IRM-003

Data Protection of University Information

Effective Date Monday, October 23, 2017

Status Final

Last Revised Wednesday, December 21, 2022

Policy Type University

Contact Office
University Information Security (InfoSec)

Oversight Executive
Vice President and Chief Information Officer

Applies To
Academic Division The Medical Center The College at Wise University-Associated Organization

Table of Contents

Reason for Policy

The University of Virginia (the “University”) is strongly committed to safeguarding information assets against unauthorized access, alteration, or loss. This policy establishes a data protection strategy for all University information assets based upon sensitivity and defines responsibilities of members of the University community, each of whom has a duty to protect institutional data. The appropriate level of protection is reached when data handling restrictions are sufficient to offset the risk of harm posed by a data breach but do not interfere with the University’s mission.

In addition to institutional considerations, there are numerous legal, regulatory, and contractual obligations that govern how data must be protected. This policy is meant to establish the baseline approach for how data is classified. It is intended to be used in concert with related standards, procedures, and guidelines and in consultation with data stewards.

Definition of Terms

Access (to data)

The capacity for data users to enter, modify, delete, view, copy, or download data.

Data Users

Individuals who acknowledge acceptance of their responsibilities, as described in this policy, and its associated standards and procedures, to protect and appropriately use data to which they are given access; and meet all prerequisite requirements, e.g., attend training before being granted access.

Classified Data

Data whose sensitivity level falls within a hierarchical schema established by the federal government according to the degree to which unauthorized disclosure would damage national security. Access to classified data typically requires a formal security clearance level relative to the sensitivity of the classified data for which the access is requested. Ranging from most sensitive to least, those levels include Top Secret, Secret, Confidential, and Public Trust. The misuse of classified data may incur criminal penalties and significant reputational damage.

Controlled Technology

For purposes of this policy, this term includes any item, component, material, software, source code, object code, or other commodity specifically identified on the Commerce Control List [Part 774 of the Export Administration Regulations (EAR)] or U.S. Munitions List [Part 121 of the International Traffic in Arms Regulations (ITAR)]. This term also includes information to the extent required in the applicable regulation.

Data

Text, numbers, graphics, images, sound, or video and in any format, electronic or paper. The University regards data maintained in support of a functional unit's operation as University data if they meet at least one of the following criteria: If

1. at least two administrative operations of the University use the data and consider the data essential;
2. integration of related information requires the data;
3. the University needs to verify the quality of the data to comply with legal and administrative requirements for supporting statistical and historical information externally;
4. a broad cross section of University employees refers to or maintains the data;
5. the University needs the data to plan; or
6. created, received, maintained, and/or transmitted in the course of meeting the University’s teaching, research, public service, and healthcare missions.

Some examples of such University-owned data include student course grades, patient records, employee salary information, research, vendor payments, and the University's annual Common Data Set.

Data Stewards

University officials who have operational oversight for the life cycle of a specific data domain including the definition, intake, and usage of the data. Data Stewards will oversee the development, maintenance, and enforcement of appropriate policies, standards, and procedures for the use of data in their functional areas, including defining criteria for data access authorization and have final sign-off authority for users seeking to access, retrieve, manipulate, or view data for their respective data domains.

Data Stewards are assigned by, and are accountable to, Data Trustees. Institutional data stewards help define, implement, and enforce data management policies and procedures within their specific data domain. Institutional data stewards have delegated responsibility for all aspects of how data is acquired, used, stored and protected throughout its entire lifecycle from acquisition through disposition.

Data Domain

The entire collection of data for which a University employee assigned the role and responsibilities of a Data Trustee, Data Steward, or Deputy Data Steward is responsible. Each Data Domain (or subdomain) has a Data Trustee and a Data Steward. Deputy Data Stewards are appointed as needed by Data Stewards to complete data stewardship activities. The data domain also includes rules and processes related to the data.

Data Trustees

Senior University officials who have planning and policy-level responsibilities for a large subset of the institution's data resources. They: (1) oversee the implementation of this policy for their data domains; (2) determine the appropriate classification of institutional data (highly sensitive, sensitive, internal use, or public) in consultation with executive management and appropriate others; and (3) appoint Data Stewards for their data domains.

