Published on *UCSF Institutional Review Board* (http://irb.ucsf.edu)

Electronic Data Security

We offer our thanks to the University of Pittsburgh for its generous contribution to this guidance.

Introduction

Federal regulations require IRBs to determine the adequacy of provisions to protect the privacy of subjects and to maintain the confidentiality of their data. To meet this requirement, federal regulations require researchers to provide a plan to protect the confidentiality of research data.

Today, the majority of data is collected, transmitted or stored electronically at some point.

UCSF offers a wide range of information technology [1] services for all faculty, staff and students to safeguard this data.

Read the guidance below and develop standard best practices for managing electronic data by collaborating with your school, department or center IT staff, who have the expertise to evaluate the security methods most appropriate for the sensitivity of the research data. These best practices will need to adapt as technology evolves, so review this page and the Information Technology [1] site on a regular basis.

Policies, Guidance and Laws

All investigators and research staff should be familiar with information security policies and procedures of their department or unit, UCSF and the University of California, the state of California laws and federal privacy laws. In addition, because research is now a global enterprise, you should understand the international laws or regulations that may apply when conducting research outside the United States.

Policies, guidance and laws related to information security

Below are policies, guidelines and laws of note. This is by no means a complete list.

- **UCSF Information Security Policies and Guidelines[2]**
- **UCSF Administrative Policy 650-16 [3],** each member of the campus community is responsible for the security and protection of electronic information resources over which he or she has control.
- **UCSF Minimum Security Standards for Electronic Information Resources[4]**
- **UC Office of the President [5]** policies and guidelines
- **California Law AB 1298 [6],** which requires that residents be notified when their electronic medical information or health insurance information has been exposed. The costs of notification can be significant and departments may be at risk for notification costs if identifiable medical data are lost, stolen or otherwise exposed.
- **HIPAA [7],** a federal law designed to protect health information privacy.
- **Children?s Online Privacy Protection Act (COPPA) [8]**, 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 UCSF Office of Legal Affairs with any questions. It is the responsibility of the researcher to ensure they are fully compliant with the COPPA regulation.

Contacts and resources

- For questions about information security: IT Security and Policy [9], 415-514-4100
- For questions about HIPAA and patient privacy: UCSF Privacy Office [10], 415-353-2750

Assessing the Data Security Methods Needed

In the IRB application, you must address issues related to subject privacy and confidentiality,

HIPAA and information security. Based on the type of data involved in the study, the IRB is required to 1) assess potential risks to participants, and 2) evaluate the researchers? plan to minimize risks. The researcher has the responsibility to mitigate the risk of improper disclosure.

What is the risk?

- Is the data identifiable, de-identified (coded) or anonymous [11]? Are you keeping the code key separate from the records?

- Is sensitive information being collected that could result in harm to participants?

- What is the risk of harm to the subject or others?

- Are you collecting or retaining any data beyond what is absolutely necessary for the study (see UCOP guidance on records retention [12])?

- Have you consulted with information security experts to make sure your research and/or clinical data are secure from both physical and electronic theft?

Do the methods meet the IRB's minimum standards for the collection, storage, use and transmission of subject identifiers for human subjects research?

1. Do not collect any subject identifiers you do not need.

2. Remove/destroy subject identifiers as soon as they are no longer needed, subject to UCOP guidance on records retention [12].

3. Restrict *physical* access* to any area or computer system that contain subject identifiers.

4. Restrict *electronic* access* to any computer system that contains subject identifiers.

5. Subject identifiers should never be *stored* on laptops, PDA?s, flash drives or other portable devices. If there is a necessity to use portable devices for the initial collection of subject identifiers, the data files *must* be encrypted*, and the identifiers must be transferred to a secure system as soon as possible.

6. Subject identifiers must be removed from data files, and must be encrypted if stored electronically. Identifiers must be stored in a physically separate and secure location from the data files, and associated with data files through a code that is also stored in a separate and secure location.

7. If subject identifiers must be retained in the data files because of the specific needs of the research study, additional explanation must be provided by investigators to justify such retention. If the data are electronic, the information must be encrypted during storage and decrypted only during the limited time it is needed for matching or other similar purposes. Exceptions may be made for databases that serve both research and clinical purposes, but in these cases the server must be configured to comply with Medical Center Information Security policies.

