Health Insurance Portability and Accountability (HIPAA) Training for myQIportal/myCasereview

Midwest Regional Children's Advocacy Center

Children's MINNESOTA

Course Outline

1. **Applicability**
2. **Protected health information (PHI)**
3. **Security Safeguards**
   - Administrative
   - Physical
   - Technical
   - Scenarios
4. **Privacy**
   - Use and disclosure
   - Minimum necessary
   - Verification
   - De-identification
   - Limited data sets
   - Business associates
   - Individual rights
   - Scenarios
5. **Breach Notification**
   - Scenarios

Children's MINNESOTA

Applicability

- The HIPAA privacy, security, and breach notification rules apply to:
  1. Health plans;
  2. Health care clearing houses; and
  3. Health care providers who transmit any health information in an electronic transaction as covered by HIPAA
- If you fit one of the three descriptions listed above you are a Covered Entity.
- HIPAA also applies to business associates. A business associate is a person or entity, that is not part of your workforce, that on behalf of your covered entity, creates, receives, maintains, or transmits protected health information for a function or activity regulated by HIPAA.

Protected Health Information (PHI)

- **Protected Health Information** means individually identifiable health information, including demographic information, that is created or received by a covered entity, and relates to:
  1. the past, present, or future physical or mental health or **condition** of an individual;
  2. **provision** of health care to an individual; or
  3. the past, present, or future **payment** for the provision of health care to an individual.
- PHI can exist:
  1. Electronically
  2. On paper, or
  3. Verbally

Children's MINNESOTA

Security Safeguards

- Covered Entities must implement administrative, physical and technical safeguards to:
  1. ensure the **confidentiality**, **integrity**, and **availability** of all electronic PHI (e-PHI)
  2. Protect against any reasonably anticipated threats or hazards to the security of e-PHI
  3. Protect against any reasonably anticipated uses or disclosures of e-PHI that are not permitted under HIPAA

- When deciding which security measures to implement a covered entity should consider the following factors:
  1. Your size and complexity
  2. Your technical environment
  3. Costs of security measures, and
  4. Probability and criticality of security risks

Children's MINNESOTA

Security Safeguards (Administrative)

- Administrative safeguards are administrative actions, and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect e-PHI and to manage the conduct of your workforce in relation to the protection of e-PHI.

  Examples include:

  1. Analysis of risks and vulnerabilities
  2. Management plan to address risks and vulnerabilities
  3. Sanctions policy
  4. Assign security responsibility to an individual
  5. Audit activity within your information systems
  6. Access controls for workforce
  7. Security awareness training
  8. Security incident plans
  9. Contingency plans

Security Safeguards (Physical)

- Physical safeguards are physical measures, policies, and procedures to protect your e-PHI electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

Examples include:

1. Facility access controls
2. Workstation use procedures
3. Device and media procedures

Security Safeguards (Technical)

- Technical safeguards means the technology and the policy and procedures for its use that protect e-PHI and control access to it.

  Examples include:

  1. Access controls that limit access to authorized individuals
  2. Audit controls
  3. Integrity controls that prevent improper alteration or destruction
  4. Person or entity authentication to confirm someone seeking access is who they claim to be
  5. Transmission security to guard against unauthorized access over a communications network (Encryption)

Privacy

- A covered entity or business associate may not use or disclose PHI except as permitted or required by HIPAA.
- **Permitted uses and disclosures of PHI include:**
  1. To the individual the PHI pertains or the individual's personal representative
  2. For treatment, payment, or health care operations
  3. Incident to a use or disclosure permitted or required under HIPAA
  4. Pursuant to and in compliance with a valid authorization
  5. Pursuant to situations that allow an individual to agree or object to the use or disclosure
- **Required disclosures:**
  1. To an individual when requested pursuant to a HIPAA compliant request
  2. When required by the Secretary of Health and Human Services

Privacy (Use and Disclosure)

- **Treatment, Payment, and Health Care Operations**
  - In general, a covered entity can:
    - use or disclose PHI for its own treatment purposes
    - Disclose PHI to another health care provider for treatment purposes
    - Disclose PHI to another covered entity for the payment purposes of the covered entity
    - Disclose PHI to another covered entity for health care operations activities if each entity has or had a relationship with the individual who is the subject of the PHI
  - In general, **health care operations** includes:
    - conducting quality assessment activities,
    - Reviewing the competence or qualifications of health care professionals
    - Training and education
    - Conducting medical reviews and compliance evaluations
    - Business management and general administrative activities

Children's MINNESOTA

Privacy (Use and Disclosure)

- **Use and disclosures requiring a valid authorization**
  - A covered entity must acquire a valid authorization prior to disclosing PHI for the following purposes:
    1. Disclosure of Psychotherapy notes
    2. Marketing
    3. Sale of PHI
- **Uses and disclosures requiring the ability to Opt-Out**
  - A covered entity may use of disclose PHI for the following purposes provided the individual is informed in advance of the use or disclosure and has an opportunity to opt-out or restrict the use or disclosure:
    1. Facility directories; and
    2. To friends and family involved in the individual's care

Privacy (Uses and Disclosures)

- Uses and Disclosures where an **authorization or opt-out is not required.** In general, these uses and disclosures are to facilitate public health programs and law enforcement.

