Confidentiality and Data Security Guidelines for 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

TABLE OF CONTENTS

INTRODUCTION

The federal Common Rule requires research studies involving human subjects to 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 (HS) IRB considers whether this Common Rule requirement will be met during all the stages of the research. Principal Investigators (PIs) are responsible for ensuring that privacy and security controls are accurately described in their protocol and that the controls are followed throughout their research. Failure to protect participants' personal, private information, including Protected Health Information (PHI), from a security breach will risk exposing the research participants, Tufts Medical Center (Tufts MC), Tufts University, and the researchers to financial, reputational, and other significant harm.

TO WHOM DO THESE GUIDELINES APPLY?

These Guidelines apply to both Tufts University and Tufts MC researchers. Some sections are labeled as applying to a particular group of researchers based on their institution.

If you are employed or affiliated with both Tufts University and Tufts MC, then it is very important for you to determine under which institution's administration you will be conducting your research. This will determine which organization's policies, guidelines, IT systems, and other services apply and are available to you. For funded research, consider which institution is the recipient of the funding. Also, consider the parties to any agreements related to your research.

WHEN DO THESE GUIDELINES APPLY?

These Guidelines outline basic practices expected of investigators to protect data during collection, transmission, analysis, storage, archiving, and destruction, realizing that device design, software, apps, tools, and university systems are constantly changing.

PIs are responsible for compliance with these Guidelines. Research assistants and other project staff must also understand and follow the procedures and practices described in these Guidelines. PIs are directly responsible for training and monitoring all project staff who work with or have access to their project's data.

These Guidelines apply to all studies involving individually identifiable participant data for human subjects research, including PHI and other personal data (including political opinions). Even if a study is considered to be minimal risk, the investigators will still need to review and follow these Guidelines. These Guidelines also apply to data that is de-identified after collection. If a study's data is fully anonymous when collected (it does not include any direct or indirect personal identifiers and the identity of the subjects is unknown) then many of these Guidelines will not apply. Yet, good information security practices should be used for all research data, whether or not anonymous/de-identified, in order to protect the data not only for confidentiality purposes, but to maintain data integrity and availability for your research. See the definitions below for more information on the terms used in this paragraph.

KEY RESOURCES

Investigators should consult with their Information Security (IS) department at Tufts MC or Tufts University for assistance in applying the recommended privacy and data security steps.

Key resources at Tufts University are:

- Restricted Data Guidelines and the online learning module, Stepping up your Game – 10 Key Strategies for Protecting Tufts Most Sensitive Information, which can be found in the Tufts Learning Center https://access.tufts.edu/tufts-learning-center.
- Research Tools: Security and Privacy and the List of Research Tools and Services reviewed by TTS.

There is also an extensive RESOURCE LIST section at the end of this document, as well as an APPENDIX for more information.

THE GUIDELINES

1. Best Practices for Data Handling and Management

- Consider the potential privacy and security risks.
- Collect only the minimum data necessary to answer the research question. Avoid collecting identifiable information (including electronic identifiers) unless it is necessary.
- Consider whether sensitive information will be collected that could result in harm to participants or others if the data is misused or disclosed.
- Whenever possible, either collect anonymous data or de-identify data after collection.
- When seeking to de-identify your dataset, consider whether the components of the dataset, when evaluated together, could enable identification of individuals, including when linked with publicly available datasets. The number of participants will be an important factor.
- Consider whether your research data will be subject to specific requirements under US or international laws/regulations; institutional policies and guidelines; or funding, data use or other agreements with government agencies or other third parties.

2. Anonymous, De-identified and Coded Data

It is important to understand the terms *anonymous* data, *de-identified* data and *coded* data in the context in which they are used. If research will involve anonymous data only, then it will not be considered human subject research and will not be subject to the Common Rule. It may, however, be subject to other regulations. On the other hand, research involving de-identified data, and coded data may be considered human subject research and be required to comply with the Common Rule. Definitions of these terms can be found below in the APPENDIX.

