Data Security:
Storing and Transmitting Data for Human Subjects Research

Institutional Review Board and Human Subjects Office

Introduction

Data security measures protect the privacy of participants and the confidentiality of research subject data. To obtain IRB approval, researchers must make adequate plans to protect subject privacy and the confidentiality of study data. These must be described in the HawkIRB application, and in the Informed Consent Document. This guidance document:

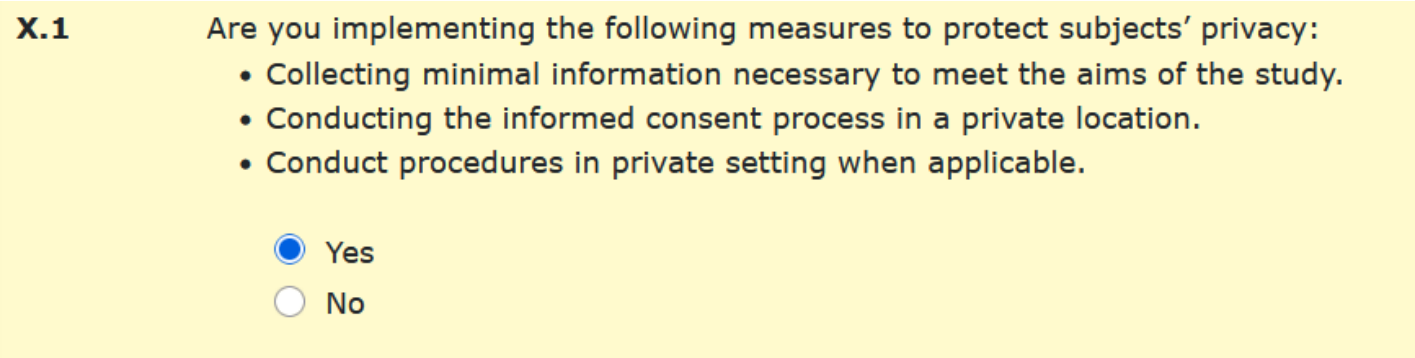
- Explains the distinction between participant privacy and data confidentiality protections
- Provides best practices:
  - to protect participant privacy at the point of data collection.
  - to protect confidentiality during data storage and transmission.

Privacy Protections

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

- Collecting only the amount and type of information necessary to address research questions.
- Obtaining informed consent in a private setting.
- Collecting data in a private setting.

Indicate in HawkIRB Section X.1 your plan to follow these measures.



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 HawkIRB Sections X.2 through X.9, including the data being stored, where it is being stored and who will have access to the data.

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.

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. 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.
- 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.

Researchers must also consider the possibility of 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. The types of Personally Identifiable Information (PII) or Protected Health Information (PHI) that is collected for the study is indicated in HawkIRB Section VII.D.1.d.

Confidentiality protections must address:

- Data transmission and storage 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

These protections will be described in Section X.4 of the HawkIRB application.

