Boot Camp: Security Risk Analysis

May 7-9, 2019 @ The Hotel at Auburn University
The Health Information Technology Evaluation and Quality (HITEQ) Center is a HRSA-funded Cooperative Agreement that collaborates with HRSA partners to support health centers in full optimization of their EHR/Health IT systems.
HITEQ Services

• Web-based health IT knowledgebase
• Workshops and webinars
• Targeted technical assistance
HITEQ Focus Areas

- Health IT Enabled Quality Improvement
- EHR Selection and Implementation
- Health Information Exchange
- QI/HIT Workforce Development
- Value-Based Payment
- Privacy and Security
- Electronic Patient Engagement
- Population Health Management
Legal Disclaimer

• The information included in this presentation is for informational purposes only and is not a substitute for legal advice.

• Please consult an appropriate attorney if you have any particular questions regarding a legal issue.
Tuesday, May 7
8:00am - 8:30am  Intro and Overview
8:30am-10:30am  HIPAA Compliance and Healthcare Security Overview
                  What is Security Risk Assessment?
                  Conducting Security Risk Assessment
                  Security Risk Management
10:45am - 12pm  Information Security Best Practices and HIPAA
                  Board-Level Responsibilities
1pm-2:30pm       ONC SRA Toolkit
2:45pm-5pm       Security Risk Assessment Exercise
Overview of Privacy and Security
Problem Statement

• Increased use of electronic health record systems increases security risk
• Increased use of IoT enabled mobile health and medical devices increases security risk
• Increased use of internet-based systems increases security risk
• Increased numbers of users on a given system increases security risk
• That can be a lot of security risks for small to medium-sized health centers to effectively manage!
Ransomware Destroys Small Practice EHR Database

by Jacob Oderhoff | Jan 20, 2018 | Health Information Technology, Newsletter, Newsletter - DD Board, Threat Intelligence |

During December, 2017, Eagle Consulting received an inquiry from a small medical practice that lost its entire electronic record database in an attack from the Hermes ransomware. By the time the practice became aware of the attack, the damaged database overwrote the only available backup. Eagle Consulting provided support for the HIPAA-mandated investigation and response to this security incident.

Ransomware is a form of malware that holds computer files hostage (by encrypting them with an uncrackable encryption algorithm) until a ransom is paid. The ransomware operates by exploiting vulnerabilities in network systems that are not protected by adequate security measures.


Your Electronic Medical Records Could Be Worth $1000 To Hackers

We’re not a Target...

- Name and Contact Info
- SSN/SIN
- Birth Date
- Insurance Information
- Other Identification
- Payment Information
We’re not a Target…?

1. Insurance Fraud
2. Identity Theft
3. Privacy

<table>
<thead>
<tr>
<th></th>
<th>Medical Record</th>
<th>Credit Card</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black Market Value per record</td>
<td>~$5</td>
<td>~$.50</td>
</tr>
<tr>
<td>Demographics</td>
<td>Yes</td>
<td>Maybe</td>
</tr>
<tr>
<td>Payment Information</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lifetime of Information</td>
<td>Forever</td>
<td>Short</td>
</tr>
<tr>
<td>Risk to Consumer</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Privacy Concerns</td>
<td>High</td>
<td>Moderate</td>
</tr>
</tbody>
</table>
Maybe we are a Target?

### Medical Identity Theft

<table>
<thead>
<tr>
<th>Estimated U.S. population of medical identity theft victims</th>
<th>Calculus</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. population in 2014 (source: Census Bureau)</td>
<td>320,073,000</td>
</tr>
<tr>
<td>U.S. population below 18 years of age</td>
<td>29%</td>
</tr>
<tr>
<td>U.S. adult-aged population</td>
<td>223,940,455</td>
</tr>
<tr>
<td>Base rate for medical identity theft in 2014</td>
<td>0.0102</td>
</tr>
<tr>
<td>Estimated number of medical identity theft victims</td>
<td>2,317,969</td>
</tr>
</tbody>
</table>
Maybe we are a Target?

