PROTECTING YOUR PRACTICE: STRATEGIES TO IMPROVE CYBERSECURITY

March 12, 2021

MHCC MARYLAND HEALTH CARE COMMISSION

ABOUT MHCC

- Advance health information technology and innovative value-based care delivery statewide by promoting adoption and use, identifying challenges, and raising awareness through outreach activities
- Provide timely and accurate information on availability, cost, and quality of health care services to policy makers, purchasers, health care providers, and the public

AGENDA

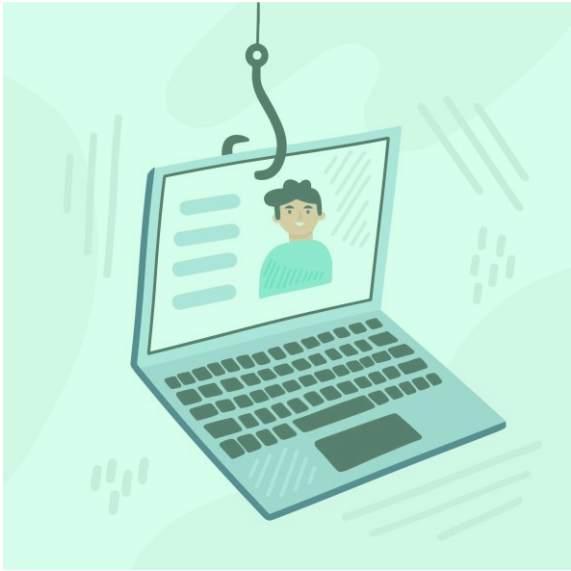
- Overview of Cybersecurity
- Practice Perspective
- Industry Perspective
- Q&A

CYBERSECURITY IN HEALTH CARE

- Cyberattacks can disrupt health care operations and put patient privacy and safety at risk
- Health care is among the most targeted industries in large part due to greater diffusion of electronic information and systems
- Cyberattacks do not target technology alone; they target people
  - Phishing attempts are most common

BEST PRACTICE TIPS

- Everyone has a role to play in cybersecurity – it's important to increase awareness so all staff can understand potential risks
- Common ways to reduce risks include:
  - Install system updates timely
  - Implementing strong password practices
  - Regularly back up all data, including on mobile devices



RESOURCES

- MHCC Cybersecurity Self-Assessment Readiness Tool

mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/Cybersecurity_Self-Assessment_Tool.pdf

- NIST Cybersecurity Framework

www.nist.gov/cyberframework

- Top 10 Tips for Cybersecurity in Health Care

www.healthit.gov/sites/default/files/Top_10_Tips_for_Cybersecurity.pdf

- Cybersecurity Practices for Small Health Care Organizations

www.phe.gov/Preparedness/planning/405d/Documents/tech-vol1-508.pdf

- MHCC Cybersecurity

mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/hit_cybersecurity.aspx

DISCLAIMER

This webinar is intended for informational purposes only. Information provided by presenters regarding any specific product or service, does not constitute or imply MHCC's endorsement or recommendation of such product or services

PRACTICE PERSPECTIVE

Cybersecurity for the Podiatric Office

Jay Seidel, DPM

HAMILTON FOOT CARE

Cybersecurity Discussion Topics

- Identifying Threat Areas
- Implementing Threat Prevention
- Security Improvement Pearls

HAMILTON FOOT CARE

Cybersecurity Threat Areas

Employee access

- Employees have easy access to patient files. While the majority won't abuse this power, there's no guarantee some won't steal sensitive information.
- There are multiple ways in which staff can steal records. In some cases, employees access confidential financial documents and use patients' credit card numbers to commit a series of fraudulent purchases. Other workers have been found to steal face sheets, including demographic and social security information, which can then be used to commit a variety of crimes.

Cybersecurity Threat Areas

Malware and phishing attempts

- One of the most challenging issues dealing with malware is that it only takes one seemingly-authentic link to introduce a nefarious cyber presence into your network. It’s essential to train staff to recognize common phishing attempts.
- One common scam is to have emails from authentic-looking sites request login information — something reputable companies never ask through an email. Once a user provides that information, the hacker on the other end can log in to the system.

Cybersecurity Threat Areas

Vendors

- Healthcare providers often work with vendors without assessing the accompanying risk. For example, if a hospital hires a cleaning company, its employees might gain access to computers. While patient information should be locked in ways that the average employee cannot view, it can be difficult to safeguard all points of access since cleaning and maintenance are integral to maintaining a healthy work environment.
- A Business Associate Agreement (BAA), is a written arrangement that specifies each party's responsibilities when it comes to PHI.

