- Family Educational Rights and Privacy Act (FERPA) Policies and Procedures:  
<http://www.unc.edu/policies/ferpapol.pdf>

#### V. EFFECTIVE DATE

This protocol is effective January 1, 2010

*This document is maintained by the HIPAA Privacy Officer.*