41% of Healthcare Organizations have reported that they experienced a breach in 2018

Ok, we are a Target... but we’re Secure, Right?

Hospital Gets Hacked Through Its Internet-Connected Heart Monitor

Sunday, April 15, 2018  Wang Wei
Entry Points

- Phishing
- Ransomware
- Connected Medical Devices (IoT)
- Social Engineering
- Misconfigured Servers
- Inadvertent Disclosures
- Unpatched Systems
- Vendors and Business Associates
- Facilities and other supporting systems

1. Assume Breach
2. Defense in Depth
3. Risk-based Approach
4. Detection and Response
5. Continuous Improvement
• **Health Insurance Portability and Accountability Act** of 1996 (HIPAA): required HHS to adopt national standards for electronic health care transactions and code sets, unique health identifiers, and security. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

• **Health Information Technology for Economic and Clinical Health (HITECH) Act’s Meaningful Use program**: required objective measures for ensuring the safety of electronic Protected Health Information (ePHI) as dictated by the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) (OCR 2009).
## Security Rule Requirements

<table>
<thead>
<tr>
<th>Security Components</th>
<th>Example Variables</th>
<th>Example Security Measures</th>
</tr>
</thead>
</table>
| Physical Safeguards         | • Facility structure  
                              • Data storage center  
                              • Computer hardware  | • Building alarm system  
                              • Locked doors  
                              • Monitors shielded from view |
| Administrative Safeguards   | • Designated security officer  
                              • Staff training and oversight  
                              • Information security control  
                              • Security Risk Assessment / review | • Staff training  
                              • Monthly review of user activity  
                              • Policy enforcement  
                              • New hire background checks |
| Technical Safeguards        | • Controls on access to EHR  
                              • Audit log monitoring  
                              • Secure electronic exchanges | • Secure passwords  
                              • Data backup  
                              • Virus scans  
                              • Encryption |
| Policies and Procedures     | • Written P&P addressing HIPAA  
                              • Security requirements  
                              • Documentation of security measures | • Written protocols on safeguards  
                              • Record retention  
                              • Periodic policy and procedure review |
| Organizational Requirements | • Breach notification and other policies  
                              • Business Associate agreements | • Periodic Business Associate Agreement review and updates |

Reference: Michigan Center for Effective IT Adoption
Security Risk Assessment

- Required by HIPAA Security Rule and Meaningful Use
- Commonly conducted annually
- Not required to, but recommend following an established framework such as NIST, COBIT, or ISO
Security Risk Assessment

• Challenges
  – Can be hard to understand requirements
  – Hard to find concrete examples and expertise
  – Organizations worry about enforcement actions if they acknowledge they have security risks
  – Many “risk assessments” end up being an enumeration of security controls or simple checklists
Compliance vs. Security

Compliance is not your blueprint
Avoid checkbox compliance
Remember “reasonable and appropriate”
Compliance is an ongoing requirement

Security is not a product
Security is an ongoing program
Security is not just an IT responsibility
Security is a mindset
### Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

