A DATA PROTECTION CASE STUDY OF DATA SHARING INVOLVING A RESEARCH DATA LOSS INCIDENT

RESEARCH DATA LOSS INCIDENT – MULTI-STAKEHOLDERS

By: Lisa Griffin, JD, MPH, Heather Shea, JD

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

OVERVIEW

The Data Protection 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, and 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 education 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 each author. For additional information, visit http://catalyst.harvard.edu/about/citingsupport.html.

CASE STUDY

SCENARIO/FACT PATTERN:

A medical resident at West Coast Medical Center comes to do a six-month “research rotation” at East Coast Medical Center. The resident works on an NIH-funded clinical research study at East Coast Medical Center where use of protected health information has been authorized by the patient. The ambitious resident would also like to keep working on his study from West Coast Medical Center, which includes a database created under a waiver of informed consent.

The resident stores both data sets on his laptop, which he can take between the two institutions. Both data sets contain fully identifiable information on the 125 research subjects from East Coast Medical Center and 510 subjects from West Coast Medical Center. The resident owns the laptop, but he does back up the hard drive on the East Coast Medical Center network, just in case he loses his computer.

In July the resident decides to take a much-needed vacation, leaving his laptop in his East Coast Medical Center Office. Unfortunately, several offices are burglarized during the resident’s vacation and the computer goes missing. The theft is initially reported to security by the affected department. When asked, the resident swears that he has encrypted his computer.
REGULATORY, ETHICAL, & TECHNICAL ISSUES:

• Is this reportable to NIH? If yes, what should be reported?
• What other reporting requirements should be considered (e.g., state law)?
• What follow-up actions should be considered, such as mitigating measures, corrective action, and/or disciplinary action?

CONSIDERATIONS:

Contractual Considerations
• What agreements were entered into, if any, to share the data outside of the institutions?
• Did the agreement delineate the researchers’ responsibility with respect to the data set?

Researcher Considerations
• What is the researcher’s responsibility with respect to the data set?
• Is this an unanticipated problem that requires reporting to the IRB? Which IRB?
• Is there anyone else at the institution who should be notified?

IRB Considerations:
• If you are the chair of the West Coast medical center’s IRB, how do you approach the question of notifying participants?
  o Do you coordinate with your medical center’s privacy office (and another privacy office, such as the new hospital’s)?
  o How do you handle the waiver aspect, i.e., that individuals are not aware they were in a study?
• Is this an unanticipated problem that requires reporting to OHRP?

IT Considerations
• Does the institution have a policy for how to manage data security when it pertains to personally owned devices?
• How does the institution identify situations where data sharing may occur?

Privacy Officer Considerations
• Is this a reportable breach under HITECH? Is the resident’s attestation that he encrypted his laptop enough to trigger the safe harbor provision for “secured” PHI?
• If reportable under HITECH, how does the number of subject data exposed impact the reporting requirements (e.g., media notice and/or prominent posting on website)?
• Is it the type of data that credit monitoring would be beneficial to the subject?
• If reportable, which institution will contact the subjects and develop potential questions and answers to be prepared for inquiries?
• Are there any state reporting requirements for the Personally Identifiable Information (e.g. first name coupled with SSN or other information that could be used for financial benefit)?
• Whose PHI is affected? What state or country is the individual a resident of? Who has a reporting obligation, and to whom?

RESOLUTION & DISCUSSIONS:

Process to identify, assess, and mitigate risks:
Today’s research environment encourages multi-disciplinary and multi-institution collaboration. Research teams are highly mobile and facile with technology to support their research activities. Institutions must be responsive to this new environment by prospectively identifying situations where data sharing is likely to occur and developing tools to allow data to be accessed and shared in a secure manner:

- When staff are leaving the institution or taking a sabbatical or leave, specifically ask about the plan for data created at the institution, where it will be stored, who will have access to it, and whether the investigator will take a copy?

- When staff are coming on board, especially if they are transferring from another institution or joining for the short-term, such as with a residency or research rotation, evaluate the plan to migrate data from another institution.

- Provide tools for investigators to store data in a secure, central location that can be accessed from outside the institution, eliminating the need for storage on mobile devices.

By initiating conversations with staff around data security as they move between research centers and engage in collaborative activities, institutions can better mitigate the risks in this environment and steer staff toward the tools and best practices that will keep their research data secure.

REFERENCES:

Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 C.F.R. Parts 160, 162, and 164
http://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules” (Omnibus Rule), 78 Fed. Reg. 5566 (Jan. 25, 2013).

201 CMR 17.00: Standards for the Protection of Personal Information of Residents of the Commonwealth
www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

APPENDIX:
Please see Appendix A, a Template on Incident Investigation Plan