BONE MCALLESTER NORTON PLLC
ATTORNEYS | www.bonelaw.com

HIPAA and HITECH

An Overview for Compliance

Anne Sumpter Arney
Susan R. High-McAuley
Attorneys
Bone McAllester Norton PLLC
www.bonelaw.com

Law. Life. Passion.

Agenda

- About Us
- HIPAA
- HITECH
- Key Definitions
- The Privacy Rule
- The Security Rule
- Direct Liability of Business Associates
- Business Associate Agreements
- Security Breach Notifications
- Tiered Penalties
- Mandatory Audits

BONE MCALLESTER NORTON PLLC
ATTORNEYS | www.bonelaw.com

About Us: Anne Sumpter Arney

Anne has more than 30 years of experience working with many of Nashville's healthcare companies and medical professionals. She advises her healthcare clients on business law and transactional issues, as well as assisting them in navigating ever changing healthcare laws and regulations. In order to help medical professionals stay informed on a variety of legal concerns, Anne publishes a newsletter entitled "*Physicians' Legal Update*" and blogs at www.OnCall.Bonelaw.com. In addition to her health law practice, Anne advises both healthcare and non-healthcare entrepreneurs on how to start, grow, operate and sell their businesses.

Contact: asarney@bonelaw.com

Law. Life. Passion.

BONE MCALLESTER NORTON PLLC
ATTORNEYS | www.bonelaw.com

About Us: Susan R. High-McAuley

Susan High-McAuley concentrates her practice in the areas of corporate and business law, focusing on healthcare law, employment law, appellate advocacy and commercial and business litigation. Susan provides legal advice to Middle Tennessee's growing businesses, advising them on matters ranging from corporate formation through complex negotiations, mediation and litigation. She also assists business owners and employers with the operation of their businesses drafting contracts, negotiating on their behalf, preparing employee handbooks, advising on enforcement of non-compete agreements, unwinding businesses, advising on partnership and shareholder disputes and assisting in the merger and acquisitions of businesses.

Contact: shigh-mcauley@bonelaw.com

Law. Life. Passion.

Health Insurance Portability and Accountability Act

"HIPAA"

HIPAA

- Part of Administrative Simplification that required HHS to adopt national standards for "covered transactions"
- Technology although efficient could erode privacy
- Transaction Rule- Transactions and Code Sets Standards , Employer Identifier Standard , National Provider Identifier Standard

- **Privacy Rule-** standards for the protection of individually identifiable health information

- **Security Rule-** sets national standards for protecting the confidentiality, integrity, and availability of electronic protected health information

Health Information Technology for Economic and Clinical Health Act

"HITECH"

HITECH

- Promote the meaningful use of health information technology
- Expanded Privacy and Security Rules
  - direct application to Business Associates
  - breach reporting requirements
  - Additional privacy requirements
- Strengthen the civil and criminal enforcement

Who Is Covered by HIPAA ?

Covered Entities

- Healthcare providers who transmit protected health information (PHI) in electronic form

  in a covered transaction
- Health plans
- Healthcare clearing houses

Business Associates

- Person/entity that performs services for covered entity that involves use or disclosure of protected health information

Key Definitions

Key Definitions

- Protected Health Information - individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral.

- Electronic Protected Health Information -a subset of protected health information which a covered entity creates, receives, maintains or transmits in electronic form (e-PHI).

- Health Plans- Individual and group plans that provide or pay the cost of medical care

- Health care provider-Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions.

- Health Care Clearinghouses - Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa.

- Minimum Necessary Standard – HIPAA standard that requires that when protected health information is used or disclosed, only the information that is needed for the immediate use or disclosure should be made available by the health care provider or other covered entity. This standard does not apply to uses and disclosures for treatment purposes or to uses and disclosures that an individual has authorized, among other limited exceptions.

Business Associate

- Business Associate is a person or organization, other than a member of a covered entity's workforce, that performs (1) certain functions or activities on behalf of, or (2) provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

- Functions or activities on behalf of a covered entity include claims processing, data analysis, utilization review, and billing.