8. Subject identifiers transmitted over public networks *must* be encrypted.

9. Subject identifiers and contact information may not be distributed outside of UCSF without the specific informed consent of the subjects, and approval by the IRB.

10. All collaborating investigators at UCSF and at other institutions must comply with these standards.

?* *This is a UCSF policy (*Administrative Policy 650-16 [3]*). Consult with information security experts for specific advice on controlling access and also see the IT Encryption Solutions page [13].?*

What are the 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

- Store data behind a secure UCSF firewall whenever possible

- Ensure strong data security controls on all storage sites

- Routinely and regularly review and update data security procedures

Continue to assess electronic security throughout the study

Research team meetings should include discussions about topics including, but not limited to, the following:

- 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
- Data collected is only that data necessary to answer the research question
- 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)

Methods for Securing Data

You have a responsibility to be a good data steward. Simply password-protecting a computer may not be sufficient to meet the rigorous security standards mandated by the University and/or sponsors. The University offers extensive security solutions [14] that can benefit researchers, some of which are described below.

Encryption

Encryption [13] protects data by encoding information so that only authorized parties may read it. You need to encrypt all of your electronic devices (e.g., laptops, iPads, cell phones, etc.) ? whether UCSF-owned or personal ? if they are used for any UCSF purpose or to access any UCSF information.

IT Encryption Solutions [13] are available to the UCSF community to deploy proper encryption with appropriate key management.

OnCore

The Online Collaborative Research (OnCore) [15] environment, is a free, comprehensive

clinical research data capture system in use at UCSF. There are three components of OnCore designed to meet investigator and program needs:

1. Clinical research management
2. Biospecimen management
3. Unified registries management

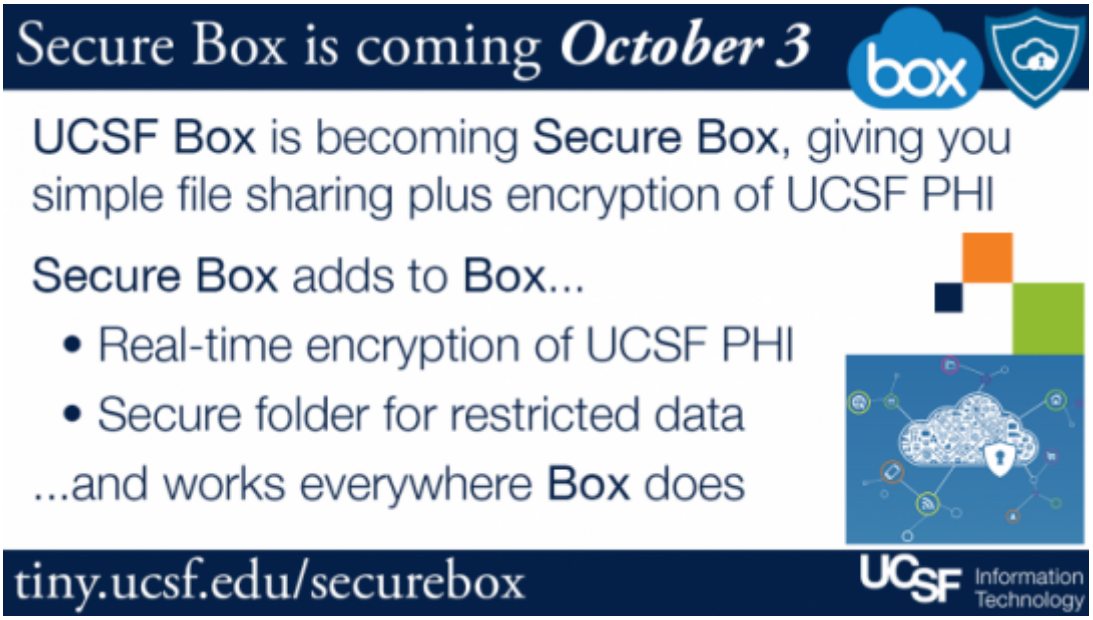
All subject information contained in OnCore is strictly confidential and treated as Protected Health Information [7], as defined in 45 CFR 164.501 (HIPAA Privacy Rule). Data entered into OnCore is stored behind university firewalls in a secure Oracle database.

