HIPAA – What You Need to Know

April 25, 2018

RKLcpa.com

FOCUSED. ON YOU.

Disclaimer

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

FOCUSED. ON YOU.

Objectives

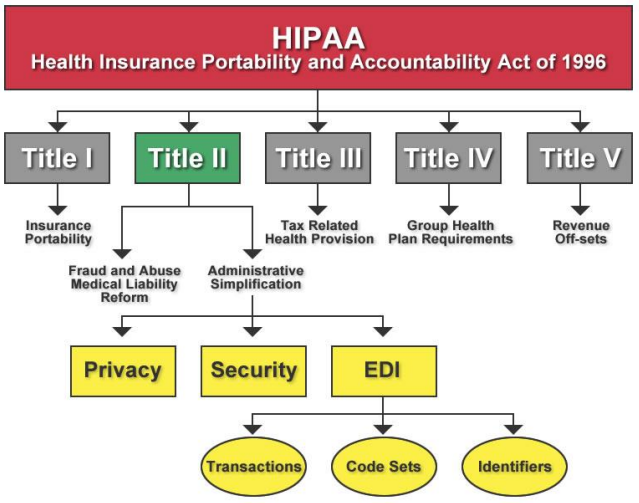
- The attendees will:
  - Gain an understanding of the HIPAA Rule
  - Identify the differences between the Security and Privacy Rules
  - Describe how HIPAA is relevant to Non-Emergency Medical Transportation
  - Recognize the criminal and civil penalties of non-compliance

FOCUSED. ON YOU.

What is HIPAA

FOCUSED. ON YOU.

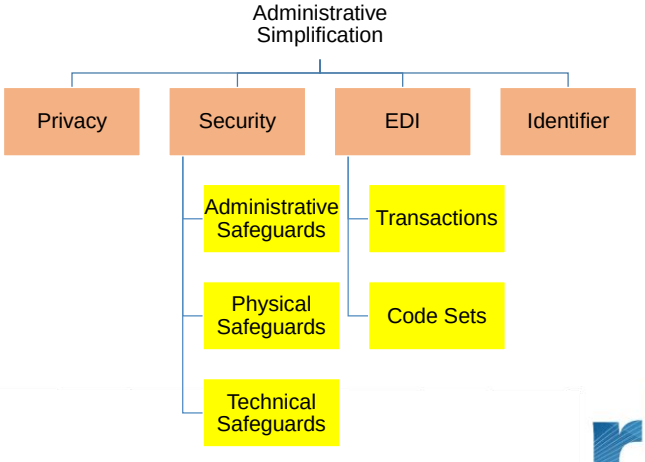
What is HIPAA



4

FOCUSED. ON YOU.

Title II



5

FOCUSED. ON YOU.

Title II

Administrative Simplification

Privacy

6

Title II - Privacy

Covered Entity and Business Associate

- Covered Entity – must comply with HIPAA regulations and standards because they transmit health information in electronic form in connection with HIPAA covered transactions
  - Health Plans
  - Health Care Clearinghouses
  - Health Care Providers
- Business Associates – A person or organization that performs a function or activity on behalf of a covered Entity, but is not part of the Covered Entity's workforce.
  - This individual or company needs to have access to PHI in order to perform a function for the Covered Entity

7

Title II - Privacy

Privacy Rule

- The Standards for Privacy of Individually Identifiable Health Information (IIHI)
  - Went into effect April 14, 2001
  - Set national standards for the protection of certain health information
  - Set real penalties for non-compliance including fines and prison time
  - The rule applies to Covered Entities as well as Business Associates

FOCUSED. ON YOU.

Title II – Privacy

Privacy Rule (cont'd)

- The Standards for Privacy of Individually Identifiable Health Information (IIHI)
  - Protected Health Information (PHI) is protected from being shared (paper, electronic, or oral)
  - With Electronic Medical Records, as of January 1, 2014, there is a greater urgency to comply with Privacy and Security Rules
    - IIHI with Patient Identifiable Information (PII) removed (i.e., ZIP, name, SSN, birthday, phone, city, etc.) is de-identified.
      - De-identified information can be used by anyone for any purpose

FOCUSED. ON YOU.

