Data Security:
Storing and Transmitting Data for Human Subjects Research

Institutional Review Board and Human Subjects Office

Table of Contents

Version 4 (March 25, 2022)

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. Although these terms are commonly used interchangeably, “privacy” and “confidentiality” are two distinct concepts. This guidance document:

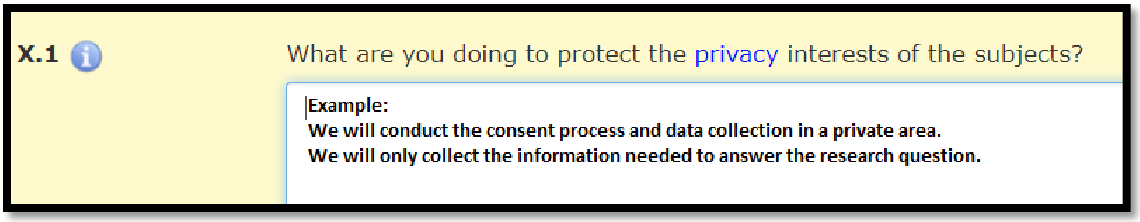
- Explains the distinction between privacy and confidentiality protections
- Provides best practices:
  - to protect privacy at the point of data collection
  - to protect confidentiality during data storage and transmission

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 amount and type of information necessary to address research questions or hypotheses

In a HawkIRB application, describe privacy protections in Section X.1.



X.1 What are you doing to protect the privacy interests of the subjects?

Example:
We will conduct the consent process and data collection in a private area.
We will only collect the information needed to answer the research question.

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. Data security measures must be appropriate for the sensitivity level of the data and whether the dataset includes subject identifiers or if subjects could be reidentified. Researchers protect data by limiting who has access to it and how it is identified.

In a HawkIRB application, describe confidentiality protections in Section X.4, including:

- Plans to use an ID code or pseudonym
- Plans to maintain or break the link between the ID code and subject identifiers
- If the study will not record any identifying information about subjects

The rest of this educational tool focuses on confidentiality protections or data security methods. See below for screenshot examples of how to complete Section X.4.

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. There is a list of 18 identifiers in the Health Insurance Portability and Identifiability Act (HIPAA) regulations. However, this is not an exhaustive list. Other variables or combinations of variables could be used to identify subjects. **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

Another consideration is re-identification, the act of identifying subjects from coded, de-identified or anonymous data sets. There are steps researchers can take to prevent re-identification. For additional guidance, see the Visual Guide to Practical Data De-Identification from the non-profit Future of Privacy Forum.

Protected Health Information

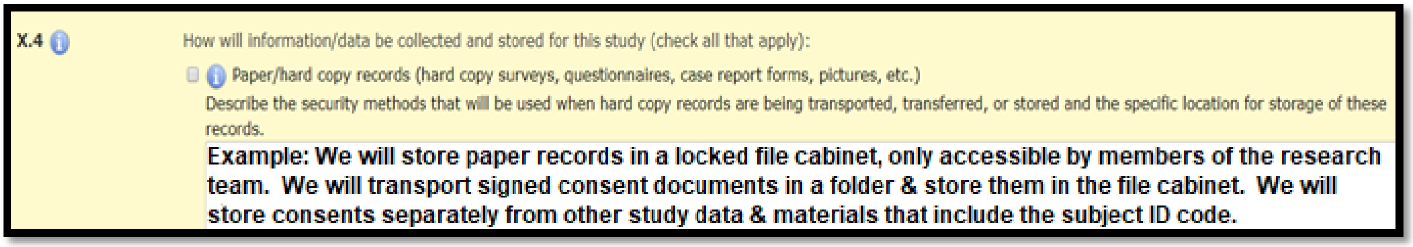
Researchers must implement additional confidentiality protections for medical records that are used for research purposes. Protected Health Information (PHI) includes health information that:

- 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 health care to an individual

Describe confidentiality protections for PHI in Section X.4 of the HawkIRB application.

Paper Records

Paper records include any paper documents that contain study data or other research-related records. Signed Informed Consent Documents 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.



X.4 How will information/data be collected and stored for this study (check all that apply):

□ Paper/hard copy records (hard copy surveys, questionnaires, case report forms, pictures, etc.)

Describe the security methods that will be used when hard copy records are being transported, transferred, or stored and the specific location for storage of these records.