MyResearch

MyResearch [16] was created to provide UCSF research teams with a professionally managed, secure, web based, collaborative environment in which to store files containing sensitive data. It provides application and database services that allow investigators to view, manipulate and save their data entirely in this protected environment without requiring files to be stored on their own computers. Applications such as SAS or Excel run on the MyResearch servers in a secure data center, but they appear as if they are running locally on the user?s computer.

UCSF Secure Box (NEW)

As of October 3, 2016, UCSF Secure Box [17] will allow UCSF Box users to store files that contain Protected Health Information [7] or other restricted data. Each UCSF Box user will get a new secure folder, and restricted data must be stored in the secure folder. Non-UCSF collaborators cannot access the secure folder. Visit the Secure Box [17] page for more info and training.



[17]

Survey software

Qualtrics [18] (recommended): Using Qualtrics, you can build, distribute and analyze online surveys ? from the very simple to the most complex. Qualtrics can be used to collect and store protected patient and personal data. It is available at no cost to all UCSF faculty, staff and students.

Research Electronic Data Capture (REDCap) [19] (recommended): This tool allows you to rapidly develop databases and online surveys. It is available for use at no cost to the UCSF research community and its collaborators. RedCAP can be used to collect and store protected patient and personal data.

Other Programs: ?If you are using other survey software such as Survey Monkey or other programs, it may first need to undergo a data security review. See the ITS Security Services [14] page.

IP Address Collection: You may wish to collect the IP addresses of survey participants to provide a method of determining whether the user has previously completed the survey. The IRB 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 Qualtrics, 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.

Cloud storage solutions

MyResearch[20],OnCore[20] orUCSF Secure Box[21] are acceptable cloud storage solutions.

Some UCSF faculty and staff use other programs like Dropbox, Google Drive, Salesforce.com, Evernote or Amazon to exchange files with co-workers or collaborators. Using such storage solutions poses a possible liability for official use at UCSF, particularly for research data.

There are potential security risks, export control restrictions and data ownership issues (research data belongs to the UCSF, not the researcher). For example, Dropbox is not automatically HIPAA compliant [22].

If you are considering the storage of any data outside of UCSF, working through IT will help you address the following questions.

- Does the agreement with the vendor stipulate the University owns the data?
- How will the vendor make the data available in the event of a disaster?
- What security controls are in place to prevent the inadvertent or malicious disclosure of the data?
- What happens if a subpoena is issued?
- Does the vendor have Information Security/Cyber Liability insurance?

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.

Mobile apps

Many researchers are purchasing mobile apps or building their own app to interact with study participants. Seek expert IT review [1] at UCSF.

If you are developing a mobile app or other type of digital health innovation, contact the UCSF Office of Innovation, Technology & Alliances [23]. You may also wish to consult with the Center for Digital Health Innovation at UCSF [24], which collaborates with innovators from UCSF and beyond to envision, realize and evaluate digital health technologies.

Even if the participant is asked to download a free app or provided funds 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.

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 University. It is advisable to utilize a secure transmission process even if the data is anonymous, coded or 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. See the IT Networking [25] page.

Email notifications are generally not secure and generally not be used to share or transmit research data. See more information on sending secure email at UCSF [26]. Text messages are stored by the telecommunications provider and therefore are not secure.

Securing paper records

This guidance focuses on methods for securing electronic data, but you must also safeguard paper research records.

- Keep data in a locked file cabinet in a locked office or suite
- Code data and keep the key in a separate and secure location

Consent Forms and Permission to Share Data

Data that will be shared with others requires additional oversight to uphold the privacy of the research participant and the confidentiality of their data. If study data will be shared outside the research team, it is important that you obtain the appropriate consent from study participants.

In the past, many consent documents had language that limited sharing of the data more so than was necessary or intended. It is important to think about future data use and to tailor the consent language and permissions to meet your future data sharing needs.