- Services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

- Persons or organizations are not considered business associates if their functions or services do not involve the use or disclosure of PHI , and where any access to protected health information by such persons would be incidental, if at all.

- The Omnibus Final Rule expanded the definition of Business Associate to include the following:

  - A health information organization, e-prescribing gateway or other entity that provides data transmission services to a covered entity and requires access on a routine basis to PHI
  - An entity that offers a personal health record on behalf of a covered entity
  - A subcontractor
  - A person who creates, receives, maintains or transmits PHI on behalf of a covered entity

- Physical storage facilities or companies that store electronic PHI are Business Associates, even if they do not actually view the PHI.

- Final Rule distinguishes between a mere conduit of PHI, such as the U.S. Postal Service, and an entity engaged in the long-term storage of PHI.

- Final Rule does not distinguish between bulk storage providers of hard copy data, cloud storage providers and other providers of electronic data storage services, suggesting that its analysis of who qualifies as a Business Associate applies in the same manner to each of these entities.

The Privacy Rule

The Privacy Rule

- Set standards for the use and disclosure of Protected Health Information (PHI) by organizations covered by the Privacy Rule.

- Grants certain Patient Rights to control and understand how their PHI is used :
  - Notice of privacy practices
  - Access
  - Amendment
  - Disclosure accounting
  - Restriction request
  - Confidential communications requirements

Authorized Use and Disclosure

Covered Entity Must Not Use or Disclose PHI Except as Allowed by the Rule.

- Use and disclosure allowed without authorization
  - Treatment
  - Payment
  - Healthcare operations
  - Public interest and benefit activities

- Use or disclosure requires an opportunity to agree or object
  - A facility directory
  - To a person involved in the individual's care
  - For notification and disaster relief purposes

Written Authorization is Required

Unless specifically delineated in 45 CFR § 164.508 valid written authorization is required for use or disclosure of PHI

- Psychotherapy notes.
- Marketing
- Sale of PHI

Core elements and requirements for the Authorization are set out in 45 CFR § 164.508(c).

- Description of the information to be used or disclosed

- The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

- Name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

- A description of each purpose of the requested use or disclosure.

- An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure.

- Signature of the individual and date.

45 CFR § 164.512 delineates the disclosure of PHI in judicial and administrative proceedings. The rules differ depending on the type of subpoena issued:

- Order, warrant or subpoena signed by judge
- Grand jury subpoena
- Administrative demand
- Subpoena signed by clerk or attorney (most subpoenas)

Response to Subpoenas

- HIPAA provides exceptions to the general prohibition of disclosure of patients' PHI in the course of a judicial or administrative proceeding under the following limited circumstances:

  (i) In response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order; or

  (ii) In response to a subpoena, discovery request, or other lawful process, that is not accompanied by an order of a court or administrative tribunal, if:

(A) The covered entity receives satisfactory assurance, as described in paragraph(e)(1)(iii) of this section, from the party seeking the information that reasonable efforts have been made by such party to ensure that the individual who is the subject of the protected health information that has been requested has been given notice of the request; or

(B) The covered entity receives satisfactory assurance, as described in paragraph (e)(1)(iv) of this section, from the party seeking the information that reasonable efforts have been made by such party to secure a qualified protective order that meets the requirements of paragraph (e)(1)(v) of this section.

See 45 C.F.R. § 164.512(e). Section 164.512 further defines the satisfactory assurance that must be received by the covered entity and "Qualified Protective Order."

Security Rule

Security Rule Protection of EPHI

Covered Entity and Business Associate must put in place technical and not technical safeguards to secure an individuals EPHI. The Security Rule is designed to be scalable so that that the protections are appropriate to the specific covered entity.

Administrative Safeguards

- Security management process
- Security personnel
- Information access management
- Workforce training and management
- Evaluation

Physical Safeguards

- Facility access and control
- Workstation and device security

Technical Safeguards

- Access control
- Audit control
- Integrity control
- Transmission security

Policies and Procedures & Documentation Requirements

- Written policies and procedures to comply with Security Rule
- Document periodic evaluation of policies and procedures and update

Direct Liability of Business Associates

Direct Liability under the Security Rule

- Business associates are now subject to the administrative, physical, and technical safeguard requirements of the Security Rule.
- Business associates previously had to agree in their business associate agreements with covered entities to appropriately protect and safeguard PHI and should already have in place security safeguards.
- Many business associates will not have engaged in the formal administrative safeguards" required by the rule.

