HIPAA & PHI in Anatomical Donation, Education, & Research

AACA — JULY 10, 2018

Zane Wagner is an attorney and compliance officer at the University of Minnesota, where he works on privacy regulations and health law. Zane promotes HIPAA compliance by helping researchers, administrators, and students understand the need for privacy and security at every level of the organization. Drawing on a background in law and technology, he connects the dots between privacy policies and the day-to-day collection, use, and disclosure of health information.

Zane is a graduate of Washington State University and the University of Minnesota Law School. He holds the Certified Information Privacy Professional (CIPP/US) and Certified Information Privacy Technologist (CIPT) credentials from the International Association of Privacy Professionals.

E-mail: zanewagner@gmail.com
Phone: 360-823-9004

Legal Education Disclaimer

This presentation is for general informational purposes. The application and impact of laws and regulations can vary widely based on the specific facts involved. The information in this document is provided with the understanding that the author is not providing legal or compliance services, and it should not be used as a substitute for consultation with professional legal or compliance professionals.

If you need legal advice regarding the compliance of your program or any other purpose, you are encouraged to seek the advice of your compliance or legal team or a lawyer.

PRESENTATION OVERVIEW

BRIEF OVERVIEW OF HIPAA: RATIONALE AND GUIDING PRINCIPLES

- When HIPAA applies: Covered Entities and PHI.
- The three use and disclosure rules for PHI.
- Applying the three use and disclosure rules to anatomical donation, education, and research.

WHAT WILL NOT BE COVERED

- HIPAA Legislative and Administrative History.
- Personnel, policies, and procedures required by HIPAA.
- HIPAA Security Rule (except for a single slide).

RATIONALE

- HIPAA establishes uniform national standards for:

- Patient rights to access their own health information
- Privacy of individually identifiable health information
- Security of electronic health information

GUIDING PRINCIPLES: HIPAA PRIVACY RULE

- Access: Patients can access their health information and request that information be sent to the provider of their choice.
- TPO: Covered Entities may use and disclose health information for the purposes of treatment, payment, and health care operations.
- Privacy: other uses and disclosures of health information by covered entities is prohibited unless authorized by the patient, with some exceptions for uses that benefit the public.

GUIDING PRINCIPLES: HIPAA SECURITY RULE (JUST ONE SLIDE)

- The HIPAA Security Rule requires covered entities to protect the confidentiality, integrity, and availability of electronic protected health information, while permitting the appropriate access and use of that information by providers.
- Implementation of Security Rule requirements will be included in each covered entity's Policies and Procedures.

A FLOOR, NOT A CEILING

- HIPAA establishes a Federal floor of standards to ensure the privacy, security, and access rights for health information.
- State laws that provide less access and less protection are overridden by HIPAA.
- Where State laws provide more stringent standards, these will apply over and above HIPAA requirements.

PENALTIES FOR VIOLATIONS OF HIPAA

- The U.S. Department of Health and Human Services (HHS) assesses penalties for violations of HIPAA.
- $100 to $50,000 per violation, per record.
- Fines for "negligent" violations are high.
- "Willful" and "willfully neglect" violations can result in even higher fines, criminal charges, and jail time.

COVERED ENTITIES & PROTECTED HEALTH INFORMATION

COVERED ENTITIES: DEFINITIONS AND EXAMPLES

- HIPAA applies only to covered entities. Covered entities are:
  - Health care providers (e.g. a hospital, a clinic, a solo practitioner, a student clinic that bills for payment, or a medical school that provides treatment);
  - Health insurance plans (including plans run by employers); and
  - "Health care clearinghouses".
- The covered entity must transmit health information electronically for payment or billing.

COVERED ENTITIES: RESEARCHERS

- HIPAA applies to researchers and educators who are part of the workforce of covered entities.
- Researchers and educators can also be a covered entity if they are a provider and bill for services.

COVERED ENTITIES: HYBRID ENTITIES

- Where any part of an organization meets the definition of a covered entity, the entire organization is generally subject to HIPAA.
- A single legal entity that would be a covered entity may designate its components that are providers, plans, and clearinghouses as health care components (HCC).
- The non-HCC part of the organization will not be subject to the Privacy Rule.

COVERED ENTITIES: BUSINESS ASSOCIATES

- Business Associates are separate entities that create, receive, use, or disclose health information on behalf of a covered entity.
- Before a covered entity may disclose health information to a business associate, the covered entity must sign a Business Associate Agreement that ensures the business associate will appropriately safeguard the information.

PROTECTED HEALTH INFORMATION: DEFINITION

- Health information is only PHI if it is created or received by a covered entity.
- Health information is only PHI if it relates to:
    - The physical or mental health of an individual;
    - Provision of care to an individual; or
    - Payment for care of an individual.
- The health information must directly identify an individual; or there must be a reasonable basis to believe the information can be used to identify the individual.

PROTECTED HEALTH INFORMATION: DOES NOT INCLUDE

- Employment records held by a covered entity employer.
- Education records on students held by an educational agency or institution.
- Health records of persons deceased more than fifty years.

