Managing Cybersecurity Risk

An Essential Element of Every Medical Practice

Maryland Association Medical Staff Services (MAMSS) Spring 2025 Education Conference – May 2, 2025

Maryland Health Care Commission (MHCC)

WHO WE ARE

- Independent State regulatory agency whose mission is to plan for health system needs, promote informed decision-making, increase accountability, and improve access in a rapidly changing health care environment

WHAT WE DO

- Transform care delivery into a value-based care system in which providers collaborate to provide high-quality, coordinated care that emphasizes quality and outcomes and includes financial incentives tied to value

Objectives and Disclosures

- Understand the current landscape of cybersecurity in health care, including local and national data breach trends, and the impact on medical practices
- Identify nationally recognized security frameworks and best practices for vendor risk management
- Discuss key considerations with selecting and maintaining cyber liability insurance coverage
- Summarize practical ways medical practices can prepare for and respond to some of the most common and pervasive cyber risks
- No disclosures

Cybersecurity requires a combination of people, process, and technology

Why Cybersecurity Matters in Health Care

- Cybersecurity is about safeguarding patient health information (PHI) and ensuring the integrity of electronic systems
- The health care sector is a prime target for cyberattacks
  - Cyberattacks cause disruptions in care delivery and pose risks to patient safety and privacy
  - Ransomware continues to create a challenging cyber threat landscape – bad actors understand the critical need to access patient data
- Unintentional human factors increase risk (e.g., falling for deceptive emails, opening infected files, misconfiguring security settings)
  - Phishing is a common point of compromise
- The best cybersecurity does not make an organization immune to cyberattacks

A Closer Look at Health Care Data Breaches

Impacts and Lessons Learned

MARYLAND Health Care Commission

Health Care Data Breaches

Impacts and Lessons Learned from Security Incidents in Maryland and the Nation

April 2025

INTRODUCTION

Data theft crimes and ransomware attacks[1] against the health care sector are commonplace. Cyber risks extend across the various entities that make up the health care sector, including hospitals, medical practices, payers, pharmacies, labs, technology vendors, third-party contractors, and governments.[2] Protecting this essential health care ecosystem requires robust and adaptive cybersecurity approaches to safeguard patient health and financial data and maintain health care operations. Approaches include the implementation of "zero trust," a security framework where policies enforce a never trust, always verify principle.[3] Adoption of zero trust enables health care organizations to strengthen cybersecurity posture for how data is accessed and by whom to reduce the risk of a data breach.[4] The best security measures do not make organizations immune to cyber threats. Over the last decade, the health care sector has experienced a surge in reported data breaches of 100 or more records (Figure 1/Appendix A). The increased rate of breaches is attributed to the proliferation of cybercrime with a national average of 1.7 breaches reported daily from 2018-2024.[5]