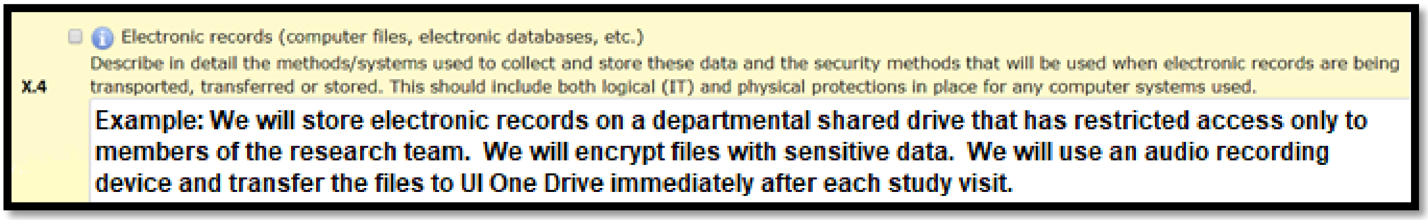
Example: We will store paper records in a locked file cabinet, only accessible by members of the research team. We will transport signed consent documents in a folder & store them in the file cabinet. We will store consents separately from other study data & materials that include the subject ID code.

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.



X.4

□ Electronic records (computer files, electronic databases, etc.)

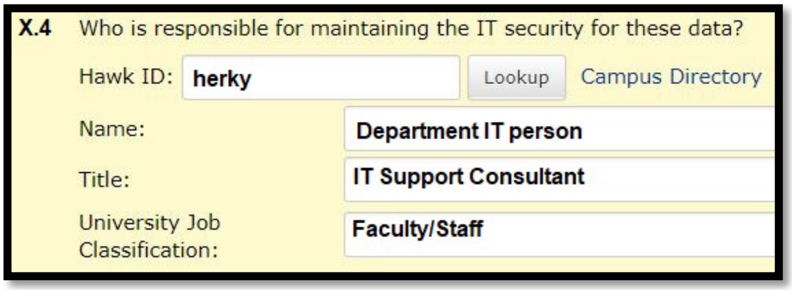
Describe in detail the methods/systems used to collect and store these data and the security methods that will be used when electronic records are being transported, transferred or stored. This should include both logical (IT) and physical protections in place for any computer systems used.

Example: We will store electronic records on a departmental shared drive that has restricted access only to members of the research team. We will encrypt files with sensitive data. We will use an audio recording device and transfer the files to UI One Drive immediately after each study visit.

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 consult with the IT representative to ensure that confidentiality protections follow best practices for storing and transmitting electronic data on hard drives, shared drives, laptops, etc.



X.4 Who is responsible for maintaining the IT security for these data?

Hawk ID: **herky** Lookup Campus Directory

Name: **Department IT person**

Title: **IT Support Consultant**

University Job Classification: **Faculty/Staff**

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: published "white pages" directory information, maps, academic course descriptions, news releases.

University/Internal: data that is non-public or internal data. Examples: 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: 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: data governed by HIPAA (protected health information), Social Security Numbers (SSNs), credit card or personal credit information, personal identifiers (passport/driver's license numbers), data governed by International Traffic in Arms regulations (ITAR, export-controlled). PLEASE NOTE – Personal Credit Information should not be stored on any of the data storage and transfer services/tools listed below. If you are working with these data, please contact the IT Security Office for guidance.

(Source: UI ITS Data Classification Guide to IT Services)

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 data storage and transfer services/tools listed below, please contact research-computing@uiowa.edu.

- **Critical - Export-Controlled**: U.S. defense-related data where disclosure to a foreign national must be prevented. Examples: military items, space-related technology, technical defense data (e.g., ITAR, EAR)

- **Critical - HIPAA**: The Health Insurance Portability and Accountability Act (HIPAA, 1996) applies to protected health information (PHI) from the University of Iowa Hospitals and Clinics or other covered entities (including Student Health, UI College of Dentistry, UI College of Nursing, Department of Athletics, University Hygienic Lab, Wendell Johnson Speech and Hearing, Seashore Psychology Training Clinic, College of Education – UI Belin Blank Center Assessment and Counseling Clinic, LGBTQ+ Counseling Clinic, and Telepsychology Training Clinic, College of Pharmacy). Refer to the list of 18 HIPAA identifiers. Example: Restricted data plus health information from medical record (e.g., name and blood pressure)

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. Tools that are not referenced in the UI ITS list below, or in the "List of Reviewed Agreements", require a Technology Review and Security Review prior to use.