PROTECTED HEALTH INFORMATION: DE-IDENTIFICATION

- There is only one way to transform PHI into not-PHI: de-identification.
- De-identification is a legal term of art defined by HIPAA. To de-identify PHI, you must remove 18 types of information from a record, and the remaining information must not identify an individual either alone or in combination with any other information.

DE-IDENTIFICATION REQUIREMENTS: 45 CFR 164.514

- Names;
- Geographic subdivisions smaller than a state;

- Any date elements (except the year) and any dates that would imply the individual is over 89 years old must be masked to imply an age of 90+;
- Telephone and Fax numbers;
- E-mail addresses;
- Social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate and license numbers;
- Vehicle identifiers (license plates),
- Device identifiers (serial numbers);
- Web Addresses (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code, except a single code that may be used to re-identify the individual, created for this one purpose and the method or re-identification is never disclosed.

PROTECTED HEALTH INFORMATION: DE-IDENTIFICATION

- You can also ask a statistical expert to de-identify PHI, if you have this approved by your compliance department.
- The statistical expert (a person with appropriate knowledge to make a determination) will remove data from the PHI until the risk of re- identifying an individual is "very small."

WHEN AND HOW COVERED ENTITIES MAY USE PHI

SUMMARY: THE THREE USE AND DISCLOSURE RULES

- A covered entity must follow one of three different rules when using or disclosing PHI, depending on the purpose of the use or disclosure:
- Rule 1: You may always uses PHI for treatment, payment, health care operations, and public benefit activities.
- Rule 2: You must give an individual the opportunity to object before using their PHI in hospital directories, and before talking to family members and other persons involved in the individual's care.
- Rule 3: You need an authorization for everything else, unless the PHI is de-identified or another exception applies.

THE MINIMUM NECESSARY STANDARD

- In addition to needing to use one of the three rules allowing uses and disclosures, the Privacy Rule requires that you use the minimum necessary amount of PHI for each use or disclosure.

RULE ONE: TPO & PUBLIC BENEFIT

- Covered entities may use and disclose PHI without patient permission for Treatment, Payment, Health Care Operations, and Public Benefit activities.

- Treatment: provision, coordination, or management of health care by one or more providers or third parties.
- Payment: obtaining or providing reimbursement for services, or determining coverage of benefits under a health plan.
- Health Care Operations: business management, quality assessment and improvement activities, training health care professionals, etc.

RULE ONE: PUBLIC BENEFIT

- Public Benefit Activities (non-exhaustive)
- Identifying decedents. PHI may be disclosed to facilitate identification of a deceased person or determining cause of death.
- Cadaveric Organ, Eye, or Tissue Donation. PHI may be disclosed to facilitate the donation and transplantation of cadaveric organs, eyes, and tissue.
- Public Health Authorities. PHI may be disclosed to public health authorities, individuals who have been exposed to communicable diseases (where required by law), and to report victims of abuse, neglect, or violence.
- To law enforcement, to report a crime on premises, or where required by law or court order.

RULE TWO: OPPORTUNITY TO OBJECT

- Covered entities may use and disclose PHI for the below purposes if they notify the patient and give them the opportunity to object:
- Directory information: including the individual's name, room number, and general health status for a hospital directory;
- Persons involved in care: providing information to family members and other persons regarding the individual's care, to the extent they were involved in the individual's care;
- Notification: notifying family members (and persons responsible for the individual's care) of the individual's location, condition, or death.

RULE TWO: APPLICATION TO DONOR PROGRAMS

- Rule two generally does not apply to donor programs.
- Rule two would apply to notifying family members of a donor's death.
- For other questions, you would be in the right to direct them to the provider who was attending the decedent at time of death, who would be better suited both to determine who was involved in care and what information is relevant to that involvement.

RULE TWO: HOW TO GIVE DONORS THE OPPORTUNITY TO OBJECT

- When/how can you give a donor the opportunity to object?
- Notify the individual of possible disclosures under rule 2 (we may disclose relevant information to persons who were involved in care, and to notify family members of death) in your consent form.
- Give the individual the opportunity to object in writing. This can be opt-in or opt-out.

RULE THREE: WITH PATIENT AUTHORIZATION

- Where a covered entity would like to use PHI for any purpose that is not treatment, payment, or healthcare operations, and does not fall within one of the public benefit exceptions, and is not allowed without objection, the covered entity must obtain the prior written authorization of the individual or their personal representative.

PERSONAL REPRESENTATIVES

- A personal representative has the right to authorize uses and disclosures as if they were the individual.
- A living individual's personal representative is a person with authority under State law to make health care decisions for the individual.
- A decedent's personal representative is a personal with authority under State law to act on behalf of the decedent or their estate.
- A personal representative is NOT the same as the Common Rule legally authorized representative.

INDIVIDUAL ACCESS

INDIVIDUAL ACCESS (GENERALLY)

- Covered entities are required to provide individuals (or their personal representative) with access to the individual's PHI:
    - This includes the right to inspect or obtain a copy of the PHI.
    - The individual may direct the covered entity to transmit a copy of their PHI to any person or entity of the individual's choice.
    - The individual access right extends to all information maintained by a covered entity, regardless of the date of creation, the form or medium of storage, or where the PHI originated.

