Overview

Federal regulations require the Institutional Review Board (IRB) to determine the adequacy of provisions to protect the privacy of subjects and to maintain the confidentiality of their data. To meet this requirement, federal regulations require researchers to provide a plan to protect the confidentiality of research data.

Today, most data are collected, transmitted or stored electronically at some point. The University of Rhode Island (URI) offers a range of Information Technology Services for all faculty, staff, and students to safeguard this data.

Read the guidance below and develop standard best practices for managing electronic data by collaborating with your school, department, or center IT staff, who have the expertise to evaluate the security methods most appropriate for the sensitivity of the research data. These best practices will need to adapt as technology evolves, so review this page and the Information Technology Services site on a regular basis.

Definitions

Anonymous data: Data that at no time have a code assigned that would permit the data to be traced back to an individual. This includes any information that was recorded or collected without any of the 18 identifiers as defined by HIPAA. Note that IP addresses are considered by the University and some international standards to be identifiable even though the address is linked to the computer and not specifically to the individual.

Coded: Identifying information (such as name) that would enable the investigator to readily ascertain the identity of the individual to whom the private information or specimens pertain has been replaced with a code (number, letter, symbol, or any combination) and a key to decipher the code exists, enabling linkage of the identifying information to the private information or specimens

De-Identified: Investigator cannot readily ascertain the identity of the individual

Electronic Protected Health Information ("EPHI"): EPHI is defined as any Protected Health Information ("PHI") that is stored in or transmitted by electronic media. For this definition, electronic media includes:

- Electronic storage media includes computer hard drives and any removable and/or transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card.
- Transmission media used to exchange information already in electronic storage media. Transmission media includes, for example, the Internet, an extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable and/or transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exists in electronic form before the transmission.

Health information: is defined as any information, whether oral or recorded in any form or medium, that:

i. is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
ii. relates to the past, present, or future physical or mental health or condition of any individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual."

Individually identifiable health information: is defined as information that is a subset of health information, including demographic information collected from an individual, and:

1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
   i. That identifies the individual; or
   ii. With respect to which there is a reasonable basis to believe the information can be used to identify the individual."

Personally Identifiable Education Records: are defined as any Education Records that contain one or more of the following personal identifiers:

- Name of the student
- Name of the student's parent(s) or other family member(s)
- Social security number
- Student number
- A list of personal characteristics that would make the student's identity easily traceable
- Any other information or identifier that would make the student's identity easily traceable

See URI's Understanding FERPA at URI presentation for more information on what constitutes an Education Record.

Personal Data from European Union (EU): The EU's General Data Protection Regulation (GDPR) defines personal data as any information that can identify a natural person, directly or indirectly, by reference to an identifier including:

- Name
- An identification number
- Location data
- An online identifier
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person

Any personal data that is collected from individuals in European Economic Area (EEA) countries is subject to GDPR. See URI's GDPR Policy.

Protected Health Information ("PHI"): Protected health information means individually identifiable health information (1) Except as provided in paragraph (2) of this definition, that is:

i. transmitted by electronic media.
ii. maintained in any medium described in the definition of electronic media; or
iii. transmitted or maintained in any other form or medium

(2) PHI excludes individually identifiable health information in:

i. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
ii. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
iii. Employment records held by a covered entity in its role as employer.

Sensitive Research Data: Data are considered sensitive when disclosure of identifying information could have adverse consequences for subjects or damage their financial standing, employability, insurability, educational advancement, reputation or place them at risk for criminal or civil liability.

Policies, Guidelines and Laws

All investigators and research staff should be familiar with information security policies and procedures of their department or unit, URI, the state of Rhode Island and federal privacy laws. In addition, because research is now a global enterprise, you should understand the international laws or regulations that may apply when conducting research outside the United States.

Below are policies, guidelines, and laws of note. This is by no means a complete list.

