AN EMERGING TECHNOLOGIES, ETHICS, AND RESEARCH DATA CASE STUDY

ACCIDENTAL RECEIPT OF IDENTIFIABLE DATA

By: Kimberley J. Serpico

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

OVERVIEW

The Emerging Technologies, Ethics, and Research Data case studies provide education and guidance on how to identify, assess, and review research data security issues. These studies may be used by IRB administrators and investigators to identify key issues, considerations, and decision criteria when reviewing and designing research studies that involve data collection and sharing components.

Case studies follow a standard format that includes: 1) a fact pattern, 2) contractual, regulatory, ethical, and technical issues, 3) stakeholder considerations to identify, assess, and mitigate risks, and 4) resolution and points for discussion.

By identifying common themes, linking them directly to federal regulations and guidance, and outlining options, the case studies can be used in a variety of ways, which include: 1) as an educational tool for training individuals in human subjects research, 2) as a basis for developing reviewer checklists/worksheets, and 3) as a tool in designing research projects.

We encourage you to reproduce and use these materials freely. In doing so, we require that you acknowledge Harvard Catalyst as the publisher and that you give appropriate credit to the individual authors. For additional information, visit http://catalyst.harvard.edu/about/citingsupport.html.

CASE STUDY

Scenario/Fact pattern:
Researchers at a local university have received an IRB determination to conduct Exempt human subjects research on a secondary data set from a local hospital. The aims of the research are to study the successful pregnancies of women who have had a past miscarriage. The hospital will send the researchers a data set including the patient’s marital status, pregnancy history, miscarriage history, blood test results, immunization records, and list of medical conditions such as depression, eating disorders, cancer, STDs, and other reproductive health issues. The hospital enters into a data use agreement (DUA) with the researchers, outlining the contractual terms and conditions of the use of the data. The DUA is clear that no identifiable data about
patients will be included in the data set and that the researchers should make no attempt to try and identify patients with the information included in the data set.

Once the researchers obtain their IRB determination, they send it to the data provider. The data provider then, in turn, sends the researchers the data set via email. The following week when the researchers download the data set and begin their work, they notice the data set includes identifiers such as a medical record number, patient name, and patient date of birth. They immediately notify the IRB that the data set they received includes identifiers and was not sent via secure file transfer. They ask the IRB what they should do next. What should the IRB advise?

CONSIDERATIONS

Regulatory and Contractual Considerations:

- How has the hospital/data provider violated the data use agreement?
- Who is responsible for reporting a violation of the DUA terms - the researcher or the data provider, or both?
- Does the DUA require the data provider be notified if a breach occurs?
- What are the repercussions of violating the data use agreement from a regulatory and contractual standpoint?
- Do the researcher and the provider understand the full scope of the HIPAA Privacy Rule? (e.g. all categories of protected health information (PHI), the definition of “de-identified”, etc.)
- Because the information breached is PHI, are there applicable state law reporting requirements under HIPAA in this scenario?

Researcher Considerations:

- Has the data provider been informed that the data set that was sent included identifiers?
- Can the identifiable data set be reliably and securely destroyed?
- What research activities (e.g. data analysis) have been conducted on the identifiable data set, if any?
- Could the receipt or inadvertent use of an identifiable data set impact the scientific integrity of the study?

IRB Considerations:

- Did the researchers submit a complete report of this non-compliance to the IRB?
- Were any research activities (e.g. data analysis) conducted on the identifiable data set?
- Has the IRB received and reviewed a copy of any DUAs associated with the study?
• Does the violation of the DUA add or increase risk to participants? Was this violation expected or unexpected? Was it related to the research or not related to the research?
• Does the receipt or inadvertent use of an identifiable data set impact the regulatory criteria for approval with respect to adequate provisions in place to protect the privacy of subjects and/or to maintain the confidentiality of the data?
• Do the researchers have a plan outlined in the research protocol to make adequate provisions for monitoring the data collected to ensure the safety of subjects?
• How may the receipt or inadvertent use of an identifiable data set impact the HIPAA regulations that may or may not be in place for the study?
• Does this violation require a change to the research protocol or research activities?
• Does the study need to be suspended or terminated as a result of this violation?
• Should there be a required corrective action plan? If so, what are the next steps the researchers must take and what should they do to ensure the event does not occur again? Who are the appropriate parties involved that should be informed of the breach?
• Before this study was initially approved, did the researcher and IRB give appropriate consideration to the spectrum of non-compliance that might occur on this study? Was this event one that was considered? Why or why not? At the outset the researchers provide a sufficient plan to minimize all possible risks posed by the research?

IT Considerations:
• Can the email with the identifiable data set be securely destroyed?
• Does the hospital/data provider have a secure file transfer system?
• Do data security protections in place for the study need to be revisited or changed?

RESOLUTION & DISCUSSIONS:

It is required that all researchers report events to the IRB that deviate from what is written in their IRB-approved protocol. The specific policies may vary by institution, but reporting is always required. Even though the inadvertent disclosure of the identifiable data set was not the result of any negligence or wrongdoing on the part of the researchers, it still must be reported to the IRB because they did not have approval to receive or use it. When non-compliance or adverse events are reported, it is the IRB’s responsibility to review and determine whether the event was an unanticipated problem, serious non-compliance, and/or continuing non-compliance. In their review, the IRB should consider whether risks to subjects are still minimized and reasonable in relation to the anticipated benefits, if any, to the subjects and the importance of the knowledge that may reasonably be expected to result.

Because research can involve risks to subjects that are unforeseeable, the IRB must ensure, if appropriate, that the research includes adequate provisions for monitoring the data collected to ensure the safety of subjects. OHRP notes that adequate monitoring provisions for research, if deemed appropriate by the IRB, might include one or more of the following elements, among others:
1. The type of data or events that are to be captured under the monitoring provisions.
2. The entity responsible for monitoring the data collected, including data related to unanticipated problems and adverse events, and their respective roles (e.g., the investigators, the research sponsor, a coordinating or statistical center, an independent medical monitor, a DSMB/DMC, and/or some other entity). (OHRP notes that the IRB has authority to observe or have a third party observe the research (45 CFR 46.109(e).)
3. The time frames for reporting adverse events and unanticipated problems to the monitoring entity.
4. The frequency of assessments of data or events captured by the monitoring provisions.
5. Definition of specific triggers or stopping rules that will dictate when some action is required.
6. As appropriate, procedures for communicating to the IRB(s), the study sponsor, the investigator(s), and other appropriate officials the outcome of the reviews by the monitoring entity.

REFERENCES:


NIH HIPAA Privacy Rule - https://privacyruleandresearch.nih.gov/