

Navigating the Cybersecurity Threats in Healthcare Today:
How Do I Protect my Agency?



Welcome

SPECIAL AGENT KEVIN CONINE,
FBI Albany Cyber Task Force

JUSTIN BAIN,
CISSP, HCISPP, Vice President, Information Security Officer, VNS Health

AGENDA

1. Introductions
2. Threat Landscape / High Risk Areas
3. HICP: A Resource for Health Care Providers
4. Tips for Cybersecurity in Healthcare

SPECIAL AGENT KEVIN CONINE

8 ½ years, 4 ½ in Newark Division, 3 in Washington, DC HQ, 1 in Albany Division

Acting Supervisory Special Agent of the FBI Albany Cyber Task Force

- Covers 32 counties in NYS and all of VT
- 8 Special Agents in Burlington, Albany, Syracuse and Binghamton
- Computer Scientists, Digital Operations Specialists, Digital Forensics Examiners, Data Analysts, Intelligence Analysts, Tactical Operations Specialists, Forensic Accountants

JUSTIN BAIN

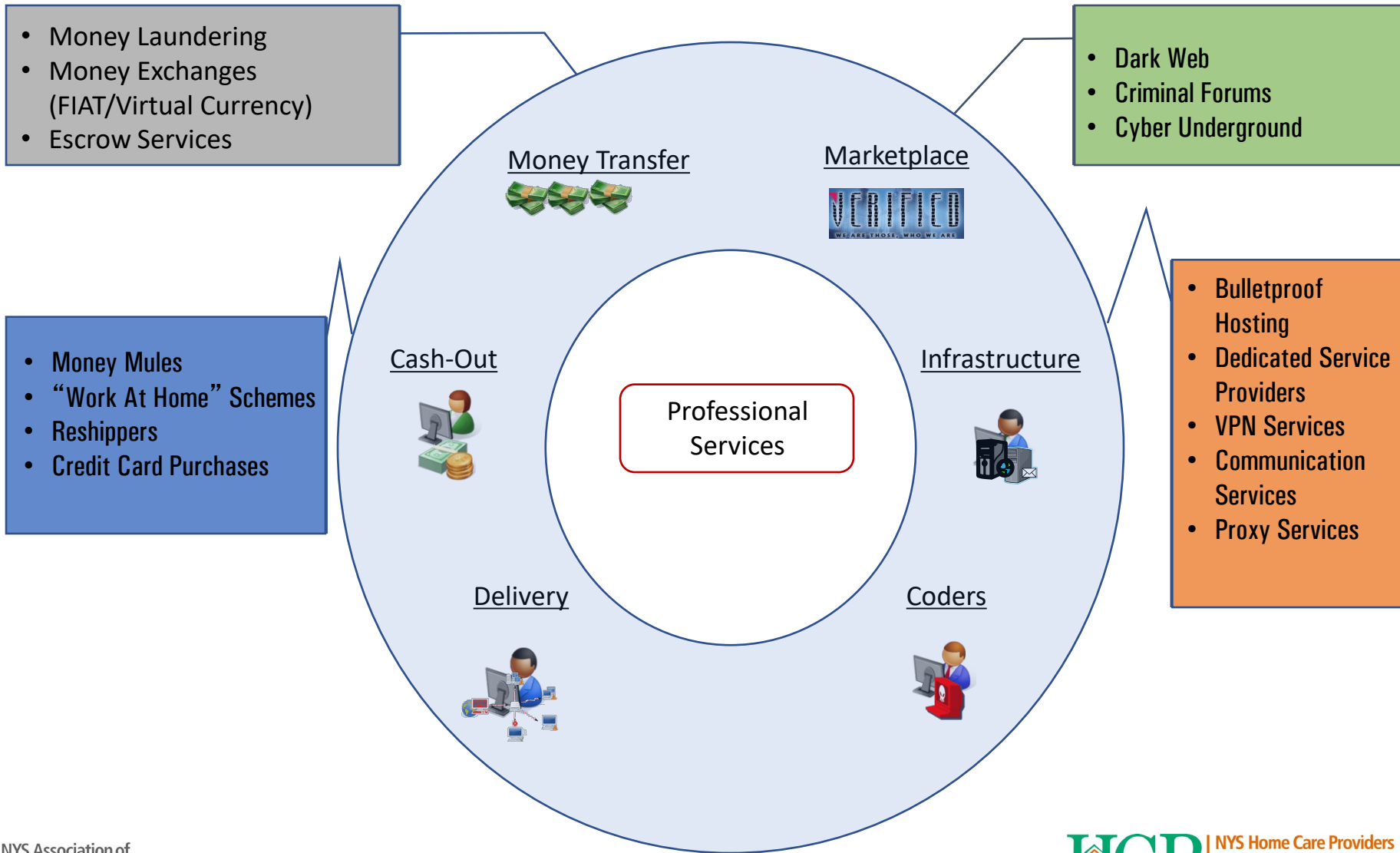
- Vice President, Information Security Officer at VNS Health
- Certified Information Systems Security Professional (CISSP)
- HealthCare Information Security and Privacy Practitioner (HCISPP)
- 25 years in healthcare I.T., primarily post-acute care
- 10 years in information security in healthcare