**Show Advanced Options**

<table>
<thead>
<tr>
<th>Expand All</th>
<th>Name of Covered Entity</th>
<th>State</th>
<th>Covered Entity Type</th>
<th>Individuals Affected</th>
<th>Breach Submission Date</th>
<th>Type of Breach</th>
<th>Location of Breached Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Dean Health Plan</td>
<td>WI</td>
<td>Health Plan</td>
<td>1311</td>
<td>06/15/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Paper/Films</td>
</tr>
<tr>
<td>0</td>
<td>Health Equity, Inc.</td>
<td>UT</td>
<td>Business Associate</td>
<td>16000</td>
<td>06/12/2018</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>0</td>
<td>Healthland Inc.</td>
<td>MN</td>
<td>Business Associate</td>
<td>514</td>
<td>06/10/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>0</td>
<td>New England Baptist Health</td>
<td>MA</td>
<td>Healthcare Provider</td>
<td>7582</td>
<td>06/08/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>0</td>
<td>Massac County Surgery Center dba Orthopaedic Institute Surgery Center</td>
<td>IL</td>
<td>Healthcare Provider</td>
<td>2000</td>
<td>06/08/2018</td>
<td>Hacking/IT Incident</td>
<td>Email</td>
</tr>
<tr>
<td>0</td>
<td>RISE Wisconsin, Inc.</td>
<td>WI</td>
<td>Healthcare Provider</td>
<td>3731</td>
<td>06/07/2018</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>0</td>
<td>Benefit Outsourcing Solutions</td>
<td>MI</td>
<td>Business Associate</td>
<td>1144</td>
<td>06/07/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>0</td>
<td>University of Utah Health</td>
<td>UT</td>
<td>Healthcare Provider</td>
<td>607</td>
<td>06/02/2018</td>
<td>Theft</td>
<td>Laptop, Other Portable Electronic Device</td>
</tr>
<tr>
<td>0</td>
<td>Capitol Anesthesiology Association</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>2231</td>
<td>06/01/2018</td>
<td>Hacking/IT Incident</td>
<td>Network Server</td>
</tr>
<tr>
<td>0</td>
<td>Florida Agency for Persons with Disabilities</td>
<td>FL</td>
<td>Health Plan</td>
<td>1951</td>
<td>06/01/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>0</td>
<td>SimplyWell</td>
<td>TX</td>
<td>Business Associate</td>
<td>597</td>
<td>06/01/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Other</td>
</tr>
<tr>
<td>0</td>
<td>Dignity Health</td>
<td>CA</td>
<td>Healthcare Provider</td>
<td>55947</td>
<td>05/31/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
<tr>
<td>0</td>
<td>The University of Texas MD Anderson Cancer Center</td>
<td>TX</td>
<td>Healthcare Provider</td>
<td>1266</td>
<td>05/31/2018</td>
<td>Unauthorized Access/Disclosure</td>
<td>Email</td>
</tr>
</tbody>
</table>

**407 Cases currently under investigation by HHS/OCR**
Approach

• The Security Risk Assessment approach is designed to allow organizations to implement “reasonable and appropriate” security controls as opposed to being prescriptive.

• For example, what is a reasonable disaster recovery plan for a large health system would be excessive for a small doctor’s office; this allows flexibility while still being enforceable.

• If other organizations of the same size are encrypting their laptops, it would seem reasonable to expect your organization to do the same.

• But how can you determine what is “reasonable and appropriate” for your organization?

**Take a Security Risk Management approach and look to industry standards and guidance**
Security Risk Analysis
Under the HIPAA Security Rule, you are required to:

… conduct an **accurate and thorough analysis** of the potential risks and vulnerabilities to the **confidentiality, integrity, and availability** of ePHI. Once you have completed the risk analysis, you must take any additional “reasonable and appropriate” steps to reduce identified risks to **reasonable and appropriate** levels.

(45 CFR 164.308(a)(1)(ii))
False. Your EHR vendor may be able to provide information, assistance, and training on the privacy and security aspects of the EHR product. However, EHR vendors are not responsible for making their products compliant with HIPAA Privacy and Security Rules. **It is solely your responsibility to have a complete risk analysis conducted.**
False. To comply with HIPAA, you must continue to review, correct or modify, and update security protections.

Under MIPS/MACRA, reviews are required for each reporting period.
True or False: I can use a security checklist as a security risk analysis

False. An “accurate and thorough” security risk analysis identifies threats, vulnerabilities, and impact in addition to existing security controls to determine risks to ePHI.
What is Security Risk Analysis?