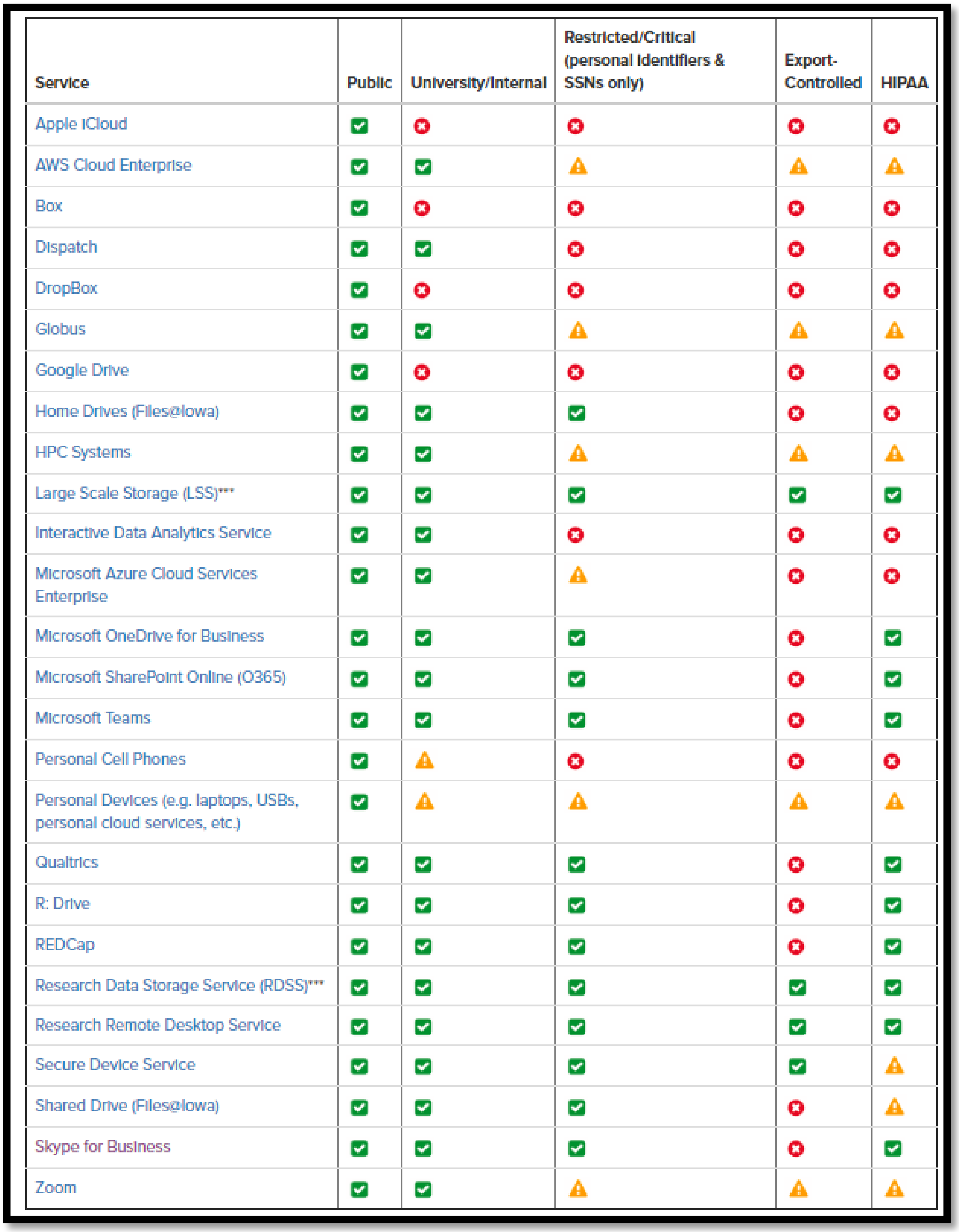
If you are using a new software, device, eConsent tool, etc. that could potentially require an IT security or technology review, discuss IT security measures with your respective departmental IT representative. Their engagement is imperative and could save the researcher, the IRB, and the UI IT Security team a lot of extra time and work. Ideally, the Technology and Security Reviews should be initiated before the IRB submission.

