Great Efficiencies or More Risk? Changes to the Common Rule Pose Increased Data Privacy and Security Risks

Presented by:

Holly B. Benton, JD, CHPC
Privacy Risk, Duke University

Marti Arvin, JD, CHC-F, CCEP-F, CHRC, CHPC
Executive Advisor, CynergisTek, Inc.

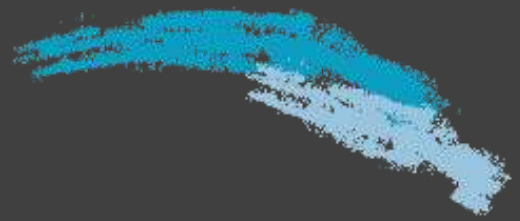
CYNERGISTEK

Duke | OFFICE of AUDIT, RISK & COMPLIANCE

Today's Agenda

1. Revisions to the Common Rule
2. Privacy Implications
3. Case Studies
4. Questions

Revisions to the Common Rule



Relevant changes to the Common Rule

- Changes to the Federal Wide Assurance
- Provisions for broad consent
- Changed and new exempt categories

Changes to the FWA

- Before the revised rule institutions could elect to have all studies covered by their FWA
- Post 1/21/19 this is no longer an option
- Non-exempt non-federally funded research thus is not covered by the Common Rule requirements

Changes to the FWA

- Without IRB oversight, who will assure protection of human subjects?
- It is technically easier to not require IRB review of these studies
- Increased concern regarding the lack of protections

Changes to the FWA

- Treating non-federally funded, non-exempt research by different rules
- Are there state law provisions that make IRB oversight a requirement?
- How would research be tracked if there was a decision that IRB oversight is not required?

Provisions for broad consent

- One time consent
- Permits the storage, maintenance and secondary research of identifiable information or biospecimen.
  - No additional consent required if future research is within the scope of broad consent
- If subject refused broad consent, IRB cannot later waive informed consent

Mandatory elements of broad consent

- General description of types of research
- Description of types of identifiable information or biospecimens that might be used for research
- Whether data or specimens might occur
- Who might conduct research with the data or specimens
- Time frame for storage and maintenance of data or biospecimens (this can be indefinite)

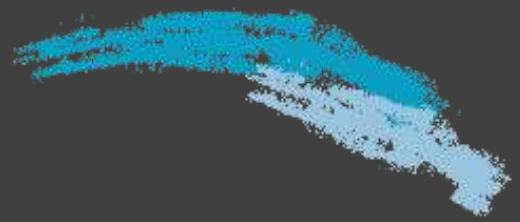
Mandatory elements of broad consent

- Description of any benefits to subject
- Description of how subject confidentiality will be maintained
- Statement that participation is voluntary and there are not adverse consequences of not participating or withdrawing
- Statement regarding possible commercial profits & subject's right to share (if applicable)
- Statement regarding know or anticipated whole genome sequencing

Changed and new exempt categories

- Revises certain existing categories
- Creates new categories of exempt research
  - Use of broad consent
  - Limited IRB review

Privacy Implications



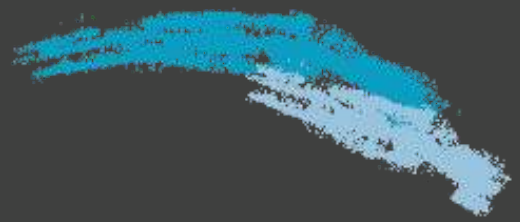
Common Rule Changes - FWA issues

- If the IRB does not need to see the study for Common Rule purposes, what about HIPAA waivers?
  - —Will the study still come to the IRB?
  - —Will the organization establish a separate structure for a Privacy Board?
- If research is not tracked by IRB, how would a study be audited for privacy and security compliance?
- What about ensure appropriate authorization is obtain for studies without IRB oversight?

Common Rule Changes - FWA issues

- For studies that no longer require ongoing review is there a need for any HIPAA oversight?
  - If so who is responsible?
  - Will covered entities start putting more stringent terms in clinical trial agreements?
- Is there an increased risk that sponsors may have data they are not legally entitled to receive?

Case Studies



Case Study 1

- At the conclusion of a study that involved data collection from clinical interventions combined with information from the research subjects' health record, one of the PIs saw an opportunity to explore the use of the data set in a novel way that included combining it with a publicly available data set. The result, she hypothesized, would serve as a basis for an algorithm to deploy and, ultimately, address questions that the original project had neither been scoped, nor able, to address.

Case Study 1

After submission, the IRB determined the protocol fell within that contemplated by 45 CFR 46.104(d)(4) and deemed the project exempt.

Months into the research, the PI realized the need for additional expertise and partnered with a colleague in the computer science department. Though her original hypothesis proved less viable, the algorithm showed promise. The PI moved on to other projects.

Case Study 1

Her computer science colleague presented a poster at a machine learning conference where the work gained some traction and even garnered a few requests for the data set for additional research use. Based on his understanding that the original project was exempt, used public data anyway, and, regardless, nothing was readily ascertainable about the information and, he personally assumed, other researchers would never contact or re-identify anyone associated, the researcher shared the data set.

Case Study 1

A few years later the data set, having been further shared and made publicly available on another institution's research site, was used to show advancements in re-identification techniques and successfully identified the original data subject population. Your institution is clearly associated and facing considerable inquiry, including the real possibility of a reportable breach and the resulting reputational and financial hits.

Case Study 1

- How could this have been avoided?
- What processes or other mitigation measures would ensure this situation does not present again?

Case Study 2

A researcher submits a protocol to the IRB to conduct research using information for which broad consent was appropriately obtained. The Chair of the IRB conducts and documents a limited review and makes the determination that “adequate provisions are in place to protect the privacy of the subjects and maintain the confidentiality of the data,” consistent with the requirements of 45 CFR 46.111(a)(7), based on the researcher’s plan to store the data in a protected network, and exempts the project under 45 CFR 46.104(d)(8).

Case Study 2

The researcher stores the information in a protected network drive and shares the information via secure transfer mechanism with her collaborator at another institution. The collaborator saves the information on an unencrypted device that is discovered stolen. He alerts the researcher to be sure all steps are taken, in the event individuals must be notified, but the researcher says they should be good because the IRB deemed the study exempt from its oversight.

- Is the researcher correct?
- Should the IRB be alerted?
- Should the privacy officer be alerted?
- Has the information been handled appropriately under the revised Common Rule and other legal obligations, including HIPAA?
- As it stands, is the documentation captured sufficient?

Case Study 2 - Additional facts

The information for which broad consent was obtained was collected in (a) France, or (b) in the US but was collected initially for a project funded by a sponsor based in the UK (or Germany).

- How does this change the analysis?

Case Study 3

XYZ Healthcare had a process in place that the Institutional Review Board (IRB) reviewed retrospective records reviews for waiver of informed consent. The same group of individuals who served as the IRB serve as the organization's Privacy Board. The Privacy Board would also review the retrospective records review for waiver of authorization. The changes to the Common Rule resulted in some studies the IRB/PB previously reviewed for waiver of informed consent no longer requiring IRB review. The organization has not addressed what this change means to the processes of the Privacy Board.

Case Study 3

- What needs to happen?
- Before the change did the minutes reflect the IRB work and separately the Privacy Board work?
- Does the organization have a process to convene the Privacy Board?

Thank You!

Marti Arvin
Executive Advisor
marti.arvin@cynergistek.com
512.450.8550 x7051

Holly B. Benton
Assoc. Director, Privacy Risk
Holly.Benton@duke.edu
919-684-0497