CHCANYS DEFINING NEW DIRECTIONS
Community Health Care Association of New York State

Community Health Center Privacy & Security Best Practices and Cloud-based EHR Considerations

Workshop for the
Community Health Care Association
of New York State

November 28th, 2017

COMMUNITY HEALTH CENTER FQHC QUALITY

HITEQ Purpose

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 QI

EHR Selection & Implementation

Health Information Exchange

Achieving Meaningful Use

Health IT/QI Workforce Development

Value-Based Payment

Privacy & Security

Electronic Patient Engagement

Population Health

Telehealth

Today's Presenter

Nathan Botts, PhD, MSIS

- Senior Study Director – Healthcare Delivery, Research, and Evaluation, Westat
- Health informatics specialist, with over 11 years of clinical software and systems research and development experience
- Privacy & Security domain lead for the HRSA HITEQ Center project.
- Facilitator for the Privacy and Security Community of Practice of the ONC Knowledge Sharing Network for Regional Extension Centers.
- Co-lead of the HL7 Consumer Mobile Health Application Functional Framework for Privacy and Security Considerations

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.

Session Agenda

- Healthcare Privacy & Security Background
- Implications for Health Centers
- Cloud-Hosted EHR Security Implications
- Key Considerations for Health Center Staff
- Leadership Oversight and Responsibilities
- Questions and Discussion

Overview of Privacy and Security

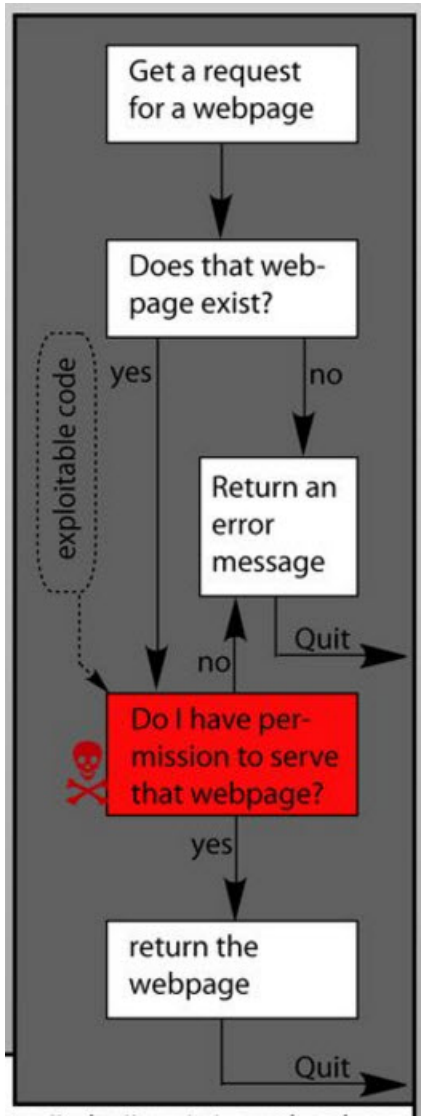
Problem Statement

- Computer programs are made up of instructions
- Humans write the instructions
- Humans are smart, but..
- Humans can get distracted
- Distractions increase the opportunities for loopholes

Hacking Basics

1. Understand the decision tree of a program
2. Find faulty or penetrable logic
3. Insert new logic according to hacking goals

Consequence: *Relatively easy to do QA on loopholes for a singular independent program, much tougher to do on a system of systems with high dependencies.*



Hacking and Data Breach

- Exploiting these loop holes whether through a web server, database, or email hack is how data breaches occur
- These hacks are sophisticated and often leave very little indication of a breach
- Many organizations don’t learn about the breach until their data surfaces on the black market. This can sometimes take upwards of five years

Adding to the Troubles:
Its not just the computers that gets hacked

- Kevin Mitnick, who once earned a spot on the FBI's most wanted list after hacking more than 40 corporations, but now serves as a security consultant to Fortune 500 companies and governments. "All it takes is one employee inside the business to screw up," he says.

- During the HIMSS 2017 keynote "The Art of Deception: How Hackers and Con Artists Manipulate You and What You Can do About it," Kevin Mitnick carried out real-time hacking demonstrations, through the most common form of attack used today — "social engineering," he says.