Threat x Vulnerability x Impact

= Security Controls
A Threat may be defined as: “[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”
Examples of threats:
– Natural
  • Flood, earthquake, tornado, ice storm, fire
– Human
  • Outsiders such as hackers, patients
  • Insiders such as workforce members, contractors
  • May be intentional or unintentional (i.e. inadvertent modification, deletion, or disclosure of information)
Vulnerability is defined in NIST Special Publication (SP) 800-30 as “[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.”
Examples of vulnerabilities:

- Technical
  - Unpatched systems
  - Weak, default, or no passwords
  - PHI on unencrypted media
  - Poorly configured firewalls or servers
  - Open wireless networks or using weak encryption

- Non-Technical
  - Lack of security awareness training
  - Lack of (or ineffective) policies and procedures
A Risk can then be defined as: "[t]he net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur."
Elements of Security Risk Analysis
Elements of Security Risk Analysis

As defined by OCR/NIST:

1. Define the scope
2. Data collection
3. Identify and document potential threats to ePHI
4. Assess current security measures
5. Determine the likelihood of threat occurrences
6. Determine the potential impact of threat occurrences
7. Determine the level of risk
8. Finalize documentation
9. Regular risk analysis
Continuous Risk Analysis

A truly integrated risk analysis and management process is performed as new technologies and business operations are planned, thus reducing the effort required to address risks identified after implementation.

For example, evaluate security risks when you:

– Have experienced a security incident
– Have change in ownership or turnover in key staff/management
– Are planning to incorporate new technology to make operations more efficient
– Are making changes to your servers or network devices
– Are changing workflows
Methodology

- Observe
- Interview
- Test
Resources

• HealthIT.gov

• The Office for Civil Rights
  – Guidance on Risk Analysis Requirements under the HIPAA Security Rule

• The National Institute for Standards in Technology (NIST)
  – NIST SP 800-30 Guidance for Conducting Risk Assessments
  – NIST SP 800-66 An Introductory Resource Guide for Implementing the HIPAA Security Rule
  – HIPAA Security Rule Toolkit
Security Risk Management
“Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).”
“(i) The size, complexity, and capabilities of the covered entity.

(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to EPHI.”
On two occasions in 2015, the FBI notified 21CO that PHI was illegally obtained by an unauthorized third party and produced 21CO patient files purchased by an FBI informant

21CO determined that 2,213,597 individuals were affected

Failure to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of the ePHI

Failure to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

Failure to implement procedures to review information system activity, such as audit logs

Disclosed PHI to 3rd party vendors without BAAs

May 25, 2017, 21CO filed for Chapter 11 bankruptcy protection

$2.3 million - December 2017
Security Risk Management – Case Study

- Review all vendor and contractor relationships to ensure BAAs are in place as appropriate and address breach/security incident obligations
- Risk analysis and risk management should be integrated into business processes; conducted regularly and when new technologies and business operations are planned
- Dispose of PHI on media and paper that has been identified for disposal in a timely manner
- Incorporate lessons learned from incidents into the overall security management process
- Provide training specific to organization and job responsibilities and on regular basis; reinforce workforce members’ critical role in protecting privacy and security
NIST Risk Management Framework (RMF)
When a company manages cyber risk through a COSO lens, it enables the board of directors and senior executives to better communicate their business objectives, their definition of critical information systems, and related risk tolerance levels.

This enables others within the organization, including IT personnel, to perform a detailed cyber risk analysis by evaluating the information systems that are most likely to be targeted by attackers, the likely attack methods, and the points of intended exploitation. In turn, appropriate control activities can be put into place to address such risks.
Break
Information Security Basics
Information Security Basics

Protect the confidentiality, integrity, and availability of electronic PHI

- Identify everywhere PHI is stored or transmitted:
  - Stored PHI may include EHR/PM, patient portal, medical devices, file storage, scanned documents, web-based systems, removable storage, photocopiers, fax machines, or electronic fax systems
  - Transmitted PHI may include email, fax, or text messages for purposes of billing, insurance, prescriptions, communicating with other healthcare providers, communicating with patients, communicating within the office, research, or other third parties
Information Security Basics