Data trustees provide a broad, university-wide view of data, approve policies, resolve questions of procedure, and ensure that data plans are consistent with and in support of university strategic plans.

Deputy Data Stewards

Individuals appointed as needed by Data Stewards to complete data stewardship activities, such as authorizing or rejecting access requests based upon approval criteria established by the Data Stewards who appoint them.

Electronic Device

Electronic equipment, whether owned by the University or an individual, that has a processor, storage device, or persistent memory, including, but not limited to: desktop computers, laptops, tablets, cameras, audio recorders, smart phones and other mobile devices, as well as servers (including shared drives), printers, copiers, routers, switches, firewall hardware, network-aware devices with embedded electronic systems (i.e., "Internet of Things"), supervisory control and data acquisition (SCADA) and industrial control systems.

Electronic Media

All media, whether owned by the University or an individual, on which electronic data can be stored, including, but not limited to: internal and external storage devices (e.g., solid state and hard drives, USB thumb drives, Bluetooth connected storage devices), magnetic tapes, diskettes, CDs, DVDs.

Electronically Stored Information (ESI)

Information created, manipulated, stored, or accessed in digital or electronic form.

Employee (5)

An individual who is an *employee (2)*, *contractor employee*, *medical center employee*, and/or *affiliated organization employee*, as well anyone else to whom University IT resources have been extended. These include, but are not limited to, recently terminated employees whose access to University IT resources have not yet been terminated, deleted, or transferred, and individuals whose University IT resources continue between periods of employment. This also includes student workers, volunteers, and other individuals who may be using state-owned or University IT resources and carrying out University work.

Affiliated Organization Employee

An individual who is an employee of one of the officially recognized University-Affiliated Organizations.

Contractor Employee

An individual who is an employee of a firm that has a formal contractual relationship with the University and has been assigned to work at the University for the duration of the contract.

Employee (2)

As used in this policy, includes all faculty (teaching, research, administrative and professional), professional research staff, university and classified staff employed by the University in any capacity, whether full-time or part-time, and all those employees in a wage or temporary status.

Medical Center Employees

Individuals employed by the University of Virginia Medical Center in any capacity.

Export and “Deemed Export”

An export is any shipment or transmission of controlled technology out of the U.S. The term "deemed export" is commonly used to refer to the release of controlled information (as specified in the regulations) to a foreign national in the U.S. Under the regulations, such a transfer is deemed to be an export to the individual’s home country.

Highly Sensitive Data

Data that require restrictions on access under the law or that may be protected from release in accordance with all applicable laws or regulations, such as Virginia Code § 18.2-186.6. Breach of Personal Information Notification. Highly Sensitive data (HSD) currently include personal information that can lead to identity theft. HSD also includes health information that reveals an individual’s health condition and/or medical history.

Specific examples include, but are not limited to:

- *Any store or file of passwords or user-ids and passwords* on any multi-user system or computer.
- *Personal information that, if exposed, can lead to identity theft.* This may include a personal identifier (e.g., name, date of birth) as well as one of the following elements:
    - Social security number;
    - Driver’s license number or state identification card number issued in lieu of a driver’s license number;
    - Passport number;
    - Financial account number in combination with any required security code, access code, or password that would permit access to a financial account;
    - Credit card or debit card number, including any cardholder data in any form on a payment card; or
    - Military Identification Number.
- *Health information, which is any information that, if exposed, can reveal an individual’s health condition and/or history of health services use, including information defined by* Health Insurance Portability and Accountability Act *(HIPAA) as protected health information (PHI).*

- **Cardholder Data (CHD):** Primary cardholder account number that identifies the issuer and a particular cardholder account, which can include cardholder name, expiration date and/or service code.

Note: Credit card numbers must never be stored either alone or in combination with any other identifiers.

Also considered HSD are any form of personally identifying information in combination with social security number (SSN), driver's license number, passport number, financial account number and required security code, and/or military ID number. For example, computing ID and driver's license number, or home address and SSN.