Enter Health IT

- An EHR system or medical device is essentially no different than any other type of computer program
- Except…that there is a greater chance that it could have a direct impact on someone's health
- Healthcare services, and payment for those services, have been supported by Health IT at some level since at least the introduction of Medicare and Medicaid in the mid 1960s. Requirements for its use has been steadily growing and evolving since then.
- "White Hat" initiatives for protecting the privacy and security of that data have steadily grown and evolved as well.

Call to Arms: White Hats vs Black Hats

Black Hats = The Villains

- A person who illegally gains access and sometimes tampers with information in a computer system
- Considered to be motivated by greed, destruction, infamy, etc
- Example: The organizations or persons behind the recent spate of Ransomware attacks

White Hats = The Defenders

- Find faulty or penetrable logic to help fix security holes before the happen or as quickly as possible
- Help outline QA processes and workflows for investigating potential security problems
- Example: OCR Auditing Team

Health Center Security Problem Statement

- Increased use of electronic health record systems increases security requirements
- Increased use of IoT enabled mobile health and medical devices increases security requirements
- Increased use of internet-based systems increases security requirements
- Increased numbers of users on a given system increases security requirements
- *That can be a lot of security requirements for small to medium health centers to effectively manage.*

Rise in Healthcare Cybersecurity Attacks

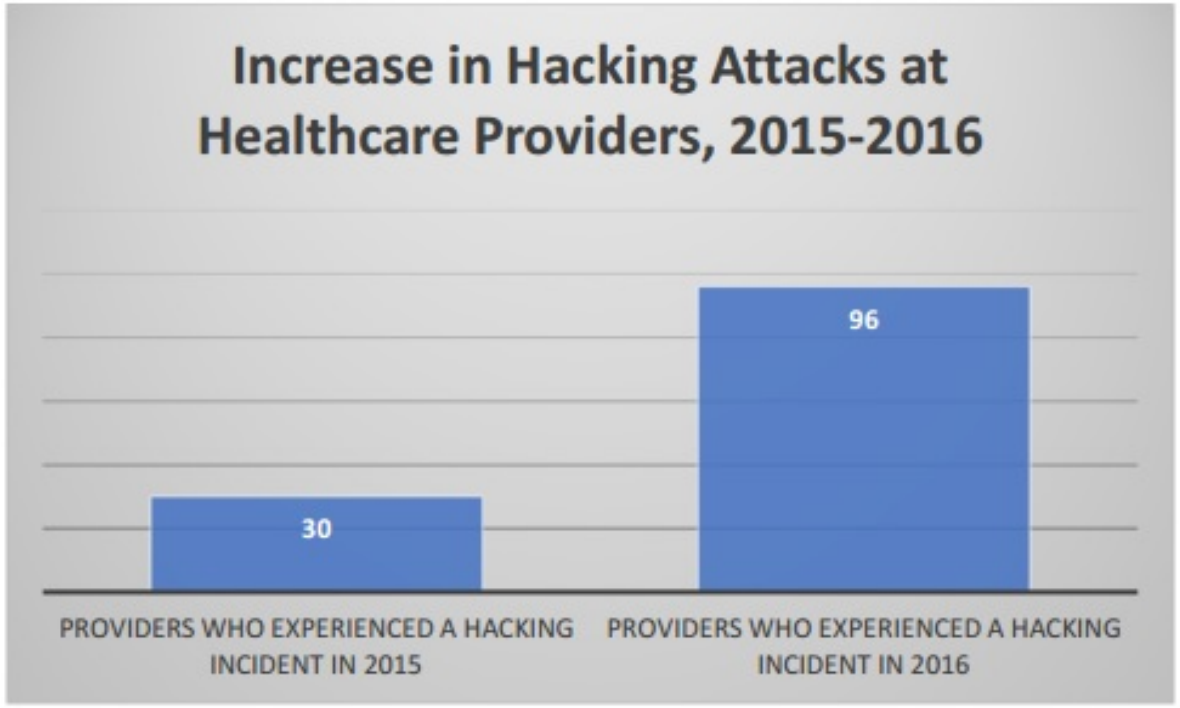
HEALTH INFORMATION TECHNOLOGY, EVALUATION, AND QUALITY CENTER

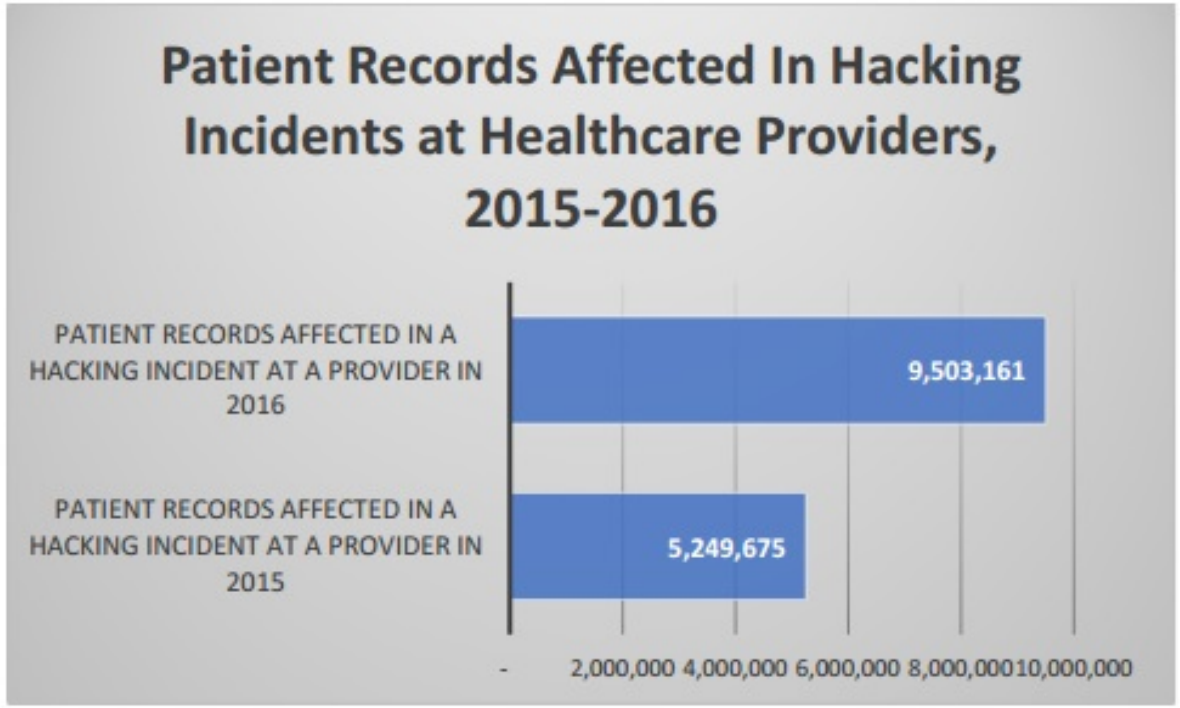
Privacy & Security Gap

- A rapid increase in the computerization of health care organizations, many without the capacity to keep up to date with the extensive privacy and security measures required, has made them targets for cyber-criminals. In the last couple of years there have been numerous ransomware attacks that has held critical hospital data at ransom.

- Health Centers may be perceived as more vulnerable targets by cyber-criminals due to a potentially smaller IT staff and older set of IT infrastructure (e.g., operating systems without latest security updates).

Healthcare Cybersecurity Attacks Rise 320%





Reference: HealthIT Security: https://healthitsecurity.com/news/healthcare-cybersecurity-attacks-rise-320-from-2015-to-2016

Ransomware Proliferation

House Energy and Commerce Oversight Subcommittee witness statement:

"In 2016, we started to see a rise of ransomware attacks against the [health care] sector. In these attacks, computer malware was used to lock up the files of victim health care organizations, while criminals demanded a ransom payment in exchange for access to be returned," the witnesses will state. "These attacks shifted the threat landscape considerably, as they no longer threatened just personal information but also the ability of health care organizations to provide patient care."