- Protect PHI in transit
  - Only send over the internet encrypted (encrypted email, https, secure ftp)

- Protect PHI at rest
  - Unique logins
  - Access controls (password protect all devices)
  - Consider encryption of PHI and full disk encryption for laptops, tablets, and smartphones
– Practice continuous maintenance, patching, and upgrades
  • Apply operating system updates regularly
  • Where possible, set programs to update automatically
  • Subscribe to information security alert services such as the US Computer Emergency Readiness Team (https://www.us-cert.gov/)
  • Regularly test your backups as they can fail frequently.
Antivirus is important, but not sufficient!

- Today’s attacks are adept at circumventing AV
- Consider full endpoint protection
  - Including:
    - Malware removal based on existing signature files and heuristic algorithms
    - Built-in antispyware protection
    - Ingress/Egress firewall
    - IPS/IDS sensors and warning systems
    - Application control and user management
    - Data input/output control, including portable devices
Information Security Basics

• Administrative Controls
  – Security Awareness Training
    • Build a culture motivated and dedicated to securing patient data
    • Train users on handling of PHI as well as detecting and responding to suspicious activity such as phishing and social engineering attempts
  – Information Handling Policies and Procedures
  – If you are unsure, hire external consultants to help you build a strategy and test that strategy frequently
Security for IT Managers and System Administrators
IT Managers and System Administrators

- While the HIPAA Security Rule does provide a framework for security risk management, it can be difficult to know what specific steps to take to implement “reasonable and appropriate” security controls
- What are other organizations doing? What are the most effective controls?
- Look to industry standards
- The Center for Internet Security (CIS) maintains a list of the Top 20 Security Controls
  - Internationally recognized
  - Guidance on varying levels of maturity
  - Specific and practical
- According to the Australia Signals Directorate (ASD): “Incorporating the Top 4, the eight mitigation strategies with an 'essential' rating are so effective at mitigating targeted cyber intrusions and ransomware that ASD considers them to be the cyber security baseline for all organizations.”
IT Managers and System Administrators

Center for Internet Security (CIS) Top 20 Security Controls

Includes:

- CSC 1: Inventory of Authorized and Unauthorized Devices
- CSC 2: Inventory of Authorized and Unauthorized Software
- CSC 3: Secure Configurations for Hardware and Software
- CSC 4: Continuous Vulnerability Assessment and Remediation
- CSC 5: Controlled Use of Administrative Privileges
CIS Controls V7 separates the controls into three distinct categories: basic, foundational, and organizational.

- **Basic (CIS Controls 1-6):** Key controls which should be implemented in every organization for essential cyber defense readiness.
- **Foundational (CIS Controls 7-16):** The next step up from basic – these technical best practices provide clear security benefits and are a smart move for any organization to implement.
- **Organizational (CIS Controls 17-20):** These controls are different in character from 1-16; while they have many technical elements, CIS Controls 17-20 are more focused on people and processes involved in cybersecurity.

https://www.cisecurity.org/blog/cis-controls-version-7-whats-old-whats-new/
CIS Top 20 Security Controls

• Implementation Group 1
  – An organization with limited resources and cybersecurity expertise available to implement Sub-Controls

• Implementation Group 2
  – An organization with moderate resources and cybersecurity expertise to implement Sub-Controls

