HIPAA and Data Storage, Handling, and Destruction

11/30/2016

Why is data storage, handling, and destruction important?

Protect people's privacy and the confidentiality of their data

Ensure compliance with HIPAA and human subjects research regulations

Respond to changing technology and threats to data security

What are PHI and PII (or PI)?

PHI = Protected Health Information

PII = Personally Identifiable Information

PI = Personal Information

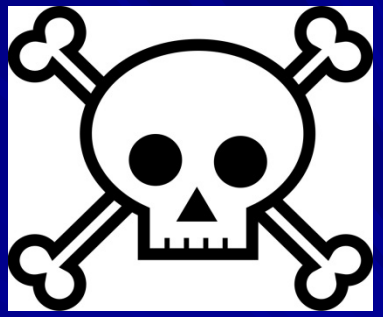
Why are the best ways for investigators to store their research data?

The general recommendation is to use a secure university network drive or REDCap. This covers many (but not all) projects.

Code data sets with a subject ID instead of name, MRN, etc. and store the key separately from the data set

Do NOT use the following for research data with identifiers

- Google docs
- Dropbox
- Sharepoint
- Unencrypted anything
  - Email
  - Laptops
  - USB or other portable devices



What are university network drives or REDCap, and how do investigators get access to them?

http://umassmed.edu/it/how-do-i/get-connected/r-drives/

http://www.umassmed.edu/it/services/research-computing/red-cap/

http://www.umassmed.edu/it/services/research-computing/red-cap/redcap-security-best-practices/

Technology is always changing. Check the IT website frequently for new resources.

Are there any cases where REDCap may not be the best choice for data management?

Screening Logs

Screening logs are better handled as paper or e-docs so that you can more easily delete identifiers for anyone who declines to enroll.

Are there any cloud options for investigators?

REDCap

Technology is always changing. Check the IT website frequently for new resources.

What should investigators consider before sharing data?

- Do I have IRB approval? Did subjects consent?
- Am I violating my HIPAA waiver in which I agreed that I would not redisclose PHI?
- Does my data use agreement/grant/contract have any stipulations on data sharing?
- Am I using a vetted technology that is appropriate to the type of data I want to share?
- Have I consulted with Office of Technology Management for data sharing agreements?
- Are my data appropriately deidentified?

What is deidentification?

All of the identifiers as defined by HIPAA must be removed.

What is a limited data set?

PHI from which certain specified direct identifiers have been removed

Used in conjunction with a data use agreement

How can investigators de-identify data?

- Take only what you need
- Convert identifiers to non-identifiers (DOB → age, MRN & name → Subject ID)
- Paper: Redact, shred, or discard in HIPAA bin
- REDCap: Export fields appropriately marked as non-HIPAA identifiers and then delete the project
- Excel, Word, etc.: Delete the identifiers, or delete the document and empty the trash

How can investigators destroy their research records?

- Paper: Redact, shred, or discard in HIPAA bin
- REDCap: Delete the project
- Excel, Word, etc.: Delete the document and empty the trash; Contact IT for overwrite tools

See *HRP-800 INVESTIGATOR GUIDANCE: Investigator Obligations* for data retention requirements: http://www.umassmed.edu/ccts/irb/investigator-guidance/

HIPAA waiver instructions

4. Describe the plan to protect identifiers from improper use or disclosure. Be sure to indicate where PHI will be stored, who will have access (researchers must list all of the entities that might have access to the study's PHI such as IRB, sponsors, FDA, data safety monitoring boards, and any others given authority by law), and the procedure used to destroy them. (Note that identifiers must be destroyed at the earliest opportunity, unless there is a justification for retaining the identifiers or retention is required by law.)

Let's look again at the samples from the 11/2/16 Basics of HIPAA and Research slides

UMass Memorial Medical Center
HIPAA IRB WAIVER OF AUTHORIZATION***

Principal Investigator:
IRB Study ID #: H
Protocol Title:

Remember to complete the header

---

1. Indicate if you are requesting a waiver of authorization to review electronic/paper medical records just to find potential subjects or to conduct the entire study.

To find potential subjects

2. The HIPAA regulation requires reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. List the PHI to be collected and its source(s).

Sample 1:
Weekly OR schedule: Name, DOB, gender, surgery type, date of surgery

Allscripts/Meditech: Address, phone number

3. Explain why the research could not practicably be conducted without this PHI.

Sample 1:
We are conducting a study of adult men undergoing surgical removal of belly buttons. The inclusion and exclusion criteria depend on age, gender, surgery type, and date of surgery. Name, address, and phone number are required to contact potential subjects.

4. Describe the plan to protect identifiers from improper use or disclosure. Be sure to indicate where PHI will be stored, who will have access (researchers must list all of the entities that might have access to the study's PHI such as IRB, sponsors, FDA, data safety monitoring boards, and any others given authority by law), and the procedure used to destroy them. (Note that identifiers must be destroyed at the earliest opportunity, unless there is a justification for retaining the identifiers or retention is required by law.)