Repercussions

- Financial
  - Ransoms through ransomware continue to grow in costs as ransomware methods become more sophisticated.
  - Outside of the ransom, the cost due to downtime, recovery, and security maintenance can be considerable
- Legal
  - Privacy and security negligence may constitute legal ramifications based on state and federal policies and regulations (e.g. HIPAA).
  - Personal lawsuits may be leveled if there is perceived harm
- Reputation
  - Ransomware events have become a hot topic and speak poorly of the victims regardless of the exact circumstances.
  - Patient's may be hesitant to initiate or reconsider care if they perceive that a provider is unsafe with their health data

Primary Prevention Methods

- Employee Security Training and Awareness
  - Educate staff on what ransomware is and common traps they might experience
    - Instill email and website suspicion. Help staff know what to look for and what to do if they find something suspicious
    - Teach staff to not click on any links or files un-related to work and inform them of the possible consequences of these types of actions
    - Test and educate: Send a false email with a traceable link

Primary Prevention Methods

- Backups
  - Confirm that backup routines are actively deployed
  - Confirm that backups can be effectively restored
- Anti-Virus programs
  - Scan both inbound and outbound emails regularly
  - Authenticate inbound emails
- Firewalls & Network Access Control
  - Block access to known malicious IP addresses. Many are well documented.
  - Provide concise configurations for access to files, directories and networks

Ransomware Defense Guidance

- Several entities have published guides and checklists for increasing protection against these types of attacks:
  - A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)
  - National Cybersecurity and Communications Integration Center - WannaCry Fact Sheet
  - Symantec - Ransom.Wannacry Security Response

Healthcare Privacy & Security Context

Privacy vs Security

- **Privacy:** application of safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization.

- **Security:** protection of an individuals' electronic personal health information that is created, received, used, or maintained by a covered entity.

Healthcare Privacy & Security Policies and Regulations

- **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

Security Components	Example Variables	Example Security Measures
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
- Should be conducted annually
- Not required to, but should follow an established framework such as NIST, COBIT, or ISO

Meaningful Use and SRA

- **MU supports the HIPAA Security Rule**

- **MU Objective:** Protect electronic health information created or maintained by the certified EHR technology (CEHRT) through the implementation of appropriate technical capabilities

- **MU Measure:** Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the security (to include encryption) of ePHI created or maintained by CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of its risk management process

- **MU Stage 3 2018 Updates:** – Protected Patient Health Information: EPs must attest YES to conducting the security risk analysis upon installation or update to the new Edition of certified EHR Technology.

MU Impact on Eligible Providers

- In order to successfully attest, providers must conduct a security risk assessment (SRA), implement updates as needed, and correctly identify security deficiencies.

- By conducting an SRA regularly, providers can identify and document potential threats and vulnerabilities related to data security, and develop a plan of action to mitigate them.

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

General OCR HIPAA Settlements

Issues:

