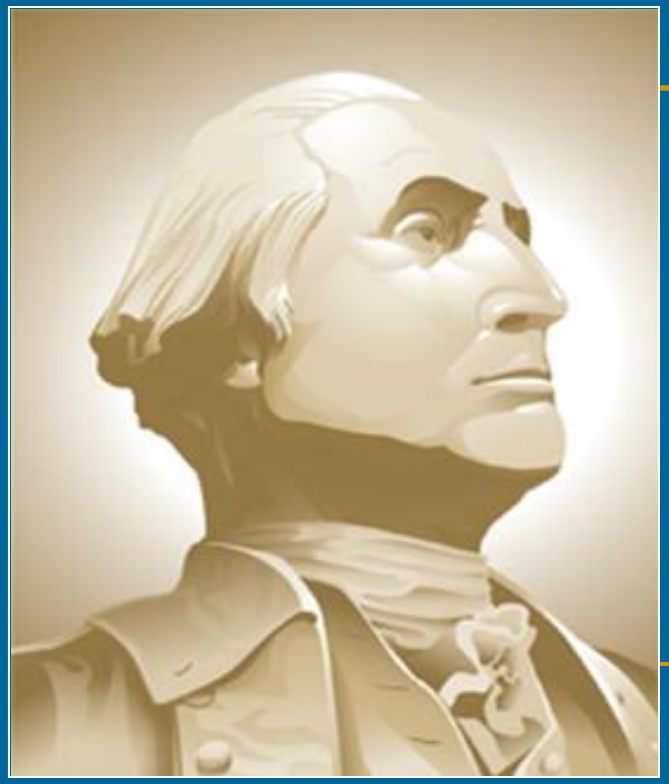

Patient Privacy Requirements Beyond HIPAA

Jane Hyatt Thorpe, J.D.

Department of Health Policy
School of Public Health and Health Services
George Washington University

Carrie Bill, J.D.

Feldesman Tucker Leifer Fidell LLP

The George Washington University Healthcare Corporate Compliance Graduate Certificate Program

HIPAA Privacy Rule: Key Definitions

- Protected Health Information (PHI)
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium (paper, electronic, oral)
  - Created or received by a covered entity or business associate
  - Relating to health care or payment
- Covered Entity (CE)
  - Health care providers
  - Insurers
  - Clearinghouses

HIPAA Privacy Rule: Disclosures

- Covered entities may only use and disclose PHI according to Privacy Rule provisions
- Only two required disclosures
  - Required disclosure to the HHS Secretary
  - Required disclosure to the individual
- All other disclosures permissive (7 categories)
  - Treatment, payment, and health care operations
  - Incidental uses and disclosures
  - Individual has opportunity to agree or object
  - Specific "public purpose" disclosures
  - Limited data set (facially de-identified, requires data use agreement between parties)
  - De-identification (all identifiers removed)
  - With authorization
- Other important elements
  - Minimum Necessary
  - Business Associates
- HIPAA Privacy Rule controls unless stricter state law

HIPAA Privacy Rule: Disclosures, cont'd

- Treatment
  - CE may disclose PHI for treatment activities to another health care provider
- Payment
  - CE may disclose PHI to another CE or health care provider for the CE's payment purposes
- Health Care Operations
  - CE may disclosure PHI to another CE for certain specified activities (e.g., quality improvement initiatives)
- Authorization
  - Individual may authorize the release of their PHI in writing with a signature and date provided other requirements met

HIPAA Privacy Rule:
Required Elements of a Patient Authorization

- Description of the PHI to be used or disclosed
- People/persons authorized to use or disclose the PHI
- The person to whom the covered entity may disclose the PHI
- The purpose of the use or disclosure
- Patient's right to revoke the authorization at any time
- Consequences if the patient refuses to sign the authorization, but note that signature is not required for treatment
- An expiration date
- Signed and dated by the patient or patient's representative with a copy provided to the patient
- PHI may be re-disclosed by a third party and therefore not subject to HIPAA
- Plain language