Cybersecurity Threat Areas

Online medical and mobile devices

- The security of online medical devices is often lacking, making them easy targets for hackers. These devices are designed to export the information to external sources and otherwise interact with the world outside the doctor's office. This data could be intercepted or manipulated, creating a host of issues. Moreover, hackers could gain access to manage most items connected to the network, including how the machines function.

Cybersecurity Threat Areas

Inadequate disposal of old hardware

- It’s easy to believe that once you’ve deleted information, you no longer have to worry about people accessing it. But when users improperly dispose of hard drives, old computers and other hardware used to access a network with EHRs or credentials, that information is well within a criminal’s grasp. Well after drives have been deleted — and even reformatted — it is possible to rescue this information, meaning anything that the user saved is still vulnerable.

Now What?

- Once potential threats have been identified, implementing practices and protocols for prevention will greatly reduce risk.
- This is especially important given that HIPAA violations can be very expensive. The penalties for noncompliance are based on the level of negligence and can range from $100 to $50,000 **per violation (or per record)**, with a maximum penalty of $1.5 million per year for violations of an identical provision. Violations can also carry criminal charges that can result in jail time.

Cybersecurity Threat Prevention

Understand Your Network Map

- Utilize technology that provides an overview of the devices and storage on your network. In this way, you can see exactly what information is vulnerable in which ways, and you'll know when new or unauthorized devices have joined the system. This layout will also help you establish the access and restrictions for each device on the network, cutting down on inappropriate staff conduct.

Cybersecurity Threat Prevention

Update Your Software

- Be sure all software and operating system information is up to date. These updates include critical patches that discourage potential cybercriminals who jump on previously-found weaknesses in software. If you do not utilize the proper software updates, criminals can still take advantage of the holes left behind by earlier versions.

Cybersecurity Threat Prevention

Virtual Private Network Encryption

- Encrypting your network connection is a great way to enhance network privacy and block potential hackers. A Virtual Private Network (VPN) encodes your data so that other viewers cannot see what goes out or comes in on your computer. So even if they are monitoring your connection, they would not receive anything unless they already had access to your computer.

Cybersecurity Threat Prevention

Conduct Regular Audits

- System administrators should conduct regular audits, and there should be two-step authentication in place that requires anybody looking to adjust information or enter new data to verify their identity. All users should be required to create strong passwords and change them after a predetermined number of weeks. Access credentials should also be reviewed regularly to ensure previous or transferred employees do not have access to patient data.
- A Security Risk Assessment is also a necessary component of participating in Medicare's Merit-Based Incentive Payment System (MIPS) program, and can earn you a bonus and/or prevent a penalty.

Cybersecurity Threat Prevention

Set Strict Access

- Rather than thinking solely about what you need to restrict, consider data from this viewpoint: What do certain employees need to access to do their job? This establishes a context in which the minimum amount of information is available, cutting out the possibility for staff misuse.

HAMILTON FOOT CARE

Security Improvement Pearls

- Using a cloud based service, for your EMR, billing software and/or scheduling software, shifts the security responsibility and risks to the software vendor. Just like hosting your website or facebook account, you don’t do that in house, you leave it to the professionals! They are better equipped to handle the specifics of their software hosting security needs.
- This also ends up saving some $$, as less hardware, support and maintenance is required in office.
- Additionally, a cloud based system allows for access from anywhere with an internet connection.

HAMILTON FOOT CARE

Security Improvement Pearls

- The right hardware can also be used to help provide security.
- Chromebooks utilize security built in from the ground up, including: sandboxing, verified boot and auto updates.
- EMV chip readers, as well as touchless ‘tap’ card readers protect against credit card fraud, as well as chargebacks/disputes from patients.
- 2-step verification for online applications and software ensures that you are the only one accessing your accounts. Options include: text message verification code,USB or GPS dongle, or authenticator apps.
- Credit card processing terminals also need to ‘call in’ to verify payments and batch out sales. Using a phone line is more secure that wifi. Also be sure to complete yearly payment card industry (PCI) compliance reporting.

HAMILTON FOOT CARE

Questions??

