The University of Vermont

Responsible Official: Chief Compliance and Privacy Officer

Effective Date: August 17, 2012

Privacy Procedures for Protected Personal Data

Goal

The goal of the Privacy Policy and accompanying Procedures is to meet the University's stated commitment to protecting the privacy of individuals whose Protected Personal Data (PPD) has been obtained by the University These procedures are intended to provide additional guidance as to the responsibilities and expectations of individuals with respect to this information.

Application

These Procedures apply to all PPD maintained in printed form, on computers, through network accounts, via the University e-mail system, or within other information and communication technology services. The Procedures apply whether UVM information resources are accessed remotely or through the use of a University-owned device or UVM network connection.

Definitions

In addition to the types of protected University information defined in the Privacy policy, these procedures outline responsibilities according to the roles of University community members. Accordingly, this section defines these specific roles as well as providing additional terms pertaining to the use of protected University information.

Roles.

"Component HIPAA Privacy Officers (CHPOs)" are the designated HIPAA privacy officers for each of the University's covered HIPAA component. The University is a hybrid entity under HIPAA which means that only certain identified components of the University are subject to the HIPAA Privacy rules.

"Data Stewards" are those members of the University community who have the operational responsibility for particular collections of information such as student, employee, library patron, or alumni records (collection(s)). Refer to the Information Security Policy and Procedures for list of Data Stewards [http://www.uvm.edu/policies/cit/infosecurityprocedures.pdf]

"Managers and Supervisors" are individuals that are responsible for directing the work of University employees, contractors or University affiliates.

"Technology Managers" are individuals who develop, implement, or maintain information systems or who have privileged access to information technology systems such as servers, networking equipment, and personal workstations in order to manage or support development on those systems, whether those systems are housed in UVM facilities or hosted externally.

"University Employees" includes student employees, staff, faculty, contractors, consultants, temporary employees and affiliates of the University of Vermont.

"User" is an individual who uses University Information or University Information Systems, even if they do not have responsibility for managing institutional resources.

Additional Terms:

"Biometric Identifiers" -_refers to the records created through technologies using a person's unique physical attributes for identification and/or authentication purposes. Unique physical attributes can include, but are not limited to, fingerprints, hand geometry, retina and iris patterns, voice waves, signatures, and facial patterns.

"University Information" is information in any form and recorded on any media that the University or its agents use or create in the course of conducting University business, including research and teaching activities, except those materials specifically excluded from University ownership as set forth in the University's Intellectual Property Policy.

"University Information Systems" includes electronic or physical University or externally-hosted systems that are used to collect, store or transmit information, including, without limitation, email, University-owned computers, communications equipment and software, University network accounts, file cabinets, storage cupboards, and internal mail or delivery systems.

Summary of Responsibilities

General Responsibilities for Users

All members of the UVM community are Users of UVM's information resources even if they do not have responsibility for managing information resources. Students, staff, faculty, contractors, consultants, and temporary employees all have access to University information (e.g., file cabinets, documents, office desks, account passwords). Users should be aware of and comply with the University's policies that pertain to the privacy of information as identified in the Privacy policy's elaboration section. In circumstances where Users have access to, or use of, PPD, they are responsible for protecting the privacy of that information wherever it is located; this responsibility includes preventing non-approved disclosure or sharing of PPD. In addition, Users that become aware of a potential breach of PPD should report the incident in accordance with the University's Data Breach Notification policy.

Responsibilities for University Employees

In addition to the above described User responsibilities, Employees have the following responsibilities

1. In accordance with the University's Code of Conduct and Ethical Standards, University Employees must use reasonable diligence to maintain the confidentiality of information entrusted to them by the University or its students, alumni, employees or others with whom the institution has a business or fiduciary relationship, except when disclosure is properly authorized or legally mandated. This confidentiality principle applies to non-public information that may personally identify an individual, regardless of whether that information meets the definition of PPD under this policy University personnel must take reasonable steps to protect and restrict the transfer of such confidential information to unauthorized persons and must share such information within the University on a "need-to-know" basis. All relevant protocols applicable to the safeguarding of information, including computer use protocols, must be followed.
2. University Employees must be able to identify and recognize what information constitutes PPD in the course of their professional activities.
3. University Employees may access only the PPD needed to perform their legitimate duties as a University employee.
4. University Employees must shred physical documents, CDs, DVDs, or other similar media containing Protected Personal Data using a University-approved device or service before being discarded.
5. University Employees may not in any way obtain, divulge, copy, release, sell, loan, alter or destroy any PPD except as authorized within the scope of their professional activities.
6. University Employees must keep work areas clear of PPD and configure computer workstations to blank and lockout screens after ten minutes of inactivity, requiring a password to unlock upon return. Employees should consciously activate screensaver/lockout when leaving visual proximity of their workstations.
7. University Employees must report any activities that are suspected to compromise PPD according to the Data Breach Notification Policy.
8. University Employees' obligation to protect PPD continues after leaving the University
9. Federal and state laws create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, University Employees who receive such compulsory requests must contact the Office of the General Counsel before taking any action.
10. University Employees must be careful not to disclose PPD entrusted to their care by an outside party, especially when such information is governed by the terms of a confidentiality agreement or clause ("non-disclosure agreement") with that party.
11. University Employees must follow relevant security procedures identified in the Information Security Policy and Procedures for Protected University Information (PPD is a form of Protected University Information as defined in that policy) under the "Employees Responsibilities" section.

