elliott davis

Does HIPAA Really Apply?

OFFICE of the STATE CONTROLLER

2020 Governmental Accounting Update

June 4, 2020

Ira Bedenbaugh, Consulting Principal

elliott davis

Disclaimer

This material was used by Elliott Davis during an oral presentation; it is not a complete record of the discussion. This presentation is for informational purposes and does not contain or convey specific advice. It should not be used or relied upon in regard to any particular situation or circumstances without first consulting the appropriate advisor. No part of the presentation may be circulated, quoted, or reproduced for distribution without prior written approval from Elliott Davis.

Does HIPAA Really Apply?

- History of HIPAA
- Who is subject to HIPAA
- Privacy Rule
- Security Rule
- Areas of focus

elliott davis

History of HIPAA

- Health Insurance Portability and Accountability Act
  - Title I – Health Care Access, Portability and Renewability
  - Title II – Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform
  - Title III – Tax-related health provisions governing medical savings accounts
  - Title IV – Application and enforcement or group health insurance requirements
  - Title V – Revenue offset governing tax deductions for employers

History of HIPAA

- Health Insurance Portability and Accountability Act
- Privacy Rule
- Security Rule
- HITECH Act
- Enforcement

elliott davis

Protected Health Information

- Individually identifiable health information, including demographic data, that relates to
  - The individual's past, present or future physical or mental health or condition
  - The provision of health care to the individual
  - The past, present, or future payment for the provision of health care to the individual
- Information which identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual (Demographic)

Source: US Department of Health and Human Services; Summary of the HIPAA Privacy Rule

Demographic Information

- Name
- Geographical subdivisions
- All elements of dates
- Telephone and fax numbers
- Vehicle identifiers
- Email addresses
- URLs
- Social Security numbers
- IP addresses
- Medical record numbers
- Biometric identifiers
- Health plan beneficiary numbers
- Account numbers
- Full face photographs

Source: US Department of Health and Human Services; Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with HIPAA

elliott davis

Subject to HIPAA

- Covered Entities
  - Health Plans
  - Health Care Providers
  - Health Care Clearinghouses
- Business Associates

Source: US Department of Health and Human Services; Summary of the HIPAA Privacy Rule

elliott davis

Hybrid Entity

- A legal entity whose business activities include both covered and non-covered functions that designates its healthcare components as covered entities
- The entity must draw lines of separation in which the designated healthcare components are required to comply with HIPAA and only those designated healthcare components have the right to use, maintain, store or transmit PHI
- If the entity does not deem itself a hybrid entity and identify the covered healthcare components, then the entire entity is considered to be a covered entity

Source: Ableitner, Alexndra; McNees Wallace & Nurick LLC; Are You a Hybrid Entity Under HIPAA

Examples Hybrid Entities

- Post-secondary institutions
- IT companies
- Research centers
- County and municipal governments

Source: Ableitner, Alexndra; McNees Wallace & Nurick LLC; Are You a Hybrid Entity Under HIPAA

elliott davis

Hybrid Electronic Transactions

- Health plan enrollment or disenrollment
- Health plan eligibility determinations
- Health plan premium payments
- Referral certification and/or authorization
- Claim submissions and status inquiries
- Coordination of health plan benefits
- Payment and remittance advice

Source: Ableitner, Alexndra; McNees Wallace & Nurick LLC; Are You a Hybrid Entity Under HIPAA

elliott davis

UMass Settlement with HHS

- On June 4, 2013, UMass notified OCR of a breach of ePHI, from workstation infected with malware, effecting 1,670 individuals
- Findings
  - UMass failed to include each component, which would be considered covered, in its hybrid entity designation
  - UMass did not conduct an accurate and thorough risk analysis
  - UMass did not implement technical security measures
- In November 2016, UMass agreed to pay HHS $650,000 and enter into a correction action plan

Source: UMass Resolution Agreement and Corrective Action Plan

Privacy Rule

- The Privacy Rule protects all protected health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- The Privacy Rule excludes from protected health information employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.
- A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected heath information may be used or disclosed by covered entities.

