A DATA PROTECTION CASE STUDY OF DATA SHARING INVOLVING MULTIPLE INSTITUTIONS

A STUDY INVOLVING MULTIPLE INSTITUTIONS, A COMPANY, AND CMS DATA

By Joe Zurba, Kris Bolt, and Sabune Winkler, 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, 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 give appropriate credit to each author. For additional information, visit http://catalyst.harvard.edu/about/citingsupport.html.

CASE STUDY

SCENARIO/FACT PATTERN:

Researchers at a local hospital submit a proposal to Centers for Medicare and Medicaid Services (CMS) to obtain a data set is using Medicare and Medicaid identifiable data. The hospital researchers are not skilled in using CMS databases so they partner with an epidemiologist at the local school of public health who routinely does CMS analysis. However, the researchers find themselves in a challenging situation when presented with the standard CMS Data Use Agreement (CMS DUA). While the researchers have experience with the standard hospital DUAs, the researchers are unfamiliar with the CMS DUA process.

In team meetings with the epidemiologist, the researchers learn that they are required by CMS to comply with the National Institute of Standards and Technology (NIST) and Federal Information Security...
Management Act (FISMA). Additionally, they learn that they need to submit a Data Management Plan (DMP) for review by a third party auditor prior to the approval of the data request application.

Concerned about achieving compliance with terms of the CMS DUA, the researchers contact a local compliance consulting company as the third party auditor. The company specializes in distilling the requirements of the DUA down to actionable items and the services include a checklist for the researchers to follow in order to achieve compliance.

After consulting with the company, the researchers decide to hire them. They contact the hospital contracts office to (1) enter into a contract with the consulting company; (2) to review the CMS DUA; and (3) to find out if a contract is needed to share the data among the hospital researchers and the local school of public health epidemiologist.

The hospital’s contracts office refers the researchers to other offices and officials in the hospital. First, the contracts office refers them to the institution’s Research Information Security Officer (RISO) to review the IT and security portions of the CMS DUA. The RISO tells the researchers that among the requirements of the DUA are requirements for secure file storage and data security training. The RISO recommends the hospital’s secure file share be used and that the study staff complete NIH data security training. The epidemiologist is given access to the hospital’s secure file area via VPN connection. Second, the contracts office refers the researcher to the hospital’s Privacy Officer for help with the CMS DUA. The hospital’s contracts officer signs the CMS DUA and submits the DMP to CMS. And, third, the contracts office refers the researcher to the IRB to submit an IRB application. Study staff from the School of Public Health are listed on the protocol. The hospital’s IRB approved the protocol.

CONSIDERATIONS:

Regulatory and Contractual Considerations

- What are CMS requirements? How can one find out more information about these requirements?
- What contracts are needed in the first place? How can you determine if a DUA is needed?
- What office/who at your institution is responsible for negotiation the DUA? Is it a template form?
- Who can sign data use agreements at your institution? What is the process for ensuring that researchers are not signing their own DUAs?
- Do you need IRB approval in order to sign a DUA?
- Who monitors compliance with the DUA requirements established in the contract?
- How are reporting requirements met when multiple institutions are involved? Must all parties receiving the data each sign an agreement? Or can the reporting requirements be flowed down through subcontract?
- As required by CMS, how will compliance with the National Institute of Standards and Technology (NIST) and Federal Information Security Management Act (FISMA) be monitored, measured, and reported?
- How will the FISMA level of the data be assessed and by whom?
- A DMP must describe a number of processes such as: on-boarding and off-boarding procedures for study personnel; notification mechanisms and timelines; data procedures such as access, documentation, tracking, storage and back-up. The DMP must also include specific plans for data sharing, retention, and disposal. How can the institution obtaining the data ensure members of another institution will adhere to the DUA and DMP?

Researcher Considerations

- What procedures are in place to help the researchers know parties involved (e.g. contracts office, IT, IRB, general counsel, etc.) in the drafting of the contracts, DUA and DMP, etc.?
- What is the researcher’s responsibility with respect to the data set?
• What is the researcher’s responsibility for managing compliance with the contract?
• Can the researcher sign the DUA?