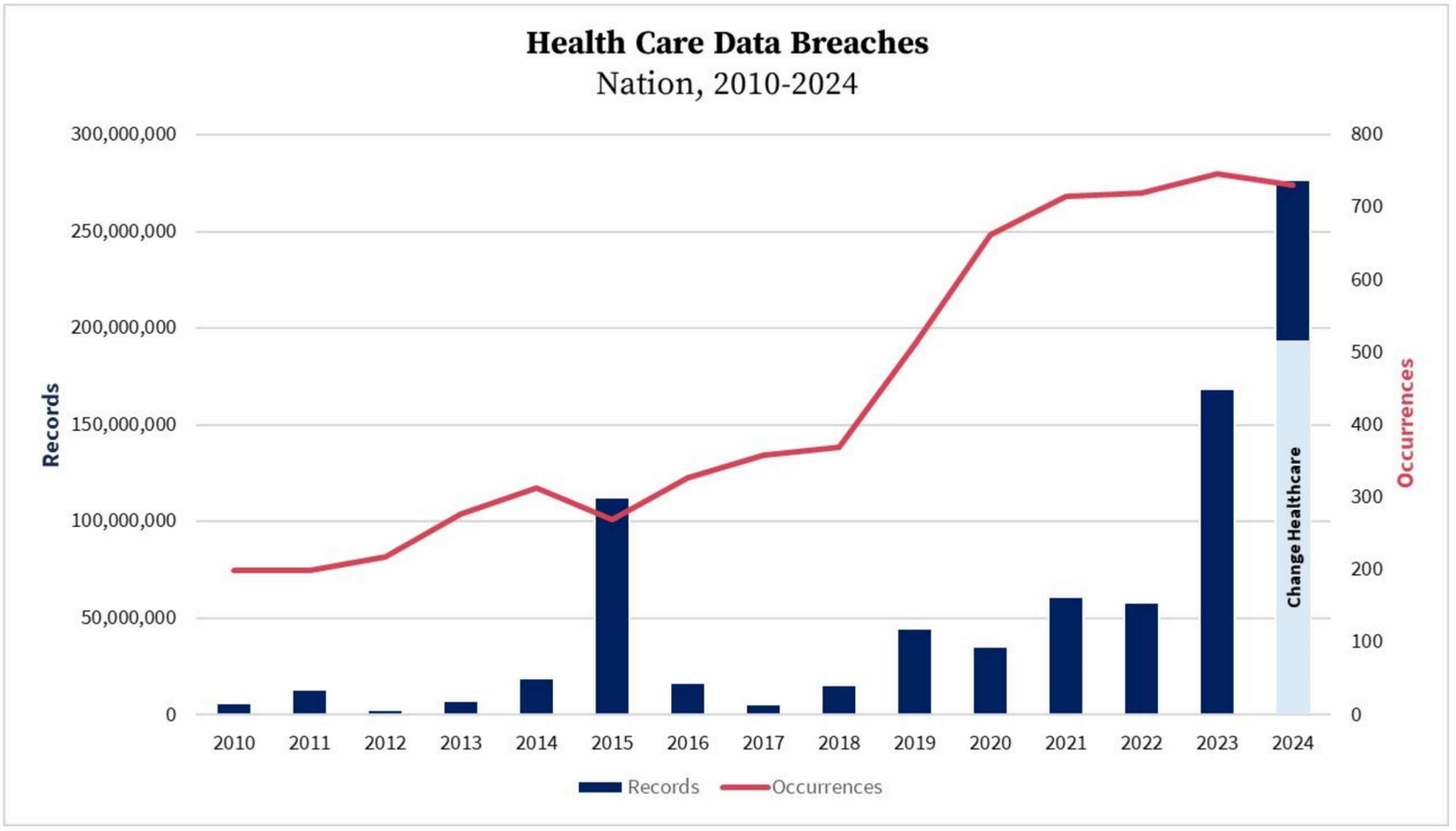
Figure 1: Health Care Data Breaches
Nation, 2010-2024

Breach Reporting

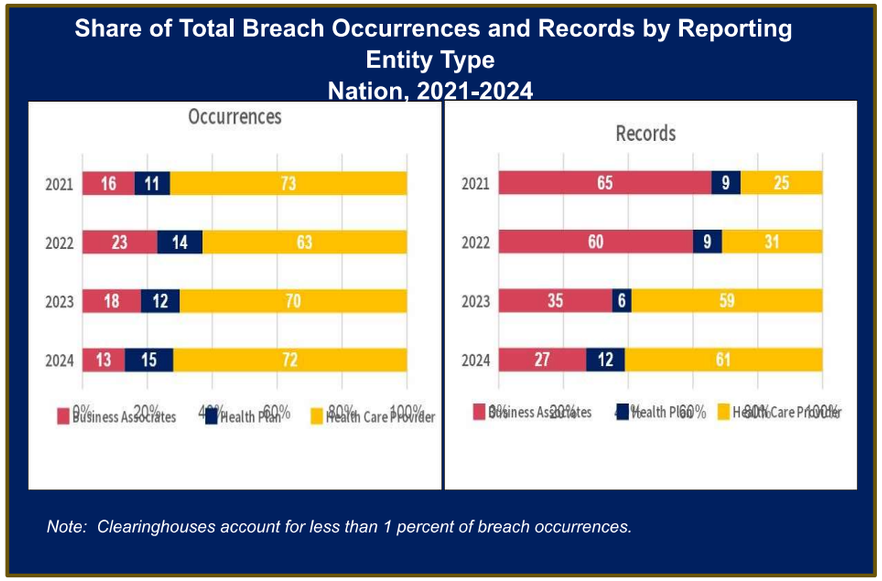
- The Health Information Portability and Accountability Act of 1996 (HIPAA) as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, requires covered entities and their business associates to report breaches to the Department of Health and Human Services, Office for Civil Rights (OCR)
- The MHCC analyzes patterns and trends in breach data made available by OCR in a public use file (for breaches affecting 500 individuals or more*)

