Research Privacy and Security Considerations Beyond HIPAA: What are the Compliance Concerns

Presented by:

Marti Arvin, JD, CHC-F, CCEP-F, CHRC, CHPC

Executive Advisor, CynergisTek, Inc.

CYNERGISTEK

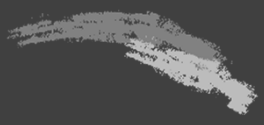
CynergisTek won the 2017 Best in KLAS Award for Cyber Security Advisory Services

CynergisTek has been recognized by KLAS in the 2016 and 2018 Cybersecurity report as a top performing firm in healthcare cybersecurity.

Today's Agenda

1. GDPR Overview
2. HIPAA & GDPR comparison
3. GDPR & Common Rule Comparison
4. Revisions to the Common Rule
5. Privacy Implications
6. Questions

GDPR Overview



General Data Protection Regulations

- Standardizes data protection for all 28 EU countries
- Covered “processing” of personal information by an individual or legal entity.
  - Broad term that covers virtually everything done to and with personal data

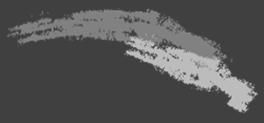
General Data Protection Regulations

- GDPR applies to any entity
  - operating within the EU
  - Outside of the EU that processes personal information of an individual physically in the EU if it
    - Offers goods or services to such individual
    - Monitors the behavior of such individual

General Data Protection Regulations

- Two types of data handlers GDPR applies to:
  - Controllers
    - Entity or person that determines the purpose and means of processing of personal data
    - This might include a sponsor, PI, or primary research site
  - Processors
    - Covered by GDPR when engaged by a controller to provide data processing services.
- GDPR has special rule for transferring personal information outside the EU

GDPR and HIPAA Comparison



Comparing HIPAA and GDPR

- De-identification versus anonymization
- Requirement for notice
- Breach notification
- Fines for non-compliance

Comparing GDPR and HIPAA

HIPAA	GDPR
• De-identification – Safe harbor – data set is de-identified if all 18 identifiers regarding the individual, their family members and household members is removed	• Anonymization – direct and indirect identifiers removed – Technical safeguards added – Zero risk of re-identification

9

GDPR pseudonymization

- Processing of personal data in a way that it cannot be linked to a specific subject without the use of additional information
  - Honest Broker concept
- Coded data is identifiable personal data under GDPR
- Coded data where the research team does not have access to the code is not PHI under HIPAA

Comparing GDPR and HIPAA

HIPAA	GDPR
• Notice requirement – Must be provided at the first episode of care by a covered entity – No obligation specific to the research team	• Notice requirement – Must be provided by the controller prior to collection of personal information direct and indirect identifiers removed – Likely built into the consent document for research

CYNERGISTEK

11

Comparing GDPR and HIPAA

HIPAA	GDPR
• Breach reporting – Must report a breach without undue delay but not more than 60 days after breach discovered. – Must notify the individual and OCR	• Breach reporting – Must notify regulator without undue delay o Notice should be no later than 72 hours after awareness of incident – Notice to the individual only if likely to be high risk to the individual's rights and freedoms

CYNERGISTEK

12

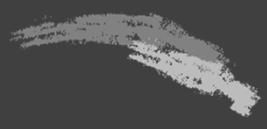
Comparing GDPR and HIPAA

HIPAA	GDPR
• Fines – Tiered approach between $100 to $50000 per violation of each individual standard – Max fine per standard violated is between $25,000 and $1.5 million per standard violated per year	• Fines – Tiered approach o The higher of 10 million euro 2% of global turnover (revenue) or o The higher of 20 million euro 4% of global turnover (revenue)

CYNERGISTEK

13

GDPR and Common Rule Comparison



CYNERGISTEK

14

Comparing GDPR and the Common Rule

Common Rule	GDPR
• Consent – Informed consent required from research participants – Waiver of informed consent permitted.	• Consent – Use of data is permitted if there is freely given, specific, informed, unambiguous, express written consent

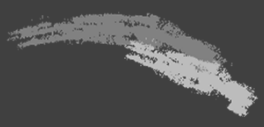
Comparing GDPR and the Common Rule

Common Rule	GDPR
• Withdrawing consent – Individual is no longer a participant – Data already collected can be used for the study.	• Withdrawing consent – Required deletion or anonymization of data unless the informed consent expressly states the data can continue to be used

Comparing GDPR and the Common Rule

Common Rule	GDPR
• Broad consent – Intent to make use of information for research easier – Can use information or biospecimen consistent with consent	• Broad consent – Required deletion or anonymization of data unless the informed consent expressly states the data can continue to be used – Unclear if additional processing of the collected data requires re-consent

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)

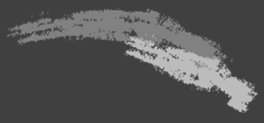
Mandatory elements of broad consent

- 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



GDPR

- Do you know when a subject's information is governed by GDPR?
- Can you handle the differences in regulatory obligations between GDPR governed data and other data?
- What if a subject withdraws from the study?

GDPR

- Would you consent meet the requirements of GDPR?
- Can you make the required notification within 72 hours of a data compromise?
- What do you do if you learn your study has data covered by the GDPR and you are non-compliant?

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?

Thank You!

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