Source: Summary of the HIPAA Security Rule; HHS.gov

Privacy Rule - Disclosures

- Required disclosures
  - To individuals or their representative
  - HHS when it is undertaking a compliance investigation

Source: Summary of the HIPAA Security Rule; HHS.gov

elliott davis

Privacy Rule - Disclosures

- Required disclosures
- Permitted disclosures
    - To the individual
    - Treatment, payment and health care operations
    - Opportunity to agree or object
    - Incidental to an otherwise permitted use and disclosure
    - Public interest and benefit activities
    - Limited data set

Source: Summary of the HIPAA Security Rule; HHS.gov

elliott davis

Privacy Rule - Disclosures

- Public interest and benefit activities
  - Required by law
  - Public health oversight activities and essential government functions
  - Victims of abuse, neglect or domestic violence or serious threat to health or safety of an individual
  - Judicial and administrative proceedings including law enforcement purposes
  - Decedents
  - Workers compensation

Source: Summary of the HIPAA Security Rule; HHS.gov

elliott davis

Security Rule

- The Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical and physical safeguards for protecting e-PHI. Covered entities must:
    - Ensure the confidentiality, integrity and availability of all e-PHI they create, receive, maintain or transmit;
    - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
    - Protect against reasonably anticipated, impermissible uses or disclosures; and
    - Ensure compliance by their workforce.

Source: 45 C.F.R. § 164.306(a)

Security Rule

- Implementation and successful of the Security Rule requires all components of an entity to be part of the implementation
- Security Rule Safeguards
    - Administrative
    - Physical
    - Technical
- Implementation
    - Required – Safeguard must be implemented
    - Addressable – Allows entity to determine whether the Safeguard is reasonable and appropriate and allows entity to adopt an alternative measure to meet the standard

Source: Summary of the HIPAA Security Rule; HHS.gov

elliott davis

Security Rule – Administrative

- Security Management Process
- Assigned Security Responsibility
- Workforce Security
- Information Access Management
- Security Awareness and Training
- Security Incident Procedures
- Contingency Plan
- Evaluation
- Business Associate Contracts

Source: Summary of the HIPAA Security Rule; HHS.gov

elliott davis

Security Rule – Administrative

- Security Management Process
  - Risk Analysis (Required) § 164.308(a)(1)(ii)(A)

    “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”

Source: § 164.308(a)(1)(ii)(A)

elliott davis

Security Rule – Administrative

- Security Awareness and Training
  - Security Reminders (Addressable) § 164.308(a)(5)(ii)(A)

    “Implement a security awareness and training program for all members of its workforce (including management).”

Source: § 164.308(a)(5)(ii)(A)

Security Rule – Administrative

- Contingency Plan
  - Data Backup Plan (Required) § 164.308(a)(7)(ii)(A)

    “Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.”

Source: § 164.308(a)(7)(ii)(A)

elliott davis

Security Rule – Physical

- Facility Access Controls
- Workstation Use
- Workstation Security
- Device and Media Controls

Source: Summary of the HIPAA Security Rule; HHS.gov

elliott davis

Security Rule – Technical

- Access Control
- Audit Controls
- Integrity
- Person or Entity Authentication
- Transmission Security

Source: Summary of the HIPAA Security Rule; HHS.gov

elliott davis

Security Rule – Technical

- Access Control
  - Encryption and Decryption (Addressable) § 164.312(a)(2)(iv)

    “Implement a mechanism to encrypt and decrypt electronic protected health information.”

Source: § 164.308(a)(1)(ii)(A)

HIPAA and COVID-19

- Enforcement discretion was issued for telehealth and COVID-19 community based testing sites during the public health emergency.
- Guidance regarding COVID-19 disclosure to law enforcement, paramedics, other first responders and public health authorities.
- Enforcement discretion regarding business associates and their good faith uses and disclosures of PHI for public health and health oversight during the COVID-19 public health emergency.

Source: HHS.gov,; HIPAA and COVID-19

elliott davis

Questions?

Ira Bedenbaugh
Consulting Principal
864.552.4715
ira.bedenbaugh@elliottdavis.com