THE UNIVERSITY OF IOWA

Institutional Review Board & Human Subjects Office

Data Security:
Storing & Transmitting Data for Human Subjects Research

Introduction

Data security measures protect the privacy and confidentiality of research subjects. These measures apply to the storage and transmission of all types of data collected for research purposes, including paper and electronic records, biospecimens, audio and video recordings, photographs, etc. To obtain IRB approval, researchers must make adequate plans to protect subject privacy and the confidentiality of study data and describe them in the HawkIRB application and in the Informed Consent Document. Privacy and confidentiality are two distinct concepts, although these terms are commonly used interchangeably. This guidance document:

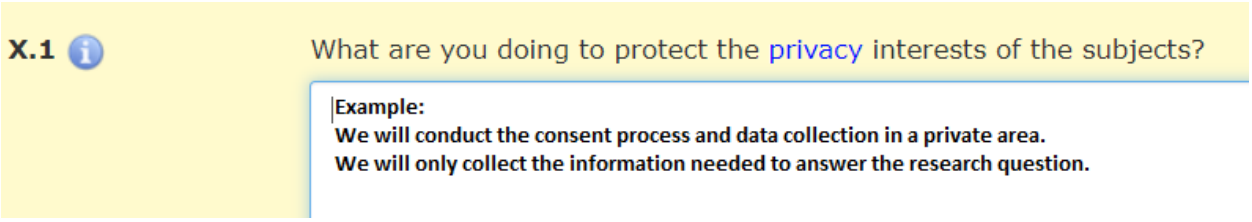
- Explains the distinction between privacy and confidentiality in research
- Provides best practices:
  - to protect privacy at the point of data collection
  - to protect confidentiality during data storage

Privacy Protections

Privacy Protections protect the person. These protections apply when data are collected directly from a subject and when the research study uses existing data about a subject for research purposes. Privacy protections respect an individual's right to keep personal information to themselves. Researchers protect subject privacy by:

- Collecting data in a private setting
- Collecting only the data necessary to address research questions or hypotheses

Describe privacy protections in Section X.1 of the HawkIRB application.



Confidentiality Protections

Confidentiality protections apply to the storage, transfer and transmission of data collected or used for research purposes, including paper records, electronic records, and biospecimens. Researchers protect data by limiting who has access to it and how it is identified.

Data identifiability

In some cases, researchers need to collect and store identifying information about research subjects. These identifiers include name, contact information, date of birth, dates of service, etc. that are referenced in the Health Insurance Portability and Identifiability Act (HIPAA) regulations. An ID code is considered an identifier if there is a link between the ID code and the identifying information. Identifiable data requires stricter confidentiality precautions.

It is important to use correct terminology to describe how data will be identified:

- Identified Data – Subject identifiers are stored in the data set
- Coded Data – There is a link between the ID code and the identifiable information
- De-identified Data – Subject identifiers were initially collected and have been removed
    - this could include breaking the link between the code and the identifiers
- Anonymous Data – No identifying information was ever collected from or about subjects

Protected Health Information

Researchers must implement additional confidentiality protections for medical records that are used for research purposes. Protected Health Information (PHI) includes health information that:

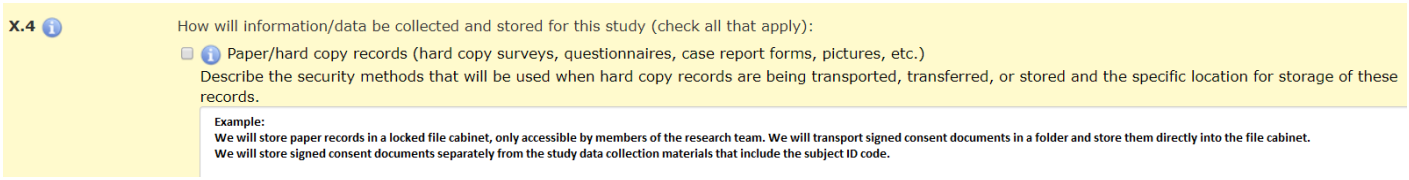
- Is transmitted or maintained in any form (electronic, oral, paper) by a covered entity
- Identifies the individual or could reasonably be used to identify the individual, including name, contact information, date of birth, dates of service, account numbers, and full face photographic images (see the list of 18 HIPAA identifiers).
- Relates to past, present, or future, physical or mental, health condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of healthcare to an individual

Describe confidentiality protections in Section X.4 of the HawkIRB application, including the use of an ID code or pseudonym. Data security measures must be appropriate given the sensitivity of the data and whether it includes subject identifiers.