*ocrportal.hhs.gov/ocr/breach/breach_report.jsf

A Snapshot of Reported Breaches



Breach Trends



- Health care generally experiences more third-party breaches than other sectors
  - Cybercriminals target third parties that provide a range of technology and services to support health care operations and the delivery of patient care
  - Unauthorized access through a third party can potentially affect multiple organizations that rely on that vendor
- Providers still account for the largest share of breach occurrences; however, providers report fewer records
  - From 2021 to 2024, records decreased from 61 percent to 24 percent; records reported by BAs have nearly doubled over that time, accounting for more than half of all records compromised in 2023 and 2024

Breach Trends *(continued)*

Table 3: Percent of Total Breach Occurrences and Records by Breach Type Nation, Maryland, & Cohort, 2021-2024									
Breach Type		Occurrences %				Records %			
		2021	2022	2023	2024	2021	2022	2023	2024
Nation	Hacking/IT	76	79	81	82	96	86	95	91
	Unauthorized Access/Disclosure	18	16	16	15	3	13	5	9
	Other*	5	5	3	3	1	1	<1	<1
Maryland	Hacking/IT	87	75	81	77	100	96	100	100
	Unauthorized Access/Disclosure	7	13	13	15	<1	1	<1	<1
	Other*	7	13	6	8	<1	3	<1	<1
Cohort	Hacking/IT	77	77	81	84	94	82	99	100
	Unauthorized Access/Disclosure	21	18	14	15	6	18	1	0
	Other*	2	4	5	1	<1	<1	<1	<1

*Notes: *Other includes breaches from improper disposal, loss, and theft.*
Percentages may not total 100 due to rounding.

- Hacking/IT incidents involving technical intrusions of computer systems or networks continue to account for the vast majority of breach occurrences
  - About four out of five breaches reported are the result of hacking/IT incidents
  - Ransomware is a pronounced issue because health care organizations are more willing to pay money to minimize disruption in accessing data necessary to provide care
- Growing nexus between cyberattacks and nation-state hackers acting on behalf of foreign governments (e.g., China, Russia)
  - A Russia-linked ransomware group (BlackCat/ALPHV) claimed responsibility for the Change Healthcare breach in early 2024, which is considered the most significant and consequential cyberattack in the health care sector to date