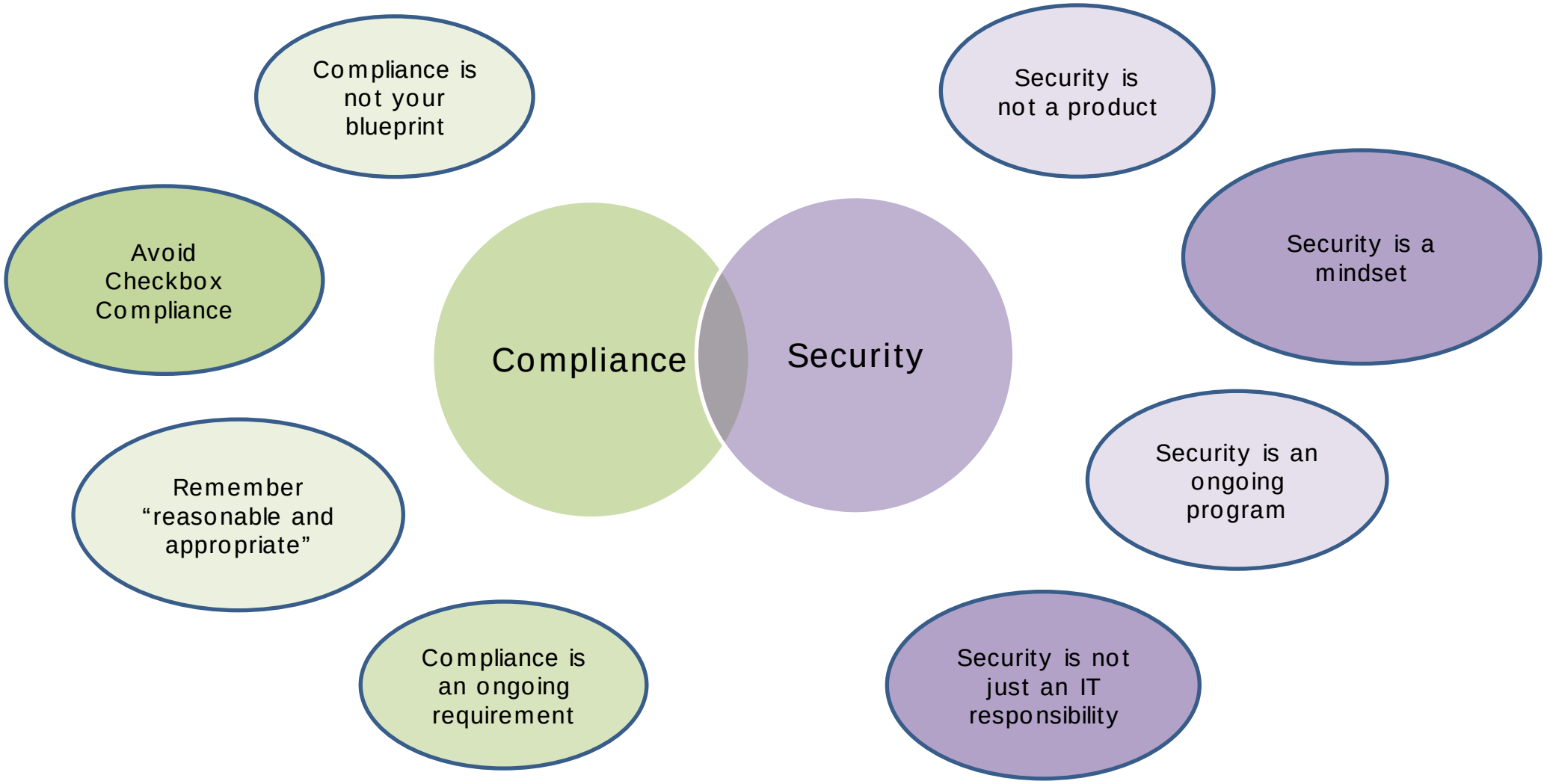
- Lack of risk analysis/risk management
- Large breaches (e.g., 300,000 or more)
- Improper disposal
- Unencrypted mobile devices
- Widespread snooping

Triggers:

- Media attention
- Breach report
- DOJ/OIG referral
- Complaints

Reference: http://www.dwt.com/people/adamhgreene/

Compliance vs. Security



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?
- Look to industry standards and guidance

Cloud-Hosted EHR Security Implications

Cloud-based EHR Security Advantages

- **Advantages**
  - Concentration on Software as a Service (SaaS)
  - Intimate knowledge of EHR system security
  - Focused security compliance
  - Stronger depth of defense

Cloud-based EHR: Access Control

- **Access Control**
  - Access to the data within the practice is controlled by centralized user authentication, user login time windows, user inactivity timeouts, the enforcement of strong login passwords, well defined user roles and access levels.

