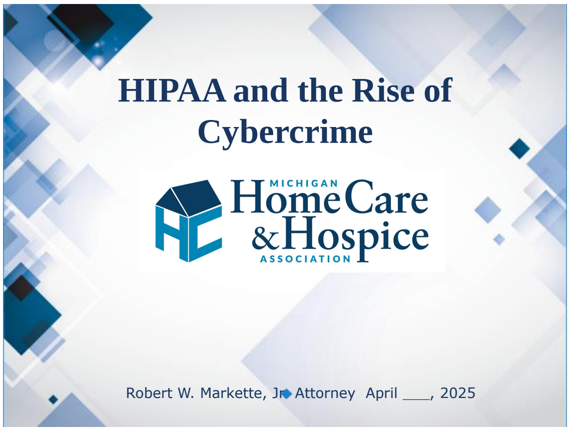
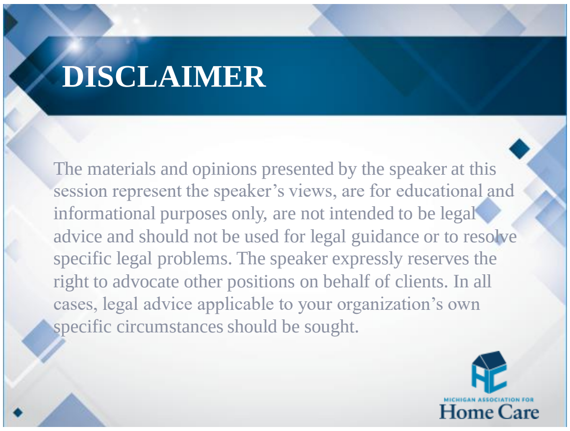


HIPAA and the Rise of Cybercrime

Michigan Home Care & Hospice Association

Robert W. Markette, Jr. Attorney April ____, 2025

1

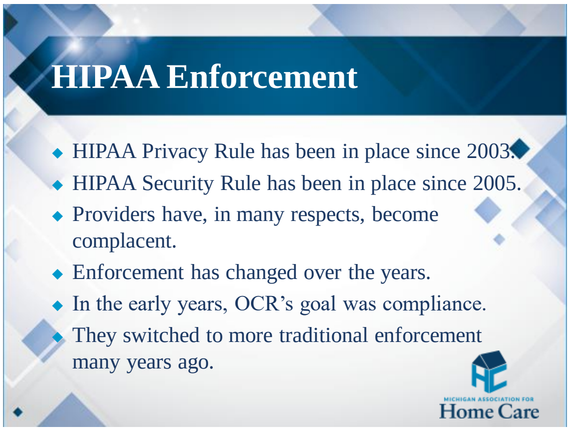


DISCLAIMER

The materials and opinions presented by the speaker at this session represent the speaker's views, are for educational and informational purposes only, are not intended to be legal advice and should not be used for legal guidance or to resolve specific legal problems. The speaker expressly reserves the right to advocate other positions on behalf of clients. In all cases, legal advice applicable to your organization's own specific circumstances should be sought.

Michigan Association for Home Care

2

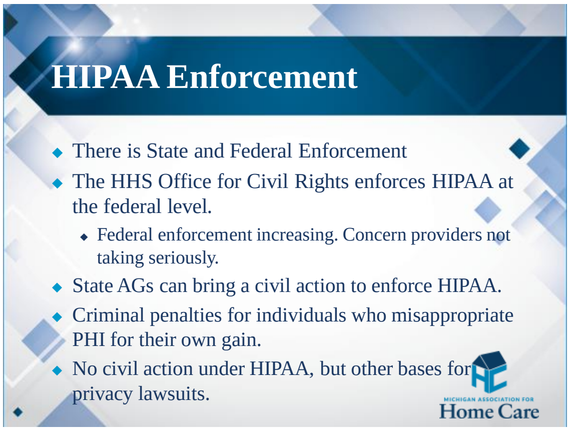


HIPAA Enforcement

- HIPAA Privacy Rule has been in place since 2003.
- HIPAA Security Rule has been in place since 2005.
- Providers have, in many respects, become complacent.
- Enforcement has changed over the years.
- In the early years, OCR's goal was compliance.
- They switched to more traditional enforcement many years ago.

Michigan Association for Home Care

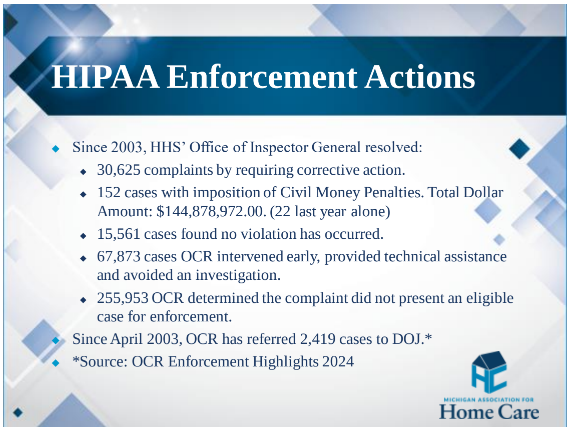
3



HIPAA Enforcement

- There is State and Federal Enforcement
- The HHS Office for Civil Rights enforces HIPAA at the federal level.
  - Federal enforcement increasing. Concern providers not taking seriously.
- State AGs can bring a civil action to enforce HIPAA.
- Criminal penalties for individuals who misappropriate PHI for their own gain.
- No civil action under HIPAA, but other bases for privacy lawsuits.