IRB Considerations:
• Is IRB review even required for receipt of this data? Do we know if CMS data is identifiable?
• Does the need for IRB review hinge on the identifiable data? The DUA requirement?
• What is the timing of IRB approval? Does the IRB require that the DUA be signed before protocol approval?
• Because there are multiple institutions, are multiple IRB approvals required? Can IRB reliance be utilized?
• If needed, how does the IRB review and approve for the corporate entity?

IT considerations
• Why does the RISO recommend use of the hospital’s secure file share and that the study staff complete NIH data security training?
• What tools or technologies can be leveraged to enable collaboration through secure sharing and help ensure compliance?
• In this case, does the institution have dedicated infrastructure for researchers to use that is compliant with FISMA and other NIST standards?
• Do training materials encompass institutional requirements as well as CMS requirements? Are these materials easily accessible? Is completion tracked or monitored?
• How is it determined that secure sharing is needed?
• What tools are available for researchers that have been approved for secure sharing?
• Does the institution have a process to assess the security of external collaborators and institutions? Does this process integrate with the IRB? Does it need to be integrated?
• Is it ok that the epidemiologist is given VPN access prior to IRB approval?

RESOLUTION & DISCUSSIONS:

Process to identify, assess and mitigate risks:
• In many institutions, the DUA process begins with a contracts office but it could also be a compliance officer or the grants office. Find out whether your institution has a process for reviewing and signing DUAs.
• A request for a DMP to accompany the DUA may be best met by reaching out to:
  o Information Security for advise and documented best practices for data hygiene,
  o The IRB or General Counsel for official language on breach notification procedures,
  o The hiring manager or local admin to set up a formal on-boarding and off-boarding notification timeline,
  o The local IT person to discuss a formal process for granting/removing data access to restricted files.
• Risks may be evaluated by different groups within an organization such as:
  o A research contracts office that may review the terms of the DUA for any contractual risks, and identifies other groups who may need to be consulted
    ▪ Some contractual risks could include: publication restrictions, IP restrictions, unacceptable review times, etc.
  o An Institutional Review Board that will assess the risk of identifiable human subject information and its necessity to the research project
    ▪ The work may be able to be completed with unrestricted data; however, the use of unrestricted data may pose a higher risk of unintentional re-identification, etc.
  o An office of the general counsel that may provide additional review for legal risk and/or contractual risk

Visit: http://catalyst.harvard.edu/programs/regulatory/data-protection.html
Email: regulatory@catalyst.harvard.edu

A Company and CMS Data
V1 January 2016
- Data breach ramifications contained in contracts may be too disproportionate or intensive; the risk to the researcher and/or institution may be prohibitive
  - An information security and privacy office that may provide additional review for security risks
  - Technological tools may be available to help mitigate risk. Dedicated IT time may be needed for some security requirements such as logging, tracking, vulnerability scans, etc.
- The use of data sets that contain identified or identifiable information about human must be reviewed by the IRB, including when users seek to merge public use data files or enhance a public use data file with identifiable or potentially identifiable data.
- Because there are two different institutions involved, and if IRB review is needed, IRB reliance may be of use to reduce the number of duplicative reviews. When there is reliance, additional questions for considerations may include:
  - How will the relying institution be assured of data security measures? Will the researchers only have access to the data they have been approved for? This could be annotated in ancillary review space, in the cede letter, etc.
  - How will the approving institution be assured of the relying institution’s adherence to data access security requirements (no sharing of passwords, no downloading etc.)? Is there language in the PI attestation that good basic computer etiquette will be followed?

REFERENCES:

CMS Data Use Agreement:
https://www.cms.gov/Medicare/Medicare-Fee-for-Service-Payment/sharedsavingsprogram/Downloads/Data-Use-Agreement.pdf

FISMA:

NIST:
http://www.nist.gov/

NIH Data Sharing Guidance:

Texas A&M Guidance on Public Use Data Sets