POLICY

Data Security Classification Policy

LAST REVISED ON 06/25/2020

This University-wide policy was approved by President Sarah Mangelsdorf.

Applies to: This policy applies to all information handled in the course of university business, including but not limited to education, research, healthcare, and administration. For purposes of this policy, information is defined as any points of data however recorded in any medium including information about the information (metadata) and regardless of the actions (e.g. use, access, storage, management) or origination (e.g. created, collected, received, contracted).

Purpose: The purpose of this policy is to define the classifications of data, introduce some appropriate handling measures, and present the required security controls associated with the data classification to establish consistency across the organization, including the University of Rochester, including but not limited to the University of Rochester Medical Center.

This policy is not intended to supersede the law but is intended to be the governing rule for instances not covered by legal statute or the policies detailed in Appendix B.

Principle: Enable the sharing of data as broadly as possible subject to legal and regulatory restrictions and following University security and privacy policies and standards.

I. Policy

University information will be classified based on the risk posed to the University by inappropriate access, use, or handling of those data.

Data should be handled in alignment with the process for the highest risk classification of any data element contained within the system, collection, or set. If you have a question on the classification of data, please contact an Information Security Officer or Privacy Officer.

II. Classifications and Guidelines

A. High Risk

Definition: Data are classified as High Risk when protection of such data is required by law or regulation, protection is necessary in order for the University or its affiliates to meet compliance obligations, or the unauthorized disclosure, access, alteration, loss or destruction of those data could have a material impact on the University or its affiliates' mission, assets, operations, finances, or reputation, or could pose material harm to individuals.

Examples: Examples include, but are not limited to, occurrences of personally identifiable information when it is specifically protected by applicable law or regulation (PII), protected health information (PHI), payment card information (PCI), employee background investigations, employee immunization information, student information protected by FERPA, special categories of personal data identified by GDPR, as well as records and supporting materials of internal investigations performed to meet policy, regulatory, or legal requirements. In addition, any data the University receives that are contractually restricted,

including research data, should be considered High Risk. For some industry sponsored research, the raw data may be considered high risk but the results can be more broadly shared. The University may extend High Risk requirements to items not specifically listed above as warranted.

Access and use: Access to High Risk information must be carefully safe-guarded. High Risk information must be stored, used, and disclosed to those who have a documented business need and who have followed the appropriate access management procedure. Such procedures may require special training, data use agreements, or other documentation. Protection of High Risk information is the responsibility of everyone who is granted access or uses such data.

Alternatives to using High Risk Information should be identified and used whenever possible.

Specific University policies may apply to particular data in this classification, e.g., Secure Handling of Social Security Numbers, Security of Electronic Protected Health Information, Information, protected by FERPA, etc. See Appendix B for related policies.

High Risk information must be protected even if the data are allowed to be shared outside the University. Disclosure of High Risk Information to a third party agent or vendor is permitted only if the agent or vendor assumes a legally binding obligation to safeguard the use and disclosure of the information (unless applicable law or regulation expressly allows for the disclosure without such a safeguard).

Storage and protection: High Risk Information in paper form must be stored in locked or otherwise secured areas when not in active use. High Risk Information in electronic form must be stored securely according to established procedures (see Appendix C). It must not be stored on desktop, laptop, or other portable devices or media without encryption or

similar protection. High Risk data stored, processed, or managed by vendors or other third parties must also be similarly protected. Contact an Information Security Officer or a Privacy Officer for advice and assistance.

Transmission: Reports and communications should not include High Risk Information unless essential to perform the function for which the communication is made. Transmission of High Risk data must be by secure methods. If High Risk data are transmitted by e-mail or other electronic transmission, they must be encrypted or otherwise adequately protected. The electronic exchange of High Risk Information outside of the University of Rochester must have proper approval and follow documented procedures (see Appendix C).

Labeling of High Risk Information: Information that is classified as High Risk should be clearly labeled as such. It is a best practice to provide such a label to warn others clearly that this information is High Risk and should be treated accordingly.

Destruction: When a record containing High Risk information is no longer needed according to record retention guidelines, it must be disposed of in a manner that makes the High Risk data no longer readable or recoverable. Destruction of paper records containing High Risk data normally should be accomplished by shredding. Destruction of electronic records containing High Risk data begins with deleting the data from its storage location(s), i.e. from all systems and devices including email, trash, backup, and file storage.

Reporting Unauthorized Disclosure of High Risk Information: Prompt reporting of unauthorized disclosure of High Risk Information is essential for the University to meets its obligations under law, regulation, and contract. The University will not take disciplinary action against any person solely because of his or her good faith reporting of a disclosure. Individuals who report violations of this Policy will be protected from retaliation resulting from providing information. Individuals who report violations of this Policy to the Hotline can remain anonymous.