Individual–Use Electronic Devices

Electronic equipment, whether owned by the University or an individual, that has a storage device or persistent memory, including, but not limited to: desktop computers, laptops, tablets, smart phones and other mobile devices. For purposes of this policy, the term does **not** include shared purpose devices, such as servers (including shared drives), printers, copiers, routers, switches, firewall hardware, clinical workstations, medical devices (e.g., EKG machines), etc.

Individual–Use Electronic Media

All media, whether owned by the University or an individual, on which electronic data can be stored, including, but not limited to: external hard drives, magnetic tapes, diskettes, CDs, DVDs, and any externally attached storage devices (e.g., thumb drives).

Information Technology (IT) Resources

All resources owned, leased, managed, controlled, or contracted by the University involving networking, computing, electronic communication, and the management and storage of electronic data regardless of the source of funds including, but not limited to:

- Networks (virtual and physical), networking equipment, and associated wiring including, but not limited to: gateways, routers, switches, wireless access points, concentrators, firewalls, and Internet-protocol telephony devices.
- Electronic devices containing computer processors including, but not limited to: computers, laptops, desktops, servers (virtual or physical), smart phones, tablets, digital assistants, printers, copiers, network-aware devices with embedded electronic systems (i.e., "Internet of things"), and supervisory control and data acquisition (SCADA) and industrial control systems.
- Electronic data storage devices including, but not limited to: internal and external storage devices (e.g., solid state and hard drives, USB thumb drives, Bluetooth connected storage devices), magnetic tapes, diskettes, CDs, DVDs.
- Artificial intelligence tools, including generative AI tools such as UVA Copilot and UVAChat+.
- Software including, but not limited to: applications, databases, content management systems, web services, and print services.
- Electronic data in transmission and at rest.
- Network and communications access and associated privilege.
- Account access and associated privileges to any other IT resource.

Internal Use Data

Data that is typically a public record available to anyone by the Virginia Freedom of Information Act (FOIA) but is also not intentionally made public (see the definition of **public data**). Examples may include salary

information, contracts, and specific email correspondence not otherwise protected by a FOIA exemption. For a complete list, see Code of Virginia § 2.2-3700 Virginia Freedom of Information Act.

Public Data

Data intentionally made public and are therefore classified as not sensitive. Any data that are published and broadly available are, of course, included in this classification. University policy holds that the volume of data classified as not sensitive should be as large as possible because the widespread availability of such information will enable others to make creative contributions in pursuit of the University's mission.

Public Record

Any writing or recording — regardless of whether it is a paper record, an electronic file, an audio or video recording or any other format — that is prepared or owned by, in possession of a public body or its officers, employees, or agents in the transaction of public business. Freedom of Information Act. All public records are presumed to be open and may be withheld only if a statutory exemption applies.

Record

Any document, file, computer program, database, image, recording, or other means of expressing information in either electronic or non-electronic form.

Sensitive Data

Data that is a University record that is not highly sensitive data and may be withheld from release under the Virginia Freedom of Information Act (FOIA).

Examples include information concerning the prevention of or response to cyber-attacks, or information that describes a security system used to control access to or use of an automated data processing or telecommunications system; or research records that do not contain Highly Sensitive Data; University ID numbers, i.e., those printed on University ID cards; and/or Family Educational Rights and Privacy Act-protected data not covered under the definition of “Highly Sensitive” data. This category of data also includes any data or record covered by the exemptions listed in the Commonwealth of Virginia Freedom of Information Act.

University Record

Recorded information that documents a transaction or activity by or with any appointed board member, officer, or employee of the University. Regardless of physical form or characteristic, the recorded information is a University record if it is produced, collected, received or retained in pursuance of law or in connection with the transaction of university business. The medium upon which such information is recorded has no bearing on the determination of whether the recording is a University record. University records include but are not limited to: personnel records, student records, research records, financial records, patient records, and administrative records. Record formats/media include but are not limited to: email, electronic databases, electronic files, paper, audio, video, and images (photographs).

Research Record

One type of University record that includes, but is not limited to: grant or contract applications, whether funded or unfunded; grant or contract progress and other reports; laboratory notebooks; notes; correspondence; videos;

photographs; X-ray film; slides; biological materials; computer files and printouts; manuscripts and publications; equipment use logs; laboratory procurement records; animal facility records; human and animal subject protocols; consent forms; medical charts; and patient research files. In addition, research records include any data, document, computer file, computer diskette, or any other written or non-written account or object that reasonably may be expected to provide evidence or information regarding the proposed, conducted, or reported research that constitutes the subject of an allegation of research misconduct.

