HIPAA Series: Why it Matters

Using PCI DSS, NIST and More to Address Your Cyber Liability

Presented by Susan Clarke

Health Care Information Security and Privacy Practitioner

Thursday, December 16, 2021 | 11:00 AM – 12:00 PM

HCCN Health Center Controlled Network

Mountain-Pacific Quality Health

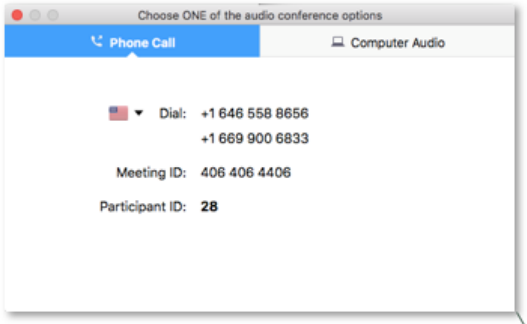
MPCA

Zoom tips and tricks!

CHAT: Please jump in if you have something to share, but we also have this nifty chat function.

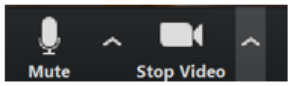
ATTENDANCE: If there are multiple attendees together on the call, please list the names and your location in the chat box

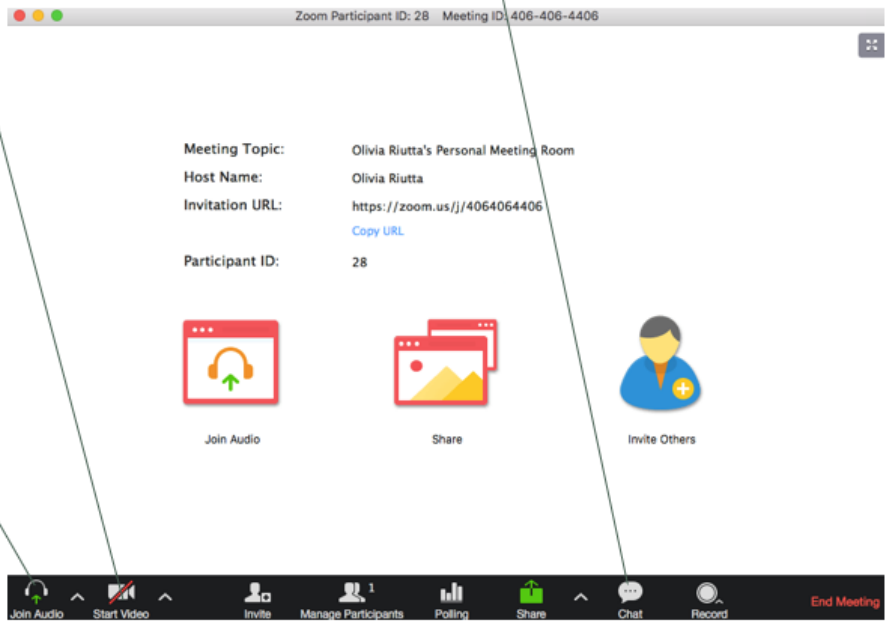
VIDEO: We want to see you!
If your camera isn't on, start your video by clicking here.



AUDIO: You can use your computer speakers or your phone for audio. The phone is generally better quality. If you click "Join Audio," this "Choose one…" box will pop up. If you dial in, just make sure you include your audio code.

MUTE/UNMUTE: *6 or click the mic on the bottom left of your screen.





Susan Clarke, HISPP

Certified Healthcare Information Security $(ISC)^2$ and Privacy Practitioner, Computer Scientist

Conducts privacy and security risk analysis in addition to HIPAA and other trainings.

20 years' experience in health care operations.

10 years' design and coding electronic health record (EHR) software including HL7 Healthcare application development.

Served on IT security, disaster recovery and joint commission steering committee at Mayo Clinic-affiliated health care system.

Legal Disclaimer

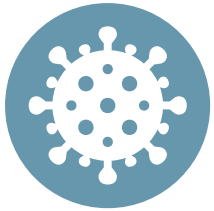
The presenter is not an attorney and the information provided is the presenter's opinion and should not be taken as legal advice. The information is presented for informational purposes only.

Compliance with regulations can involve legal subject matter with serious consequences. The information contained in the webinar and related materials (including but not limited to recordings, handouts and presentation documents) is not intended to constitute legal advice or the rendering of legal, consulting or other professional services of any kind. Users of the webinar and webinar materials should not in any manner rely upon or construe the information as legal or other professional advice. Users should seek the services of a competent legal or other professional before acting or failing to act, based upon the information contained in the webinar to ascertain what may be best for the users' needs.