Direct Liability under the Privacy Rule

Business Associates are now directly liable for

- uses or disclosures of PHI in a manner not in accord with the business associate agreement or the Privacy Rule;
- failure to disclose PHI when required by HHS
- failure to disclose PHI to the covered entity, an individual (to whom the information pertains), or the individual's designee with respect to an individual's request for an electronic copy of the information;
- failure to make reasonable efforts to limit PHI uses, disclosures, and requests to the minimum necessary amount;
- failure to enter into a business associate agreement with a subcontractor that creates or receives PHI on their behalf.

Direct Liability for Breach Notification

- Business associate must notify the covered entity when it discovers a breach of unsecured PHI "without unreasonable delay and in no case later than 60 days" following discovery of a breach.

- If the business associate is acting as an agent of the covered entity, then the business associate's discovery will be imputed to the covered entity.

BONE MCALLESTER NORTON PLLC
ATTORNEYS | www.bonelaw.com

Business Associate Agreement

Law. Life. Passion.

- Business Associate Contracts must contain the elements specified at 45 CFR 164.504 (e).

  Describe the permitted and required uses of protected health information by the business associate;

  Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law;

  Require the business associate to use appropriate s safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

- Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement.

- If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

The Omnibus Final Rule

Business Associates agreements must now specifically include the following agreements by the Business Associate:

- Comply with the HIPAA security standards
- Comply with the security breach rules
- Require subcontractors that create, receive, maintain or transmit PHI to agree to the same restrictions and conditions as the business associate
- To the extent the Business Associate is to carry out a covered entity's obligations under the privacy rule, comply with the requirements of the privacy rule that applied to the covered entity

There is a transition period for updating the Business Associate agreement where there is already an agreement in place. The Business Associate agreement must be updated by the earlier of either the next renewal after 9/23/13 or 9/24/13.

Business Associates must have in place a Business Associate agreement with any subcontractor that may use PHI of the covered entity.

Security Breach Notifications

Security Breach Notifications – 45 CFR 164, Subpart D

Background

- Section 13402 of the HITECH Act requires HIPAA covered entities to provide notification to affected individuals and the Secretary of Health and Human Services, and in some cases the media, following the discovery of a breach of unsecured PHI.

- In the case of a breach of unsecured PHI at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach.

Summary of Modifications in Final Rule 45 CFR Sec. 164.400 *et. seq.*

- Definition of breach – amended
  - Breach is now presumed
  - Risk assessment changed
- Notifications to Individuals – no modifications
- Notifications to Media – no substantive modifications
- Notifications to the Secretary – minor modification
- Notification by a Business Associate – no substantive modifications
- Law Enforcement Delay – no modifications
- Administrative Requirements and Burden of Proof – no modifications
- Preemption – no modifications

Safe Harbor – Secured PHI

Final Rule retains the Safe Harbor

- Notifications must only be given for breach of **unsecured** PHI
- Unsecured PHI continues to be defined as "protected health information that is not secured through the use of a technology or methodology specified by the Secretary in guidance."
- The Guidance continues to specify **encryption and destruction** as the two methods for rendering PHI unusable, unreadable or indecipherable to unauthorized individuals or "secured" and thus exempt from the breach notification obligations.

Definition of Breach

- Definition of breach found at 45 CFR 164.402
- Breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI such that the use or disclosure poses a significant risk of financial, reputational or other harm to the affected individual

Breach Continued

- 3 exceptions to Breach:

- 1. The unintentional acquisition, access or use of PHI by a workforce member acting under the authority of a Covered Entity or Business Associate.

- 2. The inadvertent disclosure of PHI from a person authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the Covered Entity or Business Associate
- Under both of these exceptions, the information cannot be further used or disclosed in a manner not protected by the Privacy Rule.
- 3. Covered Entity or Business Associate has good faith belief that the unauthorized individual is not able to retain the information.