Paper Records

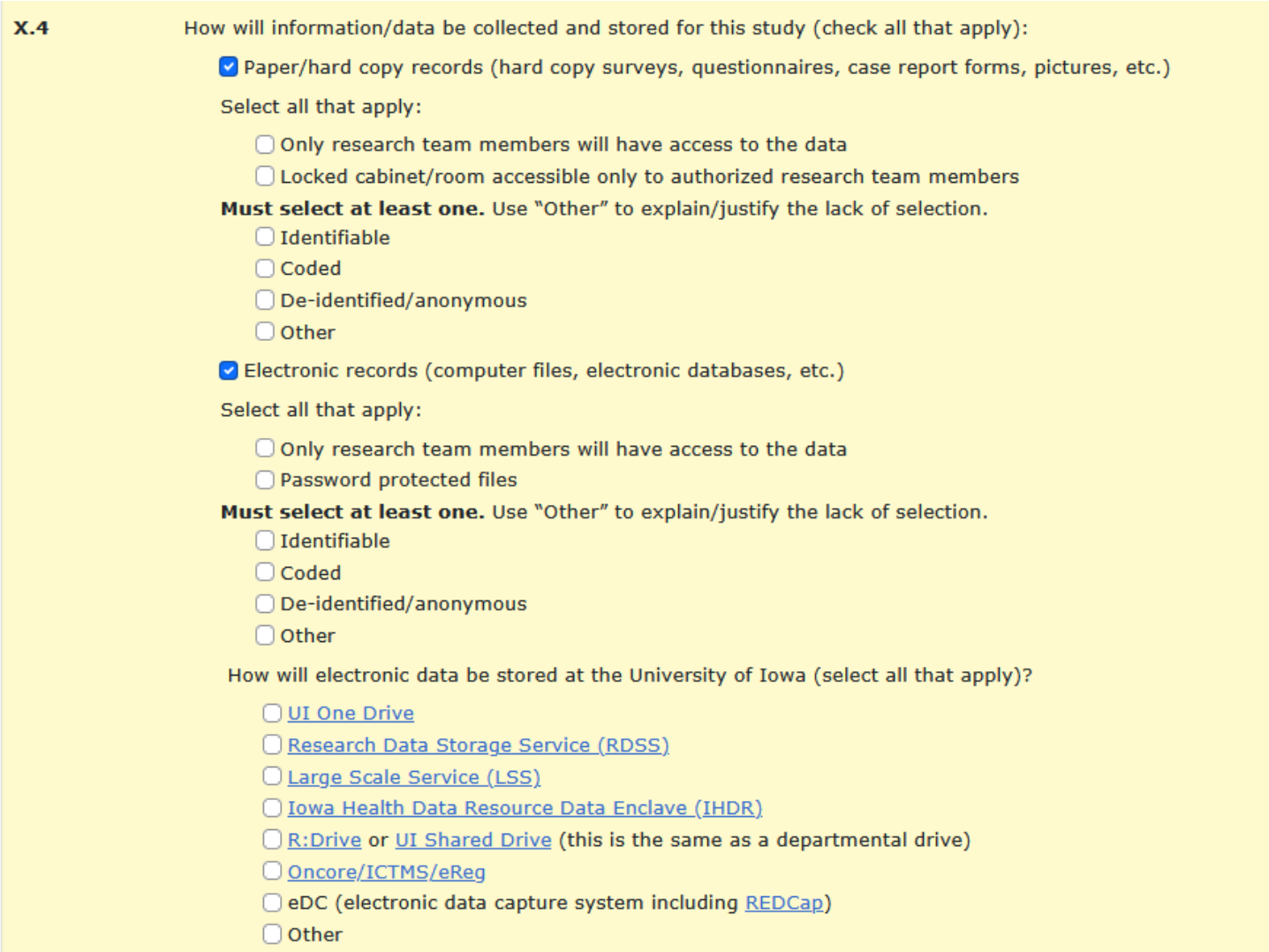
Paper records include any paper documents that contain study data or other research-related records. Signed Informed Consent Documents are considered paper records with identifiable information. The research team is responsible for maintaining confidentiality protections for all paper records, including 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. These protections will be described in Section X.4 of the HawkIRB application.

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

- [x] Paper/hard copy records (hard copy surveys, questionnaires, case report forms, pictures, etc.)

Select all that apply:

- [ ] Only research team members will have access to the data
- [ ] Locked cabinet/room accessible only to authorized research team members

Must select at least one. Use "Other" to explain/justify the lack of selection.

- [ ] Identifiable
- [ ] Coded
- [ ] De-identified/anonymous
- [ ] Other

- [x] Electronic records (computer files, electronic databases, etc.)

Select all that apply:

- [ ] Only research team members will have access to the data
- [ ] Password protected files

Must select at least one. Use "Other" to explain/justify the lack of selection.

- [ ] Identifiable
- [ ] Coded
- [ ] De-identified/anonymous
- [ ] Other

How will electronic data be stored at the University of Iowa (select all that apply)?

- [ ] UI One Drive
- [ ] Research Data Storage Service (RDSS)
- [ ] Large Scale Service (LSS)
- [ ] Iowa Health Data Resource Data Enclave (IHDR)
- [ ] R:Drive or UI Shared Drive (this is the same as a departmental drive)
- [ ] Oncore/ICTMS/eReg
- [ ] eDC (electronic data capture system including REDCap)
- [ ] Other

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, utilize the **ITS Self-Service Portal.**

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: Critical, Restricted, University-Internal and Public.