Abbreviations and Acronyms

- BA: Business Associate
- BAA: Business Associate Agreement
- CE: Covered Entity
- CEHRT: Certified Electronic Health Record Technology
- CMS: Centers for Medicare & Medicaid Services
- EDR: Endpoint Detection and Response
- EHR: Electronic Health Record
- ePHI: Electronic Protected Health Information
- FISMA: Federal Information Security Management Act
- HIPAA: Health Insurance Portability and Accountability Act
- HIT: Health Information Technology
- MDR: Managed Detection & Response
- MSP: Managed Service Provider
- NIST: National Institute of Standards and Technology
- OCR: Office for Civil Rights
- PCI DSS: Payment Card Industry Data Security Standards
- PHI: Protected Health Information
- SLA: Service Level Agreement
- SRA: Security Risk Analysis

Learning Objectives



Changes Due to COVID-19

Cyber Insurance Defined

Maturity Level Matters

How to Respond

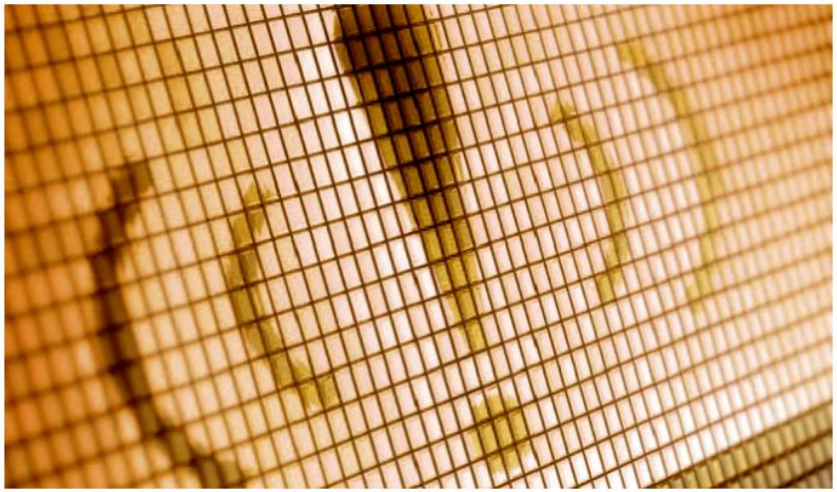
Role of Frameworks

Security Risk Analysis and Safe Harbor

Breaking News!

Severe Apache Log4j Vulnerabilities Could Result in Healthcare Cyberattacks

HC3 issued a sector alert regarding severe Apache Log4j vulnerabilities that could result in healthcare cyberattacks if exploited.



Source: Getty Images

By Jill McKeon

Source: https://healthitsecurity.com/news/apache-log4j-vulnerabilities-could-result-in-healthcare-cyberattacks

COVID-19 Brought Change

COVID-19 and the recent transformation in the way people work is having impact on security.

The surge in remote working and use of cloud service has **increased potential exposure**.

This includes both technical vulnerabilities and nontechnical threat vectors.

Risk of Remote

The rush to work at home in the face of COVID-19 brought several extra risk factors:

- Rushed technology deployment, prioritizing remote working but not its security implications
- Heightened personal stress generally due to the pandemic, leaving less mental capacity to maintain a strong security culture and mindset
- Lack of robust remote-working security training prior to working from home
- Untrusted home and coffee shop remote-working environments

What is Cyber Insurance?

Cyber insurance covers liability arising from cybersecurity attacks like ransomware.

Unlike flood and other types of insurance, cyber insurance is relatively new.

More on Cyber Insurance

Mostly designed to protect your health center from consequences of a successful cyber attack.

Depending on coverage details, might include financial payments for operational support, IT forensics, legal implications and public relations.

Offset Risk

IMPORTANT: Not designed as an alternative to cybersecurity measures. Rather, generally intended to offset residual risk once a company has already put suitable defenses in place.

What may be covered?

- ✓ Forensic analysis to confirm nature and extent of attack
- ✓ Ransom demands and negotiations – May or may not include meeting payment demands from ransomware attack
- ✓ Costs to regain or restore data, e.g., from backups or other sources
- ✓ Legal costs, either direct costs or third-party lawsuits
- ✓ Public relations specialists to limit reputational damage
- ✓ Notifying patients or regulatory bodies following compliance and attempting to limit fines
- ✓ Credit monitoring for customers and other individuals affected by personal data breach
- ✓ Loss of revenue or health center interruption costs

Growing Losses

Cyber insurance payouts are climbing, and insurers are taking action to reduce their losses, which has potential implications for cybersecurity risk management practice.

There’s no cybersecurity equivalent to a category five hurricane.

Maturity Level Matters

Health centers with well established cybersecurity controls and emergency support:

- Typically buy insurance to offset risk, so they may see cyber insurance as an investment in case of a major incident.
- In this case, there is limited potential for an insurer to influence their behavior.