These reviews can sometimes take weeks or months and may delay the start of your project if completed later. If you are unsure who your departmental IT representative is, please contact research-computing@uiowa.edu.

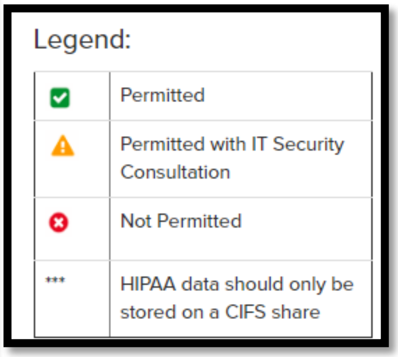
Notes about Zoom and Google:

- Zoom can only be used with University-Internal data;
- Google Drive and 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.



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	✓	✓	⚠	⚠	⚠



Legend:

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

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 UI IRB expects researchers to comply with these institutional standards and to describe the confidentiality protections and data security plans in Section X of 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. Use the UI ITS Data Classification Guide to establish appropriate plans for data storage and data sharing.

Storing University of Iowa Health Care Data

There are limitations on where researchers at UI Health Care and the Carver College of Medicine (CCOM) can store UI research data extracts (data extracted from UI Health Care patient records, operational or personnel data). It is not necessary to have approval from the Data Governance Task Force to store patient data extracts on the R:Drive (managed by Carver College of Medicine Office of Information Technology), UI Health Care and CCOM departmental drives, or ShareFile.

To store data on UI Information Technology Services (ITS) servers that are not managed by Health Care Information Systems (HCIS) or shared outside of the University of Iowa, there must be an "external data sharing request" reviewed by the UI Health Care Data Governance Task Force. The following are links to the external data sharing request forms:

- To request storage of patient data extracts on services outside of UI Health Care: https://redcap.icts.uiowa.edu/redcap/surveys/?s=4WCM7EMNMTP4PMA4

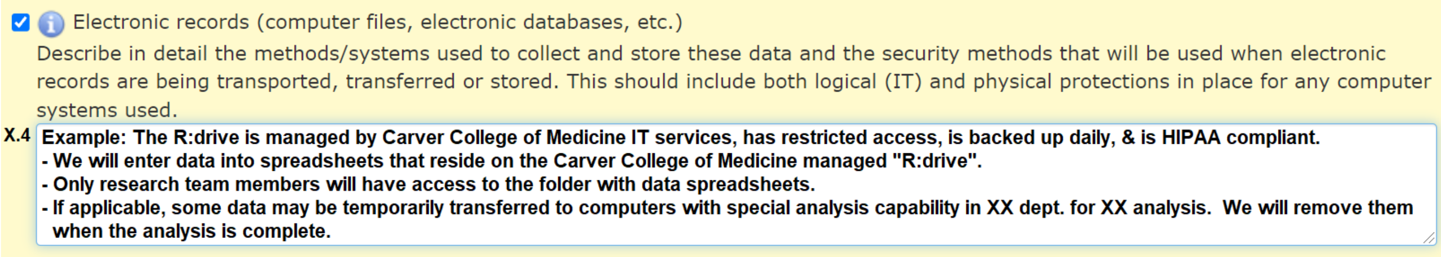
- If you are unsure if a request is needed: https://redcap.icts.uiowa.edu/redcap/surveys/?s=99HLXDRMNXJFX9R9

Research Data Storage Options that are HIPAA compliant include: Research Data Storage Service (RDSS), Large Scale Storage (LSS), R:Drive, UI Health Care departmental drives, ShareFile, and OneDrive. RDSS, LSS and OneDrive are stored on managed UI ITS systems and are secure enough for protected health information. However, researchers need approval from the UI Health Care Data Governance Task Force and a Data Use Agreement prior to using them.

- Data Use Agreements for **UI shared storage** are completed between the PI's department and the UIHC Joint Office for Compliance.
- Data Use Agreements for **external sharing outside of the UI** are completed between the PI's department and the Division of Sponsored Programs.

Note: OneDrive has an agreement with Microsoft to safeguard UI data. Depending on the amount of data stored, and the researcher's UI employment appointment, there may be a cost associated with these storage options.

Describe the storage, transport and transfer of UI research patient data extracts in Section X.4 of the HawkIRB application:



☑ Electronic records (computer files, electronic databases, etc.)

Describe in detail the methods/systems used to collect and store these data and the security methods that will be used when electronic records are being transported, transferred or stored. This should include both logical (IT) and physical protections in place for any computer systems used.