One reported breach can have a far-reaching impact

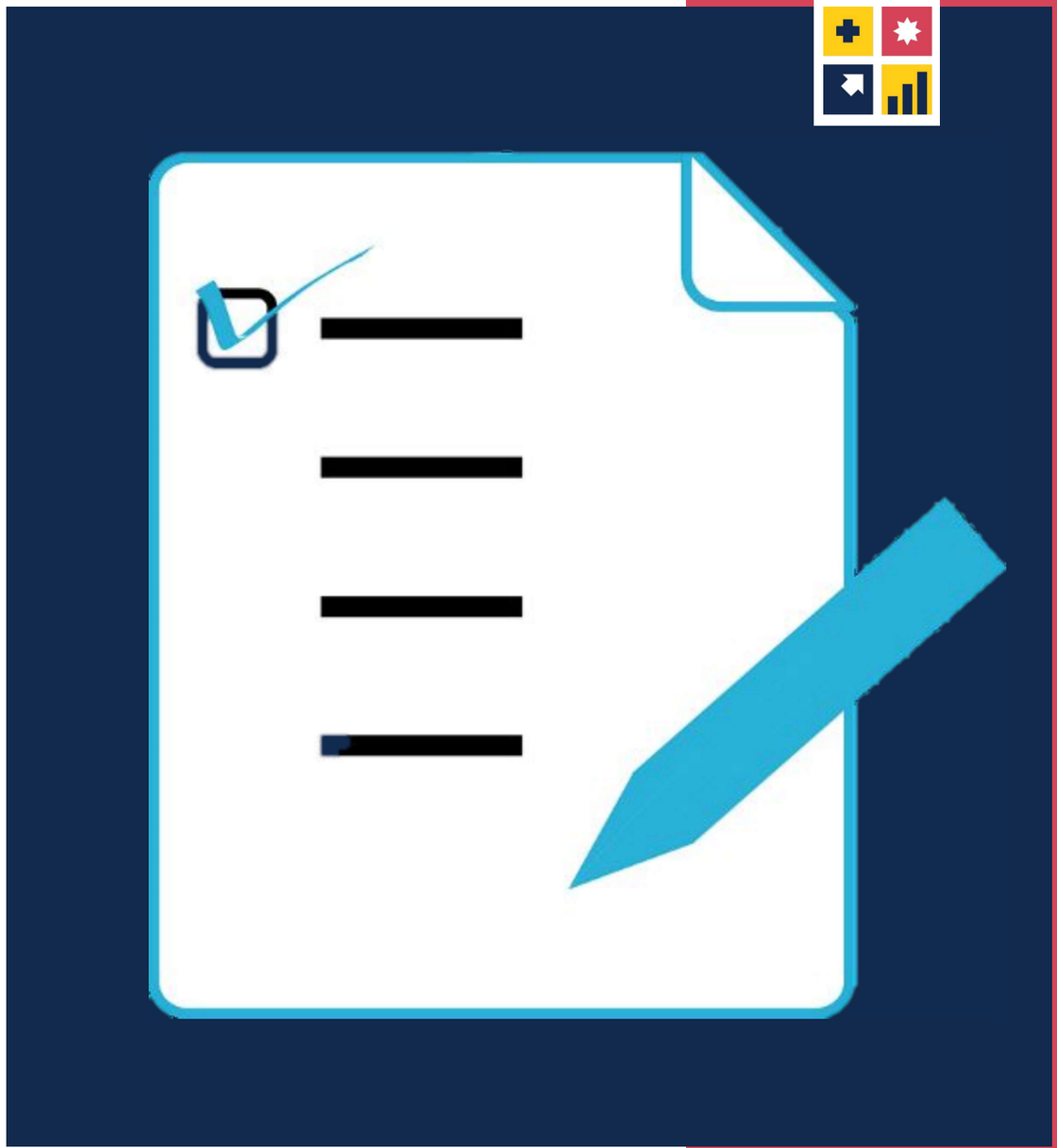
MOVEit

- A third-party file transfer software exposed multiple organizations (worldwide) to a vulnerability in May 2023
  - Allowed CLOP, a Russian-linked ransomware group, to infect applications and steal data from MOVEit databases
- Across all industries, around 2,700 organizations were impacted by the MOVEit vulnerability
  - Estimated that one in five organizations were from the health care sector

Change Healthcare

- Change Healthcare, a unit of UnitedHealth Group, experienced a cyberattack after a bad actor compromised a server not protected by multifactor authentication
  - The incident was discovered in February 2024 and required Change to disconnect its systems
- The incident disrupted operations in revenue management (e.g., verifying eligibility and submitting claims) and patient care (e.g., delays in filling prescriptions)
- Largest number of records ever reported to OCR (190M as of March 2025)