Some researchers may request permission to share identifiable data, but the majority will be sharing de-identified data. Many sponsors, including federal agencies, require data sharing as a condition of funding, and this must be reflected in the consent document and in the consent process (discussion). This includes the acknowledgement of the data sharing practices and the possible risk of re-identification when applicable. One should never guarantee that de-identified data cannot be relinked and the participant?s identity disclosed. As technology evolves, so does the potential risk of re-identification.

?See the consent form templates [27] and the Consent Form Guidelines and Suggested Wording [28] page for suggested language.

Training

The PI is responsible for ensuring that research data is secure when it is collected, stored, transmitted or shared. All members of the research team should receive appropriate training about securing research data and discuss data security regularly at research team meetings. For example, the research team should understand they need to document their standard practices for protecting research data so that they can provide these details to the IRB, the Privacy Office, IT, etc. if a mobile device is lost or stolen.

The IT Security Awareness and Training [29] program provides programs to educate UCSF faculty, staff and students on the risks associated with using, transmitting, and storing electronic information; how to maintain the confidentiality, integrity, and availability of data; and the roles and responsibilities of each community member in protecting UCSF's data and systems.

National Institute of Health (NIH) Grants

The NIH has specific requirements about ensuring data security when collecting identifiable research data in section 2.3.12 Protecting Sensitive Data and Information in Research [30]. See also Public Policy Requirements and Objectives?Federal Information Security Management Act [31].?

The NIH also instituted the Genomic Data Sharing (GDS) Policy [32] to promote sharing, for research purposes, of large-scale human and non-human genomic data generated from NIH-funded research. The policy requires investigators to incorporate a genomic data sharing plan in the "resource sharing" section of their application. More information is available here [33].

Page last updated:
Apr 14, 2017

Source URL: http://irb.ucsf.edu/electronic-data-security

Links
[1] http://it.ucsf.edu/
[2] http://security.ucsf.edu/EIS/policies_guidelines.html
[3] http://policies.ucsf.edu/policy/650-16
[4] http://it.ucsf.edu/policies/ucsf-minimum-security-standards-electronic-information-resources
[5] http://www.ucop.edu/ucophome/policies/ec/
[6] http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_bill_20071014_chaptered.html
[7] http://irb.ucsf.edu/hipaa
[8] https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[9] http://it.ucsf.edu/security
[10] http://hipaa.ucsf.edu/privacyoffice/
[11] http://irb.ucsf.edu/definitions
[12] http://www.ucop.edu/research-policy-analysis-coordination/policies-guidance/record-retention/index.html
[13] http://it.ucsf.edu/services/category/encryption
[14] https://it.ucsf.edu/services/category/security
[15] http://hub.ucsf.edu/oncore
[16] https://myresearch.ucsf.edu/myresearch
[17] http://tiny.ucsf.edu/securebox
[18] https://it.ucsf.edu/services/qualtrics-web-surveys
[19] https://it.ucsf.edu/services/redcap
[20] http://irb.ucsf.edu/#methods
[21] http://it.ucsf.edu/projects/secure-box-cloud-risk-management-box-ciphercloud
[22] https://www.dropbox.com/help/238/en
[23] https://ita.ucsf.edu/researchers
[24] http://centerfordigitalhealthinnovation.org/
[25] http://it.ucsf.edu/services/category/networking
[26] https://it.ucsf.edu/services/secure-email
[27] http://irb.ucsf.edu/consent-and-assent-form-templates
[28] http://irb.ucsf.edu/consent-form-guidelines-and-suggested-wording
[29] http://it.ucsf.edu/services/category/awareness
[30] http://grants.nih.gov/grants/policy/nihgps_2013/nihgps_ch2.htm#protecting_sensitive_data
[31] http://grants.nih.gov/grants/policy/nihgps_2013/nihgps_ch4.htm#fed_info_security_management_act
[32] http://irb.ucsf.edu/nih-genomic-data-sharing-gds-policy-and-genome-wide-association-studies-gwas
[33] http://grants.nih.gov/grants/guide/notice-files/NOT-OD-14-124.html