User

Everyone who uses University IT resources. This includes all account holders and users of University IT resources including, but not limited to: students, applicants, faculty, staff, medical center employees, contractors, University-Associated Organization employees, guests, and affiliates of any kind.

Policy Statement

This policy applies to data in any format, electronic or paper (non-electronic) and to all users of the University's information technology resources, regardless of location or person's affiliation.

Users must comply with all University policies, standards, and procedures for the data to which they have been granted the ability to view, copy, generate, transmit, store, download, or otherwise acquire, access, remove, or destroy. Users must also meet any additional compliance requirements for data protection stipulated by various governmental, legal, or contractual entities, including, but not limited to, those defined for classified information, Controlled Unclassified Information (CUI), International Traffic in Arms Regulations (ITAR) covered data, Payment Card Industry (PCI) regulated data, Health Insurance Portability and Accountability Act (HIPAA) covered data, and Federal Educational Rights and Privacy Act (FERPA) covered data.

A user must protect any data to which they are granted access against unauthorized disclosure and must only use the data for the purpose(s) for which access to the data was granted. In this context, disclosure means giving the data to persons not authorized to have access to or view it. The University also forbids the use of any data for one's own personal gain or profit, for the personal gain or profit of others, or to satisfy personal curiosity.

The University expressly forbids the use of data for anything but the conduct of official University business. It is the responsibility of the data stewards, IT resource owners, IT resource administrators, and users to:

- Verify the correct University data classification (i.e., highly sensitive data, sensitive data, internal use or public data) of any data they view, collect, receive, generate, copy, transmit, store, disclose, or otherwise acquire, access, remove, or destroy.
- Handle such data in compliance with this policy and its associated data protection standards and procedures, including, but not limited to, the University Data Protection Standards (UDPS).
- Observe requirements for confidentiality and privacy, including policy IRM-012: Privacy and Confidentiality of University Information.
- Present the data accurately in any use.

The University and its users must comply with applicable local, state, and federal laws and regulations.

Investigations and/or urgent business needs sometimes require the collection of electronic communications and files that have been stored on University systems by employees or students. Access to electronically stored information (ESI) will only be done with proper approvals from authorizing University and Medical Center officials, as detailed in policy IRM-012: Privacy and Confidentiality of University Information.

Highly sensitive data may not be stored locally on any device including on any individual-use electronic device or media without written approval of an exception by University Information Security (See HSD Protection Standard for Individual-Use Electronic Devices or Media).

Highly sensitive data must be securely encrypted on any individual-use electronic device or media, and while in transit to/from any electronic device or media, according to encryption methods recommended by the:

1. University Information Security Office for academic users, or,
2. Health Information and Technology Security Office for UVa Health System users.

Acceptable authentication must be enabled for every electronic device and, if available, electronic media. The acceptable authentication must meet or exceed the requirements as defined in the University Data Protection Standards (UPDS) and the Authentication Standard.

Authentication must not be shared with anyone or used to allow others access they are not otherwise granted.

The collection, storage, or transmission of University data may not be outsourced to any party external to the University that does not have a contract with the University without the written approval of the appropriate UVa Academic or Health System Chief Information Officer (CIO) or their designate using the University Information Security exception process.

1. **Data Release:**
   All University data must be appropriately protected to provide for a controlled and lawful release. Access to legally restricted (e.g., Family Educational Rights Privacy Act - FERPA) or limited-access data by University users or non-UVa employees sponsored by a University manager, requires that a written request be made to the appropriate Data Trustee, Data Steward, or Deputy Data Steward, following the guidance in the Highly Sensitive Data Protection Standard.

   The removal of all software and data on electronic devices and electronic media when the device or media will be returned, repaired, surplussed, removed from service or transferred to another employee must follow the standards and procedures provided in the Electronic Data Removal Standard and Electronic Data Removal Procedures. The University's policy IRM-017: Records Management must be used for guidance regarding what is required for the retention, disposition, and destruction of University records.

