UNH Policy on Compliance with the
Health Insurance Portability and Accountability Act (HIPAA)

Approved August 5, 2014

1 Preamble

1.1 The Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191 as amended) (HIPAA) regulates organizations that electronically maintain or transmit protected health information in connection with a covered transaction. HIPAA requires each organization to maintain reasonable and appropriate administrative, technical and physical safeguards for privacy and security. Entities or individuals who contract to perform services for such an organization and who have access to protected health information are also required to comply with the HIPAA privacy and security standards. The University of New Hampshire (UNH) recognizes its responsibility to comply with HIPAA to ensure reasonable protection of protected health information. Accordingly, UNH maintains a policy for HIPAA compliance. UNH strives to ensure that all members of its workforce understand and adhere to this policy.

2 Definitions

2.1 Business Associate: A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, UNH. A member of UNH’s workforce is not a business associate of UNH. UNH, through its covered units, also may act as a business associate of other entities outside of UNH.

2.2 Covered Unit: A UNH department/unit is designated as a covered unit only to the extent that it performs HIPAA covered functions, or engages in activities that would make it a business associate of another UNH covered unit or a business associate of an entity outside of UNH. The UNH HIPAA Advisory Committee is responsible for designating and identifying the UNH departments/units that are covered units and thus subject to HIPAA, based on performance of covered functions, and these shall be listed in the UNH HIPAA procedures.

2.3 Electronic Protected Health Information (PHI): Individually identifiable health information that is transmitted by or maintained in electronic media. Examples include, but are not limited to internet, extranet, leased lines, dial-up lines, private networks, hard drives, flash drives, magnetic tape/disk, CD, digital memory card.
2.4 Health Insurance Portability and Accountability Act of 1996 (HIPAA): The federal law that establishes national standards for the privacy and security of health information and electronic health care transactions, which are found in 45 CFR Parts 160, 162 and 164.

2.5 HIPAA Advisory Committee: The UNH committee providing oversight of UNH’s compliance with HIPAA and applicable state laws governing the use, storage and disclosure of Protected Health Information (PHI).

2.6 Health Information Technology for Economic and Clinical Health Act (HITECH): Part of the American Recovery and Reinvestment Act of 2009. It is a federal law that affects the health care industry that provides expanded reach of HIPAA. Section 13400-13423 Subtitle D-Privacy.

2.7 Hybrid Entity: For purposes of HIPAA, UNH has designated itself a hybrid entity. This means that UNH performs functions covered by HIPAA and functions not covered by HIPAA. The UNH HIPAA Advisory Committee is responsible for designating and identifying the UNH departments/units subject to HIPAA (covered units), based on performance of covered functions, and these shall be listed in the UNH HIPAA procedures and on the UNH website.

2.8 Notice of Privacy Practices: HIPAA provides that an individual has a right to adequate notice of how a covered entity may use and disclose protected health information about the individual, as well as his or her rights and the covered entity’s obligations with respect to that information. The document containing this information is UNH’s Notice of Privacy Practices.

2.9 Privacy Officer: The individual responsible for overseeing compliance with the privacy provisions of HIPAA (Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164) and applicable state laws.

2.10 Protected Health Information (PHI): Individually identifiable health information created, maintained or transmitted by UNH or any other covered entity in any form or medium, including information transmitted orally, or in written or electronic form.

2.11 Security Officer: The individual responsible for overseeing compliance with the security provisions of HIPAA (Security Standards for the Protection of Electronic Protected Information, 45 CFR Parts 160, 162 and 164) and applicable state laws.
2.12 Workforce Member: UNH workforce member means employees, students, trainees, volunteers and other persons whose conduct, in performance of work for UNH, is under the direct control of UNH, whether or not they are paid by UNH. It does not include business associates or their employees and agents.

3 Policy Statements

3.1 It is the policy of the University of New Hampshire (UNH) to comply with the Health Insurance Portability and Accountability Act of 1996 and its federal regulations (collectively, “HIPAA”) to the extent that HIPAA is applicable to UNH.

3.2 UNH’s designated covered units shall maintain the security and privacy of PHI in accordance with the requirements of the HIPAA statute and regulations.

3.3 UNH’s workforce members are expected to follow federal and state laws, as well as UNH’s policies and procedures regarding the privacy and security of PHI.

4 Status and Designations

4.1 UNH’s activities include both HIPAA covered and non-covered functions. Accordingly, UNH has determined that it is a hybrid entity for HIPAA compliance purposes.

4.2 UNH has designated certain departments/units as covered units. Covered units must comply with UNH HIPAA procedures. The UNH Privacy Officer may amend UNH’s designation of covered units as appropriate. UNH’s covered units shall be listed in the UNH HIPAA procedures and on the UNH website.

4.3 Other UNH departments/units that perform health care functions that are not covered by HIPAA may voluntarily choose to comply with or participate in some or all HIPAA requirements, policies or procedures. Such voluntary compliance or participation shall not affect a unit’s status as a non-covered unit.