When considering what the appropriate security controls are a particular project, it's necessary to think not only about what will be disclosed publicly, for example, in a journal article, but what data the project team will have.

Note: See HIPAA De-identified Data *in Section 12* - Health Insurance Portability and Accountability Act (HIPAA), *below.*

Tips:

- The "key" that enables identification of individuals with their participant number or other code should always be stored separately from other research data. Access to the key should be strictly limited to the PI and one or a small number of other study team members who have a specific need to access it.
- Unless necessary for the study's goals, it's a preferred privacy practice to have any audio or video recordings that include facial images or voices transcribed and the original recording destroyed.

3. Encryption

Encryption is a means of making digital data unreadable by using one or more mathematical algorithms. 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. Both Tufts MC and Tufts University provide tools and services that use encryption to protect data. For example, Box uses encryption in transit and at rest. Selecting IT tools that use encryption is important for protecting your study data.

4. Collection Tools and Practices

Protect the privacy of your research subjects by using the following practices:

- Conducting interviews/obtaining consent – whether in person or remotely - in private settings to prevent others from overhearing responses.
- Provide for private return of surveys that are completed on paper (sealed envelopes, lock boxes, etc.)
- Collect email addresses for compensation separately from responses (e.g., a separate Qualtrics survey).
- When feasible, keep the location of research sites or the identity of an organization private, such as the name of a school or health center.

Review/collection of HIV/AIDs data from medical records, recording interviews and other interactions with research participants in Massachusetts will require their consent. Consent is also required in many other states and countries.

When you choose an IT tool to collect data, that tool will often involve sharing your research data with the tool's vendor. For example, when you record a call on Zoom, Zoom retains a copy of that recording on its servers. Survey tools collect not only the responses to the questions, but may also collect location and IP address information from your study participants. For these reasons, both Tufts MC and Tufts University limit what IT tools, apps and services may be used for research.

Tools approved for Tufts University Researchers

Surveys and Questionnaires

- Qualtrics: Approved for PHI and data subject to either the European Economic Area or the UK GDPR. See Qualtrics - Create and Edit a Project. Don't use Qualtrics for longer term storage. Copy the data to your storage solution and delete from Qualtrics.
- Survey Monkey and similar tools: Not approved.
- Tufts MC REDCap/Managed by Tufts CTSI: Approved. The data will be stored on Tufts MC servers. Consider whether this will need to be disclosed in a data use agreement when using data collected by a third-party. Review by TU TTS office is required for use of PHI with REDCap - Contact TTS Office of Information Security to discuss.
- Tufts HNRCA REDCap: Approved for HNRCA affiliated researchers.

Confidentiality and Data Security Guidelines for Research Data

- See List of Research Tools and Services reviewed by TTS for other tools.

Video Conferencing

Tufts University provides regular Zoom and HIPAA Compliant Zoom. For information on how to use Zoom securely, such as avoiding Zoom bombing, see Zoom Hosting Best Practices.

Identifying Research Participants

See the Research Tools and Service Reviewed by TTS, including MTurk and Prolific.

Tools approved for Tufts MC Researchers

Surveys and Questionnaires

- Qualtrics: Approved for PHI. Don't use Qualtrics for longer term storage. Copy the data to your storage solution and delete from Qualtrics. Sign-in with your network log-in.
- HIPAA-compliant version of SurveyMonkey: Approved for PHI and PII. Contact TuftsMCSecurityAdmin@tuftsmedicalcenter.org for account creation.
- Tufts MC REDCap/Managed by Tufts CTSI: Approved. The data will be stored on Tufts MC servers. Contact the CTSI for account creation.
- See List of Reviewed Research Vendors for other Tufts MC tools.

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.

Video Conferencing

Tufts MC has a HIPAA-compliant version of Zoom available for use in research if PHI will be included. Best practices for the use of Zoom include measures to prevent non-participants from accessing the meeting, confirming identities of participants before interviews and focus groups begin, and maintaining the privacy and confidentiality of participants following Protocol procedures.