- **URI Information Security Policies,** URI policies on IT Resources, Acceptable Use, and Endpoint Protection.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA) at URI,** URI HIPAA Security Policies, Privacy Policies, Forms and Guidance Documents.
- **Children's Online Privacy Protection Act (COPPA)**, which applies to the online collection of personal information from children under the age of 13. This Act requires websites to display a privacy policy, obtain verifiable parental consent, and disclose how the information will be used. It is important that researchers who plan to collect data from children online carefully review the provisions of the Act and contact the URI Office of General Counsel with any questions. It is the responsibility of the researcher to ensure they are fully compliant with the COPPA regulation.
- **FERPA,** The Family Educational Rights and Privacy Act is a federal law that protects the privacy of student education records by restricting the release of and access to those records. You must check with the appropriate office before releasing directory information. Any record, with certain exceptions, maintained by an institution that is directly related to a student or students is an education record. This means any and all information, maintained in any medium, that is directly related to students and from which students can be personally identified. Also see URI's Understanding FERPA at URI presentation for more information on what constitutes an Education Record.

Guidelines

Researchers have a responsibility to be good data stewards. In the past, most data were collected and stored on paper. At a minimum, data was protected by being locked in a file cabinet in a locked room that only members of the research team could access. Today, data are collected, transmitted, and stored on computers and mobile devices. Simply password-protecting a computer may not be sufficient to meet the rigorous security standards mandated by the University and/or sponsors. Researchers need to collaborate with their school, department or IT staff who have the expertise to evaluate the security methods most appropriate for the sensitivity of the research data.

Data that will be shared with others requires additional oversight to uphold the privacy of the research participant and the confidentiality of their data. If data from the study are to be shared outside the research team, it is important that the researchers obtain the appropriate consent from study participants.

In the past, many consent documents had language that limited sharing of the data more so than was necessary or intended. It is important to think about future data use and to tailor the consent language and permissions to meet your future data sharing needs.

Some researchers may request permission to share identifiable data, but the majority will be sharing de-identified data. Many sponsors, including federal agencies, require data sharing as a condition of funding, and this must be

reflected in the consent document and in the consent process (discussion). This includes the acknowledgement of the data sharing practices and the possible risk of re-identification when applicable. One should never guarantee that de-identified data cannot be re-linked, and the participant's identity disclosed. As technology evolves, so does the potential risk of re-identification.

Assessing the data security method needed

In the IRB application, you must address issues related to subject privacy and confidentiality, HIPAA and information security. Based on the type of data involved in the study, the IRB is required to

1. Assess potential risks to participants, and
2. Evaluate the researchers' plan to minimize risks. The researcher has the responsibility to mitigate the risk of improper disclosure.

What is the Risk?

- Are the data identifiable, de-identified (coded), or anonymous?
- Are you keeping the code key separate from the records?
- Are you collecting or retaining any data beyond what is absolutely necessary for the study?
- Is sensitive information being collected that could result in harm to participants?
- What is the risk of harm to the participant or others?
- Have you consulted with IT Security Services to make sure your research and/or clinical data are secure from both physical and electronic theft?

Do the methods meet the IRB's minimum standards for the collection, storage, use and transmission of subject identifies for human subject research?

- Do not collect any subject identifiers you do not need.
- Remove/destroy subject identifiers as soon as they are no longer needed.
- Restrict physical access to any area or computer system that contain subject identifiers.
- Restrict electronic access to any computer system that contains subject identifiers.
- Subject identifiers should never be stored on laptops, flash drives or other portable devices. If there is a necessity to use portable devices for the initial collection of subject identifiers, the data files must be encrypted, and the identifiers must be transferred to a secure system as soon as possible.
- Subject identifiers must be removed from data files and must be encrypted if stored electronically. Identifiers must be stored in a physically separate and secure location from the data files and associated with data files through a code that is also stored in a separate and secure location.
- If subject identifiers must be retained in the data files because of the specific needs of the research study, additional explanation must be provided by investigators to justify such retention. If the data are electronic, the information must be encrypted during storage and decrypted only during the limited time it is needed for matching or other similar purposes.
- Subject identifiers transmitted over public networks must be encrypted.
- Subject identifiers and contact information may not be distributed outside of URI without the specific informed consent of the subjects, and approval by the IRB.
- All collaborating investigators at URI and at other institutions must comply with these standards.