• Implementation Group 3
  – A mature organization with significant resources and cybersecurity experience to allocate to Sub-Controls
<table>
<thead>
<tr>
<th>Control Family</th>
<th>HIPAA Security Rule Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSC #1: Inventory and Control of Hardware Assets</td>
<td>164.310(c): Workstation Security - R</td>
</tr>
<tr>
<td></td>
<td>164.310(d)(1): Device and Media Controls: Accountability – A</td>
</tr>
<tr>
<td>CSC #2: Inventory and Control of Software Assets</td>
<td>164.310(c): Workstation Security - R</td>
</tr>
<tr>
<td>CSC #3: Continuous Vulnerability Management</td>
<td>164.308(a)(8): Evaluation</td>
</tr>
<tr>
<td></td>
<td>164.308(a)(6): Security Incident Procedures</td>
</tr>
<tr>
<td>CSC #4: Controlled Use of Administrative Privileges</td>
<td>164.310(b): Workstation Use - R</td>
</tr>
<tr>
<td></td>
<td>164.310(c): Workstation Security - R</td>
</tr>
<tr>
<td></td>
<td>164.312: Access Control: Unique User Identification - R</td>
</tr>
<tr>
<td></td>
<td>164.312(b): Audit Controls</td>
</tr>
<tr>
<td></td>
<td>164.312(d): Person or Entity Authentication</td>
</tr>
<tr>
<td>CSC #5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers</td>
<td>164.310(c): Workstation Security – R</td>
</tr>
<tr>
<td></td>
<td>164.312(b) – Audit Controls</td>
</tr>
</tbody>
</table>
**CSC 1: Inventory and Control of Hardware Assets**

- "Know what you have" is the basis of information security
- You can’t secure it if you don’t know about it
- Actively managing hardware inventory provides the basis for CSC 2-20
- This is important in regard to the HIPAA Security Rule and conducting a Security Risk Assessment because it allows you to create an inventory of ePHI

**Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.**

164.310(c): Workstation Security - R  
164.310(d)(1): Device and Media Controls: Accountability - A
“Know what you have” Part 2
Maturity Model
Whitelisting is one of the best protections against malware and hardest things to do
Create an inventory of software systems that store or transmit ePHI including cloud-based systems

Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

164.310(c): Workstation Security
“Most attacks exploit known vulnerabilities that have never been patched despite patches being available for months, or even years. In fact, the top 10 known vulnerabilities accounted for 85 percent of successful exploits.” Verizon 2016 Data Breach Investigations Report

164.308(a)(8): Evaluation
164.308(a)(6): Security Incident Procedures
“The misuse of administrative privileges is a primary method for attackers to spread inside a target organization”
- Workstation users running as privileged users
- Attacker elevates permissions by compromising the password of a network administrator gaining access to all systems on the network

- Only use administrative accounts when they are required
- Keep an inventory of administrative accounts
- Set up alerting/reporting on the use, creation, and modification of administrative accounts

164.310(b): Workstation Use - R
164.310(c): Workstation Security - R
164.312: Access Control: Unique User Identification - R
164.312(b): Audit Controls
164.312(d): Person or Entity Authentication
Now that you “Know what you have”, you can manage it

Secure Configurations for hardware and software on mobile devices, laptops, workstations, and servers

Put systems in place to enforce ongoing compliance with security benchmarks

Benchmarks available:
- The Center for Internet Security Benchmarks Program (www.cisecurity.org)
- The NIST National Checklist Program (checklists.nist.gov)

Establish, implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

164.310(c): Workstation Security
Monitoring and Logging are critical to detecting and responding to security incidents.

HIPAA requires that CEs take steps to actively detect and respond to security incidents.

Consider Network, Operating System, and Application layers.

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

164.308(a)(1): Information System Activity Review – R
164.312(b) – Audit Controls
Additional Best Practices

• Network segmentation
• IDS/IPS
• Two-factor authentication for remote access and sensitive/privileged accounts
• Encryption of data at rest
Board of Directors
As the costs and organizational impacts of breaches rise, boards are paying more attention to cybersecurity.

While a board is generally not involved in the day-to-day operations of cybersecurity, they do have a responsibility to ensure that proper structures are in place and that the organization is taking appropriate steps to identify and address cybersecurity risks.

