Sharing PHI for Research

J. T. Ash
University of Hawaii System
HIPAA Compliance Officer
jtash@hawaii.edu
hipaa@hawaii.edu

Agenda

- HIPAA is a "**TEAM SPORT**" and everyone has a role in protecting protected health information (PHI).
- Privacy Rule, Security Rule, & Breach Notification Rule
- Methods to Share PHI (Privacy Rule)
- With Individual Authorization
- Without Authorization
- Accounting for Research Disclosure
- De-Identified Data
- Security Rule & Breach Notification

HIPAA Privacy Rule

- https://www.youtube.com/watch?v=y751i4QqP0g
- The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- https://www.hhs.gov/hipaa/for-professionals/privacy/index.html
- 45 CFR Part 160 and Subparts A and E of Part 164.

HIPAA Security Rule

- The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
- https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
- 45 CFR Part 160 and Subparts A and C of Part 164.
- Safeguards:
  - Administrative
  - Physical
  - Technical

Breach Notification Rule

- **Notification to Individuals**: Individuals whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of such breach must be notified without unreasonable delay and in no case later than 60 calendar days following the discovery of such breach.

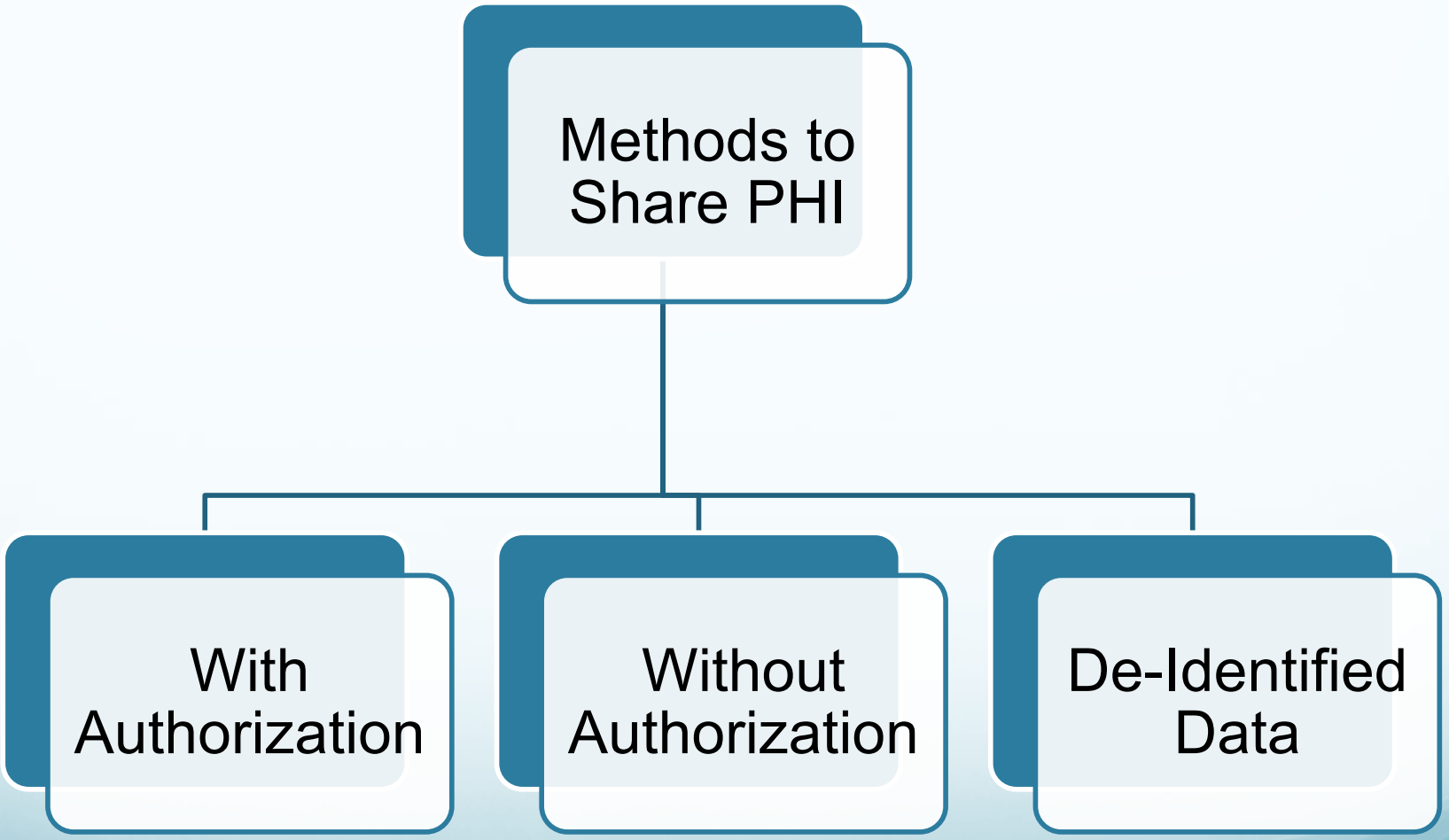
- **Notification to Others**: A UH Covered Component shall also notify prominent local media outlets if the breach involves more than 500 residents of the State no later than 60 days after discovery of the breach.