Title II - Privacy

Privacy Rule (cont'd)

- Three ways to de-identify information
  - Small Groups
  - Safe Harbor Method
  - Limited Data Set

Title II – Privacy

Using and Disclosing PHI

Use

- Sharing
- Employing
- Applying
- Utilizing
- Examining
- Analyzing

Information used when moved INSIDE organization

Disclosure

- Release
- Transfer
- Provision of access to your PHI
- Divulging in any manner

Information used when moved OUTSIDE organization

Title II - Privacy

- Mandatory disclosures
  - Patients have the right to receive a copy of their medical information
- Covered Entities are permitted to send individuals unencrypted emails if they have advised the individual of the risk and the individual still prefers the unencrypted email
- Must follow NIST standards for encryption

Title II - Privacy

- Forms
  - Consent
  - Authorization
  - Notice of Privacy Practices

Title II - Privacy

- Business Associates
  - Agreements are required
    - Exemptions for:
      - Conduits
      - Financial Institutions
      - Other Covered Entities
      - Hybrid Covered Entities
      - Employers

Title II - Privacy

- Minimal Necessity
  - The Final Rule requires that when a Business Associates use, disclose or request PHI from a Covered Entity that they limit the PHI to the minimum necessary to accomplish the intended purpose of the use, disclosure or request.
  - Reasonable steps must be taken to see that Use and Disclosure of PHI is limited to its intended use and nothing more.

Title II - Privacy

- Considerations regarding Privacy
  - Should be considered on a daily basis
  - Always protect PHI (paper, electronic, oral)
  - What can you do to improve privacy on a daily basis
- Compliance considerations
  - Assign a Privacy Officer
  - Update Notice of Privacy Practices
  - Educate staff
  - Policies
  - Obtain BAAs
  - Post reminders
  - Consider volume of voice and voice mail message wording
  - Protect audiotapes, videotapes, and photos
  - Guard cell phone dialogue (emails), text messages
  - Monitor social media

Title II

Administrative Simplification

Security

Title II - Security

- Security Standards for the Protection of Electronic Protected Health Information – Final Rule February 20, 2003
  - aka “Security Rule
  - Make sure important security safeguards are adopted to protect ePHI which may be at risk
  - Set up a methodology which permits appropriate access and use of ePHI, encouraging electronic means of using and transmitting ePHI
- The electronic exchange of ePHI has increased synergies between healthcare providers, health plans, clearinghouses and their BA
  - Significant savings
  - Increased patient safety
  - Reduced hospital readmission rates

Title II – Security

- Security breaches
  - Anthem Blue Cross
  - Equifax
  - Catholic Health Services
  - East Texas hospital
  - Aetna
  - Oregon Health and Science University
  - Lahey Hospital in Massachusetts
- Who is next? You?
  - Let’s discuss those Administrative, Physical and Technical Safeguards

Title II - Security

- The Security Rule is applicable to all healthcare information electronically maintained or used in an electronic transmission, regardless of format (standard transaction or a proprietary format).
- There is no distinction between internal corporate entity communication and communication externally to the corporate entity.
- Each of the three safeguards/standards we are going to discuss have implementation standards
  - They are required or addressable
- Two options for Standards are Compliant or Not Compliance
- Three options for Implementation Specifications are Compliant, Partially Compliant and Not Compliant

Title II - Security

- Administrative Safeguards
  - Actions, policies, and procedures to manage the selection, development, implementation and maintenance of security measures to protect ePHI and to manage the conduct of the CE's workforce in relation to reaching HIPAA compliance
  - A Risk Analysis is required by HIPAA
  - Implementation Specifications that are required – All CEs and BAs must comply
  - Policies should consider the Privacy Rule, Security Rule, HITECH Act, and Final Rule

Title II - Security

Administrative Safeguards

Standard	Implementation Specification	Required (R) or Addressable (A)
Security Management Process	• Risk Analysis • Risk Management • Sanction Policy • Information System Activity Review	R R R R
Assigned Security Responsibility		R
Workforce Security	• Authorized and/or Supervision • Workforce Clearance Procedure • Termination Procedure	A A A

22

Title II - Security

Administrative Safeguards (cont'd)

Standard	Implementation Specification	Required (R) or Addressable (A)
Information Access Management	• Isolation Healthcare Clearinghouse Function • Access Authorization • Access Establishment and Modification	R A A
Security Awareness and Training	• Security Reminders • Protection from Malicious Software • Log-in Monitoring • Password Management	A A A A
Security Incident Procedure	• Response and Reporting	R