Cybersecurity may be incorporated into existing corporate risk management frameworks (RMF):
- e.g. COSO/COBIT
- Results of the Security Risk Assessment should be summarized and reported to the board through the RMF
- Report security incidents to the board
Board Responsibility for Cybersecurity Oversight

- **People**
  - Assign board-level responsibility for cyber security

- **Processes**
  - Boards should inform themselves of specific operational, reporting, and compliance aspects of cybersecurity, using at least one recognized framework to do so
  - Recognized international frameworks include COBIT, ISO27001/2, NIST 800-53, HITRUST

- **Technology**
  - The Board should have representation from a person with specific technical and cybersecurity experience and familiarity with industry standards and privacy law
  - If these capabilities are not available internally, the organization may wish to seek outside assistance

“Members of the board need to be aware of the organization’s information assets and their criticality to ongoing business operations. This can be accomplished by periodically providing the board with the high-level results of comprehensive risk assessments and business impact analyses.”

Source: Global Network of Directors International, Guiding Principles for Cybersecurity Oversight
Cybersecurity questions directors should be asking:

1. What steps is management taking to identify and address cybersecurity risks?
2. How is the organization protecting customer, employee and other important information from significant threats?
3. How much are we spending on information security and what are the outcomes?
4. How are our disaster recovery, business continuity, and incident response plans kept up-to-date? Are they thoroughly tested, and communicated to the right people so we minimize the impact of a breach when it happens?

Source: Cybersecurity Risk — Questions for Directors to Ask
Cybersecurity questions directors should be asking:

5. What cyber-threats could really damage this organization?
6. How are we distinguishing between the systems, networks, and users we control or have strong assurance over as a third party, and those which we do not? Which digital relationships and what data and identities from outside our organization can we trust?
7. What are the soft spots in our cyber-defenses (and those of our business partners)? Have these soft spots resulted in a breach impacting our business, and what is being done to identify root causes and remediate these ‘weak’ links?

Source: Cybersecurity Risk — Questions for Directors to Ask
Conclusion

• Everyone from the Board of Directors to the system administrators and end users have responsibilities for privacy and security
• Those responsibilities will vary depending on the position
• There are known best practices and frameworks that can be followed to help ensure information security is addressed appropriately
Want more information?

Small to medium provider organizations such as community health centers, rural clinics, and critical access hospitals work to provide the highest quality health services with limited resources. Because they operate with a smaller staff than larger health systems, many employees take on tasks outside their job description. Provision of information technology (IT) services is often a task non-experts at these smaller operations must take on to achieve organizational objectives. The impact of this was never more apparent than when the Health Information Technology for Economic and Clinical Health Act's Meaningful Use policies required objective measures for ensuring the safety of electronic Protected Health Information (ePHI) as dictated by the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA).

Privacy & Security Resource Sets

- Health IT Leadership & Best Practices
- Mastering HIPAA
- SRA Toolkit for Health Centers
- Breach Mitigation & Response Basics
- The Ransomware Guide

Need Assistance?

Would you like more assistance regarding Privacy & Security strategies or support in using any of the include resource sets?

Request Support
Questions? Comments?

Contact HITEQ at: hiteqcenter.org
hiteqinfo@jsi.com
@HITEQCenter
1-844-305-7440
THIS PROJECT WAS SUPPORTED BY THE HEALTH RESOURCES AND SERVICES ADMINISTRATION (HRSA) OF THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) UNDER COOPERATIVE AGREEMENT NUMBER U30CS29366, TRAINING AND TECHNICAL ASSISTANCE NATIONAL COOPERATIVE AGREEMENT FOR $1,954,318 WITH 0% OF THE TOTAL NCA PROJECT FINANCED WITH NON-FEDERAL SOURCES. THIS INFORMATION OR CONTENT AND CONCLUSIONS ARE THOSE OF THE AUTHOR AND SHOULD NOT BE CONSTRUED AS THE OFFICIAL POSITION OR POLICY OF, NOR SHOULD ANY ENDORSEMENTS BE INFERRED BY HRSA, HHS OR THE US GOVERNMENT.