USES AND DISCLOSURES OF DECEDENT PHI

IS THE PHI OF DECEDENTS PROTECTED BY HIPAA?

- Yes: for fifty years following the date of death of the individual.
- During this period, the personal representative can authorize uses and disclosures of that information.

CAN I USE DECEDENT PHI FOR TREATMENT PURPOSES?

- Rule 1 allows use and disclose for any treatment, payment, health care operations, and public benefit activities.
- Disclosures for the purpose of treatment (even the treatment of another individual) are always permitted under Rule 1.
- For example, a covered entity may disclose the PHI of a decedent to providers who need that information to treat family members.

CAN I USE DECEDENT PHI TO EDUCATE MEDICAL STUDENTS?

- Rule 1 allows use and disclose for any treatment, payment, health care operations, and public benefit activities.
- Health care operations includes education: it is permitted to disclose PHI of decedents to health care teachers and students within a covered entity for the purpose of education.
- Remember the minimum necessary standard!

WHAT OTHER USES OF DECEDENT PHI ARE ALWAYS ALLOWED?

- HIPAA allows these disclosures under public benefit activities:
- To law enforcement when there is a suspicion that death resulted from criminal conduct;
- To coroners, medical examiners, and funeral directors;
- To researchers when the research is solely on the PHI of decedents;
- To organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of organs, eyes, or tissue, to facilitate donation and transplantation.

WHEN CAN I DISCLOSE DONOR PHI TO FAMILY MEMBERS?

- It depends!
- Rule 2 allows a covered entity, after giving the patient the opportunity to object, to disclose a decedent's PHI to family members or other persons involved in the decedent's care or payment prior to the decedent's death.
    - This disclosure is limited to information relevant to their involvement in the decedent's health care or payment.
    - If the decedent objected to this disclosure, then the covered entity may not disclose the PHI.
- A decedent's personal representative has the right, under rule 3, to authorize disclosure of PHI to the personal representative or any other individual or entity.
    - The personal representative can authorize disclosure and then provide this to family members.
    - This is true even if the decedent objected to disclosures allowed under rule 2.

USES AND DISCLOSURES FOR RESEARCH

- The general rule is that use and disclosure of PHI for research requires written patient authorization. There are three exceptions to this limitation on use and disclosure of PHI for research:
    - Waiver of Authorization: An Institutional Review Board or Privacy Board has approved an alteration or waiver of authorization.
    - Preparatory to Research: The researcher requests, and the covered entity approves, use of PHI solely for the purpose or preparing a research protocol. The PHI must be necessary for the research, and the researcher may not remove any PHI from the covered entity.
    - Research solely on Decedents: The researcher requests, and the covered entity approves, use of PHI which is be used solely for research using PHI of decedents. The PHI must be necessary for the research.

ARE PHOTOS PROTECTED BY HIPAA?

- Identifying photos and videos are included in the definition of PHI:
- "Full face photographic images and any comparable images"
- The general rule of thumb is that if a photo could identify an individual either alone or in combination with any other information, then you shouldn't disclose the information without authorization.
- Identifying examples: tattoos, piercings, rare external conditions (e.g. congenital disorders), dental records.
- Non-identifying examples: anything else, although there may well be ethical concerns.

ARE BIOMETRICS PROTECTED BY HIPAA?

- Biometrics are included in the definition of PHI:
- "Biometric identifiers, including finger and voice prints;"
- The definition of biometrics is not necessarily limited to finger and voice prints, but there is no explicit guidance on what else might be included in this definition.
- Tissue is excluded from the definition of PHI.
- What about biometrics beyond finger and voice prints?
- Biometrics are physical characteristics that can be matched against a database of recorded characteristics or summaries and thus identify an individual.
- Finger prints and voice prints meet this definition.
- Retina scans would meet this definition.
- Genetic data?

WHEN CAN I DISCLOSE DONOR PHI TO THE MEDIA?

- Unless you have their written authorization, you can never disclose donor information to the media.
- This includes talking to the media in the same conversation as family members who are talking to the media!
- This is true even if the information is already widely known, and even if the media already has the information.
- Provider disclosures of PHI to the media is one of the few circumstances where people have served time in prison for violations of HIPAA.

WHEN CAN I DISCLOSE DONOR PHI TO THE PUBLIC?

- This comes up in context of donor celebrations. As an example, you would want to include names and photographs of each donor in the celebration.
- You need the donor's authorization for this disclosure.

WHAT INFORMATION CAN I INCLUDE IN AN ONLINE DONOR REGISTRY?

- If you have patient authorization under Rule 3, then you can disclose any information the authorization permits.
- If you do not have authorization, then no other rule permits you to disclose the information, so you can only disclose de-identified information: age (0-89 or 90+), and

occupation and health status, so long as these wouldn't otherwise identify the individual alone or in combination with any other information.