5 Privacy Officer, Security Officer, and Privacy Coordinators

5.1 UNH has designated a Privacy Officer for HIPAA compliance purposes. The HIPAA Privacy Officer designation and contact information are posted on the UNH website. The designation of the Privacy Officer is subject to change by the UNH President.
5.1.1 The Privacy Officer is responsible for the development and implementation of general operating procedures as required by HIPAA and approved by the UNH HIPAA Advisory Committee.

5.1.2 The Privacy Officer is designated to receive complaints concerning UNH’s HIPAA related policies, procedures and HIPAA compliance, and to provide further information about matters covered by UNH’s Notice of Privacy Practices.

5.1.3 The Privacy Officer is responsible for initial and on-going HIPAA privacy training, monitoring use and disclosure of PHI and investigating HIPAA privacy concerns/complaints. The Privacy Officer may delegate tasks as needed, but shall retain overall responsibility for these activities.

5.2 UNH has designated a Security Officer who is responsible for developing and implementing HIPAA security policies, providing initial and on-going HIPAA security training, monitoring security of UNH electronic PHI and investigating of HIPAA security breaches, concerns, and complaints.

5.3 Each covered unit shall designate a Privacy Coordinator to interact with the Privacy Officer and coordinate HIPAA compliance within the unit. Documentation of each Privacy Coordinator designation shall be provided to and maintained by the Privacy Officer.

6 Procedures

6.1 UNH’s Privacy Officer is responsible for adopting and implementing general operating procedures governing HIPAA compliance by all covered units. Such procedures shall be distributed to all covered units and posted on UNH’s website.

6.2 Each covered unit is responsible for complying with UNH’s HIPAA general operating procedures, as applicable, and for developing procedures and forms as needed to implement and comply with such procedures and HIPAA including, but not limited to, appropriate administrative, technical and physical safeguards to protect the privacy of protected health information.

6.3 Each covered unit is responsible for providing the Privacy Officer with current copies of its procedures and any forms or other HIPAA compliance related documents in use by such covered unit.

6.4 Each covered unit shall have in place and operational procedures and forms to comply with UNH’s HIPAA general operating policies. Each covered unit
shall provide to the Privacy Officer copies of its procedures and forms. The Privacy Coordinator and the administrative head of each covered unit shall work with the Privacy Officer and the Security Officer to ensure appropriate implementation of UNH’s HIPAA general operating policies by the covered unit. Once approved by the Privacy Officer, copies of any material changes to a covered unit’s HIPAA procedures and forms shall be provided to the Privacy Officer for review and approval in writing prior to such revised procedures taking effect.

6.5 The Privacy Officer may require a covered unit to change its procedures, forms or related compliance documents if those procedures, forms or documents are deemed inconsistent with or contrary to the HIPAA general operating policies.

7. HIPAA Advisory Committee

7.1 UNH has established a HIPAA Advisory Committee to assist the Privacy Officer and oversee UNH’s HIPAA compliance. The Privacy Officer shall chair the committee. The advisory committee shall have representation from each covered unit, as well as other UNH department/units as appropriate. UNH’s Security Officer will also serve on the committee. Additional members may be appointed by the Privacy Officer. A representative of the USNH General Counsel’s Office shall provide advice to the committee.

8. Training

8.1 UNH will train its workforce members in each covered unit on the UNH HIPAA policy and operating procedures with respect to protected health information as required by HIPAA. Such training will be as necessary and appropriate for the workforce members to carry out their function within the covered unit. The Privacy Officer, in conjunction with each covered unit’s Privacy Coordinator, is responsible for developing training materials and implementing, updating and overseeing workforce training.

8.2 Training for covered units shall be completed within a reasonable time, not to exceed 60 days, after the department/unit is identified as a covered unit. Thereafter, each new member of a covered unit’s workforce shall be trained within a reasonable time (within 30 days) after joining the workforce. Additional training will be provided to each member of a covered unit’s workforce whose functions are materially affected by a change in HIPAA related policies or procedures. Such training will be provided within a reasonable time (within 30 days) after the material change becomes effective.
8.3 The Privacy Officer and the covered units’ Privacy Coordinators shall maintain copies of the training materials and document that the required training has been provided.

9. Enforcement

9.1 The Privacy Officer is responsible for implementation of this policy and overall responsibility for UNH’s compliance with the HIPAA regulations.

i [http://www.unh.edu/research/health-insurance-portability-accountability-act-hipaa](http://www.unh.edu/research/health-insurance-portability-accountability-act-hipaa)

ii [http://www.unh.edu/research/health-insurance-portability-accountability-act-hipaa](http://www.unh.edu/research/health-insurance-portability-accountability-act-hipaa)

iii [http://www.unh.edu/research/health-insurance-portability-accountability-act-hipaa](http://www.unh.edu/research/health-insurance-portability-accountability-act-hipaa)