Breach Continued

- Presumption of breach – US Dept. of Health and Human (HHS) Services has clarified that an impermissible use or disclosure of PHI is presumed unless the covered entity or business associate demonstrates that there is a low probability that the PHI has been compromised.

- Thus, the risk of harm to the individual standard has been modified to a risk of compromise standard. -- HHS' attempt to set a more objective standard

- Breach notification is not required under the Final Rule if a covered entity or business associate demonstrates through a risk assessment that there is a low probability that the PHI has been compromised, rather than demonstrate that there is no risk of harm to the individual.

Factors to be Considered in Risk Assessment

4 Factors must be considered in risk assessment:

1. The nature and extent of the PHI involved, including the type of identifiers and the likelihood of re-identification.
2. The unauthorized person who used the PHI or to whom the disclosure was made.
3. Whether the PHI was actually acquired or viewed.
4. The extent to which the risk to the PHI has been mitigated.

Additional factors may also be considered to properly assess the risk of compromise, but the above 4 factors MUST be considered.

Factor 1 – Type of PHI involved

- Covered entities and business associates must evaluate the nature and extent of PHI involved, including the types of identifiers and likelihood of re-identification of the information.
- Ask: Is the information of a more sensitive nature.
- Example: financial information – would include credit card numbers, SSN, or other information that increases the risk of identity theft or financial fraud
- Example: clinical information – would include nature of services or other information and amount of detailed clinical info included i.e., treatment plan, diagnosis, medication, medical history, test results.
- Ask: Can the PHI be used by an unauthorized recipient in a manner adverse to the individual or to further the unauthorized recipient's own interests.
- Example: If a list of patient discharge dates and diagnoses are disclosed, covered entity must consider whether any individual could be identified based on specificity of diagnosis and size of community or whether the info when combined with other available info to re-identify the affected individual.

Limited Data Set Exception Abolished

- The Final Rule has deleted the "limited data set" exception. Before, an incident was an exception to the definition of breach if the PHI used or disclosed a limited data set that did not contain any birthdates or ZIP codes. Under the Final Rule, breaches of limited data sets – regardless of their content – must be assessed like all other breaches of PHI.

- HHS explained that Factors 1 and 2 are well suited to address the probability that a data set without direct identifiers has been compromised following an impermissible use or disclosure.

Factor 2 – Person who impermissibly used PHI or to whom Disclosure was Made

- Ask: Does the person who received the information have an obligation to protect the privacy and security of the information.
- Example: If the PHI is disclosed to another entity obligated to abide by HIPAA Privacy and Security Rules or to a federal agency required to abide by other federal privacy acts, there may be a lower probability that the PHI has been compromised since the recipient has a similar obligation to protect the PHI.
- This factor must be considered in conjunction with the other factors.
- Example: Disclosure to employer – If the disclosed information contains dates of service and/or diagnosis, employer may be able to re-identify individual based on other information available to employer such as dates of absence from work. Therefore, probability of compromise may be greater.

Factor 3 – Actually Acquired or Viewed

- Ask: Was the PHI actually viewed or acquired?
- Example: Stolen/lost laptop computer – If recovered quickly, perform a forensic analysis to determine if the PHI was viewed, accessed, acquired, transferred or otherwise compromised.
- Easy analysis of this factor if PHI mailed to wrong recipient who calls regarding the mailing.
- Easier analysis if mailed PHI to wrong recipient returned as undeliverable or unclaimed registered/certified mail.

Factor 4 -- Mitigation

- Covered entities and business associates should consider the extent to which the risk to the PHI has been mitigated following impermissible use or disclosure through a satisfactory assurance that the PHI will not be further used or disclosed.
- Examples of mitigation – Confidentiality Agreement, Destruction
- HHS notes that this factor may yield different results when considered in combination with Factor 2 (person to whom disclosed).
- Example: Covered entity may be able to obtain and rely on satisfactory assurances of employee, affiliated entity, business associate, or other covered entity that the entity or person destroyed information it received in error, while such assurances from third parties may not be sufficient.

