Confidentiality and Data Security Guidelines for Electronic Research Data

Tufts Health Sciences Institutional Review Board (IRB)
Tufts Medical Center Information Services (IS) and Tufts University Technology Services (TTS)
Tufts Medical Center Internal Audit & Corporate Compliance

Federal regulations require that research studies involving human subjects include adequate provisions to protect the privacy interests of participants and to maintain the confidentiality of data. In its review of research, the Tufts Health Sciences IRB considers whether adequate provisions exist for the security of research data, whether in paper or electronic form, throughout the research. All electronic research data containing protected health information (PHI) must be used and stored in a HIPAA compliant manner. Principle Investigators (PIs) are responsible for ensuring that adequate controls, as described in the research protocol, are in place and followed to protect identifiable and confidential information and that only the minimum PHI necessary for purposes of the research is collected. Failure to do so could potentially result in a security breach of a subject's PHI or Personal Identifying Information (PII). A breach of PHI poses a significant risk of financial, reputational, or other harm to the individual affected, as well as to the organization.

Research practices routinely involve electronic data in a variety of ways. Traditionally provisions for the confidential handling of research data referenced keeping data in locked filing cabinets and in locked offices. While these provisions still have application when research data or materials are in hard-copy, there is a growing complexity in how research data must be protected while it is collected and stored electronically. With the anticipated increase in use of electronic devices including portable devices and drives, as well as web-based survey tools, data security requires more attention from investigators. The wide range of diversity in studies, methods, and electronic data devices means that investigators need to evaluate confidentiality and data security when electronic data is collected and/or stored. These guidelines attempt to outline basic protection provisions expected of investigators to protect data during data collection, transmission and storage, realizing that advances in device design, software, and university systems are constantly changing.

To what do these guidelines apply?

This guideline applies to all studies involving individually identifiable participant electronic data for non-exempt, human subject research. This can include even low to minimal risk studies if the information is personal or health related. Thus, even individually identifiable minimal risk research surveys on smoking and/or drug and alcohol use would be included in these guidelines.

Studies which would be excluded from the guidelines include surveys which collect no direct or indirect personal identifiers, or if identifiable, studies which are non-personal in nature, such as participation in hobbies, special or political interests, etc.

In this guideline two terms are used for personal information: (1) personal health information (PHI consistent with HIPAA concepts) and (2) personal identifying information (PII for other non-HIPAA-related studies – see the definitions section below for clarification.

In reviewing the guidelines below, investigators should also consult their Information Security (IS) department at Tufts Medical Center (Tufts MC) or Tufts University for assistance in applying the recommended data security steps.

All referenced resources, guidelines, standards, etc., in this document are available in the *Resources* section at the end of this document.

1. Consider the potential risks related to data security:

- Is the data identifiable, de-identified (coded), or anonymous?
- Is sensitive information being collected that could result in harm to participants?
- What is the risk of harm to the participant or others?

2. **Examples of protections against anticipated threats or hazards (during collection, transmission, 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
- Implementing controlled access to data files, e.g. no access, read only, read and write or administrator only permissions
- Store data behind a secure Tufts University/Tufts Medical Center firewall whenever possible
- Identify single location for the storage and regulate access to it
- Control access to rooms and buildings where data, computers or media are held
- Transport sensitive data only under exceptional circumstances
- Ensure strong data security controls on all storage sites
- Destroy data in a consistent manner when no longer needed. The study protocol should include the following information:
    - The length of time the data is required for the project
    - The length of time the data needs to be retained past the end of the study (if at all)
    - Data will be destroyed via Tufts MC IS or Tufts University TTS baseline standards. If alternative standards are proposed, obtain confirmation from Tufts MC IS or Tufts University TTS that these standards are acceptable.

3. **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 institution. It is advisable to use a secure transmission process even if the data is anonymous, coded, or limited to 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, except in very limited circumstances, and should not be used to share or transmit research data.

Text messages are stored by the telecommunications provider and therefore are not secure.

Data should be encrypted when "in-transit," and the institution provides extensive guidance, software, and resources to assist researchers in this. Terms such as Secure Sockets Layer (SSL and HTTPS) or Secure File Transfer Protocol (SFTP) are indications that the data is being encrypted during transmission.