HIPAA Privacy Rule: Minimum Necessary

- Minimum Necessary Standard applies to most uses and disclosures
  - When using, disclosing, or requesting PHI, a CE must make reasonable efforts to limit PHI to the minimum amount necessary to accomplish the intended purpose of the use, disclosure, or request

HIPAA Privacy Rule: Business Associates

- What is a Business Associate (BA)?
  - Person or entity that performs certain functions "on behalf of" a CE involving the use, disclosure or creation of PHI
  - Excludes employees, workforce members
  - Examples: TPAs, attorneys, billing services, data aggregators
- Requirements
  - A CE may not disclose PHI to a BA unless it obtains "satisfactory assurances" that the PHI will safeguard the PHI
  - "Satisfactory assurances" usually means a business associate agreement (contract that stipulates how the data may/may not be used or released with penalties for violations)
- Direct Liability
  - Post HITECH, BAs directly subject to HIPAA requirements (no longer indirect via contractual liability to CE)

HIPAA Privacy Rule: Individual Rights

- Individuals have six rights
  - Notice: Right to receive a notice of privacy practices of PHI
  - Restriction: Right to request a restriction on uses and disclosures of PHI
  - Confidential Communication: Right to request confidential communications of PHI
  - Access: Right to access and copy PHI
  - Amendment: Right to amend PHI
  - Accounting: Right to receive an accounting of disclosures of PHI

HIPAA Security Rule

- Protects electronic or "e-PHI"
  - Against any reasonably anticipated threats or hazards to security or integrity of e-PHI
  - Against any reasonably anticipated uses and disclosures of e-PHU not permitted or required under the Privacy Rule
- Administrative Safeguards (e.g., workforce security, information access management, and security awareness and training)
- Physical Safeguards (e.g., workstation use, device and media controls)
- Technical Safeguards (e.g., access controls, audit controls, authentication)
- Flexible

HIPAA Breach Notification

- New requirement mandated by HITECH; OCR Released "Breach Notification Rule"
- Requires CEs and BAs to notify individuals of unauthorized acquisition, access, use or disclosure (breach) of unsecured PHI
  - Violations of Privacy Rule
  - Impermissible use or disclosure of PHI is presumed to be a breach unless CE can demonstrate low probability that PHI compromised; Four factor standard for determination
    - Nature and extent of PHI involved
    - Persons to whom disclosure made
    - Whether PHI actually viewed or acquired
    - Extent to which risk of breach mitigated
  - Exception for "secured" PHI (HHS guidance re technologies and methodologies that render PHI "secured")

HIPAA Enforcement

- No private right of action, complaints to HHS Secretary
- Enforced by HHS Office for Civil Rights and Department of Justice
- Civil Monetary Penalties (increased by HITECH) – Four Tiers
  - Unknown violations: $100 - $50,000 not to exceed $1.5/year for violations in a calendar year
  - Violations with reasonable cause: $1000 - $10,000 not to exceed $1.5/year for violations in a calendar year
  - Violations resulting from willful neglect: $10,000 - $250,000 not to exceed $1.5/year for violations in a calendar year
  - Violations resulting from willful neglect and not corrected: $50,000 not to exceed $1.5/year for violations in a calendar year
- Significant recent enforcement activity, including large settlements (e.g., CVS for $2.25 million)

42 CFR Part 2 ("Part 2")

- 42 CFR Part 2 restricts the disclosure and use of "patient identifying" information about individuals in substance abuse treatment
  - Patient identifying information: reveals that a person is receiving, has received, or has applied for substance abuse treatment
- More prohibitive that HIPAA, which generally allows disclosure of individually identifiable "protected health information" for the purposes of treatment, payment, health care operations
- Check state law requirements

Part 2: Key Definitions

- "Disclose" means the "communication of patient identifying information, the affirmative verification of another person's communication of patient identifying information, or the communication of any information from the records of a patient who has been identified."

- "Patient identifying information" means the "name, address, social security number, fingerprints, photographs of similar information by which the identity of a patient can be determined with reasonable accuracy and speed either directly or by reference to other publicly available information."