5. Transmitting and Transporting Data; Communication Tools and Practices

The process of transmitting or transporting data is often overlooked as a risk. The plan to protect confidentiality should describe secure methods to protect the data during sharing (both internally and externally) from the institution. Tools specifically approved for use in research will need to provide for encryption in transit.

Confidentiality and Data Security Guidelines for Research Data

Email

Email is generally not a secure method to collect, share or transmit research data, and should not be used for that purpose, except in very limited circumstances (e.g. to share recruitment materials not containing sensitive information). When sending mass emails, use the "bcc" – blind copy – function.

For communications among Tufts University study team members, the researchers should only use their "@tufts.edu" email account. Messages between "@tufts.edu" accounts are encrypted in transit, while messages to another email domain, such as "@tuftsmedicalcenter.org," generally are not. To send secure encrypted email messages to persons at an email address outside of the "@tufts.edu" domain, see Instructions for Sending Encrypted Email.

SMS or Text Messages

Text messages are not secure and should not be used to collect, share or transmit research data. Only use text messages for basic administration and when sensitive information is not included. For other uses, request a security review. See Selecting New Tools, Apps and Services below.

USBs and External Hard Drives – Physically Transporting Data

Using a USB, external hard drive or other portable device to transport data exposes the data to theft and loss. If you must use one, be sure the device is encrypted. Don't use a USB or external hard drive to store data.

6. Storage, Collaboration and Computer Tools and Practices

Research data may only be stored using IT apps, tools or services approved by your institution.

Note: Dropbox and Evernote are NOT approved in any case for use at Tufts University or Tufts MC.

Tools approved for Tufts University Researchers

In most cases, Tufts University researchers should use Tufts Box or the R drive. TTS Research Technology may also recommend using other tools for especially large datasets or when special requirements need to be met. When using the R drive, human subject data should be encrypted at rest. To ensure the data will be encrypted at rest when using the R drive, consult with TTS Research Technology. If your study requires high compute capacity, the High Performance Compute (HPC) cluster may be the preferred solution.

The configuration of Box is by the owner/admin of the project. They are responsible for limiting access to only those members of the study team and other authorized personnel who require access through the permissions provided within the Box account. For information on using Box securely and applying access controls, see Box Security Tips and Sharing Files and Folders.

Tools approved for Tufts MC Researchers

Box - The configuration of Box is by the owner/admin of the collaboration project, and they are responsible for limiting access to include only the study team and other authorized personnel via the setup within the Box account assigned to them.

Box logins are monitored by IS. Once your study is completed, email IS, and they will remove your login and data access. If you do not log in 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.

Office 365 – This cloud service is approved for data sharing by Tufts Medicine IS and Tufts University TTS. Contact Tufts Medicine IS or Tufts University TTS for information on how to implement this for your study.

For identifiable information, the best practice is to store the data on a server maintained by Tufts Medicine IS or Tufts University TTS or a server that has been sanctioned by Tufts Medicine IS or Tufts University TTS. **Using departmental servers (such as a local C: G: or H: drive) to store research data is not recommended.** If data will be stored on one of these drives, it must be in a password-protected, secure folder that is only accessible by the study team. These servers must be approved by the Tufts Medicine IS 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 baseline standards as it relates to secure data management. Also, cloud vendor selection should be reviewed by Tufts MC Risk Assessment to insure that security and audit requirements are met.

7. Data Access Controls for all Apps and Tools

It is especially important to limit the access to any app or tool, including storage tools, so that any individual only has access to what they need to access for their role. Tufts University Box, for example, includes several choices of access, which you can tailor to your study team's needs. These include previewer uploader, which enables uploading and viewing, but not editing or downloading.

When using a new app or tool, whenever possible integrate with Tufts University's SSO/Duo, and if Tufts University's SSO is not available, but multi-factor authentication (MFA) is for the app or tool, then use the MFA.

The "key" that enables identification of individuals with their participant number or other code should always be stored separately from other research data. Access to the key should be strictly limited to the PI and one or a small number of other study team members who have a need to access it.

