HIPAA

Bryan Watters
ND DVA
Fall 2017

Agenda

- Key Definitions
- HIPAA Privacy Rule
- HIPAA Security Rule
- “Part 2” Privacy Rule
- Breach Notification Rule
- Questions

HIPAA Definitions

- Covered entity – entity subject to HIPAA
  - health care provider that conducts certain transactions electronically,
  - health care clearinghouse,
  - health plan

- Protected Health Information (PHI) (Individually Identifiable Health Information) – electronic, paper or oral information that relates to an individual's past, present or future physical or mental health or condition , the provision of health care to the individual, or the past, present or future payment for the provision of health care to the individual

- Business Associate – person or organization that performs certain functions on behalf of a covered entity that involve the use or disclosure of PHI

HIPAA Definitions, cont.

- Personal Representative – someone legally authorized to make health care decisions for an individual or to act for a deceased individual's estate
  - For HIPAA purposes, a personal representative is treated the same as the individual who is the subject of PHI
- Breach – generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information.
  - Exceptions for employees and contractors, persons authorized to access or use the PHI, and persons who cannot retain the information

HIPAA Definitions, cont.

- Unsecured PHI – PHI that has not been rendered unusable, unreadable or indecipherable to unauthorized persons through the use of certain technology or methodology specified by HHS guidance.

Fundamentals

- Covered Entities and Business Associates must keep protected health information (PHI) private and secure.
- If a Covered Entity or Business Associate fails to keep PHI private and secure, the covered entity or business associate will need to perform a breach notification.
- The Office of Civil Rights (OCR) within the federal Department of Health and Human Services (HHS) enforces HIPAA
  - Fines for noncompliance = up to $1.5 million per violation

HIPAA Privacy Rule

- Unless PHI has been "de-identified," it cannot be disclosed in any manner unless there is a legal exception that applies.
- "De-identified" information does not identify the individual and cannot reasonably be used to identify the individual
- There are 2 ways to de-identify PHI:
  - Have a qualified statistician certify it has been de-identified, or
  - Remove 17 specific data fields and have no knowledge the remaining data can be used alone – or in connection with other publicly-available information – to identify the individual

Some of the Exceptions to HIPAA's Privacy Rule

- You can release an individual's PHI (or some of it)…
  - To the individual who is the subject of the PHI
  - According to the terms of a valid release signed by the individual
  - For treatment, payment or health care operations (TPO)
  - When it is required by law
  - For certain public health activities
  - To government authorities regarding victims of abuse
  - For some law enforcement purposes
  - To prevent or lessen certain threats to health and safety
  - To carry out certain essential government functions

Law Enforcement Exception

- PHI can be released to law enforcement:
  - As required by law, including court orders, subpoenas, etc
  - To identify or locate a suspect, fugitive, missing person, material witness
  - In response to law enforcement's request for info about a victim or suspected victim
  - To alert law enforcement of a death if death is suspected to be from criminal activity
  - When PHI is believed to be evidence of a crime on CE's premises
  - In a medical emergency not on CE's premises when necessary to tell law enforcement about a crime

Sharing PHI with Family and Friends

- Do not assume you can share PHI with family or friends, even when it comes to paying for care
- Sharing PHI according to the terms of a signed authorization is always ok
- If you don't have a signed authorization, **contact your State's Attorney** to determine whether a following exception applies…

Sharing PHI with Family and Friends, cont.

- If the patient has had a chance to agree or object and has agreed (verbally or in writing), the Patient's directory information can be given out
- PHI related to a person's involvement in the patient's care can be given to that person, for example:
  - A relative can pick up a prescription if the pharmacist, in his or her discretion, believes the relative meets these criteria
  - A doctor can inform a friend about a patient's mobility limitations if the friend is transporting the patient somewhere
  - **Do VSOs have any similar situations?**
- Notification of death can be made for claims puposes.
- But remember: a patient's expressed wishes override these exceptions to the privacy rule

Sharing PHI with Department of Veterans Affairs

- Dept of Veterans Affairs entities that are covered by HIPAA can use and disclose PHI (except psychotherapy notes and disclosures for marketing purposes) to other entities within the Dept of Veterans Affairs that determine a patient's eligibility for benefits or that provide benefits to veterans under laws administered by the Secretary of Veterans Affairs
- VBA has access to VHA data but the VHA does not have access to the Veteran's claim file

“Minimum Necessary”

- Disclosures of PHI generally must be limited to the “minimum necessary” amount of PHI needed to carry out the purpose of the disclosure
- Exceptions include:
  - Disclosure to a provider for treatment of the patient
  - Disclosures made according to the terms of a patient’s signed authorization
  - Disclosures required by law
- How do you apply this to Private Treatment Records submitted to VBA for a claim?