X.4 **Example: The R:drive is managed by Carver College of Medicine IT services, has restricted access, is backed up daily, & is HIPAA compliant.**
- We will enter data into spreadsheets that reside on the Carver College of Medicine managed "R:drive".
- Only research team members will have access to the folder with data spreadsheets.
- If applicable, some data may be temporarily transferred to computers with special analysis capability in XX dept. for XX analysis. We will remove them when the analysis is complete.

Audio/Video Recording Best Practices for In-person and 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 and 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.

Cell phones cannot be used for *any* recording functions – in-person or phone conversations, Zoom, or Skype for Business sessions. 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 (e.g., UI OneDrive, RDSS, H:Drive) at the conclusion of the research visit. Once securely stored, the audio and/or video recording should be deleted from the recording device. **Identifiable and highly sensitive data should be saved directly to a UI-managed location**. For additional guidance, see Secure Zoom Meetings and Recordings for Restricted and Critical Data.

Investigators seeking only audio recordings should take care **not** to obtain video recordings via Zoom or Skype for Business. To capture only audio content, investigators should ask Zoom participants to disable their cameras before recording sessions begin. Both Zoom and Skype for Business applications have the capability to automatically store 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.

Using Zoom for Research with Minors

Zoom can be used for research involving minors. It is best to consult with the research team's local IT representative to ensure Zoom settings are consistent with IT privacy and confidentiality requirements. Audio and/or video recordings of minors makes the data identifiable. Implement appropriate confidentiality protections. Zoom recordings should be saved directly to a UI-managed location, such as a shared drive or UI

One Drive. For additional guidance, see Secure Zoom Meetings and Recordings for Restricted and Critical Data.

Sharing Data Outside the University of Iowa

The University of Iowa owns all data collected at UI by faculty, staff, and student researchers (Researcher Handbook, 7g. Data ownership and transfer). It may be necessary to establish 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 are shared with former research team members or individuals outside the UI

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.

The UI Health Care Data Governance Task Force must approve the sharing of UI Health Care data. To initiate the request, contact them at bmi-consulting@healthcare.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. The following eConsent tools are available for research that is not regulated by the Food and Drug Administration (FDA):

- REDCap - Contact the Institute for Clinical and Translational Science (ICTS) Biomedical Informatics Core for more information about this eConsent tool. NOTE: REDCap is available for biomedical and non-biomedical (social/behavioral/educational) research.
- DocuSign – Contact ui-docusign@uiowa.edu to set up a DocuSign account and activate it through the UI system. See Using DocuSign as an eConsent Tool. Contact the UI Purchasing Department to request training.
- Qualtrics could also be used in limited instances as an eConsent tool.

Any eConsent tool used for a human subjects research project must be approved by the IRB of record prior to use. See the following educational tool for additional guidance: Alternatives to an In Person Informed Consent Process

For additional assistance, contact the Human Subjects Office via email (irb@uiowa.edu) or call (319)335-6564.

Virtual options for conducting human subjects research visits and 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. If the tool is not approved by UI ITS, a technology or IT security plan will be required.

For additional guidance, see Secure Zoom Meetings and Recordings for Restricted and Critical Data

Data Security for Research Activities Conducted Virtually or at a Non-UI Site

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. If necessary, UI ITS advises the study team establish remote access to study files for team members working at an alternate location. This would require appropriate IT security and confidentiality measures consistent with UI ITS policies (e.g., encryption, use of VPN, use of OneDrive, etc.).

PI/Research Teams should also comply with grant or contractual obligations related to data security, storage, and IRB-approved 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 any applicable requirements. Remote study activities may need to be described in the HawkIRB application. If you have any questions about whether remote option study activities are possible or approvable (especially for consent), contact the IRB at irb@uiowa.edu.

Conducting Research from a Remote Location

For any research activities from a remote location, the HSO/IRB recommends applying the security and IT best practices outlined by UI ITS:

- Secure your computer with the most up-to-date operating system, anti-virus and anti-malware. Use a strong password. Lock or sign out when not in use.
- Connect to campus resources, such as the Cisco AnyConnect VPN Client. Do not connect to public wi-fi unless connected to the UI VPN.
- Follow guidance on using personal computers for research.
- Do not store data on a personal computer. Use UI-managed network drives described above (RDSS, LSS, ShareFile, OneDrive, Home Drive, etc.) by mounting them on your computer.
- Do not use personal storage drives (external hard drive, USB flash drive, Box, Dropbox, Google Drive, cell phone, etc.)
- If a USB flash drive is absolutely necessary, contact the ITS Help Desk to learn how to encrypt it.
- Follow UI ITS standards for working remotely.
- Comply with UI ITS "Top 10 Security Considerations When Working From Home".