Do not use group logins for any device. Anyone accessing data should identify themselves when they log on, using their own Tufts credentials, including their unique password.

Access lists should be promptly updated whenever anyone leaves the study team or their role in the project changes. Review access rights to data regularly during the project, such as a review every six months.

8. Selecting New or Specialized Apps, Tools, and Services, including Software and Mobile Apps

Tufts University Researchers

Check whether all of the third-party provided IT apps, tools, services and software you plan to use for your study will are included on the List of Research Tools and Services reviewed by TTS. If any software or other IT app, tool or service is not listed there, then request a security and privacy review from Information Security. See Research Tools: Security and Privacy or complete Research Data Security and Privacy Review Request.

This requirement applies to software, apps, and tools that may be downloadable for free. It's still important that the study data be protected.

Any purchase of an IT app, tool, service or software must be done through the Tufts Purchasing Office, unless TTS Information Security obtains approval for the researcher to accept the online terms, i.e. click through, terms.

Exception for some software: A privacy and security review will not be required for some locally installed limited use software. See the requirements at Research Tools: Security and Privacy.

Researchers who are building their own app, either directly or by contracting with a developer, or building a website in connection with their research, either directly or by contracting with a developer, are required to request a review from TTS Information Security. See Research Data Security and Privacy Review Request.

In all cases, the PI has the responsibility to understand known or potential risks of using an app, tool or service they have selected and convey them to the study participant.

Tufts MC Researchers

Many researchers are purchasing mobile apps or building their own app to interact with study participants. Information Security Review will be required as part of the IRB review process (though can begin before submitting) and, if commercially available, the app should be purchased through the Tufts MC, so a legal and data security review is performed. Even if the participant is asked to download a free App or pay 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.

9. Desktops, Laptops, Tablets and Smart Phones – Device Controls

Tufts University Device Requirements for Research Study Related Work

Staff: Must use Tufts-owned and TTS-managed devices (laptops/desktops/tablets).

Faculty and Students, including Undergraduate, Graduate, Post Docs:

- Must use a Tufts-owned and TTS-managed device when:
  - Conducting human subject research that involves identifiable data, unless use a Restricted Access protocol (see below).
  - Required by data regulations, especially HIPAA, or by contractual obligations, including research sponsors.
- When conducting other research, use of a Tufts University-owned and TTS-managed device is strongly encouraged but not required.

Restricted Access Protocol

The user:

- Accesses, views and does all processing of the data on a Tufts University-managed service/tool (accessed through the Tufts University VPN with SSO/Duo) or Tufts University approved service/tool such as the HPC cluster, the virtual desktop service, or Tufts University Box.
- May not download, export, or otherwise copy the data to the personal device.

Requirements for using any Personal Device

Whenever a personal device is used, the user is responsible for ensuring the personal device meets TTS' device standards and follows the TTS security protocols for use of devices. See Securing your Devices Checklist and Securely Working with Technology Especially when Working Remotely or Using a Personal Device.

Tufts MC Device Requirements

- Encryption of data on devices to protect against loss/theft of device.
- 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.
- Data security to ensure all software updates and patches are being applied.

Confidentiality and Data Security Guidelines for Research Data

All computers and laptops used for research should already have the software and tools described above installed by Tufts MC IS, 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.

10. Paper and Physical Controls

To protect your research data that are on paper or other physical media, including on desktops, laptops and other devices, use the following practices:

- Control access to rooms and buildings where data, computers or media are held so that only authorized persons are provided access
- Do not leave paper documents unattended. Use a two-lock system for paper documents, by storing them in a locked file cabinet, drawer or other container, that is located in a locked space.

11. Data Disposal

Destroy data in a consistent, secure manner when it is 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.
- That data will be destroyed following 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.

For Tufts University researchers, TTS will securely wipe or destroy computers, USBs and other physical media that contain data. When shredding paper documents, use either a cross-cut shredder (not a strip shredder) or an approved shredding vendor.