23

Title II - Security

Administrative Safeguards (cont'd)

Standard	Implementation Specification	Required (R) or Addressable (A)
Contingency Plan	• Data Backup Plan • Disaster Recovery Plan • Emergency Mode Operation Plan • Testing and Revision Procedure • Applications and Data Criticality Analysis	R R R A A
Evaluation		R
Business Associate Contracts and Other Arrangements	• Written Contract or Other Arrangement	R

Title II - Security

- Physical Safeguards
  - Physical Safeguards are a series of Security rule requirements which are meant to protect a CEs electronic information system from unauthorized physical access to PHI (internal and external)

Title II - Security

- Physical Safeguards

Standard	Implementation Specification	Required (R) or Addressable (A)
Facility Access Controls	• Contingency Operations • Facility Security Plan • Access Control and Validation Procedures • Maintenance Records	A A A A
Workstation Use		R
Workstation Security		R
Device and Media Controls	• Disposal • Media Re-use • Accountability • Data Backup and storage	R R A A

Title II - Security

- Technical Safeguards
  - Technical Safeguards are a services of Security Rule requirements which involve using modern, technological advances to guarantee that PHI does not get into the wrong hands.
  - Complete a Vulnerability Assessment
  - Complete a Penetration Test

Title II - Security

- Technical Safeguards

Standard	Implementation Specification	Required (R) or Addressable (A)
Access Controls	• Unique User Identification • Emergency Access Procedure • Automatic Logoff • Encryption and Decryption	R R A A
Audit Controls		R
Integrity	• Mechanism to Authenticate Electronic PHI	A
Person and Entity Authentication		E
Transmission Security	• Integrity Controls • Encryption	A A

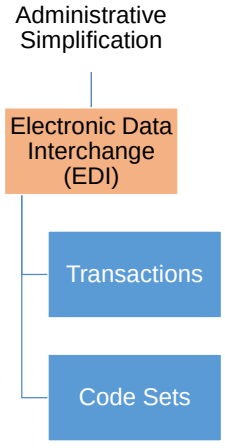
28

Title II - Security

- How to assist with compliance
  - Conduct risk analysis
  - Physical safeguards of workstations
  - Implement and maintain policies
  - Ensure unique user IDs
  - Implement procedures that record and examine activity in workstation/networks

29

Title II



Title II - EDI

- EDI – What are Transactions and Code Sets
  - Exchange electronic data between two healthcare parties
  - The electronic "bundle" sent or received will contain certain specified code sets or identifies
  - The transaction standards apply to 12 types of administrative or financial healthcare transactions used by payers, physicians, and other providers
  - i.e., claim submissions, claim status reporting, patient eligibility, referral certification and authorization and coordination of benefits
- This includes eligibility verification as well as billing and checking status of claims

Why Me? Why NEMT?

- Non-Emergency Medical Transportation (NEMT) is a covered service for beneficiaries enrolled in Medicaid programs.
- Generally, NEMT is provided through contracts between the state agency that administers the Medicaid program, or the state's Medicaid managed health care organization and local transportation brokers.
- May be a CE or BA for HIPAA purposes due to receiving, creating and/or maintaining PHI of Medicaid beneficiaries in order to carry out services for the Medicaid program.
- Have you signed a Business Associate Agreement/Contract with any healthcare providers?
- Do your drivers receive PHI during transportation to/from the hospital or medical appointments?
- Do the applications contain protected health information? Where are they stored (unlocked file cabinets, cloud storage)?

Why Me? Why NEMT?

- Do you follow minimum necessity rules?
  - Do employees only have access to what they need (i.e., Ecolane, shared drives)?
- Are all areas with PHI restricted for employees that work in that area?
- Is there open dialogue or discussion between drivers regarding passenger protected health information?
- If you are not in compliance, what are the penalties?

