POLICY

FOR PRINTED USE ONLY

Policies residing on UVM's Institutional Policy website are the most current versions available. If you are viewing a policy anywhere else

protected library records as described below. NPPD includes data maintained in any electronic, recorded or hard copy format. NPPD includes all of the following:

- Confidential Information is non-personal, non-public information that the University, a regulatory agency or another authority has determined must be kept private. This generally includes proprietary information, trade secrets, intellectual property, inventions and research data/results, user login credentials, technology systems and network information, information security plans and data mapping, and information that is otherwise exempt from the Vermont Open Records Law.

- Controlled Unclassified Information (CUI): is information that is provided by agencies of the federal government generally, but not exclusively, for research purposes. CUI requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

- Non-Public Information (NPI): under the Gramm-Leach-Bliley Act (GLBA), non-public information is defined as any information that is not publicly available and that (i) a consumer provides to a financial institution to obtain a financial product or service from the institution; (ii) resul-1.6 (o.6 ( )t0.7 r (i)-1. ( )-0.6 (s)MrC. ( )-0.6 (c)0(h)-0.9 (-1

diagnosis or treatment of the consumer, or a health insurance policy number.

- Protected Health Information (PHI) Under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), PHI includes individually 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, such as a business associate (45 CFR 160.103).

The University is a public institution and subject to Vermont Open Records Act. Not all NPPD is protected by law. Some NPPD may be considered Public Information. In certain circumstances, this information may be shared by the University; however, all public records requests must comply with UVM's Records and Documents Requests Policy. Other members of the UVM community may not respond to any Open Records request without express permission from the University's Public Records Act Official.

II. Collection

The University will collect the minimum amount of NPPD that is necessary to conduct University business. If the NPPD is not necessary to satisfy a business-related purpose, it must not be collected.

Prior to collecting NPPD, the need must be assessed to determine the minimum amount of NPPD necessary to satisfy the purpose. NPPD can only be collected by lawful and fair means and members of the University community authorized to collect NPPD must be transparent regarding the planned and anticipated uses of NPPD. Where appropriate, Data Subjects must be advised the reasons for collection no later than the time of data collection and under certain conditions consent must be obtained from the Data Subject prior to the collection and/or use of the NPPD.

III. Access and Use

The University will limit the access, use and disclosure of NPPD as prescribed by University Policies and Procedures and in accordance with applicable federal, state and international laws and regulations.

Access to NPPD will be assigned based on purpose of the access and role of the individual. Whenever possible, a technology solution will be implemented to control access. In the event that it is technologically infeasible to limit access, access will be limited based on policy. For more information on the appropriate use of assigned credentials, see the University Computer, Coclp (re) (o)6.C BT 0rnationnal ac( )-0.6 (re

V. Safeguarding/Data Security

The University's Information Security Policy and Procedures address safeguarding of NPPD, confidential information, and available technology designed to meet the University's regulatory requirements.

VI. Exclusion From UVM Directories

Employees/Affiliates:

In the event an employee has reasonable grounds to believe that the public availability of their personal information poses a safety risk, including but not limited to such circumstances as intimate partner violence, relief from abuse order, threats, harassment, or other similar circumstances, they may request their directory information be removed or limited from the available directories. Requests may be made to the payroll office at payroll@uvm

is received it shall swiftly be forwarded to police services for review and safety planning as necessary. If police services concurs that there are reasonable grounds to believe a safety concern exists, it shall swiftly communicate that information and forward the request to the information security team who will remove the information from the necessary directories. Employee information may be reinstated to the directories upon request of the affected employee.

IX. Third Parties

Agreements with third party vendors or consultants who will have access to NPPI must ensure that the vendor is subject to obligations of privacy, security and confidentiality that will enable the University to continue to comply with its own obligations under applicable laws and regulations. To reduce the likelihood that a contract or agreement will be delayed, those contemplating an agreement for information technology, digital or electronic products or services should consult with the Office of Information Security as soon as possible in the process; ideally prior to the contract phase.

X. Statutory Exemptions

Laws protecting the privacy and 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 Subpoenas, Complaints, Warrants and other Legal Documents Policy.

XI. Breach Notification

The University may have breach notification responsibility depending on the type of data that has been breached and the regulations impacting that data. Suspected breaches of NPPI must be reported in accordance with the University's Data Breach Notification Policy.

XII. Violations and Disciplinary Action

Confirmed violations may result in disciplinary action. In some instances, the University may be required to file a report with applicable branches of the federal or state government, to international enforcement agencies, or to law enforcement. In those cases, individuals may be held personally responsible for criminal sanctions imposed as a result of the violation. Procedures for the investigation of suspected violations, imposition of disciplinary action, and the availability of grievance or appeal channels shall be governed by otherwise applicable University policies, handbooks, and collective bargaining agreements.

Contacts

Questions concerning the daily operational interpretation of this policy should be directed to the following (in accordance with the policy elaboration and procedures):	
Title(s)/Department(s):	Contact Information:
Chief Privacy Officer	privacy@uvm.edu
Chief Information Officer	cio@uvm.edu
Information Security Officer	iso@uvm.edu
Dean of Libraries	bhref@uvm.edu
Registrar	

Related Documents/Policies

- Code of Conduct and Ethical Standards
- Data Breach Notification Policy
- FERPA Rights Disclosure
- HIPAA Disclosures
- Information Security Policy
- Privacy Services - Additional Information on Privacy Issues
- Records and Documents Requests Policy
- Records Management and Retention Policy
- Subpoenas, Complaints, Warrants and other Legal Documents Procedure
- University of Vermont Libraries Confidentiality Policy Statement and Procedures

Regulatory References/Citations

- Family Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)
- Genetic Information Nondiscrimination Act (GINA)
- Gramm-Leach Bliley Act (GLBA) (15 USC § 6801)
- Health Information Technology for Economic and Clinical Health Act (HITECH) of HIPAA (45 CFR Parts 160 and 164)
- Health Insurance Portability and Affordability Act (HIPAA) (45 CFR Parts 160, 162 and 164)
- The European Union's General Data Protection Regulations (GDPR)
- Vermont Disclosure of Information Statute (18 V.S.A. § 7103)
- Vermont Library Patron Records Act (22 VSA 171 et. seq.)
- Vermont Protection of Personal Information (62 V.S.A. § 2430)
- Vermont Security Breach Notice Act (9 V.S.A. § 2435)

Training/Education

Training/education related to this policy is as follows:

Training Topic:	FERPA		
Training Audience:	Employees/Faculty with Access to Student Record Information	Delivered By:	Registrar's Office
Method of Delivery:	Self-Study	Frequency:	Upon Hire

Training Topic:	Gramm-Leach-Bliley Act (GLBA)		
Training Audience:	Employees/Faculty with Access to Student Financial Aid Information	Delivered By:	Student Financial Services (SFS)
Method of Delivery:	Self-Study	Frequency:	Prior to Granting Access and Annu Refresher

Training Topic:	Health Insurance Portability and Accountability Act (HIPAA) Training	
Training Audience:	Employees/Faculty in Covered Components with Access to PHI	Delivered By: