Patient Privacy in Research Under HIPAA and the Additional HIPAA and Privacy Issues Related to Big Data Sets

CYNERGISTEK

BUTLER | SNOW

Presented by:

Marti Arvin
VP of Audit Strategy

Shannon Hoffert

Agenda

Quick Level Setting

Where is research occurring?

- Academic medical centers
  - School of Medicine
  - School of Nursing
  - School of Dentistry
- Physician offices
- Community hospitals

Basics of HIPAA and Research

The "big divide" in clinical research

Prospective Study	Retrospective Study
• Enrolls subjects who receive services according to a schedule of events	• Uses existing information, often, medical record information

CYNERGISTEK

5

What regulations need to be considered?

- HIPAA
- Common Rule
- FDA
- Possibly
  - State law
  - SAMSHA
  - FISMA

CYNERGISTEK

6

Privacy and Security Issues in the Different Phases of a Research Study

Life of a Research Study

- Development of the Protocol
- Grant Submission or Clinical Trial Agreement
- IRB Submission
- Conducting the Study
- Closing Out the Study
- Storage and Destruction of Data
- Use of Data for Other Projects

Development of the Protocol

- Does the researcher understand the implication of the privacy and security provisions in the protocol:
  - Who will data need to be shared with?
  - How will the subjects privacy be protected?
  - What data is actually necessary to conduct the study?
    - Identified or de-identified

Grant Submission

- Submitting for a governmental grant
  - What are the requirements of the granting agency?
    - Do they require compliance with regulations other than the Common Rule?
      - FISMA
      - FDA Part 11
  - Can the organization meet the requirements of the granting agency?

Industry Sponsored Research

- Clinical trial agreements with industry sponsors
  - Are there special requirements in the contract language and can the organization meet those requirements?
    - Data use issues
    - Data transmission and storage issues during study
    - Data retention issues
    - FDA Part 11 obligations

Data Use Issues

- What does the sponsor intend to do with the data once acquired?
  - Use it for additional studies
    - General studies
    - Genetic studies
  - Use for marketing or other commercial purpose

Data Transmission and Storage Issues During Study

- How is data required to be transmitted?
  - With sponsor
  - With collaborators
- How is data required to be stored?
  - Paper records
  - Electronic records

CYNERGISTEK

13

Data Retention Issues

1

Does the researcher understand retention requirement?

2

Length of data retention:

Does it go beyond the organization's standard policy?

3

Method of data retention:

Is the format in the protocol consistent with the agreement?

4

Cost of data retention:

Who will pay for the required data retention method?

i.e. Long-term security storage of paper or electronic records

CYNERGISTEK

14

IRB Submission

- What has the researcher submitted to the IRB regarding privacy and information security?
  - Are the documents submitted to the IRB consistent?
    - Informed consent document
    - Protocol
    - HIPAA authorization or waiver of authorization
    - Research on decedents
  - Who is checking for this consistency?

CYNERGISTEK

15

IRB Obligations

HIPAA	Common Rule
Review and determine appropriateness of waiving the HIPAA requirement for an authorization to use and disclose information for research.	Protect the rights and welfare of human subjects.

CYNERGISTEK

16

Researcher Conducting the Study

1. Subject Recruitment
2. Subject Enrollment
3. Data Collection
4. Data Analysis
5. Data Transmission and Storage

CYNERGISTEK

17

Closing Out the Study

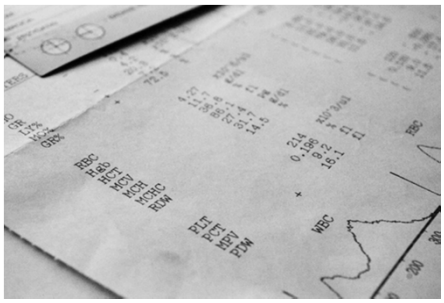
1. Closing the Enrollment Phase
2. Closing the Analysis Phase
3. Completion of the Study

CYNERGISTEK

18

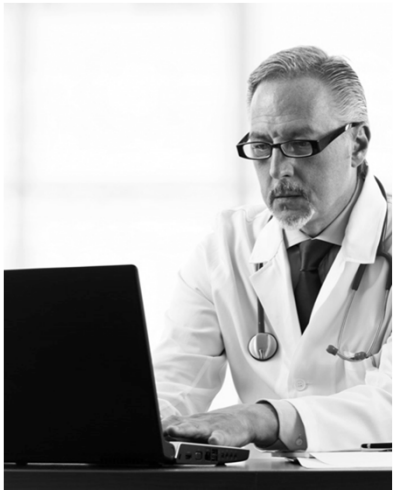
Storage and Destruction of the Data

- Storing and destruction in compliance with the applicable regulations
  - OHRP
  - FDA
  - Other
  - Grant or clinical trial agreement
  - Institution's data retention policies
- Who monitors this?



Use of Data for Other Projects

- Does the organization permit or restrict this by policy?
- Who would approve such use?
- Is the subject informed of the possible use of the data for other projects?
  - Informed consent
  - HIPAA authorization
- What if the data was gathered without informed consent or authorization?



HIPAA Issues in Creating and Maintaining Big Data Sets for Research

Big Data Repositories: Where do they Come From?

- EMR, Community Based
- HIEs
- Joint Ventures
- Third Party Analysts
- Wearable Devices

Research & Patient Portals

- Patient portals may present an opportunity for the electronic collection of patient information and downstream dissemination of patient information for many purposes, including data analytics and research.
- Covered Entities should have internal policies and procedures for monitoring use of outward facing portals and access to data collected through these portals.

CYNERGISTEK

23

Big Data Sets for Research: When Does HIPAA Kick In?

CYNERGISTEK

24

Big Data Repositories

- When does HIPAA kick in?
- Simply, when a Covered Entity determines to Use or Disclose PHI.
- For research organizations that are not covered entities, the authorization still governs PHI in repositories.
- Where can PHI sneak in?
  - Dates
  - Unique Numbers or Codes
  - Initials

If any data element is included, and the purpose of the use or disclosure is for analysis that leads to generalizable knowledge, then HIPAA research rules apply.

CYNERGISTEK

Big Data Repositories

Is It Even Research?

Research under HIPAA	Health Care Operations under HIPAA
Research is for the collection and analysis of data for "generalizable knowledge."	Healthcare operations may include "outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; [and] . . . population-based activities relating to improving health or reducing health care costs. . . ." 65 Fed. Reg. 82462, 82608 (Dec. 28, 2000).

CYNERGISTEK

Big Data Repositories

Is It Even Research?

The Department of Health and Human Services has stated that, "If the primary purpose of the activity is to produce generalizable knowledge, the activity fits within this rule's definition of 'research' and the covered entity must comply with [the HIPAA Privacy Rule requirements for research], including obtaining an authorization or the approval of an institutional review board or privacy board."

CYNERGISTEK

27

Big Data Sets for Research: Setting Parameters for Privacy

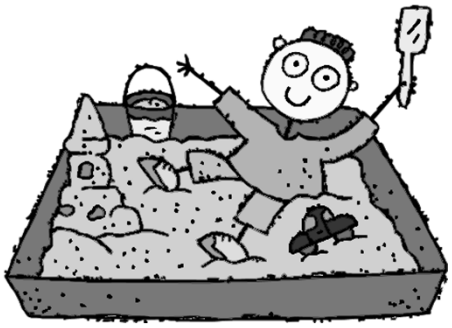
CYNERGISTEK

28

Big Data Repositories

The HIPAA Research Sandbox

- Usually research is conducted within the Authorization Sandbox.
- But with Big Data Repositories, other parameters may work.
- Waivers, De-Identified Data, Limited Data Sets/Data Use Agreements
- Avoiding the sandbox turning into the pitfall



Big Data Repositories

- Scrubbing data? Consider:
- Who is scrubbing the repository? Relative risks?
- Affiliates have to have a BAA to scrub data, unless the entities are "affiliated covered entities."
- ➢ Remember, Business Associates are only permitted to de-identify data if the Covered Entity specifically authorizes de-identification. Must be stated in the BAA.

Big Data Repositories

De-Identification vs Limited Data Sets vs Data "Sharing"

De-Identification	Limited Data Set	Data Sharing
Scrubbed of all "18 identifiers" (safe harbor) Deemed scrubbed by expert No longer PHI once de-identified Can be used for research, market analysis, etc.	Scrubbed of all 18 identifiers except: • Dates such as admission, discharge, service, DOB, DOD; • City, state, five digit or more zip code; and • Ages in years, months or days or hours. Can be used pursuant to a **Data Use Agreement** for purposes of research	"Data Sharing" can be risky business. Vendors often provide "Data Use" agreements for sharing data of a group of participants. Rule of Thumb: PHI cannot be "shared"

CYNERGISTEK

31

Big Data Repositories

- Data Use Agreement: An agreement between the Covered Entity and the Researcher for the disclosure of a LDS. The DUA must specify:

1. The permitted uses and disclosures of the LDS, consistent with the purposes of the research.
2. A statement limiting who can use or receive the data.
3. A provision requiring the researcher to:
   - Not use or disclose the information other than as permitted by the DUA or law;
   - Use appropriate safeguards to prevent unauthorized use or disclosure;
   - Report any unauthorized uses and disclosures to the Covered Entity;
   - Ensure the researchers' agents agree to the same restrictions and conditions as are in the DUA;
   - Not identify the information or contact the individual.

CYNERGISTEK

Big Data Repositories

- Be vigilant in reviewing contracts dealing with collections of data. Train staff to recognize terms that could trigger research.
- "Research" could be called "data analysis," or "data aggregation" or "population studies" or "quality studies"
- Make sure all parties understand how the data will be used/further disclosed and make sure the right agreement is in place.

CYNERGISTEK

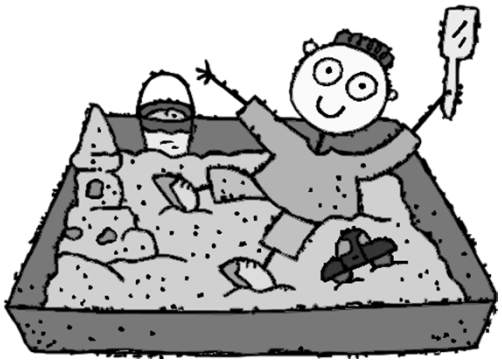
Big Data Sets for Research: Future Uses

CYNERGISTEK

Big Data Repositories

Back in the Authorization Sandbox

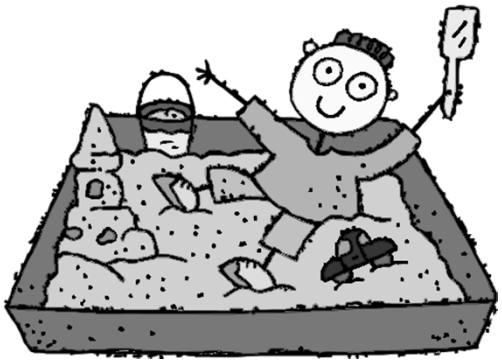
- Authorizations for Future Research
  - An authorization may be obtained from an individual for uses and disclosures of PHI for future research purposes,
  - Future research must be described so that it would be reasonable for the individual to expect that PHI could be used or disclosed for the future research purposes.



CYNERGISTEK

Big Data Repositories

- But what if the "future use" research does not include PHI?
- Does that "use" have to be described in the HIPAA research authorization?



CYNERGISTEK

Big Data Sets for Research: Biospecimen Repositories

Big Data Repositories

Are Biospecimens PHI?

- Biospecimens. Tissue samples and blood itself are not PHI under HIPAA.
- Biospecimens that have PHI identifiers attached are covered under HIPAA. Ex. Date of collection, Medical account numbers, etc.
- What about re-identification?

Big Data Repositories

OCR Guidance on De-Identification

"Much has been written about the capabilities of researchers with certain analytic and quantitative capacities to combine information in particular ways to identify health information. A covered entity may be aware of studies about methods to identify remaining information or using de-identified information alone or in combination with other information to identify an individual. However, a covered entity's mere knowledge of these studies and methods, by itself, does not mean it has "actual knowledge" that these methods would be used with the data it is disclosing. OCR does not expect a covered entity to presume such capacities of all potential recipients of de-identified data. This would not be consistent with the intent of the Safe Harbor method, which was to provide covered entities with a simple method to determine if the information is adequately de-identified."

Big Data Repositories

Brief Side Step to the Revised Common Rule

- "Nonidentifiable" Biospecimens are not subject to the Common Rule
- Allows the use of prospective, broad consent for storage, maintenance, and secondary research use of identifiable biospecimens.

Big Data Repositories

- Consent/Authorization then, comes down to identifiers
- Unidentified biospecimens do not require a HIPAA authorization or consent.

CYNERGISTEK

QUESTIONS

CYNERGISTEK

Thank You!

Questions?

Shannon Hoffert
Butler Snow, LLP
Shannon.Hoffert@butlersnow.com
901-680-7352

Marti Arvin
VP Audit Strategy
Marti.arvin@cynergistek.com
512-402-8550 x7051

CYNERGISTEK