Jumpstart Your HIPAA Compliance

By
Sheila Mints, Esq.
smints@capehart.com
856.840.4945
No Disclosures
October 30, 2019
HIPAA History – 2003 to 2008

- Privacy
- Electronic Transactions and Code Sets
- National Provider Identifier
- Security
HIPAA Privacy

- Applies to all forms of Protected Health Information (PHI)
- Requires safeguards be in place
  - Administrative
  - Physical
  - Technical
HIPAA Privacy

- Should already have in place:
  - Notice of Privacy Practices
  - HIPAA compliant authorizations
  - Policy & Procedure Manual
  - Business Associate Contracts
New HIPAA – The HITECH Act

- Promotes EHRs
- Expands HIPAA privacy & security requirements and protections
- Business Associates directly governed by HIPAA
- Increases penalties
- New Federal Data Breach Notification requirement
What is Protected Health Information (PHI)?

- Protected Health Information (PHI) is individually identifiable health information that is:
  - Created or received by a health care provider, health plan, employer, or health care clearinghouse and relates to:
    - The past, present, or future physical or mental health or condition of an individual
    - The provision of health care to an individual
    - The past, present or future payment for the provision of health care to an individual
What Does PHI Include?

- Information in the health record, such as:
  - Encounter/visit documentation
  - Lab results
  - Appointment dates/times
  - Invoices
  - Radiology films and reports
  - History and physicals (H&Ps)
  - Patient Identifiers
What are Patient Identifiers?

- PHI includes 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.
Examples of Patient Identifiers

- Names
- Medical Record Numbers
- Social Security Numbers
- Account Numbers
- Health plan numbers
- Any dates related to an individual
- Telephone numbers
- Fax numbers
- Email addresses
- Biometric identifiers
- Other unique identifying number, characteristic or code
- Full face photographic images
What Are Uses and Disclosures?

- Uses – When you review or use PHI internally, (e.g., medical care, billing, audits, training, or quality improvement)
- Disclosures – When you release or provide PHI to someone (e.g., attorney, patient, biller, to another provider)
What is Minimum Necessary?

- To use or disclose/release only the minimum necessary to accomplish intended purposes of the use, disclosure, or request
- Requests from your employees
  - Identify each workforce member who needs to access PHI
  - Limit the PHI provided on a “need-to-know” basis
What is Treatment, Payment and Health Care Operations (TPO)?

- HIPAA allows Use and/or Disclosure of PHI without need for patient authorization for purpose of:
  - **Treatment** – providing care to patients
  - **Payment** – billing/reimbursement, the provision of benefits and premium payment
  - **Health Care Operations** – other business activities (e.g., reporting, quality improvement, training, auditing, customer service and resolution of grievances, data collection, eligibility checks and accreditation)
Enforcement
How are the HIPAA Regulations Enforced?

- **Patients.** Patients are “knowledgeable” about their privacy rights and will take action

- **Office For Civil Rights (OCR).** The federal agency that enforces the privacy regulations providing guidance, monitoring compliance, auditing, investigating

- **Department of Justice (DOJ).** Federal agency involved in criminal privacy violations, assessing fines, penalties and imprisonment to offenders

- **State Attorney General.** Authorized to enforce HIPAA
Patient Rights
HIPAA Regulations

What are the Patient’s Rights Under HIPAA?
- The Right to Privacy of Their Medical Information
- The Right to Expect Health Care Providers Will Protect These Rights

Other Patient Rights Include:
- Access, Communications, Special Requests, Amendment, Accounting of Disclosures, Notice of Privacy Practices, Right to File Complaints
Notice of Privacy Practices (NPP)

- Purpose of the NPP?
  - Summarizes how the organization uses and discloses patient’s PHI
  - Details patient’s rights with respect to their PHI
Notice of Privacy Practices (NPP)

- Must request that new patients sign the NPP acknowledgment form at the time of their first visit
  - Patients sign the Acknowledgment to confirm they have been offered and/or received the NPP
  - If unable to obtain a signed Acknowledgement, must document good faith effort to obtain and reason why it couldn’t be obtained
Access and Inspect PHI

◦ Patients have the right to inspect and obtain a copy of their PHI

◦ Some situations where access may be denied or delayed:
  ◦ Psychotherapy notes
  ◦ PHI compiled for civil, criminal or administrative proceedings
  ◦ Access would endanger a person’s life or safety based upon professional judgment
Request Alternate Communication