4. Data Storage

It is important to remember that the research data belongs to Tufts MC or Tufts University and not the researcher. It has become common practice to store some level of PPI in the Cloud with services such as Box, Google Drive, Dropbox, Salesforce.com, Evernote, and Office365. Using such services can often result in cost savings; however, special attention must be paid to potential security risks, export control restrictions, data ownership issues, and HIPAA. Such services also need to approved for use at Tufts MC or Tufts University (Google Drive, Dropbox, Salesforce.com, Evernote, are NOT approved for use at Tufts)

a. Cloud Collaboration for Data Sharing:

i. Box - A cloud collaboration application approved for data sharing by Tufts MC IS or Tufts University TTS. The configuration of Box is by the owner/admin of the collaboration project and they are responsible for limiting access via the setup within the Box account assigned to him/her. Box logons are monitored by IS. Once your study is over, email IS and they will remove your logon and data access. If you do not logon for over a month IS may contact you to ask if Box access is still needed. Users can also contact IS to request that shared data is no longer available after a specified date or days.
ii. Office 365 – This cloud service is approved for data sharing by Tufts MC IS or Tufts University TTS. Contact Tufts MC IS or Tufts University TTS for information on how to implement this for your study.
iii. Amazon Web Services (AWS) – Contact Tufts MC IS or Tufts University TTS for confirmation whether this service can be used for your study.

Only data that meets HIPAA de-identification standards should be stored on a cloud server. For identifiable information, the best practice is to store the data on a server maintained by Tufts MC IS or Tufts University TTS or a server that has been sanctioned by Tufts MC IS or Tufts University TTS. Using departmental servers (such as a local C: G: or H: drive) to store research data is not recommended. These servers must be approved by the Tufts MC IS or Tufts University TTS Officer and require extensive and costly IT support to maintain all the virus signatures, malware protection, operating system updates, and incident response standards.

Data stored with a cloud provider should adhere to Tufts MC or Tufts University baseline standards as it relates to secure data management. Also, cloud vendor selection should be reviewed by Tufts MC or Tufts University Risk Assessment to insure that security and audit requirements are met.

b. Storing Data outside of Tufts MC or Tufts University Networks

If you are considering the storage of any data outside of Tufts MC or Tufts University networks, working with Purchasing will help you address the following questions that will be required by the University:

i. Does the agreement with the vendor stipulate that the institution owns the data?
ii. Does the agreement with the vendor incorporate Tufts MC or Tufts University's Personal Data Protection Addendum?

iii. How will the vendor make the data available in the event of a disaster?
iv. What security controls are in place to prevent the inadvertent or malicious disclosure of the data?
v. What happens if a subpoena or legal hold is issued?
vi. Does the vendor have Information Security/Cyber Liability insurance?

c. **Collecting or Storing Research Data Using the Internet**

Collecting or storing research data using the internet results in additional complexity as one must consider the jurisdictional authority: is it the jurisdiction of the researcher, the location of the study participants, or the location where the data is stored? Data may be collected in one jurisdiction but then stored in another. Researchers need to be aware that there may be differing data security privacy policies. It is important that researchers consider the laws, including international laws and export controls regulations, and if needed have agreements in place to ensure compliance.

5. **Encryption**

Encryption protects data by encoding information so that only authorized parties may read it. Encryption can be enforced "at-rest" where the data is being stored and "in-transit" as the data is being moved from one location to another. There are many tools and methods available to encrypt all types of data, and Tufts MC or Tufts University has resources available. Encryption standards need to be best practiced at the time of the project. Standards progress and change over time because they are replaced with stronger solutions. Keep educated on encryption standards and contact Tufts MC IS or Tufts University TTS for available resources or additional information.

6. **Mobile Apps**

Many researchers are purchasing mobile apps or building their own app to interact with study participants. Seek expert IT review and, if commercially available, purchase the app through the Tufts MC or Tufts University Purchasing Office so a legal and data security review is performed. Even if the participant is asked to download a free App or provided monies for the download, the researcher is still responsible for disclosing potential risks. It is possible that the App the participant downloaded will capture other data stored or linked to the phone on which it is installed (e.g., contact list, GPS information, access to other applications such as Facebook). The researcher has the responsibility to understand known or potential risks and convey them to the study participant. Commercially available apps publish "terms of service" that detail how app data will be used by the vendor and/or shared with third-parties. It is the researcher's responsibility to understand these terms, relay that information to participants, and monitor said terms for updates. Additionally, it is important that the researcher collect from the App only the minimum data necessary to answer the research questions.

Social Media

Research data should never be disseminated via any social media application or website due to lack of privacy and control of data with these. Refer to the IRB's policy: Direct Advertising Material for Recruitment for additional information on social media use for your study.

Phishing Campaigns- Targeted & Blanket

Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.

Be aware that targeted phishing attempts are plaguing the healthcare industry as we have valuable data stored within our systems. If you were to trigger an exploit by clicking a link within a phishing email, exposure could cause a breach and/or a ransomware event.

7. **Children's Online Privacy Protection Act (COPPA)**

The Federal Trade Commission enacted COPPA in 2000 (revised in January 2013), 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 Office of General Counsel with any questions. It is the responsibility of the researcher to ensure they are fully compliant with the COPPA regulation.

8. **Survey Software**

Survey software such as SurveyMonkey can be used to conduct some types of survey research. However, PHI, PII and study data should not be stored on their servers. Any survey software must first undergo a data security review, and if commercially available, must be purchased through the institution's Purchasing Office.

