THE UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL

PROTOCOL FOR RESPONDING TO BREACHES OF PROTECTED HEALTH INFORMATION (PHI)

I. PURPOSE

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") established Federal standards for safeguarding the privacy of individually identifiable health information. HIPAA mandates rigorous compliance with the requirements for the use and/or disclosure of protected health information ("PHI"). In strict compliance with the requirements of HIPAA, The University of North Carolina at Chapel Hill ("University") is required, following the discovery of a breach of unsecured PHI, to notify each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired, used or disclosed as a result of the breach. The University must maintain records of any instances of breach and report these to the U.S. Secretary of Health and Human Services on an annual basis. The following protocol sets forth the University's process for full compliance with these requirements.

II. PROTOCOL FOR RESPONDING TO SUSPECTED OR ACTUAL BREACHES

A. Definitions

1. **Breach** – The unauthorized and/or impermissible acquisition, access, use, or disclosure of PHI which compromises the security or privacy of 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 University unit or 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.

   d. any disclosure of PHI where a covered University unit or Business Associate has a

good faith belief that the unauthorized person to whom the information was disclosed would not reasonably be able to retain such information.

2. **Business Associate** – A Business Associate is an individual or company with whom a covered University unit enters into a contract in order to perform a service that involves the creation, maintenance, transmission, management, or disclosure of PHI on behalf of the covered University unit. HIPAA requires that all Business Associates provide appropriate safeguards and procedures to ensure the privacy and security of PHI entrusted to them under a contract with a covered University unit. Business Associates are directly liable for impermissible uses and disclosures of PHI and must report any instances of breach to the covered University unit.

3. **Covered University Entity** – A University unit that is designated by the University Privacy Officer as a "Covered University Unit" and performs the functions of a health care provider, employs health care providers, and transmits health information in electronic and conventional form in association with financial or administrative transactions.

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. All incidents involving unsecured PHI will be investigated by the University 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). Every incident investigation must include a risk analysis assessing the following factors to determine whether the PHI at issue has been compromised:

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

The results of the incident investigation will determine the actions to be taken.

1. Internal Notification (for Assessment and Response)

   Any University employee or student who becomes aware of a suspected or actual impermissible use or disclosure of PHI must immediately notify his or her supervisor and one of the following officials:

   - HIPAA Privacy Officer
   - HIPAA Security Officer
   - Information Security Officer
   - Office of University Counsel
   - HIPAA Privacy Liaison

2. Breach by Business Associate

   In the event that a Business Associate becomes aware of an impermissible use or disclosure of PHI, the Business Associate must immediately notify the covered University unit with whom it has a Business Associate Agreement per the terms. The contacted covered University unit must then immediately notify the University Privacy Officer, the HIPAA Security Officer, or the Office of University Counsel.

3. External Notification

   a. Required Notification to Affected Individuals

      In the event of a breach of unsecured PHI, 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);
         c) Steps that individuals should take to protect themselves from potential harm resulting from the breach;
         d) A brief description of the 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 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 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. EFFECTIVE DATE

This protocol is effective January 1, 2010, revised September 2013