Protecting Patient Information in an Electronic Environment - New HIPAA Requirements

SD Dental Association

Holly Arends, RHIT
Clinical Program Manager
Meet the Speaker
TRUST
OBJECTIVES

• Overview of HIPAA basic requirements
• Identify the Omnibus rule changes (new)
• Learn ways to operationalize the Administrative safeguards, physical safeguards, and technical safeguards.
• Understand individual responsibilities under HIPAA
HIPAA

Accountability

Privacy

Security

Electronic Data Interchange (EDI); Transaction Code Sets

ICD 9, 10; CPT 4; Dental claims status, eligibility, HCPCS, NDC

National Identifiers

EIN, NPI, NHI

Portability

Transferable Insurance
HIPAA 101

- Health Insurance Portability and Accountability Act of 1996
- Goal: Improve efficiency and effectiveness of health care system *by standardizing* the electronic exchange of administrative and financial data
- Effective in 2003 Privacy Rule and 2005 Security Rule
- Divided into Accountability and Portability Standards
HIPAA Omnibus Important Dates

- Published in Federal Register – January 25, 2013
- Effective Date – March 26, 2013
- Compliance Date – September 23, 2013
- Transition Period to Conform BA Contracts – Up to September 22, 2014, for Qualifying Contracts
Omnibus Components

- **HITECH Privacy & Security**
  - Business associates
  - Marketing & Fundraising
  - Sale of PHI
  - Right to request restrictions
  - Electronic access
- **HITECH Breach Notification**
- **HITECH Enforcement**
- **GINA Privacy**
- **Other (non-statutory) Modifications**
  - Research
  - Notice of privacy practices (NPP)
  - Decedents
  - Student immunizations
ePHI- Electronic Protected Health Information

- Created, received, maintained or transmitted electronically
Who must comply with the Rules?

- Covered Entities
  - Business Associates
    - Subcontractors
Electronic Transactions

- ASC2 X12 837 Health Care Claim: Professional
- ASC X12 835 Health Care Claim Payment/Remittance Advice
- ASC X12 276 Heath Care Claim Status Request
- ASC X12 277 Health Care Claim Status Response
- ASC X12 270 Health Care Eligibility Benefit Inquiry
- ASC X12 271 Response
- ASC X12 278 Health Care Services Review Information - Review
- ASC X12 278 Health Care Services Review Information - Response
- ASC X12 837 Health Care Claim: Professional
- ASC X12 834 Benefit Enrollment and Maintenance
- ASC X12 820 Payment Order and Remittance Advice
What are the Responsibilities?

• Practice level
  ▫ Policies and Procedures
    • Privacy Rule
    • Security Rule
• Individual level
  ▫ Carry out the established policies
Privacy Rule

• Purpose
  ▫ Restrict the unwarranted disclosure of PHI
  ▫ Give individual greater control over access
  ▫ Enable providers to use information to make decisions and fulfill obligations
Privacy Standards Scope

- Identifiable information
- Information that describes an individual's health status, including demographics and services provided
- All PHI - regardless of format
The Rights To Empower

- Right to Access
- Right to Amend
- Right to Accounting of Disclosures
- Right to Notice of Privacy Practices
- Right to Agree or Object
- Right to Request Restriction
Right to Access

NEW RULE:

• Copy in Electronic format, if requested
• Provide in another readable electronic form
• Access allowed or denial furnished within 30 days
Put It Into Practice

- Identify the readily available formats in your practice
- Create the workflow of how you flag those individuals that are requesting an electronic copy
- Identify responsible dept./person for tracking
Right to Request a Restriction of Uses

• NEW RULE:
  Individual can requests a restriction on disclosure pursuant to § 164.522, and the CE must agree to the requested restriction unless the disclosure is otherwise required by law, if the request for restriction is on disclosures of protected health information to a health plan for the purpose of carrying out payment or health care operations and if the restriction applies to PHI that pertains solely to a health care item or service for which the health care provider has been paid out of pocket in full.
Put It Into Practice

- Don’t create separate records
- Employ some type of flagging system
- Try to unbundle the services, if not possible
  Educate the patient on consequences of unbundling services
- Does not apply to follow up visits related to the health care service
- Downstream providers are the patients responsibility
Elements of the Privacy Rule

- Maintaining, Updating, and Approving P&P
- Designate a responsible official
- Delineate responsibilities and authority
- Staff Training
  - Role based
- Compliance and Sanctions
  - Unintentional
  - Intentional
  - Technical
Elements of the Privacy Rule

• Reporting, Investigation, Documenting violations
• Use and Disclosure of information in all situations
  ▫ TPO
  ▫ Law enforcement
  ▫ Authorized
  ▫ Required by Law
• Access, Restrictions, Amendments to Information
Elements of the Privacy Rule

• Notice of Privacy Practices
• Authorization to Release Information
• Accounting for Disclosures
• Minimum Necessary
• Fees
• Business Associates
Notice of Privacy Practices