- Large not-for-profit home- and community-based care organization
- CHHA, Hospice, LHCSA, Care Management, Behavioral Health, and five Health Plans.



THE EVOLUTION OF CYBER CRIMINAL ENTERPRISES



CURRENT THREATS/HIGH RISK AREAS OF EXPLOITATION

Phishing & Social Engineering Threats

Watering Hole Attacks

BEC

SIM Swapping

Ransomware

National Security/State Actor Threats

SOCIAL ENGINEERING: HOW DOES IT WORK?

WE ARE ALL SUSCEPTIBLE: people are always the weakest link, our nature is to trust, and as automated controls have continued to improve attackers go back to the basics

Leveraging emotion over critical thinking and judgement

- Fear, Wants, Desire to Help

Romance Scams, Grandparent Scams, Investment Fraud, Tech Support Scam

Phishing (texts/emails), vishing, spearfishing, evil twins network, spoofed domains

AI enabled

WATERING HOLE ATTACKS

- These types of attacks are the result of increased account protections like multifactor authentication
- Banking and other financial websites are scraped and the duplicate site is bumped to the top of searches
- Attackers then call to get codes and tell user to stay out of account for a short time
- Key for users to enter in or bookmark true sites
- Never provide credentials

Videos of How Do I Get My Website to the Top of A Google Search

bing.com/videos



How to Get My Website to the Top of Google

1K views · Mar 9, 2015

[YouTube](#) > [Five Free Tools](#)

Save Share



How to get your website to the top of Google search



How to Get your Website to the Top of Google - Great



How to get your Website on Google Search Engine

BUSINESS EMAIL COMPROMISE (BEC)

Happens in business, real estate, and other transactions

An intruder gains control of an email account temporarily and either sets up forwarding rules or other rules to have visibility on communications

Sends alternate account information to receive funds

Mitigations:

multi-factor authentication

verbal authorization or out of email verification method

Disabling and checking for forwarding rules or other strange rules in email

SIM SWAPPING

Just as easy as a purchase on the dark net and ordering a new phone

These attacks have been enabled by all of the data breaches over the past ten years

Once they have your phone they have all the apps on them too (email, bank accounts, investment accounts)

AND the ability to have then change your multifactor authentication

Have been used to steal individual accounts AND funds from financial institutions themselves

Phone providers help you prevent this by pin blocking

RANSOMWARE

- **Campaign or Exploitation of a vulnerability (brute forcing credentials, RDP)**
 - May be initiated by **phishing attack** which can come from a business partner
- **Infection**
 - The dropper installs **malware** on "Patient Zero" (Trickbot, Emotet, Vatet, IcedID)
- **Staging**
 - The attacker seeks to establish **persistence** and download more tools
- **Scan**
 - The attacker uses powershell scripts or tools sets like **Metasploit** or **Cobalt Strike** to navigate and exploit the network
 - Seeks network connected systems, backups to destroy, and data to exfiltrate
- **Encrypt**
 - The ransomware executable is dropped and encrypts the data (Ryuk, Prolock, Pysa.....)
- **Payday**
 - Victim placed in a situation where they accept **data loss**, **data compromise** and **downtime**
 - Or accept only **data compromise** and **downtime** in exchange for a **fee**



NATIONAL SECURITY THREATS

- Physical Attacks
- PLC/SCADA Attacks
- Supply Chain Attacks

PHYSICAL ATTACKS

Plugging into the Network or Computer Directly

- USB Rubber Duckie
- Warberry Pi
- “May I charge my phone on your computer?”