Cloud-based EHR: Communications

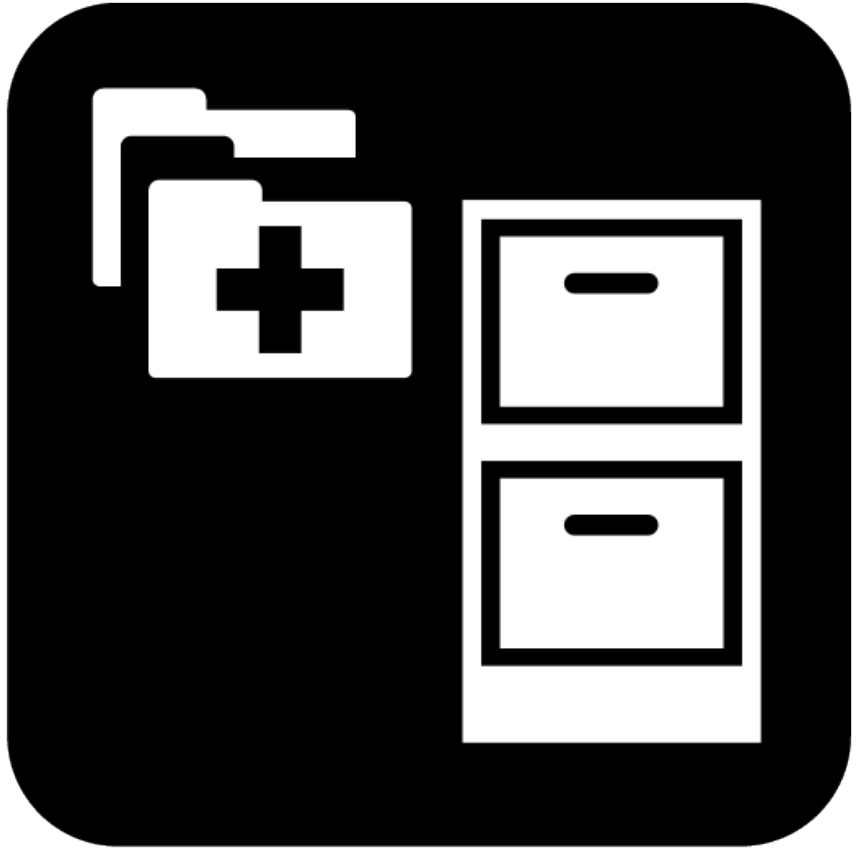
- **Communication Security**
  - Multifactor Authentication
  - All data sent between the client user and cloud-based EHR servers must be encrypted using TLS/HTTPS.

Cloud-based EHR: Data Center Security

- **Data Center Security**
  - Physical Security
  - Hardened Routing Equipment
  - Network Technicians
  - Security Policies
  - Server Software Security

Cloud-based EHR Security: Limitations

- **Limitations**
  - Cloud-based Host Confirmation of Reputation
  - Service Level Agreements
  - Compliance Control
  - Data Ownership and Extraction
  - Direct access to support team



Information Security Basics

Information Security Basics

- ***Protect the confidentiality, integrity, and availability of electronic PHI***
- Address across Administrative, Technical, and Physical domains
- 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

Information Security Basics

- 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. Backups fail frequently.

Information Security Basics

- **Antivirus is important, but not sufficient!**
  - Today's attacks are adept at circumventing AV
  - Consider full endpoint protection. Includes:
    - Malware removal based on existing signature files and heuristic algorithms
    - Built-in antispyware protection
    - Ingress/Egress firewall
    - Intrusion Prevention/Intrusion Detection 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
  - Policies and Procedures for handling of information
  - 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 organisations."*

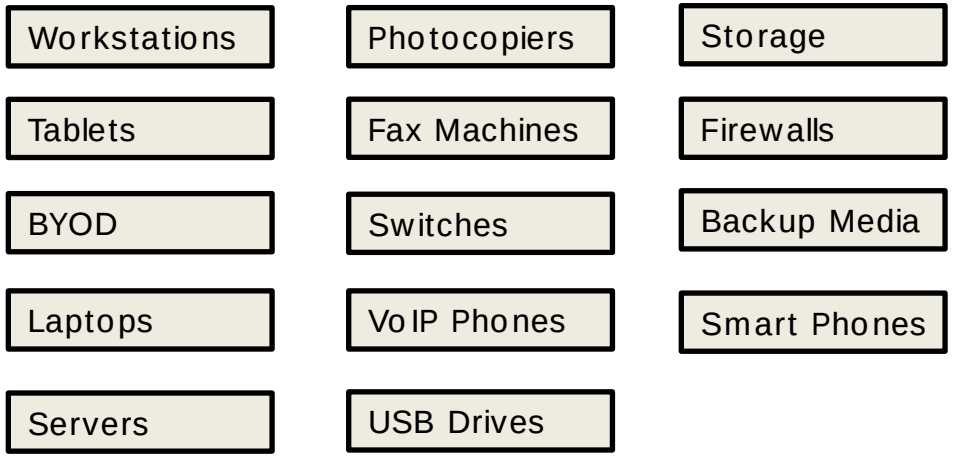
"Most attacks exploit known vulnerabilities that have never been patched despite patches being available for months, or even years. In fact, the top 10 known vulnerabilities accounted for 85 percent of successful exploits." Verizon 2016 Data Breach Investigations Report