- Where is PHI stored
- Who will have access
- How and when destroyed

4. Describe the plan to protect identifiers from improper use or disclosure. Be sure to indicate where PHI will be stored, who will have access (researchers must list all of the entities that might have access to the study's PHI such as IRB, sponsors, FDA, data safety monitoring boards, and any others given authority by law), and the procedure used to destroy them. (Note that identifiers must be destroyed at the earliest opportunity, unless there is a justification for retaining the identifiers or retention is required by law.)

Sample 1: We will keep an Excel log with the PHI listed in Question 2 in a secure university share drive in a folder dedicated to the research study.

The PI controls access to the folder such that only the study team, Save the Bellybuttons Foundation, and appropriate representatives of UMass Worcester will have access.

…

4. Describe the plan to protect identifiers from improper use or disclosure. Be sure to indicate where PHI will be stored, who will have access (researchers must list all of the entities that might have access to the study's PHI such as IRB, sponsors, FDA, data safety monitoring boards, and any others given authority by law), and the procedure used to destroy them. (Note that identifiers must be destroyed at the earliest opportunity, unless there is a justification for retaining the identifiers or retention is required by law.)

…

If someone declines to enroll, we will record their age, gender, surgery type, and their reason for declining in a separate file so that we can describe the population that was approached. Within one business day of when someone declines, we will delete their information from the screening log except for name and DOB to keep from re-approaching patients who may be rescheduled. Once the study closes to enrollment, we will delete the file that has the identifiers and empty the trash.

5. Explain why the research could not practicably be conducted if you had to obtain permission from the individuals to access their PHI for research purposes.

Because belly button removals are rare, we may miss eligible subjects and be unable to complete the research if we rely on them to self-identify. Prior attempts to recruit with flyers have failed.

Convenience is not an appropriate justification

UMass Memorial Medical Center
HIPAA IRB WAIVER OF AUTHORIZATION***

Principal Investigator:
IRB Study ID #: H
Protocol Title:

Remember to complete the header

---

1. Indicate if you are requesting a waiver of authorization to review electronic/paper medical records just to find potential subjects or to conduct the entire study.

To conduct the entire study

2. The HIPAA regulation requires reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request. List the PHI to be collected and its source(s).

Sample 2:
Clinical Data Portal*: MRN, DOB, date of myocardial infarction, STEMI or Non-STEMI, date of admission, date of discharge, LV ejection fraction, medications at time of MI…

*http://www.umassmed.edu/it/cdp/

3. Explain why the research could not practicably be conducted without this PHI.

Sample 2:
We are conducting a retrospective chart review of the relationship between prior medication (recorded as meds at time of MI) and MI severity using adult patients seen prior to January 1, 2016. We require MRN, DOB, and date of MI to identify unique adult patients prior to 1/1/16. We require type of MI, length of stay, and LV ejection fraction as measures of severity…

4. Describe the plan to protect identifiers from improper use or disclosure. Be sure to indicate where PHI will be stored, who will have access (researchers must list all of the entities that might have access to the study's PHI such as IRB, sponsors, FDA, data safety monitoring boards, and any others given authority by law), and the procedure used to destroy them. (Note that identifiers must be destroyed at the earliest opportunity, unless there is a justification for retaining the identifiers or retention is required by law.)

- Where is PHI stored
- Who will have access
- How and when destroyed

4. Describe the plan to protect identifiers from improper use or disclosure. Be sure to indicate where PHI will be stored, who will have access (researchers must list all of the entities that might have access to the study's PHI such as IRB, sponsors, FDA, data safety monitoring boards, and any others given authority by law), and the procedure used to destroy them. (Note that identifiers must be destroyed at the earliest opportunity, unless there is a justification for retaining the identifiers or retention is required by law.)

Sample 2: All data will be recorded in REDCap, and Name, MRN, DOB, and all other dates will be marked as identifiers. DOB will also be recorded as age. Admission and discharge dates will also be recorded as length of stay.

The PI controls access to REDCap such that only the study team, NIH, and appropriate representatives of UMass Worcester will have access.

…

4. Describe the plan to protect identifiers from improper use or disclosure. Be sure to indicate where PHI will be stored, who will have access (researchers must list all of the entities that might have access to the study's PHI such as IRB, sponsors, FDA, data safety monitoring boards, and any others given authority by law), and the procedure used to destroy them. (Note that identifiers must be destroyed at the earliest opportunity, unless there is a justification for retaining the identifiers or retention is required by law.)

…

Once data cleaning is complete, a data set that excludes all HIPAA identifiers will be exported and the project deleted from REDCap.

5. Explain why the research could not practicably be conducted if you had to obtain permission from the individuals to access their PHI for research purposes.

Sample 2: The research requires a large sample size extending back several years. Subjects may have moved or died, and contact information will be incomplete.

Convenience is not an appropriate justification

Is there any homework for investigators?

Make sure all HIPAA identifiers are flagged as identifiers in REDCap projects

Check to make sure your laptops are encrypted: http://www.umassmed.edu/it/security/Encryption/

Check who has access to research files, restrict access accordingly, and set a date to check again

Get rid of identifiers (other than signed consents and authorizations) that are no longer needed

Is there any homework for investigators?

Check for updated information – policies, procedures, technology change

Ask for help: IT, IRB, Privacy Office, Office of Technology Management