Regulatory and Standards-Based Frameworks

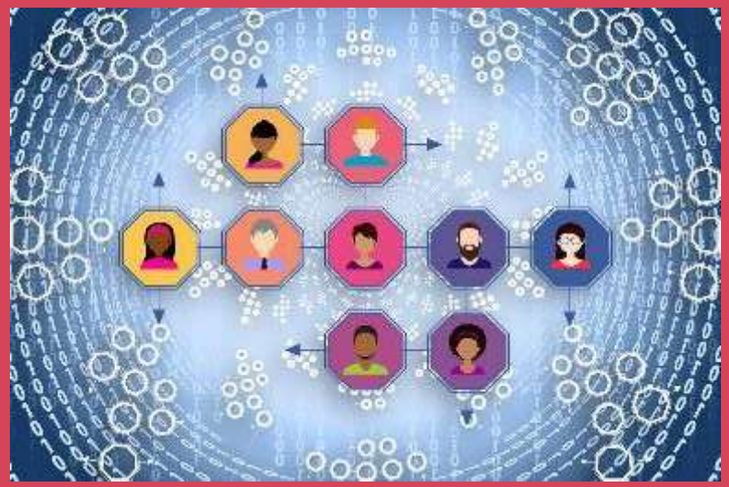


Regulatory and Standards-Based Frameworks

- Certain technology vendors operating in the State must meet privacy and security standards considered more comprehensive than HIPAA
  - Includes claims clearinghouses and health information exchanges (i.e., regional entities and electronic health record vendors)
- Among other things, must have a nationally recognized accreditation or certification (EHNAC or HITRUST) or a SOC 2 Type 2 examination by an independent auditor that provides assurances that adequate systems and controls in place
  - COMAR 10.25.07 requires payers to accept electronic transactions originating in Maryland from electronic health networks certified by MHCC
  - COMAR 10.25.18 requires health information exchanges to register with MHCC annually
- Federal requirements for using Certified Electronic Health Record Technology (CEHRT) requires EHR vendors to undergo a security evaluation as part of their certification process, including audit trails, data encryption, password protection and access control tools

Cybersecurity Best Practices

People: The First Line of Defense



- People play a significant role in protecting practices from cyber attacks
- Human behavior is both an important asset and a potential vulnerability

Mitigating Risks

- Identify emails that are out of the ordinary or unexpected
  - Unrelated to your job responsibilities
  - Sent from an unknown sender
  - Sent at an unusual time
  - Driving urgency
  - Unusual grammar or wording
- Carefully review the sender
  - Hover over the “from” name and review the email for anomalies
    - Email address that doesn’t match the person they are claiming to be
    - Subtle inaccuracies (e.g., john.smith@nycompany.com vs. john.smith@mycompany.com)
- Check links by hovering over (not clicking) over the link to make sure it matches the text
- Be cautious with attachments and do not open attachments with .exe, .vbs, .wsf, .cpl, .cmd, .scr, and .js
- Report and delete suspicious emails

Strengthening Passwords

DO

- Have a minimum of at least 8 characters
- Use a passphrase that is easy to remember but hard to guess (e.g., B1u3B!rdS1ng$)
- Have different passwords for each account
- Use multi-factor authentication whenever possible

DO NOT

- Include personal information
- Use repetitive or sequential characters
- Have the same password across multiple accounts
- Post passwords in plain sight or share log in credentials

Anti-Virus Software

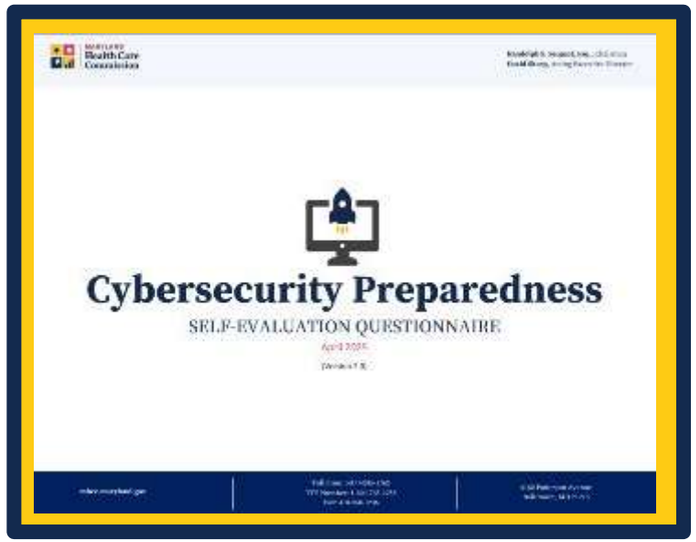
- Install and maintain anti-virus software on all devices to help protect devices and data from cybercriminals
  - Enable automatic updates
  - Scan all machines regularly
  - Ensure all staff understand updates should not be cancelled

