HARVARD CATALYST | THE HARVARD CLINICAL AND TRANSLATIONAL SCIENCE CENTER

IMPORTANT IT CONSIDERATIONS FOR IRB MEMBERS

By the Emerging Technologies, Ethics, and Research Data Subcommittee of Harvard Catalyst's Regulatory Foundations, Ethics, and Law Program

The use of technologically interconnected products and services continues to revolutionize the design and conduct of research. These emerging technologies and digital innovations raise important legal, regulatory, and ethical questions for researchers and institutional review boards (IRB) alike. Among them:

- Do IRBs understand how information is collected, used, and stored in sufficient detail to protect human research subjects?
- How does the IRB confirm that uses of technology conform to promises or assurances made during the informed consent process?

IRBs need not be IT experts to fully understand how new technologies work, however an awareness of potential risks posed by new technologies may be helpful. The IRB is also responsible for applying the regulatory criteria for approval, which includes confirmation that the research plan makes adequate provision for monitoring the data to ensure the safety of subjects, as well as adequate provisions to maintain the confidentiality of data. Providing IRB members with Information Technology (IT) considerations is one way to facilitate review and deepen IRB member comprehension.

Below is a list of questions for IRB members to consider when thinking about IT and/or data confidentiality protections, and concurrently evaluating the regulatory criteria for approval. This list is not exhaustive, but provides a baseline of questions to consider when evaluating the potential risks of the technology being utilized in the research.

1. Is the research data identifiable, coded, de-identified, or anonymous? What are the differences? Does identifiability impact the level of protection needed?

What the IRB Says	What the IRB Means
Anonymous	Participant data and/or specimens that were obtained and stored without any identification that may link to a specific individual. Anonymous samples may have population information (e.g., the samples may come from patients with diabetes).
De-identified	Participant data and/or specimens that may have been acquired from identified humans subjects, but all identifiers or codes have been removed and destroyed, or the investigator has written confirmation from the provider that they will not have access to the code/key.
Coded	Participant data and/or specimens are labeled with a code (e.g., a number), rather than a person's name or other personal identifier. Such a code can be traced or linked back to the participant by someone, who usually keeps the key to the code. As long as a link exists, data are considered indirectly identifiable and therefore, not anonymized or de-identified.

Identifiable	Participant data and/or specimens are directly identified with participant name or other personal identifier (e.g., phone number, SSN, Address, email address, etc.) - i.e., the identity of the participant is or may readily be ascertained by the investigator or associated with the information.

2. What is the data storage medium?

3. Will data storage be on personal vs. professional devices (i.e. home PC vs. work PC)?

4. Will data be stored on non-password protected and/or unencrypted device (laptop, smart phones, etc)?

5. What are the physical, technical, and administrative safeguards put in place to protect the data? Are they sufficient?

Physical Safeguards	Technical Safeguards	Administrative Safeguards
Everything from locked doors to guard dogs.	Include a broad spectrum of measures, such as device data encryption (which is unlocked with strong passwords), anti-malware software, and encrypted communications.	Can be summarized as "the rules," such as policies about who is granted access to what types of data. It also includes rules like "use a strong password" and "do not share it."

6. How does data confidentiality fit into the study's data safety and monitoring plan? How should such monitoring be conducted throughout the lifecycle of the research to ensure the safety of subjects, as well as the integrity and confidentiality of data?

    - When reviewing a data management plan consider: any contracts or agreements that may be needed, documentation, storage and back-up, sharing and reuse, and retention and disposal.

7. What data use agreements or memorandums of understanding should be in place between researcher collaborators before data is shared?

8. How will the researcher ensure the participant understands and acknowledges what will happen to information about them during the course of the study? What needs to be disclosed to the participant in the consent form? What should the participant be told about future uses of their data?

9. What research data is considered HIPAA-protected data? Are their special considerations for Protected Health Information?

- HIPAA Identifiers:
  Names, Geographic subdivisions smaller than a state, Elements of dates (except year) directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89, Telephone numbers, Fax numbers, Email addresses, Medical record numbers, Health plan beneficiary numbers, Account numbers, Certificate/license numbers, Vehicle identifiers and serial numbers, Device identifiers and serial numbers, Web Universal Resource Locators (URLs), Internet Protocol (IP) address numbers, Biometric identifiers, including finger and voice prints, Full face photographic images or any comparable images, & Any other unique identifying number, characteristic, or code

10. Who on the study staff has access to the research data? What is their role on the study and what kind of access do they have?

11. If the study utilizes secondary data, what is the source of those data sets?

12. If one or more data set is being used, how could linking this data impact identifiability and risk to participants?

13. How can researchers secure information about subjects in a way that maintains confidentiality and minimizes breaches/inadvertent disclosure?

    Some examples to look for:
    - Do not share research data without permission from the participant.
    - Develop a plan to protect the data throughout the life of the entire study (starting with identification of subjects and ending with the appropriate destruction of data once the study has concluded).
    - Clearly describe confidentiality risks in the consent form.
    - Maintain research data with a code or de-identify entirely.
    - Limit access to research data to only those individuals on the IRB-approved study personnel roster.

14. What has been promised/explained to participants in the consent form regarding data confidentiality, protection, and security? Is it complete? Is it feasible?

15. What are the participant's expectations of privacy during the course of the study? What is the participant sharing about themselves that has been disclosed and entrusted to the researchers?

16. Is a Certificate of Confidentiality appropriate for the study? A Certificate of Confidentiality enables researchers to refuse to disclose identifying information on individual participants in civil, criminal, administrative, legislative, or other proceedings at the federal, state, or local level.

17. How do the researchers describe what will occur if a data breach, theft, loss, or other reportable event occurs? Does this reporting plan adhere to IRB policies? Is it timely? Is it sufficient?

Resources and References

1. Resources:
   - Catalyst Investigator's Guide to Research Data Management Practices
   - Harvard Catalyst Data Privacy And Security Planning Checklist
   - Harvard Catalyst Emerging Technologies, Ethics, and Research Data Committee Watch Words List

2. Further Training:
   - CITI Information Privacy and Security Training Module: https://about.citiprogram.org/en/series/information-privacy-and-security-ips/

3. Articles:
   - Variety of strategies needed to educate IRB members & chairs: https://www.ahcmedia.com/articles/136322-variety-of-strategies-needed-to-educate-irb-members-chairs

4. PRIM&R
   - https://www.primr.org

5. Updates to the Common Rule:
   - https://www.hhs.gov/ohrp/regulations-and-policy/regulations/finalized-revisions-common-rule/index.html