Paper Records

Paper records include any paper documents that contain study data or other research-related records. Signed Informed Consent Documents (ICDs) are considered paper records with identifiable information. The research team is responsible for maintaining confidentiality protections for all paper records, including signed consent documents, during transport and storage of these records. Some

common confidentiality protections for paper records include: locked file cabinet, locked office, transporting documents in a folder, envelope or locked briefcase.In Section X.4, describe the transfer and storage protections for all paper records.

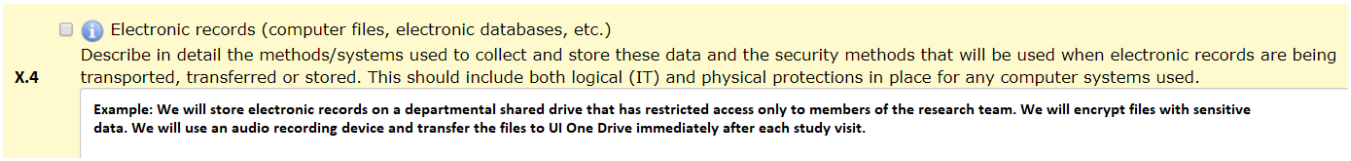


Electronic Records

Electronic records include all electronic files and digital recordings or images that are collected and/or stored for research purposes. The confidentiality protections for these records depends on the sensitivity of the data and can include:

- Password protected files
- Limited access folders on a shared drive
- Encryption

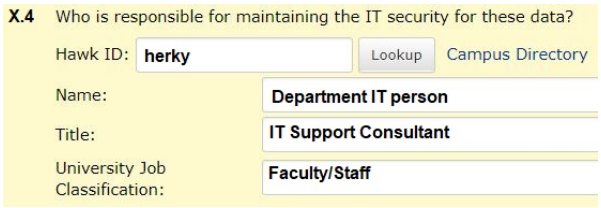
In Section X.4, describe the storage of electronic and digital research records.



The University of Iowa Information Technology Services (ITS) provides information about the sensitivity level of data for electronic data transfer and storage. Highly sensitive data that falls under the definition of "restricted" or "critical", as defined in the "Data Classification Guide" section below, requires an IT Security Plan approved by the ITS. To initiate a security plan, contact research-computing@uiowa.edu.

Person Responsible for Maintaining IT Security

The person responsible for maintaining IT security, generally a departmental IT person, is accountable if there is ever a security breach with study data. Researchers should communicate with this person to ensure they follow best practices for storing electronic data on hard drives, shared drives, laptops, etc.



Data Classification Guide

The UI ITS classifies institutional data into four primary data types and specifies the storage standards for each type. Those categories are:

Public: data that is public or published with no restrictions. Examples include: published "white pages" directory information, maps, academic course descriptions, news releases.

University/Internal: data that is non-public or internal data. Examples of institutional data include: official university records, financial reports, unofficial student records, de-identified research data.

Restricted: data that is confidential or restricted due to personal privacy considerations or compliance regulations and laws. Examples include: student transcripts, identifiable human subjects research data, full-face photogenic images or videos, financial aid data.

Critical: data that has the most stringent legal or regulatory requirements and requires special security controls. Examples include: data governed by HIPAA (protected health information), Social Security Numbers (SSNs), credit card or personal credit information (PCI), personal identifiers (passport/driver's license numbers), data governed by International Traffic in Arms regulations (ITAR, export-controlled). PLEASE NOTE - PCI data should not be stored on any of the data storage and transfer tools listed below. If you are working with PCI data, please contact the IT Security Office for guidance.

Subsets of Critical Category

There are two types of Critical data based on specific regulations regarding export control and HIPAA. If you have questions about what data in the Critical category can be stored/used on any of the below services, please contact research-computing@uiowa.edu.

- **Critical - Export-Controlled**: U.S. defense-related data where disclosure to a foreign national must be prevented. Examples include: military items, space-related technology, technical defense data (e.g. ITAR, EAR)
- **Critical - HIPAA**: Protected health information (PHI) from the University of Iowa Hospitals and Clinics or other covered entities.

Storage and Transfer tools

There are many ways to store and transfer data. The PI must choose a program that is consistent with the level of sensitivity and classification of the data. ITS offers the following recommendations regarding the acceptable storage methods based on the data classification type. Tools that are not referenced in the UI ITS list below, or in the "List of Reviewed Agreements", require a Technology Review & Security Review prior to use. Notes about Zoom and Google: Zoom can only be used with University-Internal data; Google Drive & Google Docs are only approved for Public classified data, they are not approved for storage and transmission of any other classification of data.