HAMILTON
FOOT CARE

Medical, Surgical & Cosmetic Care
For Your Foot And Ankle

410.426.5508
Fax:410.877.6979
5508 Harford Road | Baltimore, MD 21214
1050 North Point Rd #200 | Baltimore, MD 21224

Individual practice consultations available upon request

drjayseidel@gmail.com **cell: 410-905-5496**

INDUSTRY EXPERT PERSEPECTIVE

PROTECTING YOUR PRACTICE

Terri Kinsman


If you don't know where you're going, any road will get you there
Lewis Carroll

SECURITY PLAN STRATEGY

Maryland
OPEN FOR BUSINESS

HIPAA
Health Insurance Portability
& Accountability Act

PCI
Security
Standards Council

RISK ASSESSMENT

- **WHAT?** Detailed evaluation. Spec-based.
- **WHY?** HIPAA requirement! Documents. Informs.
- **HOW?** DIY. Vendor support.
- **NEXT?** Prescribes Strategy. Planning=> resources

HIPAA SRA TOOL SUMMARY REPORT -- SAMPLE

Q5. How do you ensure you are meeting current HIPAA security regulations?	We try to follow the best practices for securing our ePHI but we are not sure we're meeting all the HIPAA security regulations.	Required	TEST PODIATRY	Wed Feb 10 12:50:18 EST 2021

Section 2, Security Policies	Risk Score: 83 %
Threats & Vulnerabilities	Risk Rating
Failure to update Policies & Procedures	
Fines/penalties from mandated regulatory requirements	High
Unstructured guidance for daily tasks and duties within workforce	Critical
Inconsistent/unclear risk management documentation	
Unclear security coordination across workforce	Critical
Unstructured guidance for daily tasks and duties	Critical

Ask Yourself:
What is the risk?
critical
Costs?
20$mo/user
Distruption?
Probably minor

Make an Informed decision to *accept* risk or *mitigate* this issue.

#1 HUMAN ERROR

#2 Email: All End-Point Devices

- **91% of cyber attacks start with a phishing email (because it works)**
- **Email doesn't rely on vulnerabilities (vulnerabilities are system flaws, programming errors, config issues…) Instead, uses simple deception to lure you into opening attachments, disclosing credentials, or taking actions that by-pass normal P&P's.**
- **TRAIN & PRACTICE, SANCTIONS**
- **Harden defense with SaaS, VPN's, firewalls, anti-virus SW, email filters**
- **Take advantage of web browser and email client anti-phishing features**

#3 Passwords/User ID's/IoT Credentials

*PASSWORD POLICY w/ strict sanctions
*Change-REALLY change passwords often
*Prohibit group ID's or PW's- ONLY individual ID's/PW's
*Use 2FA wherever possible
*Complex Passwords (password lockers)
**Never* use the same business x personal x home pw's
* TRAINING

#4 Control of DEVICES with ACCESS to PHI

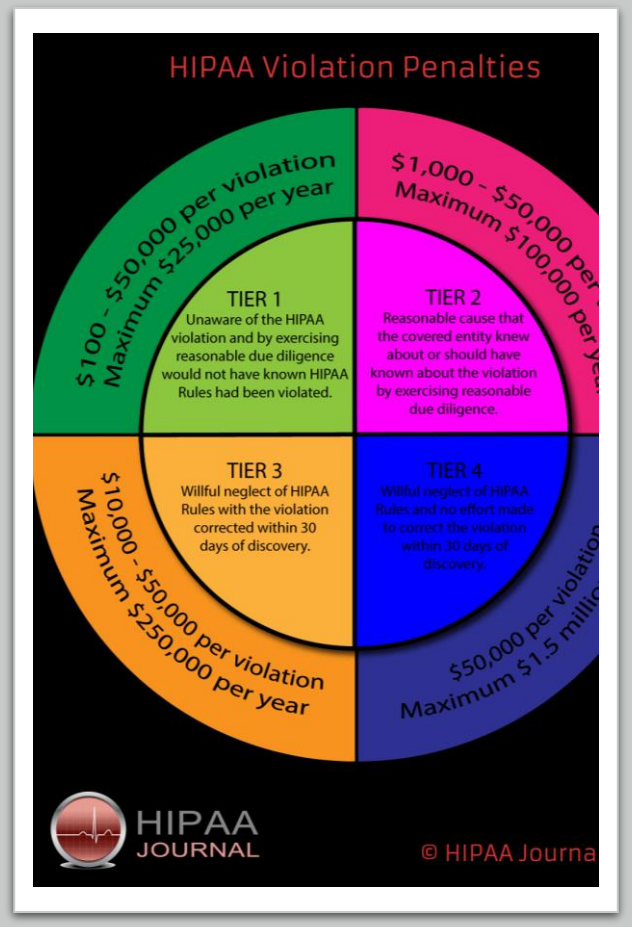
- **Asset Mgt**: Detailed HW, SW & APP Inventory for all devices that can access/process PHI
- **Change Mgt**: Patches, Version Control
- **Training**: Relevant to *your* users
- **Written Policy**: Acceptable Use and Sanctions Policies