For additional guidance, contact IT Research Services at research-computing@uiowa.edu.

Best Practices for Data Transfer

If data will be shared outside the UI, use a Secure File Transfer Protocol (SFTP):

- Provide access to a specific file/folder (e.g., RDSS drive or OneDrive).
- For large data sets, use Research Data Collaboration Service (RDCS) via Globus for high-speed data transfer.
- Rather than using email, store the file in OneDrive and email an authenticated link to the recipient.
- Request a provisional Guest HawkID to access UI resources such as RDSS, HawkIRB, UI VPN, etc.

The UI Health Care Data Governance Task Force must approve the sharing of UI Health Care data. To initiate the request, contact them at bmi-consulting@healthcare.uiowa.edu.

Using Zoom to Conduct Virtual Research Visits

The version of Zoom available through UI and UI Health Care is compliant with HIPAA standards as long as the research team follows the instructions for Secure Zoom Meetings and Recordings for Restricted and Critical Data. The HSO/IRB recommends UI ITS recommendations listed below 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
- Zoom Meetings and Recordings for Restricted and Critical Data

Resource Guide for Data Security

Resource	Link(s)	Description
Protecting Sensitive Data	https://its.uiowa.edu/protect-sensitive-data	ITS webpage with guidance about research data security
Data Classification Guide	https://its.uiowa.edu/dataclassificationguide	A list of IT services and what data types are approved for each
ITS Research Storage Services	https://its.uiowa.edu/researchstorage	A table comparing all the ITS-provided storage services
Conducting Research Remotely	https://its.uiowa.edu/working-remotely-iowa https://itsecurity.uiowa.edu/resources/everyone/working-remotely	Article about how to work remotely in a secure manner
Video Conferencing Tool Guide	https://its.uiowa.edu/support/article/118416	Comparison guide describing all ITS video conferencing tools
Zoom Best Practices and Security Guidance	https://teach.uiowa.edu/zoom-privacy https://itsecurity.uiowa.edu/resources/everyone/zoom-security-and-privacy	Articles about how to secure Zoom
Using a Personal Computer for Research	https://its.uiowa.edu/node/119981	Article about what is required before using a personal computer for research
HSO Data Security Educational Tool	https://hso.research.uiowa.edu/irb-educational-tools	HSO guide about how to safely and securely collect sensitive research data
HawkIRB Section X	https://its.uiowa.edu/support/article/120001 HawkIRB Help Messages (?)	Information about how to appropriately fill out Section X of the HawkIRB application
College of Liberal Arts and Sciences IT Departmental Assignments	https://clas.uiowa.edu/it-group/departmental-assignments	A list of department IT staff in the College of Liberal Arts and Sciences that can offer data security help and guidance

Resource	Link(s)	Description
Technology Review	https://its.uiowa.edu/campus-software-program/technology-reviews	Webpage about the Technology Review Process
Technology Review - List of Reviewed Software Agreements	https://its.uiowa.edu/campus-software-program/technology-reviews/reviewed	List of software services and applications that have been put through the Technology Review process
Security Review	https://workflow.uiowa.edu/form/security-review	Link to the Security Review workflow form
UI Health Care Data Governance Review	https://redcap.icts.uiowa.edu/redcap/surveys/?s=4WCM7EMNMTP4PMA4 https://redcap.icts.uiowa.edu/redcap/surveys/?s=99HLXDRMNXJFX9R9	Submit a request to share data outside UI Health Care Submit if uncertain whether a request is necessary to share data outside UI Health Care
How to Fill Out an IT Security Plan	https://its.uiowa.edu/support/article/119986	An article explaining how to fill out a Research IT Security Plan for IRB applications and contracts
Research Data Collaboration Service	https://its.uiowa.edu/rdcs	An ITS service for transferring large data sets to internal and external collaborators
Guest HawkID Account Request Form	https://iam.uiowa.edu/accounts	UI staff can request guest HawkIDs for external collaborators to access UI resources

Used with permission from IT Research Services