CSC and HIPAA

Control Family	HIPAA Security Rule Controls
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	164.310(c): Workstation Security - R 164.310(d)(1): Device and Media Controls: Accountability - A
Critical Security Control #2: Inventory of Authorized and Unauthorized Software	164.310(c): Workstation Security - R
Critical Security Control #3: Secure Configurations for Hardware and Software	164.310(c): Workstation Security - R
Critical Security Control #4: Continuous Vulnerability Assessment and Remediation	164.308(a)(8): Evaluation 164.308(a)(6): Security Incident Procedures
Critical Security Control #5: Controlled Use of Administrative Privileges	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

CSC 1: Inventory of Authorized and Unauthorized Devices

- "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 regards to the HIPAA Security Rule and conducting a Security Risk Assessment because it allows you to create an inventory of ePHI

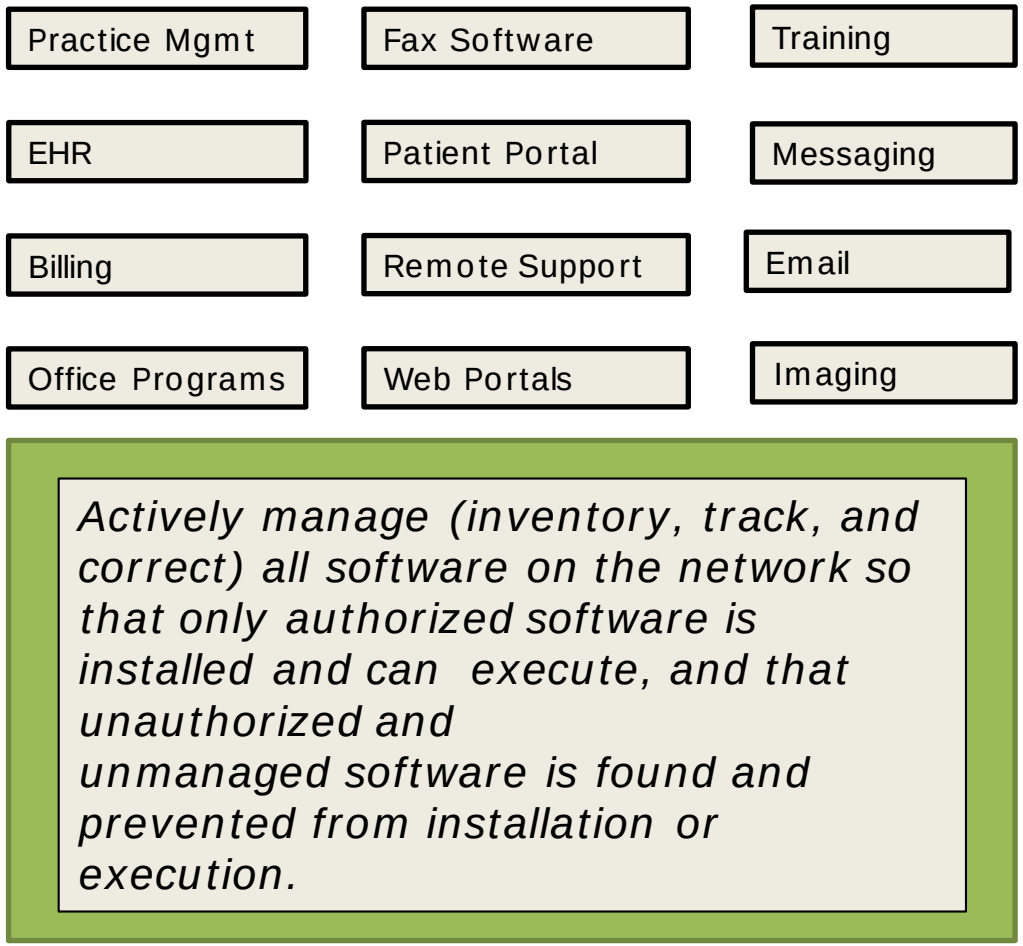


Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

164.310(c): Workstation Security - R
164.310(d)(1): Device and Media Controls: Accountability - A

CSC 2: Inventory of Authorized and Unauthorized Software

- "Know what you have" Part 2
- You can't secure it if you don't know about it
- There are different levels of implementing these controls. All the way from simply inventorying and manually correcting to application whitelisting
- Whitelisting is one of the best protections against malware
- Create an inventory of software systems that store or transmit ePHI. Include cloud-based systems



164.310(c): Workstation Security

CSC 3: Secure Configurations for Hardware and Software

- 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

CSC 4: Continuous Vulnerability Assessment and Remediation

- Now that you “Know what you have”, you can patch it
- HIPAA requires that you test your security controls. This is an excellent way to perform technical testing
- Continuous! Scans should be scheduled and run no less than weekly
- Run credentialed scans on servers
- Open Source and SaaS tools commonly available

> *Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.*

164.308(a)(8): Evaluation
164.308(a)(6): Security Incident Procedures

CSC 5: Controlled Use of Administrative Privileges

- "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

The processes and tools used to track/control/prevent /correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

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

New Roles and Responsibilities for Cybersecurity Leadership

Board of Directors Oversight