2020 HIPAA Fines-Small Practices

Date	Organization	Fine Total	Link to OCR Settlement
3/3/2020	The practice of Steven A. Porter, M.D	$100,000	Health Care Provider Pays $100,000 Settlement to OCR for Failing to Implement HIPAA Security Rule Requirements
7/23/2020	Metropolitan Community Health Services	$25,000	Small Health Care Provider Fails to Implement Multiple HIPAA Security Rule Requirements
7/27/2020	Lifespan Health System	$1,040,000	Lifespan Pays $1,040,000 to OCR to Settle Unencrypted Stolen Laptop Breach
9/15/2020	Housing Works, Inc	$38,000	OCR Settles Five More Investigations in HIPAA Right of Access Initiative
9/15/2020	Wise Psychiatry, PC	$10,000	OCR Settles Five More Investigations in HIPAA Right of Access Initiative
9/21/2020	Athens Orthopedic Clinic PA	$1,500,000	Orthopedic Clinic Pays $1.5 Million to Settle Systemic Noncompliance with HIPAA Rules

#5
VENDOR SUPPORT

- **In the event of a cyber incident, it is very important to prove you understood and accepted your vendor's cyber security position.**
- Vendor Due Diligence: common small practice mistakes
- BAA's
- Monitoring & Control



https://commerce.maryland.gov/fund/programs-for-businesses/buy-maryland-cybersecurity-tax-credit

- Buy Maryland Cybersecurity (BMC) Tax Credit
- The Buy Maryland Cybersecurity Tax Credit provides an incentive for Qualified Maryland Companies to purchase cybersecurity technologies and services from a Qualified Maryland Cybersecurity Seller. Qualified Maryland Companies may claim a **tax credit** for 50% of the net purchase price of cybersecurity technologies and services purchased from a Qualified Maryland Cybersecurity Seller. The tax credit must be claimed for the tax year in which a purchase is made.

New Habits Take Time, Consequences Usually Happen Faster…

COLDFISH LLC 6900 WISCONSIN AVE #30145 BETHESDA,MD 20824
TEL:240.300.0284 WWW.COLDFISHLLC.COM
TERRIKINSMAN@COLDFISHLLC.COM

Helpful Links

Buy Maryland Cybersecurity Tax Credit Program:

https://commerce.maryland.gov/fund/programs-for-businesses/buy-maryland-cybersecurity-tax-credit

Maryland Health Care Commission:

https://mhcc.maryland.gov/

HIPAA for Professionals direct HHS link:

https://www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-covid19/index.html

HIPAA Security Risk Assessment Tool (a DIY tool for Risk Assessments):