- Formal notice
- Direct Treatment relationship
- Amendment to form
  - Breach notification
  - Disclosure to health plan
  - Marketing
  - Sale of PHI
  - Fundraising and how to Opt out
Put It Into Practice

• Adopt the new NPP template
• Provide amended NPP to patients
• Use this tool as more than an administrative burden
  ▪ A clear message to patients of your dedication to privacy
  ▪ Compliance documentation for HIPAA audit
Fees

• Determining a reasonable fee
  ▫ Labor
  ▫ Media cost/Supplies
• Excludes Retrieval Fees
Put It Into Practice

- Identify those individuals responsible for the retrieval of electronic patient information
- Cost analysis of typical data set request, auditable
- Update policies with prices
- Notify patients at time of request
- Review on an annual basis for cost +/-
Business Associates

• **Who are my Business Associates?**
  - On behalf of CE
  - Creates, receives, maintains, or transmits PHI
NEW RULE:
Business associate includes a “subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.”
Clarifies the definition of “subcontractor” in § 160.103 to provide that subcontractor means: “a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.”
Business Associates

NEW RULE:
The final rule adopts the language that expressly designates as **business associates**: (1) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires routine access to such protected health information; and (2) a person who offers a personal health record to one or more individuals on behalf of a covered entity.
Business Associates

- Business associates (BA) must comply with the technical, administrative, and physical safeguard requirements under the Security Rule; directly liable for violations.

- BAs must comply with the use or disclosure limitations expressed in BA contract and those in the Privacy Rule; directly liable for violations.

- BA definition expressly includes Health Information Organizations, E-prescribing Gateways, and PHR vendors that provide services to covered entities.

- Subcontractors of BA are now defined as BAs.
  - BA liability flows to all subcontractors.
Business Associates Examples

- Claims processing or administration
- Data analysis, Processing, Administration, Aggregation
- Utilization review
- Quality Assurance
- Billing
- Benefit Management
- Practice Management
- Legal
- Accounting
- Consulting
- Data Center
- Cloud Hosting organizations
- Patient Safety Activities
- eRx gateway
- Financial services
- Personal Health Record Vendors
Business Associate Examples

• Why isn’t the SD Health Information Exchange on this list?

• Conduit Exception
  ▫ US Post Office
  ▫ Electronic Equivalents

• Further Guidance from OCR
• Merely transmission service
Put It Into Practice

• Identify all of those person/organizations that do work on your behalf, and those that may have subcontractors
• Adopt the new BAA template
• Review the functions and change language to reflect those specific functions
• Renew your BAAs by the deadlines
Elements of the Privacy Rule

• Marketing and Fundraising
• Sale of PHI
• Research
• Decedents
Marketing & Fundraising

• Marketing
  ▪ Communications about health-related products and services by covered entity to individuals now marketing and require authorization if paid for by third party
  ▪ Limited exception for refill reminders (and similar communications)
    • Payment must be reasonably related to cost of communication
  ▪ Face to face marketing communications and promotional gifts of nominal value still permitted without authorization

• Fundraising
  ▪ Covered entity (CE) may use additional information to target fundraising communications but must provide easy way for individuals to stop receiving solicitations
Sale of PHI

• Even where disclosure is permitted, CE is prohibited from disclosing protected health information (PHI) (without individual authorization) in exchange for remuneration
  ▫ Includes remuneration received directly or indirectly from recipient
  ▫ Not limited to financial remuneration

• If authorization obtained, authorization must state that disclosure will result in remuneration
Sale of PHI

• Exceptions:
  ▫ Treatment & payment
  ▫ Sale of business
  ▫ Remuneration to BA for services rendered
  ▫ Disclosure required by law
  ▫ Public health
  ▫ Research, if remuneration limited to cost to prepare and transmit PHI
  ▫ Providing access or accounting to individual
  ▫ Any other permitted disclosure where only receive reasonable, cost-based fee to prepare and transmit PHI
Research Authorizations

• Compound Authorizations
  ▫ Single authorization form permitted for use/disclosure of PHI for conditioned and unconditioned research activities, with clear opt in for voluntary (unconditioned) component
  ▫ Flexibility permitted on ways to differentiate the components

• Future Use Authorizations
  ▫ Permitted so long as authorization for future research includes adequate description such that it would be reasonable for the individual to expect his or her PHI could be used for the research

• Aligns with Common Rule informed consent requirements
Decedent Information & Student Immunizations

**Decedent Information**
- Decedent’s information is no longer PHI after 50-year period
- CE may disclose decedent’s PHI to family members and others involved in care/payment for care of decedent prior to death, unless inconsistent with prior expressed preference

**Student Immunizations**
- CE may disclose proof of immunization of child to schools in States with school entry laws with oral or written agreement of parent
Anyone Need a Break?!?!??
Security Rule

