Essential Steps for HIPAA Compliance

July 28, 2016

HealthInsight

This Webinar is Brought to You By….

HealthInsight

HIPAAOne
PROTECT YOUR ePHI

mountain-pacific quality health
HTS HEALTH TECHNOLOGY SERVICES
3404 Cooney Drive, Helena MT 59602 | www.gotohts.org | 406.457.5897
transforming health care through innovative technology

PASS

About HealthInsight and Mountain-Pacific Quality Health

- HealthInsight and Mountain-Pacific Quality Health are private, non-profit, community-based Quality Improvement Organizations (QIO) that have dedicated more than three decades to improving health and health care and are composed of locally governed organizations in: Alaska, Hawaii, Montana, Nevada, New Mexico, Oregon, Utah and Wyoming. As part of our efforts to assist hospitals and practices with HIPAA compliance, HealthInsight and Mountain-Pacific Quality Health teamed together to form **HIPAA Privacy and Security Solutions**, or ***HIPAA PASS***, to offer affordable, easy and comprehensive Risk Analysis and Risk Management services.

About HIPAA One®

- Following a thorough search for the best software to assist our practices and hospitals to achieve HIPAA compliance, HIPAA One® emerged as the clear solution.
- For more information about HIPAA One® please visit:

https://www.youtube.com/watch?v=9G_B7U_pnuo&feature=youtu.be

Mark Norby, CHP

- 15 Years of IT experience
- Eight Years as the CIO of the Community Health Center of Central Wyoming and University of Wyoming Family Medicine Residency Program
- Six Years as a HIPAA Compliance Officer
- Four Years as a HIPAA Compliance Consultant
- Provided help to more than 150 hospitals and clinics

The Goal of HIPAA

- Ensure the confidentiality, integrity and availability of all protected health information (PHI) the covered entity (CE) or business associate (BA) creates, receives, maintains or transmits
- **What is a CE or BA?**

Your Goals

- Protect patient dignity
- Build a stronger, more resilient business
- Build confidence in the patient care model
- Avoid audits and fines which lead to:
  - Financial and reputational harm

What Are the Challenges that You Face?

- Lack of organizational buy-in
- Time
- Turnover
- Knowledge
- Finances

Step 1: Security Risk Analysis

- (A) Risk analysis (Required)
  - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI held by the CE or BA.

Required

- (2) When a standard adopted in § 164.308, § 164.310, § 164.312, § 164.314, or § 164.316 includes required implementation specifications, a CE or BA **must** implement the implementation specifications.

Addressable

- Implement the implementation specification if reasonable and appropriate; or
- Document why it would not be reasonable and appropriate; and
- Implement an equivalent alternative measure if reasonable and appropriate

Step 2: Risk Management Plan

- (B) Risk management (Required)
  - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

Step 2: Risk Management Plan Cont.

- For each deficiency found during the Security Risk Analysis, identify the steps necessary to correct it, assign someone to fix it and establish a target date for completion
- Throughout each reporting period, consistently document your progress
- Good faith effort can make a big difference

Step 2: Risk Management Plan Cont.

- Conducting a Security Risk Analysis (SRA) and building a Risk Management Plan (RMP) is a very educational process
- The results of these two steps could reveal a need to improve your policies and procedures, training program and/or technology

Step 3: Assigned Security Responsibility

- *(Required)* Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the CE or BA.

Step 3: Assigned Security Responsibility Cont.

- Ensure that detailed job descriptions are in place for both the HIPAA privacy officer and security officer
- Train the privacy and security officer(s)
- Verify that the privacy and security officer(s) are clearly identified in the HIPAA policy and procedures manuals and the notice of privacy practice
- Have the privacy and security officer(s) add their HIPAA title to their email signature
- Build a team to assist the privacy and security officer(s) with building a culture of compliance (internal and external)

Step 4: Security Awareness and Training

- *(Required)* Implement a security awareness and training program for all members of its workforce (including management)
- Train all staff members on approved policies and procedures at least annually
- Maintain proof of training for six years