- Patient has the right to request to receive communication by alternative means or location
- For example:
  - Patient requests a bill be sent to a different address than home
  - Patient requests contacting her on cell phone instead of home telephone number
- Have a process in place to document the patient’s wishes in his/her medical record
Request Amendment

- Patient has the right to request an amendment or correction to PHI
- Situations when request may be denied include:
  - Organization did not create the information
  - Record is accurate according to health care professional that created it
HIPAA Privacy Administrative Requirements
Privacy Officer

- Privacy Officer Responsibilities
  - Implement policies and procedures of the entity
  - Receive and address complaints regarding Privacy
  - Provide additional information to patients as requested about matters covered by the Notice of Privacy Practices

- Designation of the Privacy Officer must be documented
Policies and Procedures

- Implement policies and procedures designed to comply with the HIPAA Rules
- Change policies and procedures as necessary and appropriate to comply with changes in the law and revise Notice of Privacy Practices
- Document all changes made to policies and procedures and maintain all policies for 6 years
- Train employees on changes made to policies and procedures
Training

- Members of the workforce who handle PHI require training
  - Required upon hire and annually
  - As material changes are implemented, training to workforce members affected by that change
  - Documentation of the training, who attended, the topic covered and date the training was held
Documentation

- Must maintain all compliance documentation for 6 years from the date of its creation, including:
  - Policies and procedures in written or electronic form
  - Communications in written or electronic form when such communications are required in writing
  - Written or electronic records of actions, activities, or designations as required
Business Associates
Business Associates

- Who is a Business Associate?
- What Must a Business Associate Do?
- What Happens if it Doesn’t?
- Business Associate Contracts
- Action Items
Who is a Business Associate?

- Creates, receives, maintains, or transmits PHI
- On behalf of a covered entity
- Provides certain identified services involving PHI
- Examples: legal, actuarial, accounting, billing
BA Subcontractors

- Subcontractor + PHI = Business Associate Subcontractor
- Subcontractor = person to whom a BA delegates a function, activity or service that involves access to PHI
- Not workforce member
Business Associate Obligations

- Required by HIPAA (penalties for noncompliance)
- Required by business associate contract (only breach of contract for noncompliance)
- Best practices
Investigations
Investigations

- Who may investigate?
  - HHS Office for Civil Rights
  - State attorneys general
  - U.S. Department of Justice

- How will investigation begin:
  - Complaint
  - Compliance review
  - Breach report
  - Audit
Civil Penalties

- HHS
  - $100 to $50,000 or more per violation
  - Up to $1.5 million per calendar year for all violations of an identical provision
  - Limits are per type of violation, e.g., four types of continuous violations over three years can equal $18 million
Civil Penalties

- **State attorneys general:**
  - Up to $100 per violation
  - Up to $25,000 per calendar year for all violations of an identical provision
  - Attorneys’ fees
Criminal Penalties

- Department of Justice (knowingly obtaining or disclosing PHI in violation of HIPAA
  - $50,000 and/or up to one year imprisonment
  - $100,000 and/or up to five years imprisonment if false pretenses
  - $250,000 and/or up to ten years imprisonment if commercial advantage, personal gain or malicious harm
Breach Notification
Data Breach Notice – To Whom?

- Every affected individual
  - Current patients
  - Former patients
- Or their representative if:
  - Deceased
  - Minor
  - Incompetent
- HHS/Media (in some cases)
Data Breach Notice – HHS

○ More than 500 persons
  ○ Within 60 days of discovery

○ Fewer than 500 persons
  ○ Annual Electronic Report
  ○ Within 60 days of calendar year end

○ See HHS website for form & instructions: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinSTRUCTION.html
Thank you.

Sheila M. Mints, Esq.
Capehart & Scatchard, P.A.
8000 Midlantic Dr., Ste 300S
P.O. Box 5016
Mt. Laurel, NJ 08054
Phone - (856) 840-4945
Fax - (856) 235-2786

This presentation has been carefully prepared but it necessarily contains information in summary form and is therefore not intended to be a substitute for detailed research or the exercise of professional judgment. The information presented should not be construed as legal, tax, accounting or any other professional advice or service.
These materials reflect the views of the authors and not necessarily the views of Capehart Scatchard or the Firm’s other attorneys and professionals.

These materials are for educational and informational purposes only. They are not intended to be a substitute for detailed research or the exercise of professional judgment. This information should not be construed as legal, tax, accounting or any other professional advice or service.