B. Moderate Risk

Definition: Much information necessary for people to perform their work at the University is properly available to others at the University but is not appropriate to be known by the general public. Data should be classified as Moderate Risk where the unauthorized disclosure, access, alteration, loss or destruction of those data would be expected to have an adverse but not material impact on the University and its affiliates' mission, assets, operations, finances, or reputation, or only limited harm to individuals. This information is made available to members of the University community with a business need and is not restricted by local, state, national, or international statute regarding disclosure or use.

Examples: Examples include, but are not limited to, budgets, strategic or unit business plans, proposals, contracts, many policies and procedures, correspondence, grant related documents, financial records, hire and appointment letters, salary information, performance reviews, warning and disciplinary documents, etc. Also, experimental data generated under grants (NIH, CDC, NSF, etc.) which does not contain regulated data elements (PHI, etc.), but is not ready for public release would be considered moderate risk.

Access and use: Access may be granted without requiring an explicit data use agreement but with appropriate documentation. Moderate risk data are not intended for public dissemination but may be released to external parties subject to appropriate review and controls. The University reserves the right to designate that certain subsets of Moderate Risk data require training in the appropriate use and handling of the data.

Storage and protection: Moderate Risk Information should be protected behind electronic firewalls or in private paper files in secured offices and should not accessible by the public or the University community at large without appropriate review and documentation.

Transmission: Moderate Risk data can be freely shared with appropriate parties within the University environment. If such data are transmitted by e-mail or other electronic transmission outside the University, there must be a documented business case and appropriate protection and usage guidelines must be followed. Automatic forwarding of Moderate Risk data to external email or document storage sites is prohibited without explicit permission from Information Security Officers.

Labeling of Moderate Risk Information: Information that is classified as Moderate Risk does not require labelling for internal use and distribution. If data are shared outside the University, an explicit discussion of handling requirements by the external recipient should precede transmission.

Destruction: Disposition of Moderate Risk information should adhere to Record Retention policies and archival best practices.

C. Low Risk

Definition: Data should be classified as Low Risk where the unauthorized disclosure, access, alteration, loss or destruction of that data would not be expected to have any effect on the University and its affiliates' mission, assets, operations, finances, or reputation, would not be expected to pose any harm to individuals, or where such data are intended for public disclosure.

Examples: Examples include the University's audited financial statements, schedule of classes, approved census facts and the information on the public University website, or de-identified or non-human research data.

Access and use: Low Risk data are available to all members of the University community and may be released to the general public. The University reserves the right to control the content and format of Low Risk information and may document access and use of low Risk data.

Appendix A: Definitions, Acronyms, and Related Information

Protected Health Information (PHI) is health information (oral or recorded) that associates an individual with a health care provider, a health condition or diagnosis, a health care facility, or a health care plan. Because this information is so prevalent in the health care and research operations of the University, it is recommended that staff who work in these areas assume that most communication contains PHI.

Information is considered to be de-identified under HIPAA if all of the following 18 identifiers are removed:

a. Names;

b. All geographic subdivisions smaller than a State, including: street address, city, county, precinct, zip codes and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly-available data from the Bureau of Census:

    1. the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000; and

    2. the initial three digits of the zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

c. All elements of dates (except year) for dates directly related to an individual, including: birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

d. Telephone numbers;

e. Fax numbers;

f. E-mail addresses;

g. Social Security numbers;

h. Medical record numbers;

i. Health plan beneficiary numbers;

j. Account numbers;

k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;

m. Device identifiers and serial numbers;

n. Web Universal Resource Locators (URLs);

o. Internet Protocol (IP) address numbers;

p. Biometric identifiers, including finger and voice prints;

q. Full face photographic images and any comparable images; and

r. Any other unique identifying numbers, characteristics or codes

Private Information: Private information has the meaning ascribed to it under the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act.

Under the SHIELD Act, “private information” means either:

(I) personal information (as defined below) consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired:

1. social security number;

2. driver’s license number or non-driver identification card number;

3. account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual’s financial account;

4. account number, credit or debit card number, if circumstances exist wherein such number could be used to access and individual’s financial account without additional identifying information, security code, access code, or password; or

5. biometric information, meaning data generated by electronic measurements of individual’s unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which used to authenticate or ascertain an individual’s identity; or

(II) a username or email address in combination with a password or security question and answer that would permit access to an online account.

“Personal information” means any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

“Private information” does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.

Personally Identifiable Information (PII) is a concept that includes “private information” as defined herein, and also includes any information that may be used to identify a person either alone or in conjunction with other data if the data or information is specifically protected by applicable law or regulation. Determination of what constitutes PII beyond data defined as “private information” is generally made on a case-by-case basis and may vary by jurisdiction, as further illustrated in Appendix C.