Incidental Uses and Disclosures

- These are uses and disclosures that occur incident to a permissible or required use or disclosure. For example,
  - A visitor sees a Veteran's name on your desk
  - Cleaning personnel see Veteran's names on files your desk
- Consider whether you can take reasonable steps to minimize incidental uses and disclosures
  - Ensure personnel are trained to have discussions involving PHI in locations where they are unlikely to be overheard
  - Take privacy into consideration when handling Veteran's files

HIPAA Security Rule

- Covered Entities must:
  - Ensure the confidentiality, integrity and availability of electronic PHI (e-PHI) they create, receive, maintain or transmit,
  - Identify and protect against reasonably anticipated threats to the security or integrity of e-PHI,
  - Protect against reasonably anticipated, impermissible uses or disclosures of e-PHI, and
  - Ensure compliance with HIPAA by their workforce

Security Rule Requirements

- To meet the requirements of the security rule, covered entities must:
  - Perform Risk Analyses to determine what needs to be done to secure PHI, detect breaches and unauthorized disclosures of PHI, evaluate the effectiveness of security measures
  - Implement Administrative Safeguards (eg, policies, training)
  - Implement Physical Safeguards for physical facilities and electronic media
  - Implement Technical Safeguards (eg, controlling access to e-PHI)

42 C.F.R. 2 ("Part 2")

- Information that:
  - (1) would directly or indirectly identify a patient of a federally-assisted alcohol or drug abuse program and
  - (2) pertains to the identity, diagnosis, prognosis or treatment of the patient and
  - (3) is maintained in connection with the performance of any federally-assisted alcohol or drug abuse program

is confidential and may not be disclosed unless the patient has consented in writing to the disclosure or there is a legal exception allowing the disclosure.

Part 2, cont.

- To rely on a patient's consent, you must use a specific Part 2 consent form. A general HIPAA consent form without the required Part 2 language is not sufficient.

- Part 2 records may not be used to initiate or substantiate criminal charges against the patient unless there is a qualifying court order.

Exceptions to Part 2 Prohibition on Disclosure

- Health care providers can disclose information protected by Part 2:
  - To medical providers in a medical emergency
  - To law enforcement when there is an immediate threat to the health or safety of an individual due to a crime on the provider's premises or against the provider's personnel
  - To law enforcement about an immediate threat to the health or safety or an individual or the public that do not meet another exception (patient-identifying information may not be disclosed)
  - To report child abuse or neglect to appropriate state or local authorities
  - As ordered by a court

Breach Notification

- Covered entities and business associates must provide notifications of breaches involving unsecured PHI.
  - Notify affected individuals and, if the breach is discovered by a business associate, notify the relevant covered entity "without unreasonable delay" and no later than 60 days following discovery of the breach
  - For a breach that affects more than 500 residents of a state or jurisdiction, notify "prominent" media "without unreasonable delay" and no later than 60 days following discovery of the breach
  - Notify HHS at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.
    - For a breach that affects more than 500 residents of a state or jurisdiction, notify HHS "without unreasonable delay" and no later than 60 days following discovery of the breach.
    - For other breaches, notify HHS no later than 60 days after the end of the calendar year in which the breach is discovered.

Breach Notification, cont.

- There are regulatory requirements for breach notification contents and methods. Contact your States Attorney for more guidance if you believe you may need to undertake a breach notification.

Other HIPAA Responsibilities

- Identify a Privacy Officer
- Establish and implement HIPAA Policies and Procedures
- Establish and implement a process for individuals to submit HIPAA-related complaints and to ensure their resolution
- Develop workforce training on HIPAA and ensure training occurs on an appropriate schedule
- Develop and utilize sanctions for workforce violations of HIPAA policies and procedures
- Take steps to mitigate any breaches
- Do NOT retaliate against workers or patients who report HIPAA violations or exercise rights under HIPAA
- DOCUMENT, DOCUMENT, DOCUMENT!

Discussion and Questions

- Do use cell phones? Are they *ever* used to transmit or discuss PHI? Do the cell phones comply with the security rule?
- Have you undertaken a Security Risk Assessment lately? https://www.healthit.gov/providers-professionals/security-risk-assessment
- When was the last time you trained your employees, volunteers and contractors on HIPAA?
- How do you dispose of paper and electronic PHI?
- Are there times you think it is in the patient's best interest not to share PHI with a family member involved in his or her care?
- What do you do if a patient demands a copy of his or her entire medical claim file?

Online Resources

- HIPAA Privacy Rule: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html
- HIPAA Security Rule: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
- Part 2: http://archive.samhsa.gov/healthPrivacy/docs/EHR-FAQs.pdf
- Guidance to Render PHI Unusable, Unreadable or Indecipherable to Unauthorized Individuals: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html