



Privacy

Policy Statement

The University of Vermont is committed to protecting the privacy of individuals whose Protected Personal Data (PPD) is collected or obtained by the University. The University is subject to numerous laws that govern the privacy of PPD including the collection, storage, transfer, use and access to Protected Personal Data. The requirements generally vary according to the type of information being protected. Compliance with these laws and regulations is required by this Policy and as outlined in related University Policies and Procedures governing this information. University employees are responsible for their compliance with this and other University policies and procedures.

However, the University is a public institution and subject to Vermont Open Records Act. Not all personal information is protected by law. Some personal information is considered Public Information; this information may be shared by the University in certain circumstances.

Reason for the Policy

Individuals providing PPD to the University have legal privacy rights and an expectation that the University will honor these rights and protections in accordance with Federal and State laws and regulations. This policy is intended to meet these privacy rights and expectations and to minimize the risks to individuals of compromised Protected Personal Data.

Applicability of the Policy

This Policy and accompanying Procedures apply to all members of the University community, including, without limitation, individuals who are faculty, staff, students, contractors, consultants, temporary employees, and affiliates of the University.

Policy Elaboration

The University will collect PPD when necessary to conduct University business and will limit the access, use and disclosure of this information as prescribed by University Policies and Procedures and in accordance with applicable laws and regulations. Acting within those

constraints, the University will not share PPD with third parties unless required to do so to transact University business, to comply with federal or state law or regulation, or as disclosed in University policies and disclosure statements. As defined in this policy PPD includes Personally Identifiable Information, Protected Student Information, Protected Health Information, and Protected Library Records. All PPD is protected under either federal or state law. In addition to this policy, the University has issued other policies and/or statements addressing an individual's rights and protections concerning specific personal information. These include:

- the FERPA Rights Disclosure Policy for student educational records (<http://www.uvm.edu/policies/student/ferpa.pdf>);
- the HIPAA privacy notices for protected health information obtained by the University's covered HIPAA components; and
- the University Libraries Confidentiality Policy Statement and Procedures for protected library records (<http://library.uvm.edu/about/policies/privacy.php>).

The University's commitment to protecting personal information extends beyond PPD as defined in this policy to other, non-public personal information that may identify an individual. This information should be treated as confidential, protected from unauthorized access and shared on a "need-to-know" basis. Examples of such additional personal information may include, without limitation, biometric data, vehicle registration, date of birth, and certain personnel records.

Additionally, the University's Information Security Policy and Procedures address safeguarding of PPD to meet privacy requirements.

Agreements with third party vendors or consultants who will have access to PPD must ensure that the vendor is subject to obligations of confidentiality that will enable the University to continue to comply with its own obligations under applicable laws and regulations.

Members of the University community should know that laws protecting the confidentiality of information generally include exemptions to allow compliance with subpoenas, court orders, or other compulsory requests from law enforcement agencies. University Employees who receive such compulsory requests must follow the University Policy on Subpoenas, Complaints, Warrants and other Legal Documents.

Suspected breaches of PPD must be reported in accordance with the University's Data Breach Notification Policy at http://www.uvm.edu/policies/general_html/databreach.pdf.

Failure to follow the University's policies and procedures governing the privacy of PPD may result in disciplinary action up to, and including, dismissal.

The scope of privacy regulation at the University, includes but is not limited to:

- Vermont Protection of Personal Information (Act 162)
- Health Insurance Portability and Affordability Act (HIPAA)
- HIPAA – HITECH Act

- Family Education Rights and Privacy Act (FERPA)
- Gramm-Leach Bliley Act (GLBA)
- Genetic Information Nondiscrimination Act (GINA)
- Vermont Library Patron Records Act (22 VSA 171 et. seq.)

Definitions

Protected Personal Data (PPD): includes, without limitation, personally identifiable information, protected health information, protected student information, and protected library records as described below. Protected Personal Data includes data maintained in any electronic or hard copy medium:

- Personally Identifiable Information (PII) – under 9 V.S.A. §2430(5) is defined as an individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized person:
 - Social Security number;
 - Motor vehicle operator’s license number or non-driver identification card number;
 - Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
 - Account passwords or personal identification numbers or other access codes for a financial account.
- Protected Health Information (PHI) –includes identifiable health information as defined at 45 CFR §160.103 that is transmitted or maintained by the University’s covered HIPAA components; PHI also includes identifiable health information that is obtained by a University member pursuant to an agreement with another organization or governmental entity and which is protected under the HIPAA/HITECH Act.
- Protected Student Information – means student education records maintained by the University, whether by academic or administrative units, and protected under the Family Educational Rights and Privacy Act (FERPA) and as described more fully in the UVM FERPA Rights Disclosure policy (<http://www.uvm.edu/policies/student/ferpa.pdf>).
- Protected Library Records – means patron registration records that contain the information a University library patron must provide to be eligible for library privileges and patron transaction records that contain personally identifiable information related to an individual’s activities within the University libraries.

Public Information: describes information that may be legally disclosed to any person inside or outside the University. This information includes, but is not limited to, directory information and other information that the University makes accessible in its public documents, publications or website. This information also includes information that the University may not make public or disclose as a matter of ordinary practice, but may be required to be disclosed upon receipt of a public records request.

Procedures

Privacy Policy Procedures (http://www.uvm.edu/policies/general_html/privacyprocedures.pdf)

Additional procedures concerning the safeguarding of PPD are detailed in the University's Information Security Policy and related Procedures.

(<http://www.uvm.edu/policies/cit/infosecurityprocedures.pdf>)

Procedures related to potential breaches of PPD are outlined in the University's Data Breach Notification Policy (http://www.uvm.edu/policies/general_html/databreach.pdf).

Forms

None

Contacts

Questions related to the daily operational interpretation of this policy should be directed to:

Chief Information Officer and Dean of University Libraries
(802) 656-2003

The Chief Privacy Officer is the official responsible for the interpretation and administration of this policy.

Related Documents/Policies

Code of Conduct and Ethical Standards

http://www.uvm.edu/policies/general_html/businessconduct.pdf

Data Breach Notification

http://www.uvm.edu/policies/general_html/databreach.pdf

FERPA Rights Disclosure

<http://www.uvm.edu/policies/student/ferpa.pdf>

HIPAA Disclosures

https://www.uvm.edu/compliance/hipaa_information

Information Security

<http://www.uvm.edu/policies/cit/infosecurity.pdf>

Privacy Services – Additional Information on Privacy Issues

http://www.uvm.edu/compliance/compliance_matrices

Records and Documents Requests

http://www.uvm.edu/policies/general_html/records_request.pdf

Records Retention

http://www.uvm.edu/policies/general_html/recordretention.pdf

Subpoenas, Complaints, Warrants and other Legal Documents

http://www.uvm.edu/policies/general_html/subpoenas.pdf

University of Vermont Libraries Confidentiality Policy Statement and Procedures
<http://library.uvm.edu/about/policies/privacy.php>

Effective Date

Approved by the President on August 18, 2012