What are the protections against anticipated threats or hazards (during collection, transmission, and storage)?

- Encryption of data on device to protect against loss/theft of device
- Use of secure data transmission channels to protect against data interception
- Strong passwords to protect against unauthorized access
- Store data behind a secure URI firewall whenever possible
- Ensure strong data security controls on all storage sites
- Routinely and regularly review and update data security procedures

Continue to assess security controls throughout the study

Research team meetings should include discussions about topics including, but not limited to, the following:

- Software on computers to protect against malware
- Data security to ensure all software updates and patches are being applied
- Data collection, transmission and storage methods employed
- Data collected are only that data necessary to answer the research question
- Codes are not stored with the corresponding de-identified data
- Encryption methods are being used on all portable devices (e.g., laptops, mobile devices, and removable storage)

Methods for Securing Data

You have a responsibility to be a good data steward. Simply password-protecting a computer may not be sufficient to meet the rigorous security standards mandated by the University and/or sponsors. The University offers extensive security solutions that can benefit researchers, some of which are described below.

Encryption

Encryption protects data by encoding information so that only authorized parties may read it. You need to encrypt all of your electronic devices (e.g., laptops, iPads, cell phones, etc.) — whether URI-owned or personal — if they are used for accessing sensitive or confidential university data or interacting with university owned systems using elevated privilege levels.

Secure Data Storage

IT Security Services can provide a security compliance assessment to determine how to properly store research data with identifiers.

Cloud Storage

Microsoft OneDrive, SharePoint, and Google Drive are available as cloud storage solutions; however, they are likely to not be appropriate for the storage of research data with identifiers. Some URI faculty and staff use other programs like Dropbox, Evernote, or Amazon to exchange files with co-workers or collaborators. Using such storage solutions poses a possible liability for official use at URI, particularly for research data.

There are potential security risks, export control restrictions and data ownership issues (research data belongs to the URI, not the researcher).

If you have a need to store research data with identifiers, please contact IT Security Services.

Vendor Security Review Request

When University data are processed, stored, or transmitted to entities or vendors outside of university-controlled computing infrastructure, URI IT Security Services is required to perform a security review of that entity by leveraging the HECVAT (Higher Education Community Vendor Assessment Toolkit). The HECVAT is a questionnaire framework specifically designed for higher education to measure vendor risk. It allows the university to confirm that information, data, and cybersecurity policies are in place to protect our sensitive institutional information and constituents PII. Examples of this include when applications, websites, or other tools are developed by a vendor and the data will be processed, stored, or transmitted to the vendor's IT infrastructure. To initiate a HECVAT review please contact IT Security Services.

Survey Software

- Qualtrics (recommended): Using Qualtrics, you can build, distribute and analyze online surveys — from the very simple to the most complex. Qualtrics can be used to collect, and store protected patient and personal data. It is available at no cost to all URI faculty, staff, and students. When using Qualtrics, check the option to anonymize the data collection process and do not collect the IP address. If IP addresses are necessary to the research, include in the consent process that you will be recording this information.
- Research Electronic Data Capture (REDCap) (recommended): This tool allows you to rapidly develop databases and online surveys. It is available for use at no cost to the URI research community and its collaborators. RedCAP can be used to collect, and store protected patient and personal data.
- Other Programs: If you are using other survey software such as Survey Monkey or other programs, it may first need to undergo a data security review. See the ITS Security Services page.
- IP Address Collection: You may wish to collect the IP addresses of survey participants to provide a method of determining whether the user has previously completed the survey. The IRB and some international standards consider IP addresses to be identifiable information. This is important to consider when conducting surveys, especially if the consent process indicates that a participant's responses will be anonymous.