When disposing of any electronic media that contains electronic PHI, a process must be used that makes the media unusable and/or the data inaccessible. General examples of proper disposal methods for PHI on electronic media include:

a. Clearing (using software or hardware products to overwrite the data on the 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. Doing “a” and “b” before sending the media off-site for destruction.
d. Destroying the media (disintegration, pulverization, melting, incinerating)

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

12. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal privacy law that protects Protected Health Information (PHI). PHI is individually identifiable health information created or received by a Covered Entity. The classification of research data as PHI and subject to HIPAA has implications for:

- The privacy and information security measures that may be required, including:
    - The authorizations required to obtain access to the PHI
    - The obligations to report a security incident
    - The obligations to the research participants if a breach occurs
- The apps, tools and services that may be used

When is data PHI?

It is a common assumption that all health data is protected by HIPAA. Another common assumption is that if health information is PHI, it is always PHI and therefore continues to be subject to HIPAA when it is transferred to another organization. Neither of these is fully accurate. Instead, PHI is individually identifiable health information *created or received* by a *Covered Entity*. A Covered Entity is any health plan, health care clearinghouse, or any health care provider who transmits PHI in electronic form. Health data that is PHI when in the possession of a Covered Entity will generally not remain PHI when it is transferred to another entity that is not a Covered Entity. HIPAA does, however, require compliance with its requirements for the transfer of the information.

Tufts MC is a Covered Entity. Research conducted by its workforce members with patient data from patients at Tufts MC is likely subject to HIPAA.

Tufts University, however, is a hybrid entity, with parts of it that are a Covered Entity and parts of it that are not. The only Covered Entities within Tufts University are: the School of Dental Medicine, the Benefits group under Human Resources, and the Orthopedic Sports and Physical Therapy Office operating out of the Mugar Sports Medicine Suite. Health and Wellness on the Medford campus voluntarily acts as a Covered Entity, but is technically not subject to HIPAA's rules. Tufts University School of Medicine, including the School of Public Health and Community Medicine, is not a Covered Entity.

Covered Entities will require either a patient Authorization or a waiver of Authorization to release their PHI to a researcher. However, once released to researchers outside the Covered Entity, the data will be subject to HIPAA *only* if it is disclosed to another Covered Entity.

For example:

- If Tufts MC discloses PHI to a researcher at the Tufts University School of Medicine, the data is not PHI and is not subject to HIPAA.
- If Tufts MC discloses PHI to a researcher at the Tufts University School of Dental Medicine (TUSDM), the data is PHI and subject to HIPAA.

Confidentiality and Data Security Guidelines for Research Data

- If a Tufts University School of Medicine (TUSM) researcher conducts a research study at a covered entity (such as Tufts MC or TUSDM), the data that is generated is very likely PHI and subject to HIPAA, even though TUSM is not a covered entity.

More information can be found in the APPENDIX below.

13. Additional Important Data Regulations and Requirements

Grant, Award and Data Use Agreements

The funder or sponsor of your research, or provider of any data, may include information security and privacy requirements in the grant, award or data use agreement. It is the PI's responsibility to ensure that those requirements are met. If there are any specific privacy or information security requirements, you should consult with your IT department.

Other Laws and Regulations that must be followed include State privacy laws, privacy laws of countries other than the US (such as GDPR and PIPL), laws regarding minors (such as FERPA and COPPA), and Export control. Information about these specific laws and regulations can be found below in the APPENDIX.

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. If subjects or data are located outside of the US, check with the IRB to see if GDPR regulations apply.

14. Intellectual Property Rights

It is important to remember that the rights to the results of the research, including the research data, are owned by Tufts MC or Tufts University and not by the researcher. Review Tufts MC's Intellectual Property policy and Tufts University's Policy on Rights and Responsibilities with Respect to Intellectual Property for additional information.

15. Special Concerns to Consider

Social Media

Refer to the IRB's policy on Direct Advertising Material for Recruitment, for information on social media use for your study.

Phishing Campaigns - Targeted & Blanket Campaigns

Information on how to avoid phish can be found at Phishing Hooks and Phacts as well as below in the APPENDIX.