- **Notification to DHHS Secretary**: A UH Covered Component shall notify the DHHS Secretary on an annual basis, in a manner specified on the DHHS Web site, and via a report due to the DHHS Secretary no later than 60 calendar days after the end of the calendar year in which breaches are discovered *if less than 500 individuals are involved*. *If more than 500 individuals are involved*, the UH Covered Component shall notify the DHHS Secretary in the manner provided by the DHHS Web site, which presently requires notice without unreasonable delay and in no case later than 60 days following a breach.

- **Notification by a Business Associate**. A Business Associate shall notify a UH Covered Component of a breach within 5 business days that the Business Associate discovered a breach occurred…

Methods to Share PHI

(***Satisfies Privacy Rule Obligations)



With Individual Authorization

- The Privacy Rule has a general set of authorization requirements that apply to all uses and disclosures, including those for research purposes. However, several special provisions apply to research authorizations:
  - Unlike other authorizations, an authorization for a research purpose may state that the authorization does not expire, that there is no expiration date or event, or that the authorization continues until the “end of the research study;” and
  - An authorization for the use or disclosure of protected health information for research may be combined with a consent to participate in the research, or with any other legal permission related to the research study.

Without Authorization

- A Covered Entity must obtain one of the following:
  - Documented Institutional Review Board (IRB) Board Approval
  - Preparatory to Research
  - Research on Protected Health Information of Decedents
  - Limited Data Sets with a Data Use Agreement

Documented Institutional Review Board (IRB) Board Approval

- A covered entity may use or disclose protected health information for research purposes pursuant to a waiver of authorization by an IRB or Privacy Board, provided it has obtained documentation of ***ALL*** of the following:
  - Identification of the IRB or Privacy Board and the date on which the alteration or waiver of authorization was approved;
  - A statement that the IRB or Privacy Board has determined that the alteration or waiver of authorization, in whole or in part, satisfies the three criteria in the Rule;
    - A brief description of the protected health information for which use or access has been determined to be necessary by the IRB or Privacy Board;
    - A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures; and
  - The signature of the chair or other member, as designated by the chair, of the IRB or the Privacy Board, as applicable.

Institutional Review Board (IRB) Waiver of Authorization

- The following three criteria must be satisfied for an IRB or Privacy Board to approve a waiver of authorization under the Privacy Rule:
  - The use or disclosure of protected health information involves no more than a minimal risk to the privacy of individuals, based on, at least, the presence of the following elements:
    - An adequate plan to protect the identifiers from improper use and disclosure;
    - An adequate plan to destroy the identifiers at the earliest opportunity consistent with conduct of the research, unless there is a health or research justification for retaining the identifiers or such retention is otherwise required by law; and
    - An adequate written assurances that the protected health information will not be reused or disclosed to any other person or entity, except as required by law, for authorized oversight of the research project, or for other research for which the use or disclosure of protected health information would be permitted by this subpart;
  - The research could not practicably be conducted without the waiver or alteration; and
  - The research could not practicably be conducted without access to and use of the protected health information.

Preparatory to Research

- Representations from the researcher, either in writing or orally, that the use or disclosure of the protected health information is solely to prepare a research protocol or for similar purposes preparatory to research, that the researcher will not remove any protected health information from the covered entity, and representation that protected health information for which access is sought is necessary for the research purpose.

Research on Protected Health Information of Decedents

- Representations from the researcher, either in writing or orally, that the use or disclosure being sought is solely for research on the protected health information of decedents, that the protected health information being sought is necessary for the research, and, at the request of the covered entity, documentation of the death of the individuals about whom information is being sought.

Limited Data Sets with a Data Use Agreement

- A data use agreement entered into by both the covered entity and the researcher, pursuant to which the covered entity may disclose a limited data set to the researcher for research, public health, or health care operations.

- The data use agreement must:
  - Establish the permitted uses and disclosures of the limited data set by the recipient, consistent with the purposes of the research, and which may not include any use or disclosure that would violate the Rule if done by the covered entity;
  - Limit who can use or receive the data; and
  - Require the recipient to agree to the following:
    - Not to use or disclose the information other than as permitted by the data use agreement or as otherwise required by law;
    - Use appropriate safeguards to prevent the use or disclosure of the information other than as provided for in the data use agreement;

Limited Data Sets with a Data Use Agreement

- Report to the covered entity any use or disclosure of the information not provided for by the data use agreement of which the recipient becomes aware;
- Ensure that any agents, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the recipient with respect to the limited data set; and
- Not to identify the information or contact the individual.