Data Transmission

The process of transmitting data is often overlooked as a risk. The plan to protect confidentiality should describe the methods to protect the data during collection and sharing both internally and externally to the University. It is advisable to utilize a secure transmission process even if the data are anonymous, coded or non-sensitive information. If the research team develops a best practice on using a secure data transmission process, then it is less likely a data breach will occur.

Email notifications are generally not secure and generally not be used to share or transmit research data. See more information on sending secure email at URI.

To transfer large files securely, please contact IT Security Services.

Securing Paper Records

This guidance focuses on methods for securing electronic data, but you must also safeguard paper research records.

- Keep data in a locked file cabinet in a locked office or suite
- Code data and keep the key in a separate and secure location

Consent Forms and Permission to Share Data

Data that will be shared with others requires additional oversight to uphold the privacy of the research participant and the confidentiality of their data. If study data will be shared outside the research team, it is important that you obtain the appropriate consent from study participants.

In the past, many consent documents had language that limited sharing of the data more so than was necessary or intended. It is important to think about future data use and to tailor the consent language and permissions to meet your future data sharing needs.

Some researchers may request permission to share identifiable data, but the majority will be sharing de-identified data. Many sponsors, including federal agencies, require data sharing as a condition of funding, and this must be reflected in the consent document and in the consent process. This includes the acknowledgement of the data sharing practices and the possible risk of re-identification when applicable. One should never guarantee that de-identified data cannot be relinked, and the participant's identity disclosed. As technology evolves, so does the potential risk of re-identification.

Data Use Agreement

A Data Use Agreement (DUA) by the Office of Sponsored Projects must be completed if your study involves: the collection, transmission, or storage of information when that data will be shared with or be accessible to any non-URI entity (e.g., pharmaceutical companies) or individual. This includes the use of third-party or vendor-hosted applications.

National Institute of Health (NIH) Grants

The NIH has specific requirements about ensuring data security when collecting identifiable research data in section 2.3.12 Protecting Sensitive Data and Information in Research.

"Recipients of NIH funds are reminded of their vital responsibility to protect sensitive and confidential data as part of proper stewardship of federally funded research and take all reasonable and appropriate actions to prevent the inadvertent disclosure, release, or loss of sensitive personal information. NIH advises that personally identifiable, sensitive, and confidential information about NIH-supported research or research participants not be housed on portable electronic devices. If portable electronic devices must be used, they should be encrypted to safeguard data and information. These devices include laptops, CDs, disc drives, flash drives, etc. Researchers and institutions also should limit access to personally identifiable information through proper access controls such as password protection and other means. Research data should be transmitted only when the security of the recipient's systems is known and is satisfactory to the transmitter. See also Public Policy Requirements and Objectives—Federal Information Security Management Act."

The NIH also instituted the Genomic Data Sharing (GDS) Policy to promote sharing, for research purposes, of large-scale human and non-human genomic data generated from NIH-funded research. The policy requires investigators to incorporate a genomic data sharing plan in the 'resource sharing' section of their application. This policy applies to proposals and applications submitted after January 25, 2015.

Training

The PI is responsible for ensuring that research data is secure when it is collected, stored, transmitted, or shared. All members of the research team should receive appropriate training about securing research data and discuss data security regularly at research team meetings. For example, the research team should understand they need

to document their standard practices for protecting research data so that they can provide these details to the IRB, IT, etc. if a mobile device is lost or stolen.

The IT Security Awareness Training program provides programs to educate URI faculty, staff and students on the risks associated with using, transmitting, and storing electronic information; how to maintain the confidentiality, integrity, and availability of data; and the roles and responsibilities of each community member in protecting URI's data and systems.

Contacts

- For questions about information security: URI IT Security Services: (401)-874-4787
- For questions about HIPAA and patient privacy: URI Health Services: (401) 874-4753