RESOURCES LIST

1. Federal Government

National Institute of Health (NIH)

- 2.3.12 Protecting Sensitive Data and Information Used in Research
- 4.1.9 Federal Information Security Management Act (FISMA) (The applicability of FISMA to NIH recipients applies only when recipients collect, store, process, transmit or use information on behalf of HHS or any of its component organizations.)
- Guidance Regarding Social Media Tools (Recruitment for clinical trials)

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

- How To Protect Your Privacy on Apps

HealthIT.gov

- Your Mobile Device and Health Information Privacy and Security

HIPAA Security Series

- Security Standards: Physical Safeguards
- Guidance Regarding Methods for De-identification of PHI in Accordance with the HIPAA Privacy Rule

Information Technology Asset Knowledge (ITAK)

- Electronic Healthcare Data Erasure – Concerns for Secure Disposal Management

2. 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. Many research policies are also available on the EVA Research Site.

- See List of Reviewed Research Vendors for approved Tufts MC tools.

Confidentiality and Data Security Guidelines for Research Data

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

- Restricted Data Guidelines and Quick Guide
    - Associated online learning module, Stepping up your Game – 10 Key Strategies for Protecting Tufts Most Sensitive Information, in the Tufts Learning Center
- Research Tools: Security and Privacy and List of Research Tools and Services reviewed by TTS
- Software and Apps
- Research Data Security and Privacy Review Request
- Securing your Devices Checklist
- Securely Working with Technology Especially when Working Remotely or Using a Personal Device
- Information Stewardship Policies (includes policy for classification of data)
- Policy on Information Technology Acquisitions
- Technology Buyers Guide
- Box:
    - Tufts Box Use Guideline
    - Box Guide; Box Security Tips; Sharing Files and Folders; Hints and Tips on Establishing Group Folders and Group Account Ownership
- Email:
    - Email Standards and Guidelines
    - Instructions for Sending Encrypted Email
    - Password Protecting and Encrypting Files (Adobe and Microsoft)
    - Securely Deleting Email
- Qualtrics - Create and Edit a Project, including for Anonymous Responses
- Zoom: Zoom Hosting Best Practices and HIPAA Compliant Zoom Meetings
- Export Controls
- GDPR and Research
- Policy on Fair Use of Copyrighted Materials
- Policy on Rights and Responsibilities with Respect to Intellectual Property
- Phishing Hooks and Phacts

4. HIPAA Privacy and Information Security Officers Contact Information

Tufts Medical Center & Affiliates

Carly Tucker - HIPAA Contact
Manager, Corporate Compliance
(617) 636-0198
CTucker@tuftsmedicalcenter.org

Nicole S. Huff – VP, Chief Compliance and Internal Audit Officer
(978) 322-6124
Nicole.huff@tuftsmedicine.org

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

Tufts University

Akiyo Fujii - HIPAA Privacy Officer
Deputy General Counsel for Business Affairs
(617) 627-3336
Akiyo.Fujii@tufts.edu

Lorna Koppel - HIPAA Security Officer
Director, Office of Information Security
(617) 627-0885
Lorna.Koppel@tufts.edu

Tufts University School of Dental Medicine

Jill LeClare - Program Manager
Data and Systems Security
(617) 636-2914
Jill.LeClare@tufts.edu

APPENDIX

1. Anonymous, De-identified and Coded Data

This section provides a description of these terms so that you can understand how these terms are used in the context of the Common Rule and the review done by the HS IRB.

Definitions:

Anonymous Data. Data that was collected without direct or indirect identifiers and that were never linked to an individual. The investigator does not directly interact with the research subjects and is not at any time able to identify any subjects.

De-Identified Data. Data that is originally collected with identifiers, but after de-identification can no longer be associated with a research subject (i.e. there is no key to the coded data.) This is data that has had all personal identifiers completely removed and *permanently destroyed*.