Additional information is available on the ITS website.

Legend:

✅	Permitted
⚠	Permitted with IT Security Consultation
❌	Not Permitted
***	HIPAA data should only be stored on a CIFS share

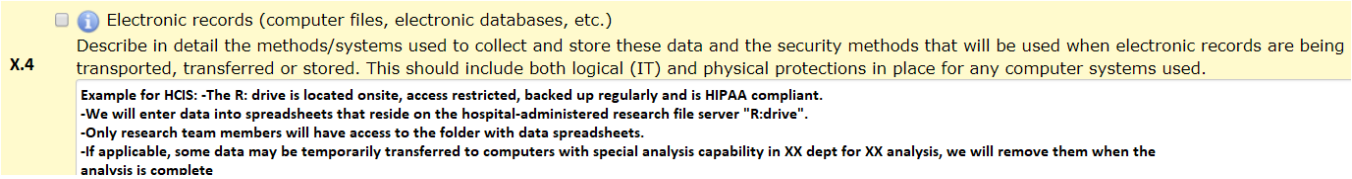
Service	Public	University/Internal	Restricted/Critical (personal identifiers & SSNs only)	Export-Controlled	HIPAA
Apple iCloud	✅	❌	❌	❌	❌
AWS Cloud Enterprise	✅	✅	⚠	⚠	⚠
Box	✅	❌	❌	❌	❌
Dispatch	✅	✅	❌	❌	❌
DropBox	✅	❌	❌	❌	❌
Globus	✅	✅	⚠	⚠	⚠
Google Drive	✅	❌	❌	❌	❌
Home Drives (Files@Iowa)	✅	✅	✅	❌	❌
HPC Systems	✅	✅	⚠	⚠	⚠
Large Scale Storage (LSS)***	✅	✅	✅	✅	✅
Interactive Data Analytics Service	✅	✅	❌	❌	❌
Microsoft Azure Cloud Services Enterprise	✅	✅	⚠	❌	❌
Microsoft OneDrive for Business	✅	✅	✅	❌	✅
Microsoft SharePoint Online (O365)	✅	✅	✅	❌	✅
Microsoft Teams	✅	✅	✅	❌	✅
Personal Cell Phones	✅	⚠	❌	❌	❌
Personal Devices (e.g. laptops, USBs, personal cloud services, etc.)	✅	⚠	⚠	⚠	⚠
Qualtrics	✅	✅	✅	❌	✅
R: Drive	✅	✅	✅	❌	✅
REDCap	✅	✅	✅	❌	✅
Research Data Storage Service (RDSS)***	✅	✅	✅	✅	✅
Research Remote Desktop Service	✅	✅	✅	✅	✅
Secure Device Service	✅	✅	✅	✅	⚠
Shared Drive (Files@Iowa)	✅	✅	✅	❌	⚠
Skype for Business	✅	✅	✅	❌	✅
Zoom	✅	✅	⚠	⚠	⚠

Storage on laptops, desktops, or mobile devices

UI researchers should use caution and implement appropriate confidentiality protections when storing data on laptops, desktops and mobile devices. UI ITS has core security standards which reflect the minimum institutional expectations for storing data, including research data, on a laptop, desktop, or mobile device. The HSO/IRB require all data be stored in a UI ITS managed service like OneDrive, RDSS, or the departmental shared drive. (See the full list of research data storage options.) The University of Iowa IRB(s) expect researchers to comply with these institutional standards and to describe the planned confidentiality protections in the HawkIRB application. The UI IRB will consult with IT Security and/or refer Principal Investigators (PI) to UI ITS to ensure that institutional standards are met. The UI ITS also offers a data classification guide for storing and sharing UI data.

Storing Data on the University of Iowa Hospitals and Clinics (UIHC) Server

Health Care Information Services (HCIS) has provided additional guidance for IRB-01 (Biomedical) researchers documenting security protections for data stored on an "R: drive". The R:drive is a hospital-administered server.



Audio/Video recording best practices for in-person & virtual research visits

UI ITS and HCIS policy prohibit the use of personal phones/mobile devices for making research-related recordings. It is best practice to store audio/video recordings on the UI One Drive account or approved campus storage solution, rather than directly on a laptop or workstation computer. The rationale for this practice is: 1) ITS monitors UI One Drive & campus storage servers to ensure there have been no security breaches 2) UI One Drive provides automatic back up, and most campus storage solutions provide routine backups. Section X.4 should describe the security precautions used for audio/video recorded data. If using One Drive or an approved campus storage solution is not possible, provide a detailed and compelling rationale in Section X.4 of the HawkIRB application.

