Patient Privacy and Security

Presented by, Jeffery Daigrepont

2400 Lakeview Parkway, Suite 400, Alpharetta, GA 30009 • 800.345.5829 • www.cokergroup.com

Jeffery Daigrepont, SVP

Disclosures

- No Financial Conflicts to Report

***Jeffery Daigrepont*,** Senior Vice President of The Coker Group, specializes in health care automation, strategic planning, operations, and deployment of fully integrated information systems for medical practices and hospitals.

A popular program speaker, Jeffery is frequently engaged by highly respected organizations across the nation. Accomplishments include the authorship of several publications including a top-selling book, *Complete Guide and Toolkit to Successful EHR Adoption*, published by HIMSS in 2011 and was a contributing author to Coker's book, *The Healthcare Executive's Guide to ACO Strategy*, published in March 2012.

Daigrepont is credentialed by the American Academy of Medical Management (AAMM) with an Executive Fellowship in Practice Management (EFPM).

No conflicts of interest with any vendors

Overview

I. EHR Privacy and Security Regulations
II. 10 Step Plan
III. Resources and Considerations
IV. Q & A

I. EHR Privacy and Security Regulations

Coker GROUP
Business Advisors for the Healthcare Industry

Health Information Technology (IT)

Health IT encompasses the exchange of electronic health information. The use of health IT is improving quality of care, reducing medical errors and health care costs, and increasing administrative efficiencies.

However, it is critical that the privacy and security of patient health information is a top priority of covered entities.

Definition of ePHI…

- ePHI or electronic Protected Health Information is patient health information which is computer based, e.g., created, received, stored or maintained, processed and/or transmitted in electronic media.

- Electronic media includes computers, laptops, CDs/DVDs/disks, memory sticks, smart phones, PDAs, servers, networks, dial-modems, email, web-sites, etc.

- ***Federal Laws: HIPAA Privacy & Security Laws mandate protection and safeguards for access, use and disclosure of PHI and/or ePHI with sanctions for violations.***

Threats

- Loss of financial cash flow
- Permanent loss or corruption of electronic protected health information (ePHI)
- Temporary loss or unavailability of medical records
- Loss of physical assets (computers, etc.)
- Damage to reputation and public confidence
- Threats to patients
- Threats to employees

Security vs. Privacy

- Security = A process / set of actions
- Privacy = Results for the above actions/consequences

Security exist without privacy, but you can't have privacy without security.

The 90/10 Rule…

- Good Security Standards follow the “90 / 10” Rule:
  - 10% of security safeguards are technical
  - 90% of security safeguards rely on the computer user (“YOU”) to adhere to good computing practices

Example: The lock on the door is the 10%. You remembering to lock, check to see if it is closed, ensuring others do not prop the door open, keeping controls of keys is the 90%. 10% security is worthless without YOU!

The data eco system…

Data at Rest	Data in Use	Data in Motion
• Work stations • Laptops • Home Computers • USB Flash Drives • File Sharing	• EHR database • Patient Portal • PM database • Patient repositories • HIEs • eRX	• Instance Messaging • Email • Smart Phones • Network Devices • Wireless Devices • Clearinghouse providers

How the hackers hack…

Social Engineering (Human Hacking)

Example: *A practice administrator was tricked into downloading a Trojan horse*.

- Social engineers found out she had a family member who was battling cancer and other information through her Facebook page. Using that emotional attachment, they tugged at her heartstrings and she was asked to donate money to a cancer research fund. The PDF that was sent, however, was malware that took control of her computer
- A seemingly harmless new patient arrives at the practice to discover he left his insurance card at home. Appealing to the front desk, he suggest accessing his home computer from an office workstations to print a copy of the card. Unfortunately, that harmless new patient is an actor looking to get into your network by bringing up a harmful file on their computers
- "Hi, this is Chris from Microsoft, we have been a victim of a virus from your network and we need to send you a file to secure and repair the threat"

How do hackers hack cont…

- Phishing
  - The act of posing as a trusted entity in order to extract sensitive information through email
  - Phishing happens several thousands of times a day across the world
  - Phishing emails 47%, most common form of social engineering for businesses
  - In a test, within 24 hours, 10% of emailed users responded and supplied usernames and passwords to the fake website

How do hackers hack cont…

- Hoaxes
  - **Nigerian scam letter** - Greetings, Sir. I got your e-mail address from a very confidential source -- the Internet. I am the prince, minister and Grand Pooh-bah of one of many foreign nations that you stupid Americans have never heard of. There is a billion, kazillion dollars in an account here that rightfully belongs to my family and my people. Due to some military coup in which my entire family, several accountants and various goats lost their lives, I cannot reach this money. But you, an American who has never heard of my country, can deposit this money. For your trouble, I'll give you a few million off the top -- because what's a few million between confidential best friends who have never actually even heard of one another?
  - **Forwarded e-mail for money or donations** - Microsoft and Disney are both beta-testing an e-mail tracker and will send you money if you forward this e-mail. The Gap is testing an e-mail tracker and will send you a gift certificate.
  - **Spoofed Messages -** UPS message claiming a package has failed to be delivered, asking the victim to print out an invoice to take to the ups center for pickup, when actually it's a malicious PDF file.

HIPAA Privacy Rule
45 CFR Part 160

- *Standards for Privacy of Individually Identifiable Health Information* (Privacy Rule)
- Goal: PHI is properly protected while allowing flow of health information needed to provide and promote high quality health care*
- Standards for use and disclosure of patient health information (PHI) and health information privacy rights
- Requires safeguards to protect privacy of PHI
- Who is responsible: covered entities (CE)

*Source: http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf
http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

HIPAA Security Rule
45 CFR Part 160

- *Security Standards for the Protection of Electronic Protected Health Information* (Security Rule)
- Goal: Protect privacy of PHI while allowing CEs to adopt new technologies to improve the quality and efficiency of patient care*
- Standards to protect electronic PHI that is created, received, used, or maintained by a CE
- Requires administrative, physical and technical safeguards, and security of PHI

*Source: http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html
http://www.hhs.gov/ocr/privacy/hipaa/understanding/srsummary.html

HIPAA Breach Notification Rule

"So you faxed a patient's records to a wrong number and you don't know who got it? Don't worry. It's not a HIPAA violation unless the patient finds out."

Coker GROUP
Business Advisors for the Healthcare Industry

HIPAA Breach Notification Rule
45 CFR Part 164

- CE and their BAs are required to provide notification following a breach of unsecured PHI
- Notification recipients: affected individuals, the Secretary, and depending on the extent, the media
- A breach under the Privacy Rule compromises the security or privacy of the PHI, unless there is a **low probability that PHI has been disclosed**

Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

HIPAA Breach Notification Rule

Any compromise of PHI is presumed to be a "Breach" unless it is shown that there is a "low probability" that the PHI has been compromised

- Based on a risk assessment that considers at least the following factors:
- The nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification;
- The unauthorized person to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which risk to the PHI has been mitigated

Source: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

Breach Notification – Final Rule

- Other aspects of breach notification remain unchanged
  - Contents of notification
    - Description and time of incident
    - Description of types of PHI
    - Description of investigation and mitigation
    - List of steps and contacts for patients to protect themselves
  - Notification within 60 days of discovery (without unreasonable delay)
  - Notification of prominent media outlets and HHS/OCR if 500 or more patients impacted
  - Annual notification of HHS/OCR if less than 500 patients impacted

II. 10 Step Plan

Privacy and Security

Coker GROUP
Business Advisors for the Healthcare Industry

Overview


I. Preparation
II. Risk Analysis & Action Plan
III. Risk Management
IV. Meaningful Use

I. Preparation

Step 1. Confirmation of "Covered Entity" (CE)

CE under HIPAA must…

- Comply with the Rules' requirements to protect the privacy and security of health information
- Provide individuals with certain rights with respect to their health information

Health Care Provider	Health Plan	Health Care Clearing House
• Doctors • Clinics • Nursing Homes • Pharmacies	• Health Insurance Companies • Company Health Plans • Medicaid/Medicare	• External companies that process nonstandard health information

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

Health Care Providers

Health care providers are CEs only if they transmit health information electronically in connection with a transaction covered by the HIPAA Transaction Rule.

HIPAA Transaction Rule Standards	
1. Medical Claims and Status 2. Care Payments and Remittance 3. Coordination of Benefits	4. Eligibility/ Enrollment/ Disenrollment in Health Plan 5. Premium Payments 6. Referral Certification/Authorization

Source: http://www.hhs.gov/ocr/privacy/hipaa/understanding/training/coveredentities.pdf

I. Preparation

Step 2. Leadership

- Designate both a privacy and security officer to develop and maintain practices that meet HIPAA requirements
- Engage EHR vendor to understand privacy and security functions that are available
- Select qualified professional to perform security risk analysis
  - In-house: Up-front investment in training staff
  - Outsource: Reliable, fast results, provides cost-effective ways to mitigate risk

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

EHR Security Features

- Encryption
- Auditing
- Firewalls and encryption on computer, software and router
- Backup and recovery
- Unique IDs and passwords
- Role based access controls
- Anti-virus and anti-spyware

I. Preparation

Step 3. Document Process, Findings, and Actions

- Retain records that support attestation
- Examples of documentation:
  - Completed checklists
  - Security risk analysis report
  - Risk management action plan
  - Agreements for business associates
  - Training for staff and any associated certificates
  - EHR logs that show utilization of security functions and monitor actions
  - Policies and procedures

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

II. Risk Analysis and Action Plan

Step 4. Conduct Security Risk Analysis

- Perform a security risk analysis that compares current security measures to what is legally required to safeguard patient information
- Risk analysis identifies threats and vulnerabilities
- Prioritize risks and actions based on the impact on patients, the organization, and others.
- Develop and implement an action plan
- Reassess risk analysis report annually as federal and state privacy and security requirements are updated

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Security Risk Analysis

- Security risk analysis requirements include ongoing processes of the following:
  - Determining and evaluating potential threats and vulnerabilities of PHI
  - Implementing new policies and procedures to ensure PHI is more secure and monitoring features are in place

Security Risks

Examples of Potential Information Security Risks with Different EHR Hosts	
Office-Based EHRs	**Internet-Hosted EHR**
Natural disaster could greatly disrupt availability of, and even destroy, protected health information.	The vendor controls many security settings, the adequacy of which may be hard to assess.
The security features on your office-based EHR may be less sophisticated than an Internet-hosted EHR.	Your data may be stored outside the U.S. Other countries have different health information privacy & security laws that may apply to data mantained in such country.
You directly control the security settings.	You are more dependent on the reliability of your Internet connection.
When public and private information security requirements change, you have to figure out how to update your EHR to comply and work out any bugs.	In the future, the vendor might request extra fees to update your EHR for compliance as federal, state, and private information security requirements evolve

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

II. Risk Analysis and Action Plan

Step 5. Develop Action Plan

- Action plans should focus on high priority threats
- To mitigate risks found in the risk analysis report, the action plan should include essential elements:
  - Administrative
  - Physical and technical safeguards
  - Policies and procedures
  - Organizational standards

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Security Infrastructure Components

5 Security Components for Risk Management		
Security Components	**Examples**	**Examples of Security Measures**
Physical Safeguards	• Your facility and other places where patient data is accessed • Computer equipment • Portable devices	• Building alarm systems • Locked offices • Screens shielded from secondary viewers
Administrative Safeguards	• Designated security officer • Workforce training and oversight • Controlling information access • Periodic security reassessment	• Staff training • Monthly review of user activities • Policy enforcement
Technical Safeguards	• Controls on access to EHR • Use of audit logs to monitor users and other EHR activities • Measures that keep electronic patient data from improper changes • Secure, authorized electronic exchanges of patient information	• Secure passwords • Backing-up data • Virus checks • Data encryption
Policies & Procedures	• Written policies and procedures to assure HIPAA security compliance • Documentation of security measures	• Written protocols on authorizing users • Record retention
Organizational Requirements	• Breach notification and associated policies • Business associate agreements	• Agreement review and updates

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

Health Information Security Good Practices

1. Prevent unauthorized access: utilize unique usernames and passwords, associate access levels with specific names
2. Encryption technology: prevents unauthorized personnel from reading PHI
3. Backup the system: backup system and allow recovery in case of an incident

II. Risk Management

Step 6. Manage and Mitigate Risks

- Implement action plan based on the following:

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

II. Risk Management

Step 7. Prevent with Education and Training

- HIPAA requires that workforce must know how to adhere to policies, procedures, and security audits
- Breach notification training is also required by HIPAA
- Training must be conducted annually and during any policy and/or procedure changes
- Reassess employee job descriptions and enable access to minimum EHR functions regarding patient information

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

II. Risk Management

Step 8. Communicate with Patients

- Implement policies for communicating with patients if a breach impacting patient health information occurs
  - Refer to 45 CFR 164.520 (Notice of Privacy Practices for PHI)
- Establish a process on how patients receive copies of their health records
- Implement procedures for patient requests to modify health information and restrict disclosure

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

II. Risk Management

Step 9. Update Business Associate (BA) Agreements

- Ensure BA* agreements require compliance with HIPAA and Health Information Technology for Economic and Clinical Health Act (HITECH) Breach Notification requirements
  - Requires BAs to safeguard PHI, train workforce, and adhere to breach notification requirements
- Update BA agreements to be compliant with new national standards

**BA- engaged by CE to carry out health care activities and functions that involve PHI*

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

III. Meaningful Use (MU)

Step 10. Attest for the Security Risk Analysis

- MU attestation is a legal statement that you have met specific standards and may be subject to an audit
- Attest for EHR incentive program after security risk analysis is complete and corrective actions have taken place to address high priority security threats

Source: http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf

III. Resources and Considerations

Coker GROUP
Business Advisors for the Healthcare Industry

Resources and Considerations

- Guidance on Risk Analysis Requirements under the HIPAA Security Rule (Issued by OCR)
- Guide to Privacy and Security of Health Information
- Local Regional Extension Center (REC)
- http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/

IV. Q & A

Coker GROUP
Business Advisors for the Healthcare Industry

Contact Us

Jeffery Daigrepont
Senior Vice President
t. 770.597.0590
e. jdaigrepont@cokergroup.com

Coker GROUP
Business Advisors for the Healthcare Industry