Coded Data. Data separated from personal identifiers through the use of a code. Coded refers to data that no one can link to a subject's identity without the key to the code. As long as a link (i.e. key) exists, data are considered indirectly identifiable and neither anonymous nor de-identified.

Examples of Direct and Indirect Identifiers. Direct identifiers are the commonly understood markers of identity, such as a person's name, address, Social Security number. Indirect identifiers, such as demographic information, could be combined with other information in order to deduce or obtain a subject's identity. A person's voice or facial image are indirect identifiers that can increasingly be used to identify an individual, even by persons who have not seen or heard the person previously. For that reason, voice recordings or video recordings with facial images or voices should not be considered anonymous, anonymized or de-identified data.

2. De-identified Datasets under the HIPAA Privacy Rule

What is De-identified Data under HIPAA?

The HIPAA Privacy Rule creates a "safe harbor" for datasets that do not include any of 18 identifiers (of the individual or their relatives, household members, or employers) which could be used alone or in combination with other information to identify the subject. Note that even if these identifiers are removed, the HIPAA Privacy Rule states that information will be considered identifiable if the covered entity knows that the identity of the person may still be determined. The 18 identifiers are listed in the Appendix.

For more information, see Guidance Regarding Methods for De-identification of PHI in Accordance with the HIPAA Privacy Rule.

Under the HIPAA Privacy Rule "safe harbor," a dataset that does not include the following identifiers is de-identified.

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
   (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   (2) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000
3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Vehicle identifiers and serial numbers, including license plate numbers
6. Fax numbers
7. Device identifiers and serial numbers
8. Email addresses
9. Web Universal Resource Locators (URLs)
10. Social security numbers
11. Internet Protocol (IP) addresses
12. Medical record numbers
13. Biometric identifiers, including finger and voice prints
14. Health plan beneficiary numbers
15. Full-face photographs and any comparable images
16. Account numbers
17. Any other unique identifying number, characteristic, or code, except as expressly permitted
18. Certificate/license number

3. Limited Data Sets

What is a Limited Data Set?

A Limited Data Set may include some possible identifiers, but must exclude others. For example, a Limited Data Set may include dates (e.g. treatment date, date of birth), state, city, and zip code. If a researcher obtains only a Limited Data Set from a Covered Entity, the Covered Entity may release that data pursuant to a Data Use Agreement (DUA). Limited Data Sets *are* PHI, but instead of being subject to HIPAA, their disclosure to the researcher is subject to a DUA with the Covered Entity, rather than general HIPAA rules.

A Limited Data Set under HIPAA is a data set that does not contain any of the following elements:

- Names

- Postal address information, other than town or city, state, and zip code
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate and license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including fingerprints and voice prints
- Full face photographic images and any comparable images.

A Limited Data Set may include dates (e.g. treatment date, date of birth), state, city, and zip code.

4. Health Insurance Portability and Accountability Act (HIPAA)

HIPAA Privacy and Information Security Requirements

Tufts MC and each Tufts University Covered Entity seeks to comply with HIPAA's privacy and information security requirements through adopting policies and required procedures and mandatory regular training. For more information on these requirements, please see the contact information in the RESOURCES section.

What are HIPAA Compliant Apps, Tools and Services?

When using PHI in research, you will need to use HIPAA compliant apps, tools and services. *It is not sufficient to rely on that statement on a vendor's website that the app, tool or service is "HIPAA compliant."* Instead, you should understand that this statement means that the vendor's app, tool or service may comply with HIPAA if and only if particular steps are also taken. These include:

- The vendor signing a Business Associate Agreement (BAA) with either Tufts MC or Tufts University, as the case may be
- Configuring the app, tool or service in a specified manner, rather than using default settings.
- Evaluating the integration of the app, tool or service with other apps, tools and services.

Other situations when HIPAA requirements must be met

Researchers should also be aware that some Data Use Agreements may require that data received from a third-party be handled and otherwise processed in a manner that meets HIPAA's

requirements even though the data is not PHI and otherwise not subject to HIPAA. It is each researcher's responsibility to be aware of the terms of their Data Use Agreements.