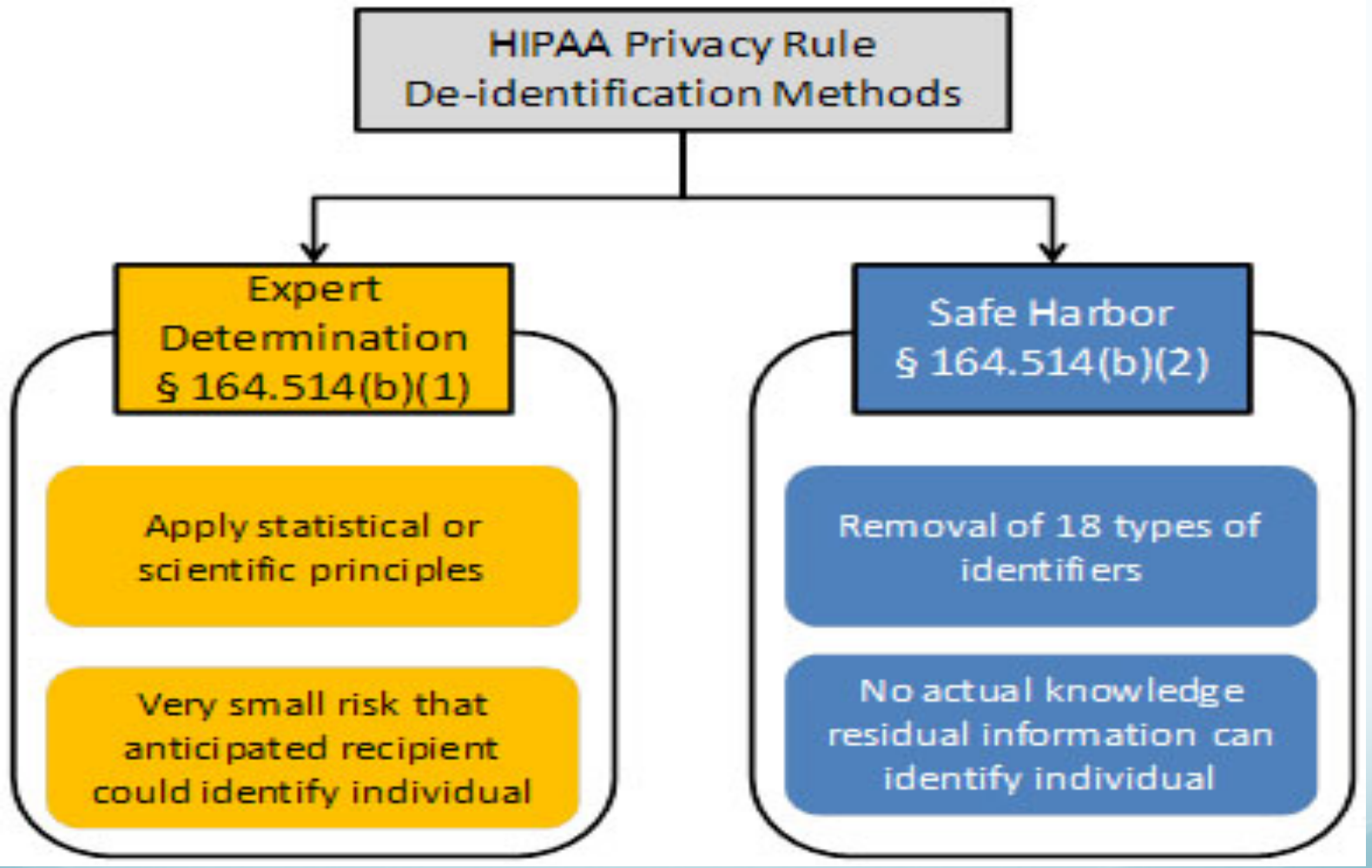
Accounting for Research Disclosure

- The Privacy Rule gives individuals the right to receive an accounting of certain disclosures of protected health information made by a covered entity.
- This accounting must include disclosures of protected health information that occurred during the six years prior to the individual's request for an accounting, or since the applicable compliance date (whichever is sooner), and must include specified information regarding each disclosure.
- A more general accounting is permitted for subsequent multiple disclosures to the same person or entity for a single purpose.
- Among the types of disclosures that are exempt from this accounting requirement are:
  - Research disclosures made pursuant to an individual's authorization;
  - Disclosures of the limited data set to researchers with a data use agreement

What is De-identified Data?

- De-identified data is not considered PHI
- No obligations to the Privacy/Security/Breach Notification Rules
- May use and disclose de-identified data without restriction

Expert Determination & Safe Harbor



What is De-identified Data?

- Removal of all 18 unique identifiers
  - Name
  - All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and (2) the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
  - All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
  - Telephone numbers
  - Fax numbers
  - Email addresses
  - Social Security numbers
  - Medical record numbers

What is De-identified Data?

- Removal of all 18 unique identifiers (Expert Determination & Safe Harbor)
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers/serial numbers
  - Device identifiers/serial numbers
  - Web URLs
  - IP address numbers
  - Biometric identifiers
  - Full-face photographic images and any comparable images
  - Any other unique identifying number, characteristic, or code; and
    - The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

Security Rule & Breach Notification

- Still need to work with your IT support to ensure they have an environment that can satisfy the obligations of the Security Rule
- Still need to work with your InfoSec support to ensure they have the policies/procedures in place to satisfy the obligations of the Breach Notification Rule

J. T. Ash
UH System HIPAA Compliance Officer
jtash@hawaii.edu • (808) 956-7241