WIRELESS NETWORK ATTACKS

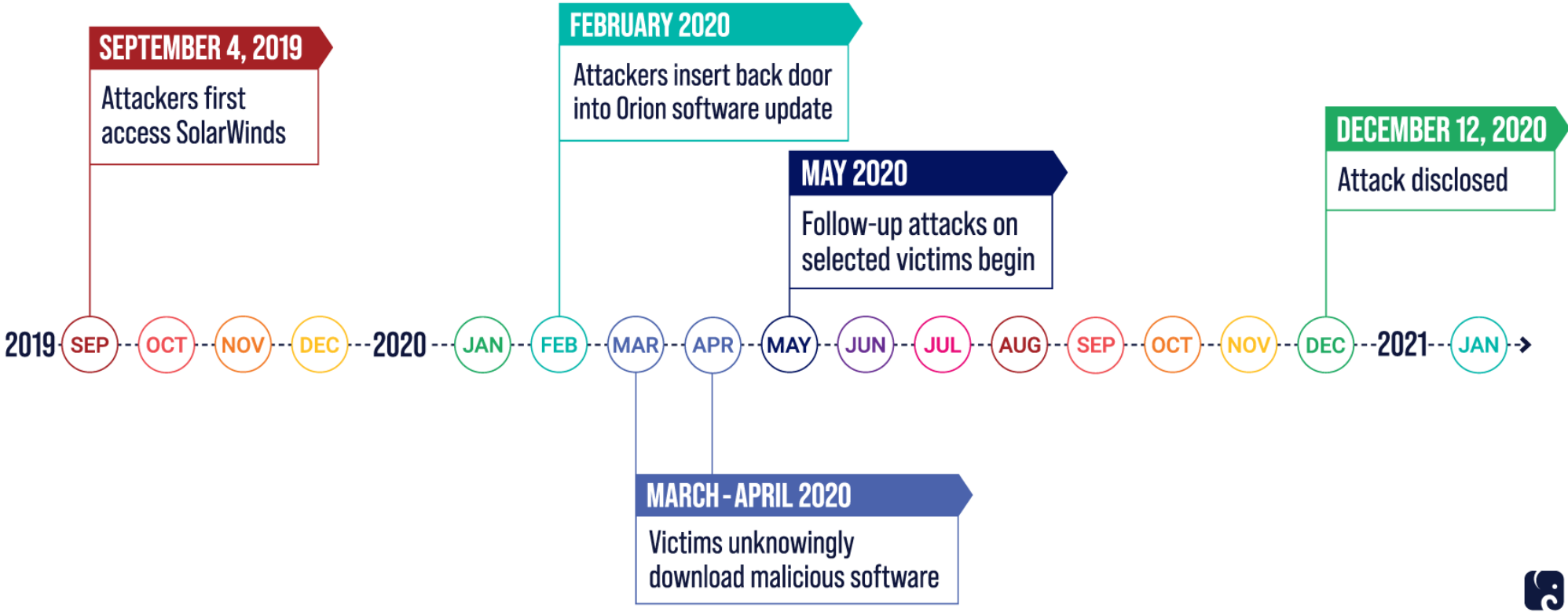
Over the Air

- Man-in-the-Middle Attacks (Pineapple, Rogue Access Point)
- Blue-bugging or Blue-snarfing
- Airdrop



SUPPLY CHAIN ATTACKS

SolarWinds aka Digital Trojan Horse



CASE EXAMPLES

Top Cyber Attacks on Healthcare in April 2024 in the Arctic Wolf Report on Top 10 Healthcare Industry Cyber Attacks

“10.93 million dollars USD. That’s the average cost of a healthcare breach in the U.S. It’s an alarming number that’s only continued to climb, increasing by over 53% in the past three years, according to IBM’s 2023 Cost of a Data Breach Report.”

HCA Healthcare-July 2023 -Tennessee based hospital and clinic operator, 11 million patients PII data exfiltrated, third party storage breach, sued because didn’t maintain sensitive data properly specifically that they didn’t encrypt or delete data after it was no longer needed. Third party/unsecured data

Cerebral- 2023 –Telehealth company had a data breach of 3.1 million patient records after an accidental insider threat issue where its third party access was improperly setup allowing third party access to PHI data. Improperly configured IT

Banner Health – 2016, improperly upgraded food and beverage processor allowed malicious actors to use malware to breach the payment processing system and then laterally move into Banner Health’s primary network and onto servers containing data on over 3.7 million patients including PII/PHI. Was undiscovered for a month! Weak configuration/malware/weak network segmentation

Anthem (Wellpoint) – 2015 – Phishing email allowed malware to be installed on network that compromised 78.8 million records of patients and employees. Anthem settled for \$115 million along with being ordered to make “changes to its data systems and policies”

CHANGE/UNITED HEALTH HEALTHCARE RANSOMWARE ATTACK – FEBRUARY 2024

02/21/24-Reported as outage

02/29/24-Confirmed ransomware-ALPHV/Blackcat

03/03-03/05- Paid \$22 million ransom. Ransomware team did a rug pull.

04/15- PII/PHI data published on dark web by different group

04/22 Change confirms breach affecting “substantial” portion of Americans

05/01-CEO confirms Change was not practicing basic cyber hygiene.

June 24-Change told hospitals what data was taken.

July 24-Change sends letter to individuals affected.

CHANGE
HEALTHCARE
PO Box 989728
West Sacramento CA 95798-9728

To enroll in free credit monitoring services,
please visit:
www.changeybersupport.com and click the
link to register online with IDX.

240F00AD9C0C0110167011-03307-01
Conor Conine

September 3, 2024

|||||

Notice of Data Breach

To Conor Conine:

We are sorry to tell you about a privacy event. This letter is from Change Healthcare ("CHC"). We work with many doctors, health insurance plans, and other health companies to help provide health services or benefits. This event may have involved your data.

What happened?

On February 21, 2024, CHC found activity in our computer system that happened without our permission. We quickly took steps to stop that activity. We began investigating right away and hired a special team to help us. We also called law enforcement. We also turned off CHC's systems to help protect our business customers and their individuals.

On March 7, 2024, we learned a cybercriminal was able to see and take copies of some data in our computer system. This happened between February 17, 2024 and February 20, 2024. We received files that were safe to look at on March 13, 2024.

What information was involved?

We have told our business customers about this event. Starting on June 20, 2024, we began notifying our business customers about what data may have been seen and taken. We encourage you to remain vigilant by checking bills and accounts. The data that may have been seen and taken includes contact information (such as name, address, date of birth, phone number, and email) plus one or more of the following:

- Health insurance data (such as health plans/policies, insurance companies, member/group ID numbers, and Medicaid-Medicare-government payor ID numbers)
- Health data (such as medical record numbers, doctors, diagnoses, medicines, test results, images, care, and treatment)
- Billing, insurance claims and payment data (such as claim numbers, account numbers, billing codes, payment cards, financial and banking, and balance)
- Other personal data (such as Social Security number, driver's license or state ID number, or other ID number)

H-ISAC.ORG



For Membership

For Sponsorship

- Home
- About ▾
- Membership ▾
- Sponsorship ▾
- Events ▾
- News ▾
- Resources ▾
- Member Login

Latest News



Health ISAC Leads Effort To Transform SBOM Information Sharing Under CISA-Facilitated Community Work



SOURCES

- April 2024 Arctic Wolf Article: The Top 18 Healthcare Industry Cyber Attacks of the Past Decade
<https://arcticwolf.com/resources/blog/top-healthcare-industry-cyberattacks/>
- June 2024 AHA Article: FBI, HHS issue advisory on cyberthreat actors targeting health care to divert payments
<https://www.aha.org/news/headline/2024-06-25-fbi-hhs-issue-advisory-cyber-threat-actors-targeting-health-care-divert-payments>
- June 2024 HHS Article: Types of Cyber Threat Actors That Threaten Healthcare
<https://www.hhs.gov/sites/default/files/types-threat-actors-threaten-healthcare.pdf>
- February 2024 Article: Healthcare Cyber Attack Statistics 2022: 25 Alarming Data Breaches You Should Know
<https://expertinsights.com/insights/healthcare-cyber-attack-statistics/>
- August 2024 Article: How the ransomware attack at Change Healthcare went down: A timeline
<https://techcrunch.com/2024/08/17/how-the-ransomware-attack-at-change-healthcare-went-down-a-timeline/>

HHS 405(d) HEALTH INDUSTRY CYBERSECURITY PRACTICES (HICP)

- HHS 405(d) was established by Cybersecurity Information Sharing Act of 2015.
- Main purpose: to enhance cybersecurity posture of healthcare sector
- Brings together public and private partners to develop and promote best practices, guidelines, and methodologies
- Developed **Health Industry Cybersecurity Practices (HICP)** guidelines for Small/Medium/Large businesses.
- HICP is a **Recognized Security Practice (RSP)** under HITECH Act
- Use of RSPs in a security program can be considered when determining fines, audit results, or other enforcement actions related to HIPAA violations.