Many investigators wish to collect the IP addresses of survey participants to provide a method of determining whether the user has previously completed the survey. As stated earlier, the institution, HIPAA, 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. When using survey software, 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.

9. **Data Disposal:**

When covered entities dispose of any electronic media that contains electronic PHI they should make sure it is unusable and/or inaccessible. General examples of proper disposal methods for PHI on electronic media include:

a. clearing (using software or hardware products to overwrite media with non-sensitive data)
b. purging (degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains)
c. destroying the media (disintegration, pulverization, melting, incinerating)
d. Do "a" and "b" before you send the data off-site for destruction.

Refer to the record retention policy in your protocol and/or Site-Specific Appendix prior to disposing any electronic study data.

10. **Other Considerations:**

- 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
- Collect only the minimum data necessary to answer the research question as per HIPAA.
- Codes are not stored with the corresponding de-identified data
- Encryption methods are being used on all portable devices (laptops, mobile devices, and removable storage)
- The Health Insurance Portability and Accountability Act (HIPAA) also applies to electronic research data. For more information about this, please contact the applicable HIPAA contact below.
- Data that becomes intellectual property. Review Tufts MC or Tufts University's Intellectual Property policy for additional information.

All computers and laptops used for research should already have installed by Tufts MC IS or Tufts University TTS, the software and tools described above. Any additional software needed for specific studies should be installed by Tufts MC IS or Tufts University TTS as needed.

11. **Resources:**

National Institute of Health (NIH)
2.3.12 Protecting Sensitive Data and Information Used in Research
4.1.9 Federal Information Security Management Act
Guidance Regarding Social Media Tools

U.S. Food and Drug Administration
Mobile Medical Applications
FDA Guidance for Industry Electronic Source Data in Clinical Investigations

U.S. Department of Health & Human Service
Human Subjects Research and the Internet
Disposal of Protected Health Information

Federal Trade Commission
Understanding Mobile Apps

HealthIT.gov
Your Mobile Device and Health Information Privacy and Security

HIPAA Security Series
Security Standards: Physical Safeguards

Information Technology Asset Knowledge (ITAK)
Electronic Healthcare Data Erasure – Concerns for Secure Disposal Management

Tufts Medical Center & Affiliates (see hyperlinks below)

- Tufts MC Policies are stored online within PolicyTech and are available 24x7 via web access. A PolicyTech link is available via the Tufts MC intranet. Users can logon to PolicyTech via their Tufts MC network credentials.
- https://tuftsmedicalcenter.policytech.com

Tufts University Resources – Policies & Guidelines (see hyperlinks below)

- Information Stewardship Policy
- Telecommuting Tech Guidelines
- Massachusetts Data Privacy Program
- Tufts Box Use Guideline
- Overview of Your Rights and Responsibilities Online
- Tufts Password Policy
- Cloud Computing Services Policy
- Tufts Active Directory Account Standard
- Network Use Policy
- Policy on Information Technology Acquisitions
    - Technology Buyers Guide
- Email Policy
- Tufts University Participant Operating Practices for InCommon Federation
- Mailing List Policy
- Copyright and Fair Use
- Policies & Standards - Intellectual Property
- Two-Factor Authentication
- Information on securely handling Sensitive Personal Information:
    - Tips and Guidelines
    - Summary one pager
- Using encrypted email:
    - https://it.tufts.edu/nws-sec-email
    - https://it.tufts.edu/qs-proofpoint-5
- Email Deletion:
- Tufts Box Use Guideline
    - Information on using Box
    - Box Collaboration/Sharing Security Tips
    - Hints and Tips on Establishing Group Folders and Group Account Ownership
    - Using Box for Sensitive Information
    - Box Sync Security Tips
- Loaner Laptops:

- https://it.tufts.edu/nws-laptop
- https://it.tufts.edu/laptop-travel

- Eduroam:
- Password Protecting and Encrypting Files (Adobe and Microsoft)
- Using Identity Finder to securely delete a document: Securely Shredding Files on your Computer

HIPAA - Privacy – Information Security Officers Contact Information

Tufts Medical Center & Affiliates

Meghan Colozzo
Privacy Officer & Director of Compliance
Corporate Compliance
(617) 636-1203
MColozzo@tuftsmedicalcenter.org

Cara Merski
Chief Compliance Officer
Corporate Compliance
(617) 636-9229
CMerski@tuftsmedicalcenter.org

Timothy Lanza
Information Security Manager
Information Services
(617) 636-3263
tlanza@tuftsmedicalcenter.org

Tufts University

Akiyo Fujii
Associate General Counsel
(617) 627-3336
Akiyo.Fujii@tufts.edu

Tufts University School of Dental Medicine

Kevin O'Dea
Director of Data and Systems Security
(617) 636-0328
Kevin.Odea@tufts.edu