  Examples include disclosures:

  1. to certain public health authorities
  2. about abuse or neglect
  3. for certain health oversight activities
  4. for judicial and administrative proceedings
  5. For certain law enforcement purposes
  6. To coroners, medical examiners, and funeral directors
  7. For organ, eye, and tissue donation
  8. To avert serious threat to health and safety
  9. For specialized government and military functions

Privacy (Minimum necessary)

- When using or disclosing PHI or when requesting PHI from another covered entity or business associate, you must make reasonable efforts to limit PHI to the *minimum necessary to accomplish the intended purpose of the use, disclosure, or request*.
- The minimum necessary rule does not apply to the following:
  1. Disclosures to or requests by a health care provider for treatment
  2. Uses and disclosures made by the person the PHI pertains
  3. Uses and disclosures made pursuant to an authorization
  4. Disclosures made to the secretary
  5. Uses and disclosures required by law
  6. Uses and disclosures that are required to comply with HIPAA

Privacy (Verification)

- Prior to any disclosure a covered entity must verify:
  - the identity of a person requesting PHI, and
  - The authority of any such person to have access to PHI

Here are some ways verification of identity can be achieved:

1. **Requests by phone** – ask questions that only an authorized individual would know
2. **Requests in person** – ask for valid ID
3. **Requests in writing** – comparing handwriting of other documents, relying on government letter head are acceptable ways of confirming identity

Privacy (De-identification)

- Health information that does not identity an individual and with respect to which there is no reasonable basis to believe that the information can be used to identity an individual is not PHI.
- A covered entity may determine that health information is de-identified if:
  1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable **determines** that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is subject of the information and **documents** the methods and results of the analysis that justify the determination; or
  2. Specific identifiers of the individual or of relatives, employers, or household members of the individual are removed. See 45 CFR § 164.514(b)(2) for list of identifiers.

Privacy (Limited Data Sets)

- A covered entity may use or disclose a limited data set for the purposes of research, public health, or health care operations if the covered entity enters into a data use agreement with the limited data set recipient.
- A limited data set is PHI that excludes direct identifiers of the individual or of relatives, employers, or household members of the individual. See 45 CFR § 164.514(e)(2) for list of identifiers.
- HIPAA also has requirements that must be included in your data use agreement.

Children's MINNESOTA

Privacy (Individual Rights)

- When it comes to PHI, individuals have certain rights. These rights include the ability to:
  1. Get an electronic or paper copy of their medical record
  2. Request a correction of their medical record
  3. Request confidential communications
  4. Ask you to limit what information you use or share
  5. Get a list of those with whom you've shared their information
  6. Get a copy of a notice of privacy practices
  7. Choose someone to act on their behalf
  8. File a compliant if they feel their rights have been violated.

Breach Notification

- **Breach** means the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which compromises the security or privacy of the PHI.
- An acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA is **presumed a breach** unless your risk assessment determines a low probability of compromise.
- **Your breach risk assessment must evaluate the following factors:**
  1. Nature and extent of the PHI
  2. The unauthorized person who used or received the PHI
  3. Whether the PHI was actually acquired or viewed; and
  4. The extent to which risk to the PHI has been mitigated

Children's MINNESOTA

Breach Notification

- A breach is **considered discovered** by the covered entity or business associate as of the first day a workforce member or agent of the covered entity knows or should have known of the breach.
- **Notifications:**
  - **Individual** notification must be made no later than 60 days after discovery of the breach.
  - **Media** notification for a breach affecting greater than 500 individuals in one jurisdiction must be made no later than 60 days after discovery of the breach.
  - **Secretary** notification for a breach:
    - Affecting greater than 500 individuals must be made no later than 60 days after discovery of the breach.
    - Affecting less than 500 individuals must be made no later than 60 days after each calendar year
  - **Business associates**, in general, should notify the covered entity associated with the breach. The business associate agreement should have specific details regarding this notification.

Children's MINNESOTA

Additional HIPAA Resources

- Here are some additional resources regarding the HIPAA privacy, security, and breach notification rule:

  – The Office for Civil Rights HIPAA for Professionals web site.
  http://www.hhs.gov/hipaa/for-professionals/index.html

  – The Health IT.gov Privacy and Security web site.
  https://www.healthit.gov/providers-professionals/ehr-privacy-security

Children's MINNESOTA