2. **International Travel:**
   Traveling with or exporting any of the following requires prior approval from the Office of Export Control as detailed in the University's policy FIN-043: Managing Exports of Controlled Technology to Foreign Persons and Destinations in Support of Research and Scholarship:

   - University-owned equipment (e.g., individual-use electronic devices or media such as a laptop or smartphone),
   - any University data that is not publicly available,
   - any controlled technology, or
   - technical information subject to publication or dissemination restrictions (which may include research results).

3. **Compliance with Policy:**
   Any misuse of data or IT resources may result in the limitation or revocation of access to University IT resources. In addition, failure to comply with the requirements of this policy and/or its standards may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies.

   Violation of this policy may also violate federal, state, or local laws.

   Questions about this policy should be directed to University Information Security (InfoSec).

Procedures

Data Protection	
Standards and Procedures	
Standards	**Procedures**
Electronic Data Removal	Electronic Data Removal
Protection of Highly Sensitive Data Standard	Protection of Highly Sensitive Data Procedures
HSD Protection for Individual-Use Electronic Devices or Media	HSD Protection for Individual-Use Electronic Devices or Media
ESI Release	ESI Release
University Data Protection 3.0	
Vendor Security Review	
	Exceptions

How to Request Access to UVA Systems

Related Information

FIN-043: Managing Exports of Controlled Technology to Foreign Persons and Destinations in Support of University Activities
Encryption and Export Administration Regulations (EAR)
Procurement and Supplier Diversity Services Surplus Procedure

In addition to being a widely accepted security and privacy practice, effective data removal is required by state and federal regulations. See:

> Gramm-Leach-Bliley Act of 1999, Standards for Safeguarding Customer Information; Final Rule
> Health Insurance Portability and Accountability Act of 1996 Health Insurance Reform: Security Standards; Final Rule

IRM-004: Information Security of University Technology Resources
IRM-017: Records Management
STU-002: Rights of Students at the University of Virginia Pursuant to the Family Educational Rights and Privacy Act

Physical Records Storage Standards

University of Virginia Registrar's guidance on FERPA

Federal regulations including but not limited to the following:

- The Family Educational Rights and Privacy Act ("FERPA", also referred to as the "Buckley Amendment"), 20 U.S.C. §1232g.
- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191 and implementing regulations issued by the U.S. Department of Health and Human Services including Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 ("Privacy Rule").
- The Gramm-Leach-Bliley Act ("GLBA") 15 U.S.C §6801 et seq, and implementing regulations issued by the Federal Trade Commission including Standards for Safeguarding Customer Information (the "Safeguards Rule"), 16 CFR Part 314; and The Privacy Act of 1974, 5 U.S.C. § 552a (2000).

Commonwealth of Virginia laws including but not limited to: Health Records Privacy Act, Va. Code 32.1-127.1:03

Information Security Awareness for Faculty and Staff

Health System Policies:
Health System's Health Insurance Portability and Accountability Act (HIPAA)
Policy No. 0201: Patient Identification
Policy HPA-005: Verification for Release of Patient Information

School of Medicine Policies:
1.430. Required HIPAA Privacy Training
1.431. Violations of Confidentiality

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191 and implementing regulations issued by the U.S. Department of Health and Human Services including Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164 ("Privacy Rule") and 42 CFR 431.305.

Institutional Review Board for Health Sciences Research: Medical Record Review

Major Category Information Resource Management

Next Scheduled Review Sunday, December 21, 2025

Revision History
Revised 12/21/22; Updated 3/17/20; Updated definition 5/15/19, Revised 10/23/17.

Applies To Text

Academic Division, the Medical Center, the College at Wise, and University-Associated Organizations.

Supercedes Policy Text

IRM-004, Electronic Data Removal; IRM-014, Protection and Use of Social Security Numbers; IRM-015, Electronic Storage of Highly Sensitive Data; Administrative Data Access; Appendix A (Data Classifications); Appendix B (Data Roles and Responsibilities); Information Release (Requests for Electronically Stored Information).

Last modified March 5, 2024 - 10:09am

Approved By Policy Review Committee

Approved Date June 27, 2017 - 12:00pm