Health center that is still working on their cybersecurity controls and emergency support:

- Might use an insurance policy to help decide what security measures it needs.
- View post-breach support services as a one-stop shop to direct its response when an incident occurs.

Maturity Level Matters

- There is also a disparity when it comes to the quoting and buying cyber insurance.
- Because smaller businesses generally represent a smaller risk, insurers may spend less time in data gathering or negotiations and quote a premium based on a fixed insurance application or proposal form.
- **Unfortunately, there is little consensus about what these forms contain.**

Look Ahead as More Issues Arise

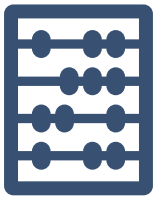
The challenges continue to appear around cyber insurance coverage

- IT is finding it not as easy as it once was for a health center to get sufficient cyber insurance cover cheaply, with minimal cybersecurity requirements.

- It is also not as easy is for health centers to “shop around.”
- They are less likely to find an insurer with significantly lower requirements around security information and robust controls.

More Offer Pre-Breach Support

Insurers are actively managing the risk they underwrite while also seeking a competitive advantage.



A growing number are offering preventative cybersecurity support to reduce the chances of a breach.

How Should You Respond?

- Check your policy details, look for possible changes in cover limits and deduction or retention amounts, as well as any specific exclusions
- Consider a package versus standalone services
- Be realistic about what your policy can and cannot do
- Not a replacement for cybersecurity

Quick Takeaways

Ensure your health center has an actionable data breach incident response plan that can be accessed at a moment's notice and includes vital third-party experts known to your cyber insurer.

Ransomware is not a fleeting trend. Carriers are staying on top of threats.

Ensure baseline must-have cyber security measures to mitigate ransomware, such as multifactor authentication, endpoint protections, segmentation, close remote desktop protocols, cloud-based backups and employee training.

Examples of Control Frameworks and Standards

- ISO/IEC 27001: International Standard
- NIST (SP 800-53): Required by U.S. Government
- COBIT: Focused on business values
- ISA/IEC 62443 (ISA 99): Industrial Automation and Control System
- FISMA: U.S. legislation framework to protect government information, operations and assets

National Institute of Standards and Technology (NIST)

- Creates and releases guidance on best practices in numerous aspects of hard sciences, including cybersecurity and risk assessments
- Standards essential for federal information security readiness and lay groundwork for government's approach to information security

NIST

Search NIST

Menu

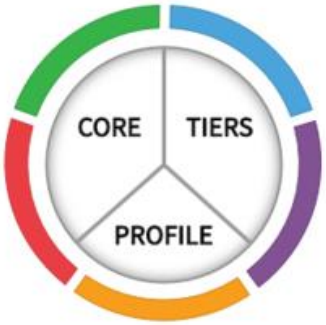
CYBERSECURITY FRAMEWORK

Helping organizations to better understand and improve their management of cybersecurity risk

- Framework
- Getting Started
- Perspectives
- Success Stories
- Online Learning
- Evolution
- Frequently Asked Questions
- Events and Presentations
- Related Efforts (Roadmap)
- Informative References
- Resources
- Newsroom
- Related Programs

Framework Version 1.1

The Cybersecurity Framework is ready to download.



New to Framework

This voluntary Framework consists of standards, guidelines and best practices to manage cybersecurity risk.

Online Learning

Intro material for new Framework users to implementation guidance for more advanced Framework users.

Source: https://www.nist.gov/cyberframework

PASS

Covered Entities

- Are covered entities required to use the National Institute of Standards and Technology (NIST) guidance documents referred to in the preamble to the final Security Rule (68 Fed. Reg. 8334 (February 20, 2003))?
- **No.** Covered entities may use any of the NIST documents to the extent that they provide relevant guidance to that organization's implementation activities. While NIST documents were referenced in the preamble to the Security Rule, their use is not required by the Security Rule.

Content created by Office for Civil Rights (OCR)
Content last reviewed July 26, 2013
Source: https://www.hhs.gov/hipaa/for-professionals/faq/2015/are-covered-entities-required-to-use-the-nist-guidance-documents/index.html

What is PCI DSS?

Payment Card Industry (PCI) standards apply to all organizations that deal with cardholder data.

- If you are processing, storing or transmit payment card data, you are subject to PCI DSS.
- 12 high-level requirements can be grouped into six categories.
- PCI DSS is not a law; it is a blueprint.