Non-Compliance

Criminal Penalties	
Penalty	**Violation**
Up to $250,000 Fine Up to 10 Years Imprisonment	Wrongful disclosure of PHI under false pretenses to sell, transfer, or otherwise misuse
Up to $100,000 Fine Up to 5 Years Imprisonment	Wrongful disclosure of PHI under false pretenses
Up to $50,000 Fine Up to 1 Year Imprisonment	Wrongful disclosure of PHI

Non-Compliance

Civil Penalties	
Penalty	**Civil Violation**
Up to $1.5M Fine (as of 2/23/2010)	Multiple violations due to (Willful Neglect Not Corrected) of an identical, requirement or prohibition made during the same calendar year
$10,000 Fine for each violation; may not exceed $250,000 (new 2010)	Violation was due to (Willful Neglect but Corrected(and identical requirement or prohibition during a calendar year
$1,000 Fine for each violation; may not exceed $100,000 (new 2010)	Violation was due to (reasonable Cause) and not willful neglect of an identical requirement or prohibition during a calendar year
Up to $25,000 Fine (as of 2/23/2010)	Single violation for a provision or can be multiple violations with a penalty of $100 each, as long as each violation is for a DIFFERENT provision (Did Not Know)

OCR Enforcement

Enforcement Results as of January 31, 2018

- Since the compliance date of the Privacy Rule in April 2003, OCR has received over 173,426 HIPAA complaints and has initiated over 871 compliance reviews. They have resolved ninety-seven percent of these cases (168,780).
- OCR has investigated and resolved over 25,695 cases by requiring changes in privacy practices and corrective actions by, or providing technical assistance to, HIPAA covered entities and their business associates. Corrective actions obtained by OCR from these entities have resulted in change that is systemic and that affects all the individuals they serve. OCR has successfully enforced the HIPAA Rules by applying corrective measures in all cases where an investigation indicates noncompliance by the covered entity or their business associate. To date, OCR has settled or imposed a civil money penalty in 53 cases resulting in a total dollar amount of $75,229,182.00. OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices.
-

OCR Enforcement

Enforcement Results as of January 31, 2018

- In another 11,399 cases, their investigations found no violation had occurred.
- Additionally, in 25,714 cases, OCR has intervened early and provided technical assistance to HIPAA covered entities, their business associates, and individuals exercising their rights under the Privacy Rule, without the need for an investigation
- In the rest of their completed cases, (105,971) OCR determined that the complaint did not present an eligible case for enforcement. These include cases in which:
  - OCR lacks jurisdiction under HIPAA. For example, in cases alleging a violation by an entity not covered by HIPAA;
  - The complaint is untimely, or withdrawn by the filer. The activity described does not violate the HIPAA Rules;

OCR Enforcement

Enforcement Results as of January 31, 2018

- The activity described does not violate the HIPAA Rules. For example, in cases where the covered entity has disclosed protected health information in circumstances in which the Privacy Rule permits such a disclosure.

- From the compliance date to the present, the compliance issues investigated most are, compiled cumulatively, in order of frequency:
  - Impermissible uses and disclosures of protected health information;
  - Lack of safeguards of protected health information;
  - Lack of patient access to their protected health information;
  - Lack of administrative safeguards of electronic protected health information.
  - Use or disclosure of more than the minimum necessary protected health information.

2017-2018 Settlements

- Consequences for HIPAA violations don't stop when a business closes - February 13, 2018
- Five breaches add up to millions in settlement costs for entity that failed to heed HIPAA's risk analysis and risk management rules - February 1, 2018
- Failure to protect the health records of millions of people costs entity millions of dollars - December 28, 2017
- Careless handling of HIV information jeopardizes patient's privacy, costs entity $387k - May 23, 2017
- Texas health system settles potential HIPAA violations for disclosing patient information - May 10, 2017
- $2.5 million settlement shows that not understanding HIPAA requirements creates risk – April 24, 2017
- No Business Associate Agreement? $31K Mistake - April 20, 2017
- Overlooking risks leads to breach, $400,000 settlement - April 12, 2017
- $5.5 million HIPAA settlement shines light on the importance of audit controls - February 16, 2017
- Lack of timely action risks security and costs money - February 1, 2017
- HIPAA settlement demonstrates importance of implementing safeguards for ePHI - January 18, 2017
- First HIPAA enforcement action for lack of timely breach notification settles for $475,000 - January 9, 2017

FOCUSED. ON YOU.

Thank You!

FOCUSED. ON YOU.

Contact Information

Stephanie Kessler, CHP
Partner
SKessler@rklcpa.com
717-885-5724

Karin Sherman
Senior Consultant
KSherman@rklcpa.com
717-885-5708

FOCUSED. ON YOU.