THE HARVARD CLINICAL AND TRANSLATIONAL SCIENCE CENTER

A DATA PROTECTION CASE STUDY OF DATA MANAGING DATA SECURITY

MANAGING DATA SECURITY WITH LOCAL AND INTERNATIONAL PARTNERS

By: Ken Carson, 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.

CASE STUDY

SCENARIO/FACT PATTERN:

A researcher at a local university's economics department is conducting a study of consumer decision-making about health insurance prescription benefits. The researcher is also affiliated with a neighboring, wholly independent, social science research center, where other research team members (postdocs) are based, and a co-PI at University of Oxford is also an affiliate of the social science research center.

The research data consists of: 1) Third-party dataset of prescription fulfillment information, which is being obtained under a data use agreement (DUA). 2) Experimental data collected by the researcher from a website hosted by the university. The website presents online participants with distinct messages and options, which are specifically designed to motivate prescription refilling and to measure the impact of co-

pays on refill behavior. Participants who wish to enter a raffle for an iPad must provide their email addresses. The email addresses are not linked to participant responses.

The research team stores project data on the social science research center's computer network. No high-risk confidential information is being gathered.

The project is funded by a grant awarded to the university. There is a sub-award to Oxford, where the co-PI recruits British consumers to participate as subjects through the project website, to compare behavior of consumers in a nationalized health care environment.

The project is being reviewed by the IRBs of both the university and the social science research center. The third-party data provider insists that the DUA be executed by the university. The university IRB typically works with the university's IT security office to ensure that data security plans satisfy human subject protection requirements. The university office of sponsored programs (OSP) similarly relies on the IT security office when DUAs have data security requirements.

CONTRACTUAL, REGULATORY, ETHICAL, AND TECHNICAL ISSUES:

The university and the center must coordinate operational, oversight, and compliance obligations. In this case, primary IT operational responsibility is at the social science research center, except for the university's hosting of the experiment website.

The recruitment of British subjects to the university-hosted website also raises several questions:

- Does the project raise European privacy considerations?
- Is it the university or the center (where the experiment data are stored), that should determine if there is an EU privacy obligation?
- If such an obligation exists, which institution should manage the issue?

CONSIDERATIONS:

Contractual Considerations
The principal sources of contractual obligation and liability that should concern the university are:

- The DUA with the third-party data provider
- The terms and conditions of the award and sub-award

Both the DUA and the award terms may have provisions that directly or indirectly commit the researchers to handling data with specified levels of security measures.

An additional 'contractual' consideration would be an agreement that is likely to be noticeably absent: a formal understanding between the university and the center about respective roles and responsibilities regarding data management and security. For example:

- The DUA will require that the dataset be returned or destroyed at the completion of the project. Because the DUA is executed by the university, it will be the university's responsibility to affirm to the provider that no copies are kept. However, the university will be relying on the center to delete the files.
- The DUA will also require that all research team members be informed of and agree to data use restrictions and security requirements. However, while the office of sponsored programs (OSP)

signs the DUA for the university, OSP has no ready means of ensuring that members of the research team located in the university's economics department, at the center, or at Oxford are so informed and committed.

Researcher Considerations:
In this case, data management poses several challenges, including:

- Compiling the ongoing generation of responses on the study website.
- Transferring the experimental data to the center where the third-party datasets are stored.
- Developing a plan to prevent copies of data from migrating away from the center on laptops, when research team members have dual affiliations (i.e., at the center and the university).

Team members may not give much thought to the question of where data may reside, and may assume that university department servers are appropriate, without informing the university's IT department that this data will live on their servers.

IRB Considerations:
The IRB review will focus on the online website and the experience of participants there, from recruitment through consent, to completion of online tasks.

- The IRB should question the researcher about the third-party dataset to ensure it is truly de-identified.
- The IRB will have to decide if the notion of "local considerations" holds for this particular online study, which would mean, in turn, that a British ethics committee should be consulted.
- The IRB will have to consider the affiliations and roles of team members, specifically those who work at the center, and the responsibilities of the Oxford co-PI.

IT considerations:
The university IT department should be informed about the project when the researcher is setting up the online experiment. Because no high-risk confidential information is being gathered and participant email addresses are not linked to participation data, the university's data security concerns will focus more on protecting the university network than on protecting the data of online participants.

OSP, the researcher, or the IRB may ask the university's IT department to provide an opinion on the adequacy of security measures at the center. However, because they do not have control over (or firsthand knowledge of) the dataset maintained at the center, university IT will be justifiably reluctant to offer any judgment.

RESOLUTION & DISCUSSIONS:

To manage the problem of having contractual responsibility for a third-party dataset maintained at the center, the OSP may consider negotiating an indemnity agreement with the center. However, this can a burdensome and difficult process.

Instead, university IT may give the center a vendor assessment questionnaire or checklist as a condition for allowing the center to transmit research data to the university IT environment. A vendor assessment will provide a framework for communicating with the IT group at the center in order to confirm that the DUA security requirements (and the IRB's) will be met.

To minimize the risk that copies of the third-party dataset would be removed from the center, the researcher may be asked to (1) maintain a roster of research team members who require access the dataset, and (2) ensure that those team members acknowledge they have received and read a data security procedures protocol for the project. Remote, secure access to the dataset may then be provided for those team members, reducing the incentive for them to make copies and remove them from the premises.

Process for identifying, assessing, and mitigating risks:

- The university OSP should review the DUA to determine which data security frameworks might apply to the third-party data set, if any.
- OSP should review the DUA for terms and conditions, including applicable data security framework.
- Terms and conditions of the DUA may be negotiated to include or exclude certain data security standards.
- The IRB should determine which identifiers are in the prescription fulfillment information.
- IRB will establish the data security level.
- OSP should work with university IT and legal offices to determine if the EU ePrivacy Directive (2002/58EC) applies. If so, then EU-US Safe Harbor protections must be implemented unless Oxford de-identifies the information in a manner that establishes that the data is exempt from the EU directive. If such de-identification occurred, it would be a best practice for Oxford to certify that de-identification was sufficient to qualify for EU Directive exemption, with the result being that Safe Harbor implementation would not be required.
- IT should work with researchers and compliance staff to establish the appropriate set of administrative, technical, and physical safeguards and systems to identify and mitigate risks on an ongoing basis (i.e. monitoring of audit logs, patch management of external threats, etc.).

REFERENCES:

The Harvard Catalyst Regulatory Foundation, Ethics, and Law Programs Data Protection Subcommittee Website
http://catalyst.harvard.edu/programs/regulatory/data-protection.html

Directive 2002/58/EC of the European Parliament and of the Council
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML