HIPAA Security Risk Assessment

Presented by
Cathy Montgomery, RN, CASC

HHS.gov Announcement

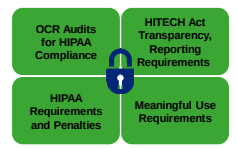
Alert: Phishing Email Disguised as Official OCR Audit Communication - November 28, 2016
It has come to our attention that a phishing email is being circulated on mock HHS Departmental letterhead under the signature of OCR's Director, Jocelyn Samuels. This email appears to be an official government communication, and targets employees of HIPAA covered entities and their business associates. The email prompts recipients to click a link regarding possible inclusion in the HIPAA Privacy, Security, and Breach Rules Audit Program. The link directs individuals to a non-governmental website marketing a firm's cybersecurity services. In no way is this firm associated with the U.S. Department of Health and Human Services or the Office for Civil Rights. We take the unauthorized use of this material by this firm very seriously.

New technologies

New Care Models

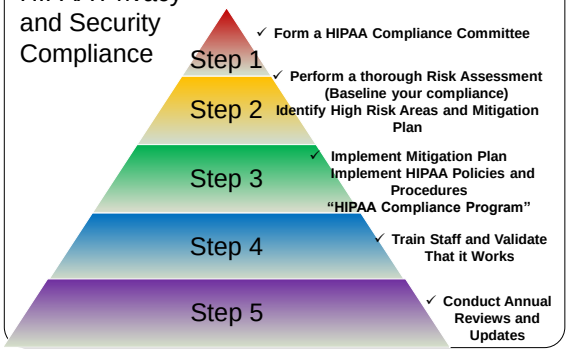
Health Care Transformation Requires Security and Privacy Integration

Growing Consumer Engagement



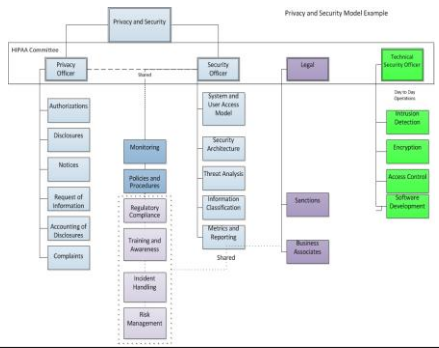
Increased Regulatory Scrutiny

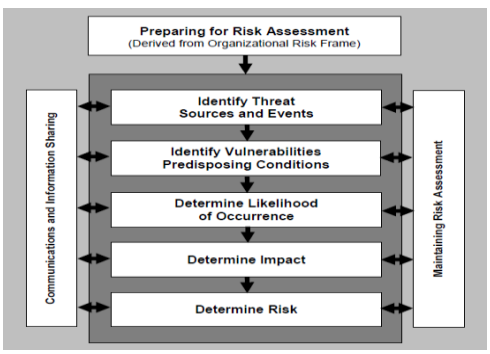
Foundation to HIPAA Privacy and Security Compliance



- ✓ Form a HIPAA Compliance Committee
- ✓ Perform a thorough Risk Assessment (Baseline your compliance) Identify High Risk Areas and Mitigation Plan
- ✓ Implement Mitigation Plan Implement HIPAA Policies and Procedures "HIPAA Compliance Program"
- ✓ Train Staff and Validate That it Works
- ✓ Conduct Annual Reviews and Updates

HIPAA Committee Example Organization





Help is Available

- Security Risk Assessment Tool (SRAT)

https://www.healthit.gov/providers-professionals/security-risk-assessment-tool

https://www.youtube.com/watch?v=V2LyAEmhq90&t=1s

Topics = Policies

- **Risk Analysis = 1**
- **Security Plan = 2**
- **Access = 15**
- **Safeguards = 13**
- **Human Resources = 2**
- **Training = 0**
- **Business Associates = 1**
- **Emergency Plan = 7**
- **Audits = 4**
- **Incident Response = 2**

Total of 47 required or addressable polices

Audit Policies

AUDITS

- **Review of IT activity**
- **Identify hardware, software that record or examine IT activities**
- **Distribution of audit reports to appropriate members of the team**
- **Retention requirements for audit reports**

Security Rule Compliance

Security Rule is separated into 3 categories:

1. **Administrative Safeguards** — Govern personnel practices and provide a framework for accessing and using ePHI, and include conducting a risk analysis and designating a Security Officer
2. **Physical Safeguards** — Methods for securing the physical spaces and devices that contain ePHI, such as servers and workstations
3. **Technical Safeguards** — Apply to information systems and ensure that hardware, software and networks are protected

The Security Rules Standards are technology neutral.

HIPAA Security Rule Components

Administrative Safeguards	Physical Safeguards	Technical Safeguards
• Security Management Process • Assigned Security Responsibility • Workforce Security • Information Access Management • Security Awareness and Training • Security Incident Procedures • Contingency Plan • Evaluation • Business Associate Agreements	• Facility Access Control • Workstation Use • Workstation Security • Device and Media Control	• Access Control • Audit Control • Integrity • Personal or Entity Authentication • Transmission Security

Implementation Specifications

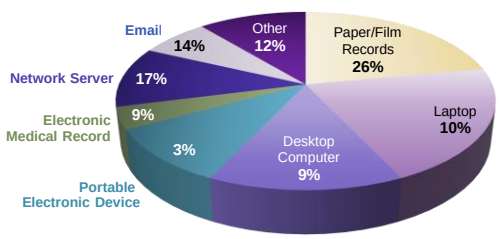
- Required = must be implemented
- Addressable = maybe
  1. Implement
  2. Implement alternatives
  3. No action

Risk Assessment

➢ **Complete a risk assessment:**

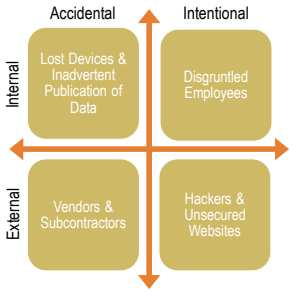
- Initial HIPAA Security Risk Assessment was likely completed several years ago
- Risk assessment is an ongoing process as reflected in the HIPAA Security Rule's requirement to periodically re-evaluate protocols in response to environmental or operational changes affecting the security of ePHI
- Periodically – every two or three years + whenever a new electronic technology is adopted or changed

Location of Reported Breach (as of September 2015)



https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

How Do Incidents Occur?



Appendix 1

RISK REGISTER

RISK MATRIX

Likelihood		Consequences: Insignificant (Any injury or disease that needs first aid treatment only. 1)	Minor (Any injury or disease requiring medical treatment and/or that is likely to result in a person being incapacitated from normal activity for a continuous period of up to 7 days. 2)	Moderate (Any injury or disease that is likely to result in a person being incapacitated from normal activity for a continuous period of 7 or more days. 3)	Major (A fatality or total and permanent disability 4)	Catastrophic (Multiple fatalities 5)
Almost Certain — The event is expected to occur in most circumstances.	1					
Likely — The event will probably occur in most circumstances.	2					
Moderate — Given time, likely to occur.	3					
Unlikely — More likely not to occur under normal conditions.	4					
Rare — The event may occur only in exceptional circumstances.	5					

Once you have determined above the likely Consequences Ratings for the identified risks refer to the Risk Analysis Matrix to determine the overall Risk Rating for the identified Risk. The higher the Risk Rating the more immediate and higher level attention is required.

Severe Risk	Discontinue operation and / or immediate corrective action required.
Significant Risk	Corrective action needed. Action in short term as appropriate.
Moderate Risk	Attention indicated.
Minor Risk	Implement practicable short-medium term control measures.

https://www.youtube.com/watch?v=Rge4k8w9tig&t=3s

Best Practices from ERISA Advisory Committee

Computers and Systems

A. Data
1. Keep only data that is needed.
2. Use effective processes to discard unnecessary data, including back-up paper and electronic copies.
3. Know where PHI is located in all of the organization's systems.
4. Understand cloud computing and/or remote data storage, including how data is stored or protected.