Cyber Liability and PCI DSS

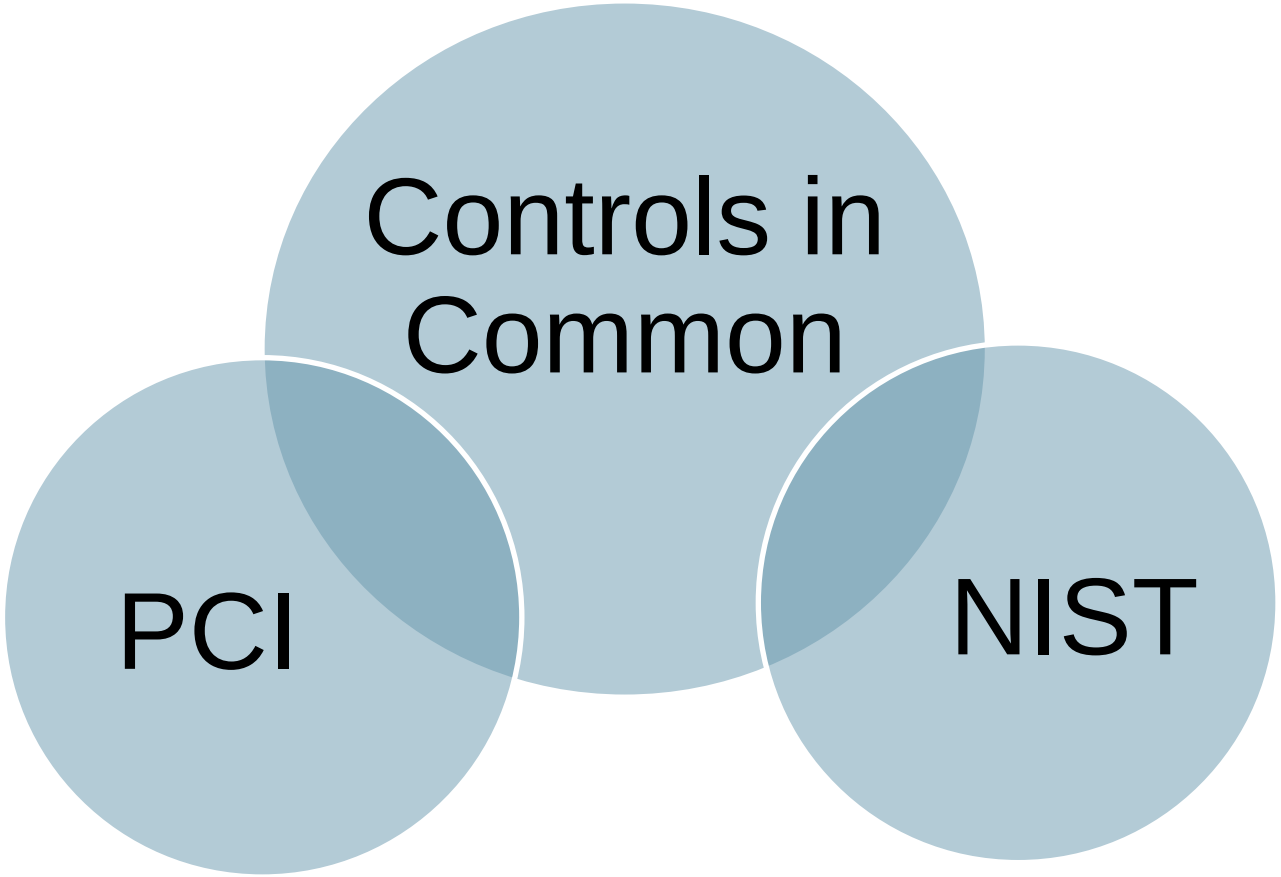
Health centers required to be PCI DSS compliant may face **multiple vulnerabilities**, reputational harm, fines and penalties, etc.,that go along with a breach.

When you accept, transmit or store any credit card information, **you run the risk of a data breach**.

Steps to PCI Compliance

- Figure out which parts of your systems and networks need to be PCI DSS compliant.
- Assess your system compliance by using PCI DSS testing requirements.
- Complete the correct Attestation of Compliance (AOC).
- Submit the documentation.
- Address any non-compliant parts of your systems and networks and then submit an updated report.

PCI and NIST



PCI Security Standards Council crosswalk:
https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework-At-a-Glance.pdf?agreement=true&time=1639165392234

Understand Who Is Responsible

Cloud Deployments	Responsibility stays with customer	Responsibility may be shared	Responsibility transfers to Cloud (SaaS)
Data	**C**		
Devices	**C**		
Access	**C**		
Training	**C**		
Endpoints	**C**		
Directory	**C**	**C**	
Applications			**C**
Network Control			**C**
Operation System			**C**
Hosts			**C**
Network			**C**
Datacenter			**C**

HIPAA Safe Harbor Bill

Signed January 5, 2021

Amends HITECH Act ("recognized cybersecurity practices")

Lenient fines if basic safeguard requirements met

- HIPAA Security Rule
- Security risk analysis

Please let me know how I can help.

For assistance, please contact:

Susan Clarke
sclarke@mpqhf.org | (307) 248-8179

THANKS FOR YOUR VALUABLE TIME TODAY!

Questions