Part 2: Covered Providers

- Individual or entity must be federally assisted and hold itself out as providing, and provide, alcohol or drug abuse diagnosis, treatment or referral for treatment.
- A general medical facility has a Part 2 program if:
  - there is "an identified unit within a medical facility which holds itself out as providing, and provides, alcohol or drug abuse diagnosis, treatment or referral for treatment;" or
  - there are "medical personnel or other staff in a general medical facility whose primary function is the provision of alcohol or drug abuse diagnosis, treatment or referral for treatment and who are identified as such providers."

Part 2: Consent

- Name of program making the disclosure;
- Who is to receive the information;
- Name of the patient;
- Purpose of the disclosure;
- How much and what kind of information is to be disclosed;
- Signature of patient (and, in some States, a parent or guardian);
- Date on which consent is signed;
- Statement that the consent is subject to revocation (oral or written) at any time except to the extent that the program has already acted on it; and
- Date, event, or condition upon which consent will expire if not previously

Part 2: Consent, cont'd

- Part 2 allows disclosure of certain information without specific patient consent:
  - Communications within a program or between a program and an entity having direct administrative control over that program
  - Communications between a program and a qualified service organization (QSO)
  - Medical emergencies, research activities and audit or evaluation activities

Caveat: Re-disclosures — secondary disclosures stemming from an initial one — are prohibited unless made back to the program from which the information was obtained

HRSA Grant Recipients (FQHCs, Title X Family Planning Providers, Maternal and Child Health)

- Regulation requires:
  - Providers must keep confidential all information as to personal facts and circumstances [about patients] obtained by the project staff
  - Providers shall not divulge a patient's individual information unless the provider has patient consent, the release is necessary to provide services to the patient, or state or federal law requires the release (with appropriate safeguards for confidentiality)
  - Otherwise information may be disclosed in summary, statistical, or other form which does not identify particular individuals

Family Educational Rights and Privacy Act (FERPA)

- Scope: FERPA applies to all educational agencies and institutions that receive federal education funding (e.g., public schools and school districts, private and public colleges, universities, and other postsecondary institutions, including medical and other professional schools).
- Records Protected: FERPA protects "education records" that contain information about a student and are maintained by an education agency or institution (e.g., immunization records, records held by school nurse). Note: HIPAA does not apply to education records.
- Disclosure: An educational agency or institution (or its agent) may disclose "education records" only with written parental consent or the consent of a student age 18 or older or enrolled in a postsecondary institution.

FERPA, cont'd

- Exceptions:
  - Where the disclosure is to the parents a student and the student is considered a dependent for tax purposes;
  - Where a disclosure is required by law;
  - Where the disclosure is to accrediting organizations to perform accrediting functions;
  - Where disclosure is needed in an emergency to protect the health and safety of the student or others; and
  - Where the disclosure involves registered sex offenders or the disclosure of drug and alcohol violations to parents so long as the student is under 21 and the student's use or possession constitutes a disciplinary violation.

State Law

- Minors
- HIV/AIDS Status
- Family Planning Services
- Mental Health

Take-Away Message

- Well-crafted patient authorizations and informed consent so that all members of a patient's treatment team can share information related to treatment and care management
- Explanation of treatment team and patient engagement with discharge planner and care manager in designating and updating treatment team membership and information
- Prudent sharing and secure systems

New Resource: www.healthinfolaw.org

- All federal and state laws relating to the use and exchange of health information
- Analyses of emerging issues in state and federal law affecting the transformation of the health care system
- Content: brief summaries of state and federal laws, comparative analyses, and longer, in-depth analyses, presented in multiple formats for a variety of audiences

Questions?

Jane Hyatt Thorpe, J.D.

Department of Health Policy
School of Public Health and Health Services
George Washington University
2021 K St, NW Suite 800
Washington, DC 20006
202/994-4183
jthorpe@gwu.edu

Carrie Bill, J.D.
Feldesman Tucker Leifer Fidell LLP
1129 20th, N.W.
Fourth Floor
Washington, DC 20036
(202) 466-8960
cbill@ftlf.com