Risk Assessment –Analysis and Results

- HHS has noted it expects risk assessments to be thorough, completed in good faith, and for the conclusions reached to be reasonable.
- Therefore, document, document, document the risk assessment.
- If the risk assessment evaluation fails to demonstrate a low probability that the PHI has been compromised, breach notification is REQUIRED.
- Covered entity or business associate has discretion to provide the notification following an impermissible use or disclosure automatically in lieu of performing the risk assessment.
- Remember, breach is now PRESUMED.
- HHS will issue future guidance on frequently occurring scenarios.

Breach Notification Requirements

- To summarize, providers and covered entities must give notice to individuals, the media (if the breach affects more than 500 residents of a state or smaller jurisdiction) and HHS (if the breach affects more than 500 individuals regardless of locale). Business associates, or those that conduct business with the covered entity involved in the use or disclosure of individually identifiable health information, must also provide notice to covered entities. All notices are required no later than 60 days after discovery of the breach of unsecured PHI.
- Notification to Individuals – 45 CFR Sec. 164.404
- Notification to Media – 45 CFR Sec. 164.406
- Notification to HHS Secretary – 45 CFR Sec. 164.408
- Notification by a Business Associate – 45 CFR Sec. 164.410

Tiered Penalties

Increased Enforcement

In 2009, the HITECH Act significantly increased and expanded the penalties for violation of HIPAA:

- Increased civil money penalties
- Reduced available affirmative defenses
- Mandatory civil money penalties violations due to willful neglect
- Expanded direct liability for HIPAA violations to Business Associates

The Final Rule implements the expanded penalties with a tiered structure for violations occurring after Feb. 18, 2009.

Penalty Increases with the Level of Culpability

Unknowing. The covered entity or Business Associate did not know and reasonably should not have known of the violation.

Penalty for each violation: $100 – $50,000
Total in a calendar year: $1,500,000

Reasonable Cause to Know. The covered entity or business associate knew, or by exercising reasonable diligence would have known, that the act or omission was a violation, but the covered entity or business associate did not act with willful neglect.

Penalty for each violation: $1,000 – $50,000
Total in a calendar year: $1,500,000

Willful Neglect – Corrected. The violation was the result of conscious, intentional failure or reckless indifference to comply with HIPAA, but the covered entity or business associate corrected the violation within 30 days of discovery.

Penalty for each violation: $10,000 – $50,000
Total in a calendar year: $1,500,000

Willful Neglect – Uncorrected. The violation was the result of conscious, intentional failure or reckless indifference to fulfill the obligation to comply with HIPAA, and the covered entity or business associate did not correct the violation within 30 days of discovery.

Penalty for each violation: at least $50,0000
Total in a calendar year: $1,500,000

Office of Civil Rights (OCR) Must Determine the Penalty Based On:

- The nature and extent of the violation, including the number of individuals affected and the time period during which the violation occurred.
- The nature and extent of the harm resulting from the violation, including whether the violation caused physical harm, resulted in financial harm, caused harm to an individual's reputation and hindered an individual's ability to obtain healthcare.
- The history of prior compliance, including previous violations.
- The financial condition of the covered entity or business associate, including whether financial difficulties affected the ability to comply and whether the imposition of the penalty would jeopardize the ability of the covered entity to continue to provide or pay for healthcare .

Other Considerations:

- OCR has the discretion to waive penalties that are not due to willful neglect
- Non-monetary penalties
- Liability for Business Associate Agents

Mandatory Audits

Mandatory Audits

The HITECH ACT requires OCR to conduct periodic audits of covered entities and Busi-ness Associates to determine their compliance with the Privacy Rule, Security Rule and Breach Notification Standards.

The Process

- Request for documentation
- Site visit
- Draft final report—10 days to review and comment
- Final report and response to OCR
- Outcome: Technical assistance or compliance review

Audit Protocol

The entire audit protocol is organized around modules, representing separate elements of privacy, security and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.

The audit protocol covers Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI and (7) accounting of disclosures.

The protocol covers Security Rule requirements for administrative, physical, and technical safeguards.

The protocol covers requirements for the breach notification rule.