https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

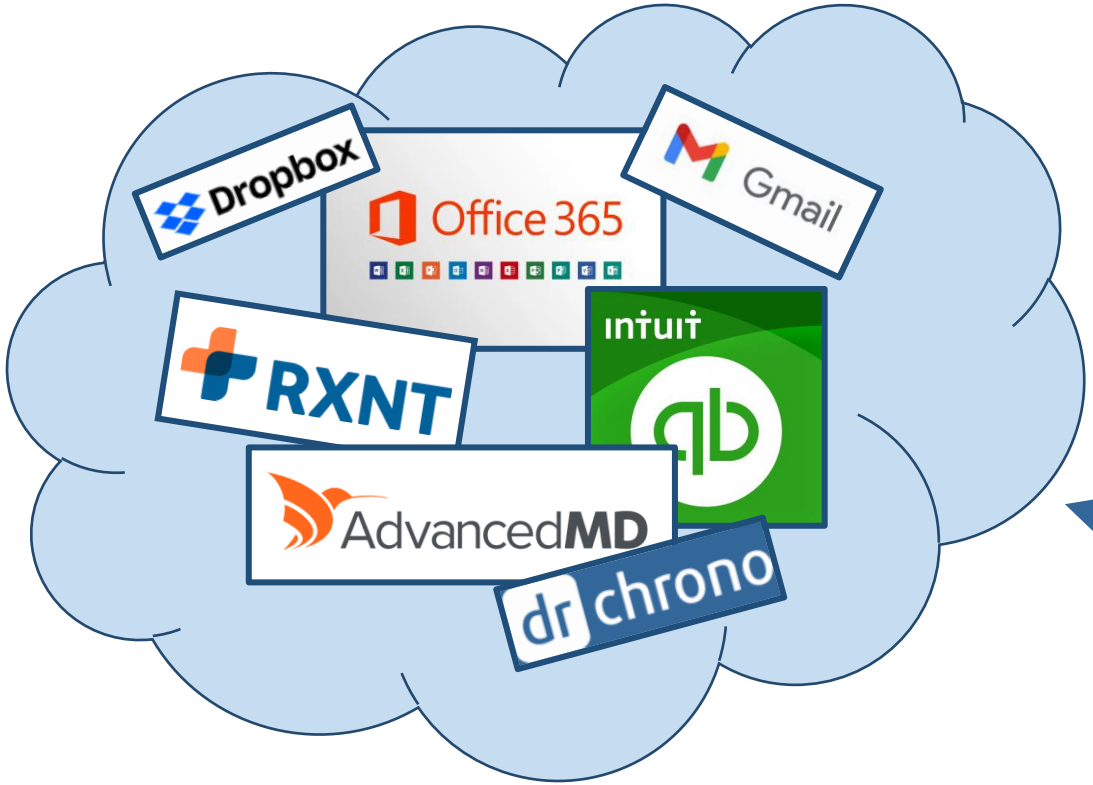
SaaS Risk Management

Shared Responsibility for Cybersecurity

March 12, 2021

Software as a Service (SaaS)

A software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted

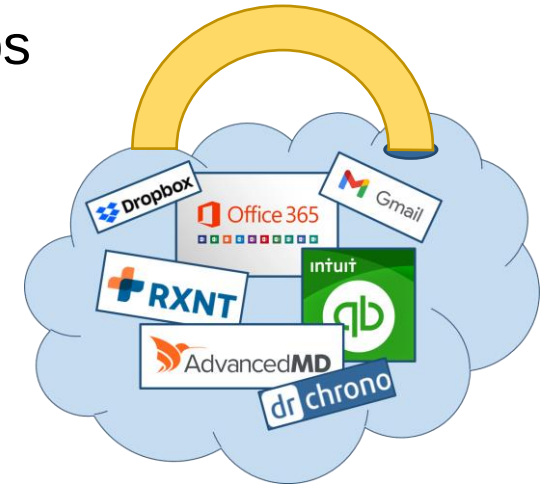


OPTIC CYBER SOLUTIONS

Supplier Responsiblities

Suppliers are responsible for protected data entrusted to them and adhering to SLA

- Data at Rest
- Data in Transit
- Data Separation
- Data Backups



NIST Special Publication 800-161

Supply Chain Risk Management Practices for Federal Information Systems and Organizations

Jon Boyens
Celia Paulsen
Rama Moorthy
Nadya Bartol

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-161

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

OPTIC CYBER SOLUTIONS

Your Responsiblities

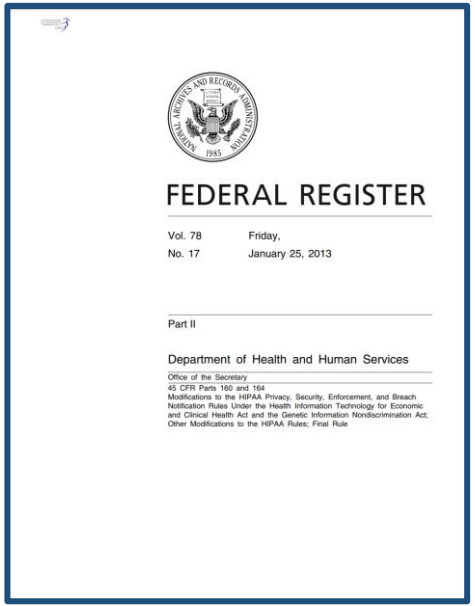
As a SaaS consumer you are responsible for protecting data too

- Account Management
- Access Controls
- Authentication
- Awareness and Training
- Physical Protections

HIPAA Security Rule

The HIPAA Security Rule establish safeguards for protecting health information

- Applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form
- General Rules
  - Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain or transmit;
  - Identify and protect against reasonably anticipated threats to the security or integrity of the information;
  - Protect against reasonably anticipated, impermissible uses or disclosures; and
  - Ensure compliance by the workforce
- Implementation measures and approaches are not dictated by HIPAA, rather covered entities should consider
  - their size, complexity, and capabilities,
  - their technical, hardware, and software infrastructure,
  - the costs of security measures, and
  - The likelihood and possible impact of potential risks to e-PHI