For more information about HIPAA, please see HS IRB - HIPAA webpage or contact the applicable HIPAA contact listed below in RESOURCES.

5. Additional Important Data Regulations and Requirements

State Privacy Laws

Each state in the United States has its own data privacy law. Those laws generally require prompt reporting to a state agency and the data subjects if there is a breach of personal information, and may impose fines and other costs, as well as provide for litigation. Among the types of information that are covered by at least some states are: HIV/AIDs-related data, Social Security numbers, other government ID numbers, credit card and other financial account numbers, health information, even if not protected by HIPAA, online account information that is sufficient to access the account, and biometric indicators that enable identification, such as fingerprints. A few of the laws also require meeting an information security standard.

Some states, such as Illinois, have also adopted laws that regulate the collection and processing of facial recognition data. If your project will be processing facial recognition data, you should submit a Research Data Security and Privacy Review Request.

Privacy Laws of Countries other than the US

It is the PI's responsibility to ensure that their project complies with the laws of the country in which they will be conducting research. If you are a Tufts University researcher and will be collecting personal information from persons in the EEA, the UK or China, Tufts University has prepared documents and procedures to support compliance with the regulations. For other countries, it is your responsibility to consider what requirements may apply to your project.

The European Economic Area (EEA) GDPR and the United Kingdom GDPR

If you will collect personal information of any kind from persons while they are in either the EEA or the UK, the General Data Protection Regulation for the EEA and/or for the United Kingdom will usually apply to your study. Both GDPRs impose additional requirements on research studies, including providing specific information in a notice and collecting a consent to transferring the data to the US. Personal data subject to the GDPRs is defined much more broadly than in the US and includes any information relating to an identified or identifiable person.

Tufts University researchers should review GDPR and Research on the Tufts OVPR website.

China's Personal Information Protection Law (PIPL)

If you will collect personal information of any kind from persons while they are in China, China's PIPL will likely apply to your study. This data protection law imposes additional requirements on research studies, including providing specific information in a notice and collecting multiple consents. Personal data subject to the PIPL is defined much more broadly than is common in the US.

Tufts University researchers who expect to collect personal data in China should request a review of their study using this questionnaire: Research Data Security and Privacy Review Request.

FERPA

If your study will involve collecting educational record data from schools that receive funds from the Department of Education, the IT tools you use will need to comply with FERPA.

Export Control

Export control regulations govern what research instruments, materials (including biologics), software and technology that Tufts University and Tufts MC are permitted to export (i.e. transfer) out of the country by any means; and what sensitive items and technology may be shared with foreign national individuals (visa holders) studying, researching, working in, or visiting our facilities. These regulations also inform what research and business partners we engage with to the extent that we must avoid partnering with U.S. government-restricted or prohibited entities (entities of concern from a national security, export control or embargoed-country perspective). For more information, Tufts University researchers may review their responsibilities related to export controls, at https://viceprovost.tufts.edu/export-controls.

Children's Online Privacy Protection Act (COPPA)

COPPA applies to the online collection of personal information from children under the age of 13 and is enforced by the Federal Trade Commission. This Act requires websites to display a privacy policy, obtain verifiable parental consent, and disclose how the information will be used. If you plan to collect data from children online, you will need to carefully review COPPA's requirements and contact the Office of General Counsel of your institution with any questions. It is the PI's responsibility to ensure their project is fully compliant with the COPPA regulation.

6. Special Concerns to Consider

Phishing Campaigns - Targeted & Blanket Campaigns

Phishing is the attempt to obtain sensitive information such as passwords, 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 higher education and the healthcare industry Threat actors will try to trick you into disclosing your Tufts MC or Tufts University credentials so they can access your personal information and leverage their access to obtain university information. They also will use attachments and links to cause malware to be downloaded on your device, often without your knowledge. If you were to trigger an exploit by clicking a link-or opening an infected attachment, that exposure could result in a breach of confidential information and/or a ransomware event that locks down your device and other systems that can be accessed through your credentials.