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)

Classification Level	Description	Institutional Data Examples
Critical	• Inappropriate handling or disclosure of this data could cause **severe harm** to individuals and the university, including exposure to criminal and civil penalties, identity theft, personal financial loss, or invasion of privacy. • Only selective access (on a need-to-know basis) may be granted. • Has the most stringent legal or regulatory requirements and requires the most prescriptive security controls.	• Patient health, payment/insurance, and treatment data • Social Security Number • Credit card information • Personal identifiers (e.g., passport, driver's license) • ITAR data • Investigative reports
Restricted	• Disclosure could cause **significant harm** to individuals and the university, including exposure to civil liability. Because of legal, ethical, or other constraints, this data may not be accessed without specific authorization. • Only selective access (on a need-to-know basis) may be granted. • Usually subject to legal and regulatory requirements due to data that are individually identifiable, highly sensitive and/or confidential.	• Financial aid data • Student transcripts • Identifiable human subject research data
University-Internal	• Disclosure could cause **limited harm** to individuals and the university with some risk of civil liability. • This data may be accessed by eligible employees and designated appointees of the University for the purpose of university business. Access restrictions should be applied accordingly. • Either subject to contractual agreements or regulatory compliance or is individually identifiable, confidential, and/or proprietary.	• Financial reports • Departmental memos • Committee meeting minutes • De-identified human subject research data

Public	• Encompasses information for which disclosure poses **little to no risk** to individuals or the university. • Few restrictions are placed on this data, as it is generally releasable to a member of the public upon request or is published. • Anyone regardless of institutional affiliation can access without limitation.	• Collegiate and departmental websites • News releases • Information subject to open records requests (email, financial, etc.)

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 utilize the **ITS Self-Service Portal.**

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)

Note: If you intend to store PHI from University of Iowa Health Care on services not managed by UI Health Care, you are responsible for obtaining approval from the UI Health Care Data Governance group. Please contact icts-bmi-consulting@healthcare.uiowa.edu for more information.

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, 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 utilize the **ITS Self-Service Portal.**See the Data Classification Guide to IT Services page of the UI Information Technology Services website to see what types of data can be used with different IT services and tools.

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://workflow.uiowa.edu/form/external_data_sharing
- 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.

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

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 of the HawkIRB application should describe the security precautions used for audio/video recorded data.

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 handheld 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, 7f. 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, utilize the **ITS Self-Service Portal.**The UI Health Care Data Governance Task Force must approve the sharing of UI Health Care data. To initiate the request, contact them at icts-bmi-consulting@healthcare.uiowa.edu.

Tools Available to Conduct Remote or Virtual Research Related Activities

For information regarding electronic consent (eConsent) please review the Alternatives to an In-Person Informed Consent Process educational tool and the eConsent Checklist educational tool.

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 remote work guidelines.

For additional guidance, utilize the **ITS Self-Service Portal.**

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 icts-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:

- Zoom Connection Issues
- Zoom Security and Privacy
- Secure 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/dataclassification guide	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

Resource	Link(s)	Description
Conducting Research Remotely	https://its.uiowa.edu/working-remotely-iowa and https://itsecurity.uiowa.edu/resources/everyone/working-remotely	Articles 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://itsecurity.uiowa.edu/zoom-security-and-privacy	Article about how to secure Zoom
Using a Personal Computer for Research	https://its.uiowa.edu/services/protecting-sensitive-data/guidance-using-personal-computers-research#:~:text=Personal%20computers%20can%20be%20used,if%20gathering%20human%20subjects%20data .	Article about what is required before using a personal computer for research
HSO Data Security Guidance	https://hso.research.uiowa.edu/get-help/educational-tools/data-security-guidance	HSO guide about how to safely and securely collect sensitive research data
HawkIRB Section X Guidance	https://its.uiowa.edu/services/protecting-sensitive-data/irb-application-section-x4-guidance ⓘ 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
Technology Review	https://its.uiowa.edu/available-software/technology-review-process	Webpage about the Technology Review Process
Technology Review - List of Assessed Technology	https://apps.its.uiowa.edu/sec-hq-courier/assessed-technology	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://workflow.uiowa.edu/form/external_data_sharing	Submit a request to share data outside UI Health Care

Resource	Link(s)	Description
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