DEFEND AGAINST PHISHING / SOCIAL ENGINEERING

- Implement Multifactor Authentication (MFA) (**1.S.A, 3.M.D**)
- Tag external emails for staff (**1.S.A**)
- Use advanced tech for email threats (**1.L.A**)
- Beware emails requesting sensitive info or stressing urgency (**1.S.B**)
- Train staff to spot and report suspicious emails (**1.S.B**)
- Avoid opening attachments from unknown senders (**1.S.B**)
- Have response procedures for phishing clicks (**1.S.C**)
- Implement plays for phishing attacks (**8.M.A**)
- Share cyber threat info with other organizations (**8.S.B, 8.M.C**)

DEFEND AGAINST RANSOMWARE

- Use strong/unique usernames and passwords with MFA (**1.S.A, 3.S.A, 3.M.C**)
- Deploy anti-malware detection and remediation tools (**2.S.A, 2.M.A, 3.L.D**)
- Limit remote desktop access (**3.S.A, 3.M.B**)
- Limit authentication attempts to prevent brute-force attacks (**3.M.C**)
- Specify computers that access sensitive data (**4.M.C**)
- Test data backup and restoration (**4.M.D**)
- Secure backups to protect them (**4.M.D**)
- Keep an updated asset inventory (**5.S.A, 5.M.A**)
- Implement network segmentation (**6.S.A, 6.M.B, 6.L.A**)
- Educate users on patching procedures and follow them (**7.S.A**)
- Test incident response procedures (**8.S.A, 8.M.B**)
- Share cyber threat info (**8.S.B, 8.M.C**)
- Develop and test a ransomware recovery plan (**8.M.B**)
- Get cyber insurance with ransomware protection (**10.S.D**)
- Initiate incident and response procedures upon ransomware detection (**HHS Ransomware Factsheet**)

DEFEND AGAINST THEFT OF EQUIPMENT OR DATA

- Promptly report lost/theft to I.T. to terminate access (**3.S.A**)
- Encrypt sensitive data when transmitting (**4.S.B, 4.M.C**)
- Encrypt data at rest on mobile devices (**4.M.C**)
- Implement and test data backups and restoration (**4.M.D**)
- Use data loss prevention tools (**4.M.E, 4.L.A**)
- Maintain an accurate, current asset inventory (**5.S.A**)
- Clean sensitive data from devices before retirement (**5.S.C, 5.M.D**)
- Implement a safeguards policy for mobile devices (**9.M.A**)

DEFEND AGAINST INSIDER, ACCIDENTAL, OR MALICIOUS DATA LOSS

- Update Business Associate Agreements (BAA) for legal safeguards, security review, and enhanced processes (**Technical Volume 1 Introduction**)
- Train staff on data access and financial controls to mitigate social engineering and to prevent errors (**1.S.B, 1.M.D**)
- Terminate access promptly when no longer needed (**3.S.A, 3.M.A, 3.M.B**)
- Limit access strictly to "need to know" basis (**3.S.A, 3.M.C, 3.L.B, 3.L.C**)
- Audit activity logs for health records and sensitive data access (**3.M.B**)
- Use privileged access management tools for critical systems (**3.M.C**)
- Employ data loss prevention tools to block PHI and PII leaks (**4.M.E, 4.L.A**)

DEFEND AGAINST CONNECTED MEDICAL DEVICES THAT MAY AFFECT PATIENT SAFETY

- Perform security risk assessments on all new devices and software vendors (**1.L.A**)
- Communicate with medical device manufacturers' security teams (**9.L.A**)
- Patch devices after validation and distribution by manufactures, and proper testing (**9.M.B**)
- Assess security controls on network-connected medical devices (**9.M.B, 9.M.E**)
- Implement security operations for medical devices, including hardening, patching, monitoring, and threat detection (**9.L.B**)

JUSTIN'S TIPS FOR CYBERSECURITY IN HEALTHCARE

- Go beyond the requirements of HIPAA Security Rule. HIPAA is old and insufficient. HICP or NIST offer updated standards. NYS DFS Cybersecurity Rule standards are better too.
- Risk Assessment and Analysis is crucial (and required annually). Set goals for incremental improvement. Focus on highest risks.
- Multifactor Authentication (MFA) everywhere. But it's not a silver bullet.
- Create Business Continuity Plans and practice with them.
- Don't have enough dedicated security staff? Use managed services.
 - Look at current managed service providers and see if they have add-on security services

Risk Assessment	Vulnerability Management	Third Party Risk Management	Social Engineering Testing
Detection and Response	Penetration Testing	Security Awareness Training	Application Security Testing

REFERENCES

- [Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients \(HICP 2023 Edition\)](#)
 - [Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations](#)
 - [Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations](#)
- [HHS Ransomware Fact Sheet \(7/11/2016\)](#)
- [Security Risk Assessment Tool - HealthIT.gov](#)
- [New York State Dept. of Financial Services Cybersecurity Requirements for Financial Services Companies](#)



Thank You