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

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](#).

<table>
<thead>
<tr>
<th>Service</th>
<th>Public</th>
<th>University/Internal</th>
<th>Restricted/Critical (personal identifiers &amp; SSNs only)</th>
<th>Export-Controlled</th>
<th>HIPAA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Research Data Storage Service (RDSS)***</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Large Scale Storage (LSS)***</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Home Drives (Files@iowa)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Shared Drive (Files@iowa)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OneDrive for Business</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SharePoint Online (O365)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dropbox</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Google Drive</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Apple iCloud</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Box</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Personal Devices (e.g. laptops, USBs, personal cloud services, etc.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AWS Cloud Enterprise</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Microsoft Azure Cloud Services Enterprise</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HPC Systems</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Dispatch</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>REDCap</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Research Remote Desktop Service</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Qualtrics</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Skype for Business</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**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 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.

**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 Recordings

When making audio or video recordings, the IRB recommends transferring the recording to One Drive, or another approved and appropriate storage solution, as quickly as possible. 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. 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.

UI ITS and HCIS policy prohibit use of a personal mobile device for making research-related recordings.

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.