Payment Card Information (PCI) is the 16-digit number on a credit or debit card, the security code, an individual’s PIN, the expiration date of the card and the individual card holder’s name. This information must comply with the Payment Card Policy.

FERPA (Federal Education Rights and Privacy Act of 1974) is federal legislation that protects the privacy of students’ records.

FERPA Education Records are any records that are directly related to a student and maintained by the University, except for a few types of records expressly exempted by law, including but not limited to certain law enforcement records records, employment records, alumni records and certain treatment records made or maintained by physicians, psychologists, and other professionals.

GDPR (General Data Protection Regulation (EU) 2016/679) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas.

CCPA (California Consumer Privacy Act) went into effect on January 1, 2020. CCPA grants California consumers robust data privacy rights and control over their personal information, including the right to know, the right to delete, and the right to opt-out of the sale of personal information that businesses collect, as well as additional protections for minors.

Data system: A technology platform that gathers or collects data as part of a business process or for reporting or other purposes.

Data collection: A group of data elements that support a business process. Collections can be logical (not technology specific) or physical (residing in a particular system).

Data set: A prepared group of data elements put together for a specific consumption or reporing purpose from one or more data collections.

Appendix B: Related policies for specific information

See the specific policies referenced for a more specific definition of each type of information and of the rules and procedures concerning their use.

- Social Security Numbers (SSN) https://tech.rochester.edu/policies/ssn-pii-policy/ (https://tech.rochester.edu/policies/ssn-pii-policy/)

- Patient Protected Health Information (HIPAA) https://intranet-secure.urmc.rochester.edu/policy/HIPAA/PolicyManual/ (https://intranet-secure.urmc.rochester.edu/policy/HIPAA/PolicyManual/)

- Student Information (FERPA)[1] http://www.rochester.edu/registrar/policies.html (http://www.rochester.edu/registrar/policies.html)

- Record Retention Policy https://www.rochester.edu/adminfinance/records.html (https://www.rochester.edu/adminfinance/records.html)

- Financial Account, Credit and Debit Card Information https://www.rochester.edu/adminfinance/treasury/pdf/Payment-Card-Policy.pdf (https://www.rochester.edu/adminfinance/treasury/pdf/Payment-Card-Policy.pdf)

- Access to and Maintenance of Personnel Records https://www.rochester.edu/working/hr/policies/pdfpolicies/404.pdf (https://www.rochester.edu/policies/policy/personnel-file-access/)

Appendix C: Related processes and procedures for specific information

See the specific procedures for data where they are not incorporated into the policy document.

- Security Procedure for policy 0SEC04: https://tech.rochester.edu/wp-content/uploads/0SEC04Procedure.pdf (https://tech.rochester.edu/wp-content/uploads/0SEC04Procedure.pdf)

- Organization of Information Security procedures for policy 0SEC05:

https://tech.rochester.edu/wp-content/uploads/0SEC05Procedure.pdf (https://tech.rochester.edu/wp-content/uploads/0SEC05Procedure.pdf)

- Information Security Incident Management procedures for policy 0SEC11: https://tech.wdev.rochester.edu/wp-content/uploads/0SEC11Procedure.pdf (https://tech.wdev.rochester.edu/wp-content/uploads/0SEC11Procedure.pdf)

- SSN custodian duties: https://tech.rochester.edu/custodian-duties/ (https://tech.rochester.edu/custodian-duties/)

- HIPAA-related procedures: https://sites.mc.rochester.edu/departments/hipaa/hipaapolicy- (https://sites.mc.rochester.edu/departments/hipaa/hipaapolicy-) manual/

- PII classification determination: under development. Will include discussion of jurisdiction issues (such as applicability of GDPR and CCP) as well as process for case-by-base evaluation.

- Restricted Administrative HR Data Authorization Procedures: under development.

- Administrative HR Data Access Provisioning Procedures: under development.

- Classification procedure: under development.

- Data handling guidelines: under development.

- Data usage guidelines: under development

- Data sharing agreements: under development

ABOUT THIS POLICY

Issuing Authority

University of Rochester

POLICY KEYWORDS

Data (https://www.rochester.edu/policies/all/?filter%5Btopics%5D=376)

Privacy (https://www.rochester.edu/policies/all/?filter%5Btopics%5D=526)

Security (https://www.rochester.edu/policies/all/?filter%5Btopics%5D=596)

<iframe src="https://www.googletagmanager.com/ns.html?id=GTM-TT7PP8Z" height="0" width="0" style="display: none; visibility: hidden" ></iframe >