Step 5: Security Reminders

- Security reminders (Addressable). Periodic security updates.
  - Maintain a comprehensive and on-going HIPAA training program that includes IT topics, posters and periodic reminders
  - Include posters at each copier/fax location and staff lounge

Step 5: Build a Security Poster (The Ten Commandments of HIPAA)

1. Protect all patient information as though your job depends on it
2. Access, use or provide only the minimum amount patient information necessary to accomplish the task
3. When you must discuss patient information do so discreetly, privately and quietly
4. NEVER discuss patient information outside of the work environment
5. Cover, turn over or put away all patient information that is not being used
6. Do not send patient information by email or text
7. Dispose of all paper-based patient information using a shredder or shred bins
8. Secure your computer, or other devices, when left unattended
9. Passwords must be changed at least each 90 days and consist of at least eight characters and include upper case letters, lower case letters and numerals
10. For any HIPAA related questions or concerns contact:

    Privacy Officer:_____

    Security Officer:_____

Step 6: Secure Your Facilities

- Perform and document periodic facility inspections (think like a thief!)
- Have all contractors, vendors, etc sign-in and maintain copies of the sign-in sheets
- Issue nametags or badges to all employees and contractors
- Position PC's, printers, copiers and fax machines with privacy and security in mind
- Maintain documentation of all security related maintenance and repairs to the facility

Step 7: Encryption

- There are two separate implementation specifications involving encryption

Step 7: “Data at Rest”

- The first is contained at 45 CFR 164.312(a)(2)(iv): *“Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic PHI.”*
- Audit request…….*Provide documentation proving encryption capabilities on end-user devices or provide proof that the electronic health record (EHR) does not store PHI on end-user devices after use of the EHR stops on these devices*

Step 7: “Data in Motion”

- The second requirement is located at 45 CFR 164.312(e)(2)(ii): *“Encryption (Addressable). Implement a mechanism to encrypt electronic PHI whenever deemed appropriate.”*
- For any transmission over the Internet we recommend encryption using TLS (which supersedes SSL) or a VPN

Encryption!

- It is included with some versions of Windows and Macs
- It doesn’t slow down your systems
- DiskCryptor is free
- The cost is installation and typing an additional password when first booting up

Step 8: Secure Your Software

- If you access the software from outside the office, ensure that access is encrypted
- Enable audit logging, periodically review the audit logs, keep proof
- Ensure that password requirements meet best practices
- Enable auto-logoff and auto-lockout
- Perform backups

Step 9: Don’t Get Hacked

- Ensure that firewall settings are optimized
- What if you fire your IT vendor?
- Maintain up-to-date network documentation and diagrams. Be prepared to change passwords ASAP
- Verify that workstations and servers have all the latest security patches, service packs and anti-virus updates
- Establish formal system monitoring procedures
- Make a decision regarding vulnerability scanning and/or penetration testing

Step 10: Keeping Up with Changes

- Have the privacy and security officer(s) join the following listservs to keep up to date on HIPAA news: **http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/listserv.html**

Misc. Links

Vulnerability Scanners

http://sectools.org/vuln-scanners.html

HIPAA Privacy Rule Blue Card for Law Enforcement:

http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/emergency/

Omnibus Final Rule versions of Business Associate Agreement and Notice of Privacy Practices

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html

http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

Join Us!

Our next free webinar:

Introduction to Preparing for a HIPAA Audit

Tuesday, August 30, 2016

1-2PM Mountain Time

To register visit:

http://healthinsight.org/hipaapass#events

Save the Date!

One-Day HIPAA Privacy and Security Bootcamp

Tuesday, September 13, 2016
At HealthInsight Utah
756 E. Winchester Street Murray, Utah
8 a.m. - 5 p.m. MT

Visit our website www.healthinsight.org/hipaapass to register now!

Questions?

Mark Norby, Certified HIPAA Professional

HIPAA Counselor

307.258.5322

mnorby@healthinsight.org

Visit our website:

www.healthinsight.org/hipaapass

for more information about our Privacy and Security Solutions!

Thank you and have a wonderful day!!