HIPAA Policy & Procedures for Covered Entities

Two Parts to HIPAA

- Privacy Rule
- Security Rule

The purpose of HIPAA is to protect the privacy of health records and information contained in a patients file, (PHI), both electronic and paper. Personal Health Information (PHI) includes:

- Names
- Email Addresses
- Social Security Numbers
- Telephone Numbers
- Any personal identifier

Privacy Rule

Focuses on the right of an individual to control the use of his or her personal information. PHI should not be divulged or used by others against their wishes. Privacy Rule is usually associated with paper charts and non-electronic PHI.

Security Rule

Focuses on the administrative, technical, and physical safeguards specifically as they relate to electronic PHI, (ePHI). Protection of ePHI data from unauthorized access whether external or internal, stored, or in transit is all part of the security rule. This includes:

- Electronic Medical Record (EMR)
- Digital XRays
- Ultrasounds

  info@smbtep.com

The Security Rule says that a covered entity must ensure…

- Confidentiality
- Integrity
- Availability

… of all ePHI that a covered entity:

- Creates
- Receives
- Transmits
- Maintains

The Rules of Confidentiality, Integrity, & Availability (CIA)

Confidentiality

- Prevent unauthorized access
- Patient or visitors viewing patient information on computer screens
- Hackers stealing patient information Integrity

- Prevent changing or destroying patient information
- Deleting records in an EMR
- Unauthorized changes to records in an EMR Availability

- Ability to access patient information
- Ensuring patient information is accessible even in the event of a system crash or disaster

OMNIBUS

September 23, 2013—Compliance Date

HHS has made it clear, this compliance deadline is NOT optional.

Omnibus Rule

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights announces a final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, to strengthen the privacy and security protections for health information established under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Business Associates

The Privacy Rule requires that a covered entity obtain satisfactory assurances from its business associate that the business associate will appropriately safeguard the protected health information it receives or creates on behalf of the covered entity. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

Examples of Business Associates.

- A third party administrator that assists a health plan with claims processing
- A CPA firm whose accounting services to a health care provider involve access to protected health information
- An attorney whose legal services to a health plan involve access to protected health information
- A consultant that performs utilization reviews for a hospital
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer

- An independent medical transcriptionist that provides transcription services to a physician
- A pharmacy benefits manager that manages a health plan's pharmacist network.

Omnibus rule made business associates (BA) directly liable for compliance with the HIPAA security rule. A BA is responsible for protecting patient information as a covered entity is. Under this rule cloud providers that store ePHI are now considered BA's. BA's now need to:

- Appoint a security officer
- Perform a yearly HIPAA risk assessment
- Ensure that employees receive yearly HIPAA training
- Have HIPAA policy and procedures
- Ensure BAA's are in place with all CE's & BA's

HIPAA 2015 update

Security Rule 18 Safeguards for ePHI

Administrative Safeguards

1. Security Management Policy – performing a risk assessment on how your organization is currently protecting ePHI and recommend additional ways to protect ePHI
2. Security Officer Policy – Someone who is responsible for the overall security of an organizations ePHI
3. Workforce Security – authorized employee access
4. Information Access Management – focuses on authorizing, establishing, and modifying access to ePHI
5. Security Awareness and Training – all employees receive HIPAA training
6. Security Incident Procedures – procedure be developed and implemented for reporting, responding to, and managing security incidents
7. Contingency Plan – disaster recovery plans and emergency operation plans in case of a disaster
8. Evaluation – periodically review how an organization is protecting ePHI
9. Business Associates Contracts – ensure you have BAA with all 3rd party vendors such as I.T. Company, billing, etc…
10. Facility Access Controls – systems that contain ePHI stored in a secure location to prevent unauthorized access
11. Workstation Use – employees know what is allowed and what is prohibited use
12. Workstation Security – restricted to only the employees that are supposed to have access to ePHI
13. Device and Media Control – need to protect devices such as laptops, tablets, smartphones, USB drives, and DVD's. Also the desensitizing of pulled PC's and their proper disposal, the tracking of devices that contain ePHI that are removed out of the organization, or any other media that contains ePHI.

  info@smbtep.com

Technical Safeguards

14. Access Control – only employees that are supposed to have access to ePHI have access and the right level of access
    - access to ePHI with unique username and password
    - encryption to protect ePHI
    - automatic logoff after a period of inactivity
15. Audit Controls – capture information on access to ePHI, who, when, and what information was accessed
16. Integrity – methods that can be used to ensure that ePHI is not improperly altered or destroyed
17. Person or Entity Authorization – ensures that a person that is accessing ePHI is verified and uses a unique user ID and password. User ID's and passwords should not be shared with anyone else.
18. Transmission Security – the need to protect ePHI that is transmitted which includes:
    - using encryption when sending email
    - accessing ePHI via a wireless network
    - sending ePHI via the internet

Computer Encryption

Encryption is a "safe harbor" under the HIPAA security rule. "Lost media that has been encrypted does not require a breach notification to patients where records are on the media."

.

  info@smbtep.com

COMPLIANCE – WHAT WE DO BEST!

Meaningful Use – Core Objective

- **Satisfy Meaningful Use (MU) Requirement** – Core Objective – Protect electronic health information *(Conduct or review a security risk assessment of the certified EHR technology)* – **You must perform a Risk Assessment each year you attest for Meaningful Use!**
- We perform your Risk Assessment
- Our process is streamlined – **you will only need to spend 1 to 2 hours working with us and then we do the rest!**
- We make additional security recommendations
- We identify all risks and analyze any threats
- Findings are clearly documented in easy to understand reports and workplans

Meaningful Use Audits

- **Meaningful Use Audits are Occurring**
- Organizations can be audited either pre or post payment of incentive funds
- Failure to perform a Risk Assessment is a frequent reason for failing Meaningful Use Audits
- **Audits targeted at 20% (1 in 5) of eligible providers**
- Failed audits may require an organization to repay a full year of incentive payments
- Incentive fund repayments average ~$10,000 per eligible provider
- Incentive payments must be repaid within 30 days of MU audit failure notice
- Failure to repay incentive payments will incur additional penalties
- Could a failed MU audit trigger to a HIPAA audit as well?
- ***Our Risk Assessments have passed Meaningful Use Audits***

Healthcare Managed Services

Let's face it HIPAA regulations are here to stay. There is no way around it and as a covered entity you have too much to lose not get compliant. The cost from start to finish is based on number of staff and is very affordable. The cost of doing nothing might cost you everything if you get audited and are found noncompliant. Find out how a Healthcare Managed Services, (HMS), plan can get you in full compliance today!