• Purpose
  ▫ CE to Implement Safeguards
  ▫ Protect Confidentiality, Integrity, Availability of ePHI
Security Standards Scope

• ePHI
Elements of the Security Rule

- Safeguards
  - Administrative
  - Physical
  - Technical
Administrative Safeguards

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
Security Management Process

- Risk Analysis
- Risk Management
- Sanction Policy
- Information System Activity Review
Put Into Practice

• Conduct a Security Risk Analysis
  ▫ PHI Inventory
  ▫ Criticality
  ▫ Threat/Vulnerabilities

• Create your Risk Management Plan

• Identify who will do the review of audit logs, frequency (daily), and flags
Information Access Management

- Isolating Health Care Clearinghouse functions
- Access Authorization
- Access Establishment and Modification
Administrative Safeguards

• Security Awareness and Training
  ▫ Security Reminders
  ▫ Protection from Malicious software
  ▫ Password Management
  ▫ Log in Monitoring
Put It Into Practice

• Password Management
  ▫ Strong Passwords
    • At least 8 characters, no recognizable words, combination of letters and numbers, at least 1 upper case letter, and 1 special character
    • Changed routinely – quarterly recommended
    • Don’t share passwords
    • Don’t write them down
    • Change default passwords immediately
    • No shared logins
Administrative Safeguards

- Security Incident Procedures
- Contingency Plan
  - Data Backup Plan
  - Disaster Recovery Plan
  - Emergency Mode Operation Plan
  - Testing and Revision Procedures
  - Applications and Data Criticality Analysis
- Evaluation
- Business Associate Contracts and other Arrangements
Physical Safeguards

- Facility Access Controls
- Workstation use
- Workstation Security
- Device and Media Controls
  - Disposal
  - Media Re-use
  - Accountability
  - Data Back up and Storage
Put It Into Practice

• Device and Media Controls
  ▫ Disposal- unusable, inaccessible
  ▫ Re-Use- Permanently delete, Wipe
  ▫ Accountability – Logs , Documentation
  ▫ Data Back up and Storage – exact copy
Remote Access

• Be Cautious
• Cases that warrant remote access
  ▫ Mobile providers
  ▫ On Call providers
• Have a way to review the cases that you are going to allow remote access – document!!
• Train staff to understand the risks of remote access
Remote Access

• Three areas to review
  ▫ Access
  ▫ Storage
  ▫ Transmission
Technical Safeguards

• Access Control
• Audit Controls
• Integrity
• Person or Entity Authentication
• Transmission Security
Put It Into Practice

• Access Control
  ▫ Unique User Identification
  ▫ Emergency Access Procedure
  ▫ Automatic Logoff
  ▫ Encryption and Decryption
Encryption
Put It Into Practice

• What data should I encrypt?
  ▫ Anywhere ePHI is contained- computers, devices
  ▫ Emails that contain ePHI
  ▫ ePHI that you transmit – claims
  ▫ Back ups
  ▫ ePHI accessed via the Internet – SSL/TLS, https

• Data Mapping – understand where your data is flowing and where are the risks
“Now open even wider, Mr. Stevens... Just out of curiosity, we’re going to see if we can also cram in this tennis ball.”
What is a Breach?

- Impermissible use/disclosure of unsecured PHI presumed to require notification, unless CE/BA can demonstrate low probability that PHI has been compromised based on a risk assessment of at least:
  - Nature and extent of PHI involved
  - Who received/accessed
  - Potential that PHI was actually acquired or viewed
  - Extent to which risk to the data has been mitigated
Breach Notification

- Makes permanent the notification and other provisions of the 2009 interim final rule (IFR), with only minor changes/clarifications
  - E.g., clarifies that notification to Secretary of smaller breaches to occur within 60 days of end of calendar year in which breaches were discovered (versus occurred)
Breach Risk Assessment

- Does it violate the HIPAA privacy rule?
- Was the PHI unsecured or unencrypted?
- Does it qualify as an exception?
- Does it pose a significant financial, reputational, or other harm to the affected individual?
  - Use a rating tool

- Document Document Document
- Policy and procedure on how to address
Enforcement

• Clarify the tiers
  ▫ Lowest – reasonably could not know of the breach
  ▫ Intermediate – Knew or would have known but did not act
  ▫ Highest – acted with willful neglect

• 30 day period begins when the provider knew or should have known of the violation
Let’s stretch our HIPAA knowledge muscles

- Security Game
Summary

- Overview of HIPAA basic requirements
- Identify the Omnibus rule changes (new)
- Learn ways to operationalize the Administrative safeguards, physical safeguards, and technical safeguards.
- Understand individual responsibilities under HIPAA
Time to Change The Conversation

- Security Should Not Be Taken Lightly
- Make Security Risk Assessment a priority
- Let your patients know you value the security of their information
Stu, you are a Doctor

NOW GO GET’EM!!!!
Questions

www.healthpoint.dsu.edu