When researchers conduct audio and video recordings in-person (via a hand held digital device or a secure recording application on a laptop or desktop computer) or virtual recordings (via Zoom or Skype for Business), the recordings should immediately be transferred to a UI-managed storage service (UI OneDrive, RDSS, H:Drive, for example) at the conclusion of the research visit. Once securely stored, the audio and/or video recording should be deleted from the recording device. Cell phones cannot be used for ***any*** recording functions – in-person or phone conversations, Zoom, or Skype for Business sessions.

Investigators seeking only audio recordings should take care **not** to obtain video recordings via Zoom or Skype for Business. Investigators should ask Zoom participants to disable their cameras before recording sessions begin; this will allow the PI to capture only audio content. Both Zoom and Skype for Business applications have the capability of automatically storing local recordings to UI-managed storage drives if the drive is first mapped to the computer and the application settings are updated. In order to set this up correctly, please refer to UI ITS Security and Privacy Tips for Zoom. Contact UI ITS with questions. Once securely stored, the recording must be deleted from the recording device.

If phone interviews are used, the research team member should engage the phone's speaker phone tool. Conversations may be recorded using a separate recording device (such as a hand-held digital recorder or a secure recording application on a laptop or desktop computer). Please contact the IT department to determine what recording applications are acceptable.

Sharing data outside of the University of Iowa

It may be necessary to use a Data Use Agreement (DUA) to transfer or share data outside of the University of Iowa. A DUA is generally required when:

1) when PI leaves Iowa and wants to take data
2) data is available to research team members or individuals outside the University of Iowa

Contact the Division of Sponsored Programs (DSP) for assistance with establishing a DUA. To ensure you are in compliance with the DUA terms for data transmission and are using approved transfer mechanisms, contact Research-Computing@uiowa.edu.

Tools Available to Conduct Remote or Virtual Research Related Activities

eConsent (Use of Electronic Consent) options available at the UI

Federal regulatory guidance must be followed if an eConsent (electronic informed consent) tool is used in the conduct of human subjects research. Limited tools are available at the UI as an eConsent Tool. REDCap is available as eConsent tools to conduct non-FDA regulated research. Contact the ICTS for more information on REDCap. Qualtrics could also be used in limited instances as an eConsent tool. Any eConsent tool used as part of a human subjects research project must be approved by the IRB of record prior to use. Contact the Human Subjects Office via email irb@uiowa.edu or call (319)335-6564 for assistance.

Virtual options for conducting human subjects research visits & procedures

There are several video conferencing options available from the UI ITS that the UI IRBs would find acceptable for conducting virtual research visits. The HSO/IRB strongly recommends using an UI ITS supported video conferencing solution. If you use a tool not endorsed by the UI ITS, the IRB will require you to discuss the tool with UI ITS Research Computing to ensure appropriate security and confidentiality measures are in place prior to submission to the HSO/IRB. A technology or IT security plan may be required.

Data Security When conducting Research Activities Virtually or Outside UI Physical Space

Remote Access Set up

Principal Investigators/Research Teams should continue to maintain appropriate data security and confidentiality measures to conduct research related activities at an alternate location. UI ITS recommends the study team ensure remote access to study files is set up for work at an alternate location (e.g. data entry, transcription, data or statistical analysis, coding data, etc.) Appropriate IT security and confidentiality measures consistent with UI ITS policies (e.g. encryption, use of VPN, use of OneDrive, etc.) would be required.

PI/Research Teams should also consider grant or contractual obligations related to data security, storage, and confidentiality measures prior to allowing research team members to work from a location outside of the University of Iowa campus. Check with the Division of Sponsored Programs or UI ITS if you have questions regarding if these obligations apply to your research. Any changes must be approved in advance by the IRB as a modification to the study. Additional information regarding best practices for data security can be found on the Educational Tools page of the HSO Website. If you have any questions about whether a remote option is possible or approvable (especially for consent), contact the IRB at irb@uiowa.edu.

IT best practices and security requirements for continuing to conduct my research from home

The HSO/IRB recommends applying the security and IT best practices outlined by the UI ITS for any research efforts continuing from a remote location. The first step is to ensure the UI ITS standards for working remotely are in place. UI ITS has also outlined the "Top 10 Security Considerations When Working From Home" to help to protect University of Iowa research data when working from home.

IT related information available when using Zoom to conduct virtual research visits

The HSO/IRB recommends below UI ITS recommendations for IT safety, security, best practices for the use of Zoom for research purposes:

- General information on the use of Zoom.
- Zoom Connection Issues
- Zoom Security and Privacy