Incident Response Planning

- Clarifies roles and responsibilities and key activities before, during, and after a confirmed or suspected cyber incident
- Helps ensure cyber threats are treated like any other disaster (e.g., fires, floods, outbreaks) and encompasses a review of preventative measures that protect patient privacy and safety and limit disruption to organization operations should a cyber-attack occur
- All staff should understand their role and be trained to respond to cyber-related incidents

Improving Cybersecurity Preparedness

- A self-evaluation questionnaire developed by MHCC helps assist practices with identifying gaps in cybersecurity and prioritizing areas for improvement
  - Consists of statements grouped by people, process, and technology
  - Each statement references select elements from the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)
  - The NIST CSF contains six core functions: Govern (“GV”), Identify (“ID”), Protect (“PR”), Detect (“DE”), Respond (“RS”), and Recover (“RC”)
    - Each function has a list of categories and subcategories that define specific cybersecurity activities that should be performed continuously and concurrently
  - Applicable to the organization as well as their vendors
  - The questionnaire is available on MHCC’s website here:



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

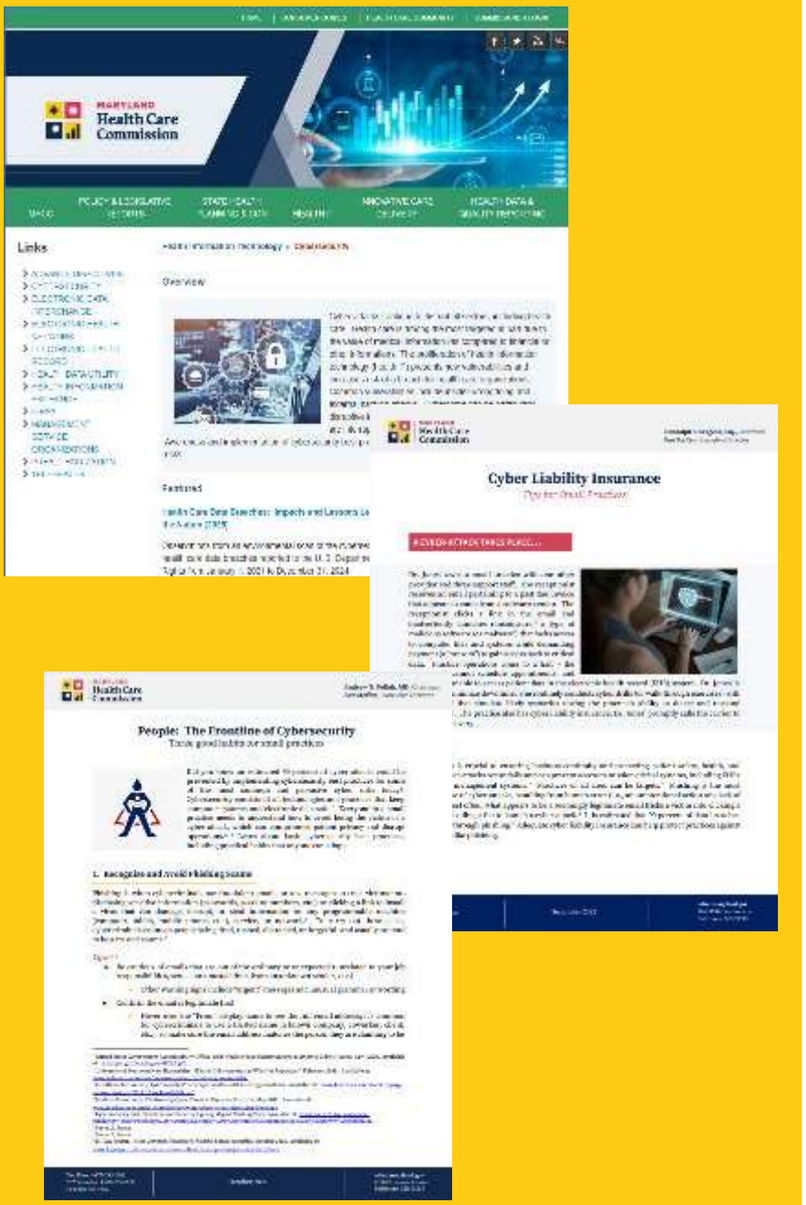
Cybersecurity Liability Insurance

What is Cyber Liability Insurance?