Special considerations regarding Personally Identifiable Information (PII)

12. (i) In order to protect against potential identity theft from unauthorized disclosure of PII, the University requires that its employees take extra precautions when collecting, using,

or storing sensitive PII. As defined in the Privacy Policy, PII is a subset of PPD that includes an individual's name in conjunction with other specific sensitive personally identifying information. This data must be collected or used only for justifiable business needs **and** only when there is no reasonable alternative. **Under no circumstances should PII be exchanged via unencrypted e-mail, since e-mail may be transmitted or stored insecurely.**

(ii) Social Security Numbers (SSN's) should not be used as an internal identifier on forms, reports, screens, etc, nor may SSN's be printed on any materials mailed to an individual unless required to do so by federal or state law.

Special considerations for the use of Biometric Data.

13. Due to the nature of biometric records, ensuring the security thereof and protecting the privacy of those using biometric technologies is of the utmost importance. Therefore, all proposed uses of biometrics must be processed in consult with the University's Chief Compliance and Privacy Officer and Chief Information Security Officer.

Responsibilities of Managers and Supervisors

In addition to the aforementioned responsibilities, managers and supervisors must:

1. Ensure that departmental procedures support the objectives of confidentiality defined by the Data Stewards (as identified in the Information Security Policy and Procedures) and designees, and that those procedures are followed.
2. Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer PPD in any form, physical or electronic.
3. Ensure that each staff member understands his or her responsibilities related to information privacy.
4. When hiring, determine the extent to which particular positions will require access to private information and will screen applicants accordingly, as the ability to properly manage and protect information may be an essential function of many University jobs. Hiring officials and supervisors may require the execution of confidentiality agreements as a condition of employment.
5. Follow relevant security procedures identified in the Information Security Policy and Procedures for Protected University Information (PPD is a form of Protected University Information as defined in that policy) under the "Managers and Supervisors" section.

Responsibilities of Technology Managers

In addition to, as applicable, the aforementioned responsibilities, those who manage computing and network environments that capture, store, process and/or transmit University information, are responsible for following industry-standard procedures to secure their systems against intrusion or accidental exposure and for ensuring that the requirements for privacy as defined by the appropriate Data Steward (as identified in the Information Security Policy and Procedures) are being satisfied within their environments. They are also responsible to ensure that staff members understand the privacy of the data being handled and the measures used to secure it. The Information Security Policy and Procedures identifies additional security measures for

PPD (which is a subset of Protected University Information as defined in that policy) under the "Technology Managers" section.

Responsibilities of Data Stewards (refer to the Information Security Policy and Procedures for list of Data Stewards [http://www.uvm.edu/policies/cit/infosecurityprocedures.pdf])

In addition to, as applicable, the aforementioned responsibilities, Data Stewards are responsible for

1. Working with the Office of Compliance and Privacy Services, the University Information Security Office, and the Office of the General Counsel to understand the privacy requirements of information as defined by federal and state laws and contractual obligations.
2. Defining the process for implementing the privacy requirements for the information for which they are responsible.
3. Following the specific procedures outlined in the Information Security Policy and Procedures to meet privacy requirements through developing systems to secure the information for which they are responsible.
4. Ensuring that contracts with third-party contractors include provisions for maintaining the privacy of the University's information resources. Refer to the Information Security Procedures for sample agreements. (http://www.uvm.edu/policies/cit/infosecurityprocedures.pdf)
5. Follow relevant security procedures identified in the Information Security Policy and Procedures for Protected University Information (PPD is a form of Protected University Information as defined in that policy) under the "Data Stewards" section.

Responsibilities of Component HIPAA Privacy Officers

Each designated HIPAA-covered University component shall identify a Component HIPAA Privacy Officer (CHPO) who is responsible for protecting the privacy of PHI for that component. The responsibilities of the CHPO include, without limitation, applying the requirements of HIPAA and HITECH within their component; maintaining and distributing Privacy Notices, ensuring training for individuals with access to PHI, and responding to, and reporting as required, incidents of alleged privacy noncompliance. The CHPO shall make any attestation with respect to compliance with the foregoing, on a periodic basis, as requested by the Chief Compliance and Privacy Officer and shall work with the Chief Compliance and Privacy Officer, collaboratively, to address any compliance gaps.