B. Systems
1. Keep computer systems updated, including prompt installation of software patches.
2. Stay current on electronic threats and effective responses.
3. Follow National Institute of Security and Technology (NIST) guidelines on computer configuration.
4. Use full disk encryption on laptops and external data storage devices that might include PHI or information on how to access it.
5. Maintain complete log-in for the network, firewalls, routers and key software applications.
6. Limit or define usage of portable devices.

PHI Safeguards Under Privacy and Security Rules

Privacy and Security Rules require the following types of safeguards: (list is not exhaustive)

- Administrative:
  - Designate Privacy Officer and Security Officer
  - Designate employees, either by title or department, who need access to PHI to perform their job functions, and identify type and amount of PHI needed
  - Limited access to space where PHI is handled (i.e., badged or key entrance)
- Related to ePHI:
  - Computer passwords
  - Automatic log-off or screensavers
  - Protective screens
  - Designated space to secure ePHI, such as secure website or secure network drive
  - Encrypted email (or limited email use)
  - Encrypted laptops
  - Encrypted portable devices or limited use of portable devices

"Red Flag" Issues

- Inadequate encryption policies and procedures
- Poor access control and activity review
- Poor mobile device and laptop policies and controls
- Lack of IT governance—standards, inventory control, basic security procedures (patching, administrative lockdown, etc.)
- Inadequate disaster recovery procedures
- Insufficient IT policies and procedures
- Lack of advanced monitoring techniques—intrusion detection system/intrusion prevention system (IDS/IPS), log correlation, data loss prevention (DLP)
- Lack of a security officer

CELL PHONES

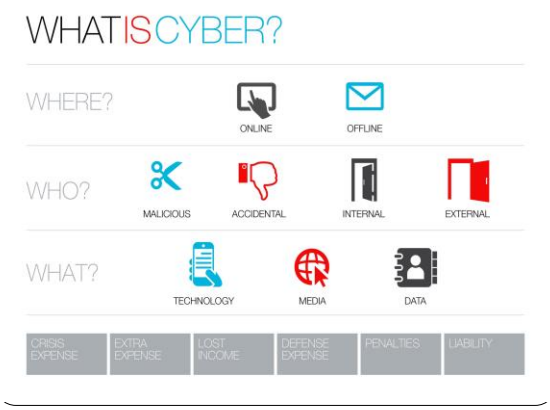
- Policies & Procedures esp. as it relates to BYOD
- Who is responsible for securing the device
- Password protection
- Remote wiping/disabling program

SECURE TEXTING

- Know who has access to private health information and control over how it is used, limit information.
- When encryption and physical data protection is in place for individuals who use their personal mobile devices to communicate private health information or to access sensitive patient data in the course of their work.
- When policies are in place to cover the scenarios in which mobile devices are lost or stolen, or if the owner wishes to dispose of their mobile device, so that private health information can be deleted remotely.
- When private health information has been breached, but the encrypted data can be deleted remotely, it will not be necessary to notify the patient or Office of Civil Rights provided that the data is removed in a timely manner.
- Inventory of devices.

New Technologies and Possible Data Threats

- **Mobile Devices:** laptops, smartphones, tablets
- **Cloud Computing:** Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS)
- **Wearables:** smartwatches, smartglasses, smart ID badges
- **Robotics:** medical kiosks



Incidents

Top 10 Healthcare Data Breaches 2015

Organization	Records Breached	Type of Breach
Anthem	78,800,000	Hacking / IT Incident
Premera	11,000,000	Hacking / IT Incident
Excellus	10,000,000	Hacking / IT Incident
UCLA Health	4,500,000	Hacking / IT Incident
mie	3,900,000	Hacking / IT Incident
CareFirst	1,100,000	Hacking / IT Incident
[illegible]	697,586	Hacking / IT Incident
Georgia Department of Community Health	557,779	Hacking / IT Incident
Beacon	306,789	Hacking / IT Incident
DJO	160,000	Laptop Theft
2015 Total	111,022,154	(almost 35% U.S. population)

Complaints Received by HHS/OCR by Calendar Year

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/data/complaintsyear.html

HIPAA Security Risk Assessment

Please email your questions and comments to:

cathy@excellentiagroup.com
Excellentia Advisory Group, LLC
1-636-875-5088 ext. 102

EXCELLENTIA
ADVISORY GROUP