- Cyber liability insurance provides practices with a combination of coverage options to assist with response and recovery, including interruption in operations, recovery expenses, network damages, and data breach lawsuits
- Can be personalized to cover a broad range of risks based on cybersecurity posture
- Cyber liability insurance does not replace the need for implementing cybersecurity best practices; it complements good cybersecurity!

Selecting and Maintaining Cyber Liability Insurance Coverage

- Consider how much and the type of electronic protected health information (or “ePHI”) is collected and stored by your practice (e.g., number of unique patient medical records and credit card information)
- Assess coverage for malpractice to determine what coverage, or if additional coverage, is needed
- Use a reputable and knowledgeable insurance broker that understands health care cyber risks and can recommend appropriate coverage for your practice
- Complete insurance questionnaires accurately and timely to ensure coverage in the event of a cyber incident
  - Questionnaires assess cybersecurity posture to gauge risk; inquires about current cybersecurity policies, technologies, regulatory compliance, incident response plans, and past cyber incidents
- Update the insurance carrier if anything changes



Resources

MHCC Cybersecurity Page

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

People: The Frontline of Cybersecurity

mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/HIT_Frontline_Cybersecurity_Flyer.pdf

Cyber Liability Insurance: Tips for Small Practices

mhcc.maryland.gov/mhcc/pages/hit/hit_cybersecurity/documents/HIT_Cyber_Liability_Flyer.pdf

MHCC AI Symposium Webpage

mhcc.maryland.gov/mhcc/pages/hit/hit/health-care-ai-symposium-series.aspx

Resources (continued)

HHS Security Risk Assessment Tool

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

NIST Cybersecurity Framework

www.nist.gov/cyberframework

10 Practices to Protect Your Organization from Cyber Threats

405d.hhs.gov/Documents/405d-infographic-10practices.p

Thank you!

Questions?

Justine Springer, MHCC Program Manager

justine.springer@maryland.gov

Appendix

FTC Enforcement

Breaches Reported to the Federal Trade Commission and Penalties, 2023		
Company Name	**Company Type**	**Penalty Amount**
Monument	Addiction telehealth	$2.5 million
Better Help	Online mental health and counseling	$7.8 million
GoodRx	Telehealth and prescription drug discount platform	$1.5 million
Premom	Fertility tracking app	$200,000
Cerebral	Mental health telehealth	$7.1 million

- The FTC aims to protect the public from fraudulent, deceptive, and unfair practices; includes making sure companies take reasonable steps to protect PHI and do not mislead consumers about what is happening with their health information
- The FTC Health Breach Notification Rule applies to companies not regulated by HIPAA (e.g., health apps and fitness trackers)
- In 2023, the FTC took enforcement action against several digital health companies for impermissible disclosures of PHI to third parties

Consumer Health Data

- Defined as health-related data created and recorded by or from consumers or family members/caregivers outside of a clinical setting
- Distinct from data generated in clinical settings in two ways:
  - Consumers are primarily responsible for capturing or recording these data
  - Consumers decide how to share or distribute these data to providers and others

Privacy and Security of Consumer Health Data

- Privacy and security protections differ across consumer health technologies that maintain and transmit consumer health data
- In many instances, consumer health data is not protected by HIPAA, presenting risks to consumers who may intentionally or unintentionally share their health-related data
- HIPAA only extends protections to protected health information (PHI) created, received, or maintained by or on behalf of covered entities (CEs) and business associates (BAs)
- Technologies that lack HIPAA-equivalent protections can result in: Selling or sharing consumer health data without users' consent or knowledge
- Responding differently to a breach
- Re-identifying consumer health data (if proper security measures to de-identify the data are not in place)