- 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 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

Board of Directors 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, 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

Board of Directors Oversight

Cybersecurity questions directors should be asking:

5. What cyber-threats could really damage this organization?
6. How are we distinguishing between systems, networks and users we do control or have strong assurance over as a third party, and those which we do not, as a basis for establishing which digital relationships and what data and identities from outside our organization we can 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

- Health Center Privacy and Security is everyone's responsibility
- Responsibilities will vary depending on the position, but awareness is critical at every level
- There are known best practices and frameworks that can be followed to help ensure information security is addressed appropriately
- Take continual steps to create a proactive privacy & security culture at your health center

Want more information?

HEALTH INFORMATION TECHNOLOGY, HITEQ EVALUATION, AND QUALITY CENTER

Home | Resources | Services | Calendar | Collaborators | About | Contact | Search

Rationale | Challenges | Approach

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).

Find HITEQ resources

Highlighted Resources & Events

The U.S. Department of Health and Human Services Office for Civil Rights Breach Portal
Health Center Breach Awareness

A Stepwise Guide to Compliance
HIPAA and Telehealth

A use case example from the Arizona Health-e Connection and SAMHSA Consent2Share project
Sharing Behavioral Health Data over an HIE

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

Comments, Questions, and Discussion

Please enter questions and comments in the chat box.

Questions? Comments?

Contact HITEQ at: hiteqcenter.org

hiteqinfo@jsi.com

@HITEQCenter

1- 844-305-7440

THIS PROJECT IS/WAS SUPPORTED BY THE HEALTH RESOURCES AND SERVICES ADMINISTRATION (HRSA) OF THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) UNDER GRANT NUMBER U30CS29366 TITLED TRAINING AND TECHNICAL ASSISTANCE NATIONAL COOPERATIVE AGREEMENTS (NCAS) FOR GRANT AMOUNT $500,000. 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 U.S. GOVERNMENT.

HEALTH INFORMATION TECHNOLOGY,
HITEQ
EVALUATION, AND QUALITY CENTER

CHCANYS DEFINING NEW DIRECTIONS
Community Health Care Association of New York State www.chcanys.org

COMMUNITY HEALTH CENTER FQHC QUALITY

For additional information on services through HCCN, please contact:

HCCN@chcanys.org