FEDERAL REGISTER

Vol. 78 Friday,
No. 17 January 25, 2013

Part II

Department of Health and Human Services

Office of the Secretary

45 CFR Parts 160 and 164
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

Addressing Requirements

Walking through the HIPAA Security Rule can ensure the supplier and you are meeting expectations

HIPAA Paragraph	Description	Supplier	Consumer	Consumer Gaps
45 C.F.R. §§ 164.310(a)(1)	**Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.			

Information captured from the HIPAA Security Rule

Addressing Requirements

Walking through the HIPAA Security Rule can ensure the supplier and you are meeting expectations

HIPAA Paragraph	Description	Supplier	Consumer	Consumer Gaps
45 C.F.R. §§ 164.310(a)(1)	**Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Provides physical protection of data centers		

Description of the SaaS providers capabilities as aligned to the HIPAA Requirement

Addressing Requirements

Walking through the HIPAA Security Rule can ensure the supplier and you are meeting expectations

HIPAA Paragraph	Description	Supplier	Consumer	Consumer Gaps
45 C.F.R. §§ 164.310(a)(1)	**Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Provides physical protection of data centers	Provides physical protection of devices (e.g., workstations) used to access SaaS	Some desktop may be left unattended during business hours with direct access to from the public

Summary for how the clinic is addressing security requirements and any gaps current capabilties

Addressing Requirements

Walking through the HIPAA Security Rule can ensure the supplier and you are meeting expectations

HIPAA Paragraph	Description	Supplier	Consumer	Consumer Gaps
45 C.F.R. §§ 164.310(a)(1)	**Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Provides physical protection of data centers	Provides physical protection of devices used to access SaaS	Some desktop may be left unattended during business hours with direct access to from the public
45 C.F.R. §§ 164.308(a)(7)(ii)(A)	**Data backup plan** (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Backups of all records and data files are performed routinely throughout the day	Information is not stored locally	N/A

Addressing Requirements

Walking through the HIPAA Security Rule can ensure the supplier and you are meeting expectations

HIPAA Paragraph	Description	Supplier	Consumer	Consumer Gaps
45 C.F.R. §§ 164.310(a)(1)	**Facility access controls**. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	Provides physical protection of data centers	Provides physical protection of devices used to access SaaS	Some desktop may be left unattended during business hours with direct access to from the public
45 C.F.R. §§ 164.308(a)(7)(ii)(A)	**Data backup plan** (Required). Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	Backups of all records and data files are performed routinely throughout the day	Information is not stored locally	N/A
45 C.F.R. §§ 164.308(a)(5)	**Security awareness and training**. Implement a security awareness and training program for all members of its workforce (including management).	Data center operators receive annual security awareness training on the security operations within the data center and supporting applications		Security training currently does not address the requirements for clinic staff to protect their authentication credentials for the SaaS system.

Next Steps

Leverage existing resources to ensure you have addressed the requirements

- HHS publishes the guidance for address requirements
- Establish a matrix to understand your current capabilties and missing activities required to meet requirements
- Review Service Level Agreements (SLAs) to ensure supplier is meeting their expectations
- Ensure Business Associate Agreements (BAAs) are in place and maintained for all SaaS providers with access to protected information

Resources

There are several freely available resources to help you get started

Optic Cyber Solutions

- Resource Home Page: https://www.opticcyber.com/resources.html
- Cybersecurity Framework Profile Template: https://www.opticcyber.com/resources/templates/CSF-PF-profile-template.xlsx

Health and Human Services

- HIPAA Security Rule Crosswalk to the NIST Cybersecurity Framework: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

National Institute of Standards and Technology (NIST)

- National Online Informative References Program: https://csrc.nist.gov/projects/olir/informative-reference-catalog

Questions?

Tom Conkle
Cybersecurity Engineer
Tom.Conkle@OpticCyber.com
(443) 292-6679

We apply cybersecurity as a lens on top of business priorities to help organizations manage risks & protect critical information and resources.

www.OpticCyber.com

Maryland DEPARTMENT OF COMMERCE

Qualified Maryland Cybersecurity Seller

CYBERSECURITY ASSOCIATION OF MARYLAND, INC.

Premium Member

Veteran Owned Small Business

OPTIC CYBER SOLUTIONS

THANK YOU