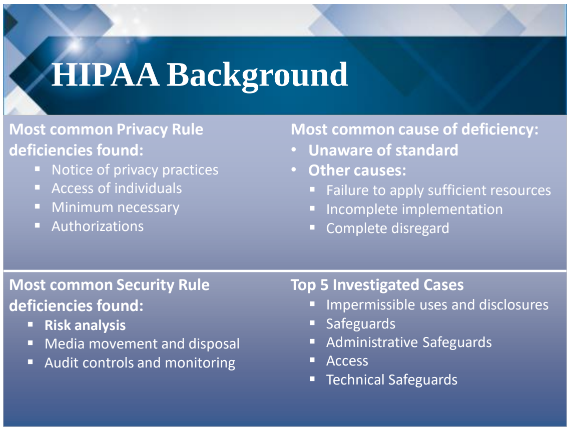
4



HIPAA Enforcement Actions

- Since 2003, HHS' Office of Inspector General resolved:
  - 30,625 complaints by requiring corrective action.
  - 152 cases with imposition of Civil Money Penalties. Total Dollar Amount: $144,878,972.00. (22 last year alone)
  - 15,561 cases found no violation has occurred.
  - 67,873 cases OCR intervened early, provided technical assistance and avoided an investigation.
  - 255,953 OCR determined the complaint did not present an eligible case for enforcement.
- Since April 2003, OCR has referred 2,419 cases to DOJ.*
- *Source: OCR Enforcement Highlights 2024

5



HIPAA Background

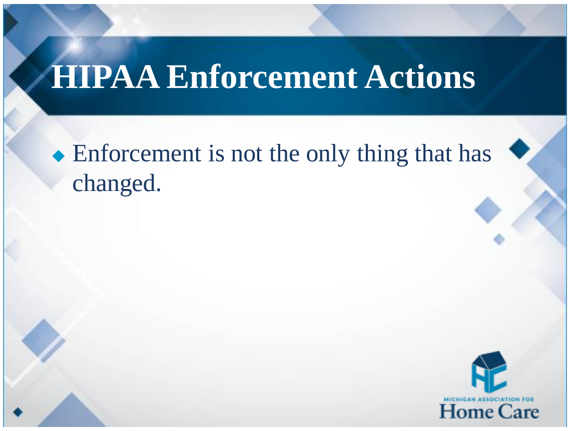
Most common Privacy Rule deficiencies found:
- Notice of privacy practices
- Access of individuals
- Minimum necessary
- Authorizations

Most common cause of deficiency:
- **Unaware of standard**
- **Other causes:**
  - Failure to apply sufficient resources
  - Incomplete implementation
  - Complete disregard

Most common Security Rule deficiencies found:
- **Risk analysis**
- Media movement and disposal
- Audit controls and monitoring

Top 5 Investigated Cases
- Impermissible uses and disclosures
- Safeguards
- Administrative Safeguards
- Access
- Technical Safeguards

6



HIPAA Enforcement Actions

- Enforcement is not the only thing that has changed.

7

Technology and Health Care

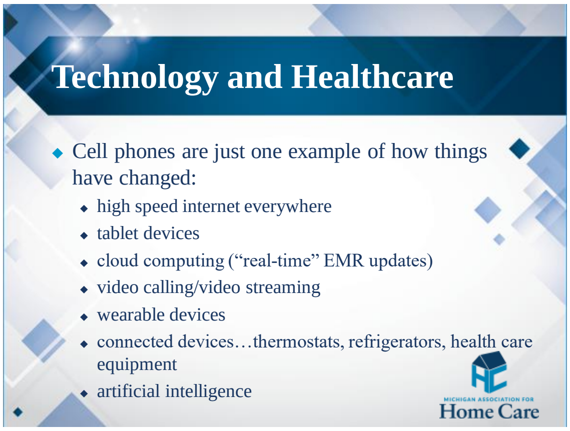
- Cell phone: 2000
  - Calling

8

Technology and Healthcare

- Cell phone: Today
  - Calling
  - Texting
  - Photography
  - Video
  - Music
  - AI
  - GPS
  - Massive storage
  - Apps
  - more…

9



Technology and Healthcare

- Cell phones are just one example of how things have changed:
  - high speed internet everywhere
  - tablet devices
  - cloud computing ("real-time" EMR updates)
  - video calling/video streaming
  - wearable devices
  - connected devices…thermostats, refrigerators, health care equipment
  - artificial intelligence

10

Technology and Healthcare

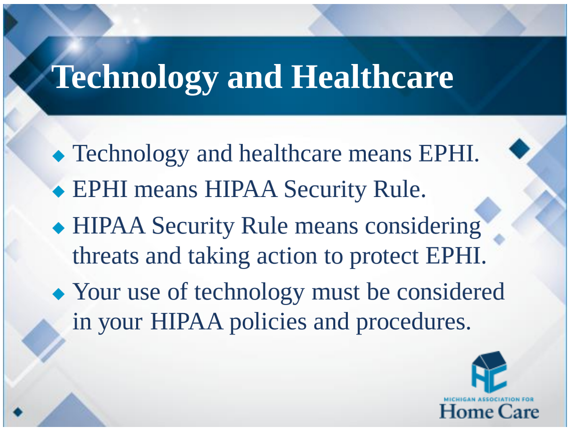
- These technologies have reshaped many areas of our lives.
- Even health care.
- One of the biggest examples: EMRs.
- Other examples: EVV, Point of care devices – laptops, tablets; cell phones and texting to communicate with staff.
- Office/Administration: Remote working, video conferencing, etc.;
- Telemonitoring – widespread availability of high-speed internet allowing for remote monitoring of patients;

11

Technology and Healthcare

- Each of these technologies provides a number of benefits to home health, hospice and private duty providers.
- But they also come with risks.
- Need to understand how you use technology throughout your agency and understand the risks that are affiliated with these various uses.

12

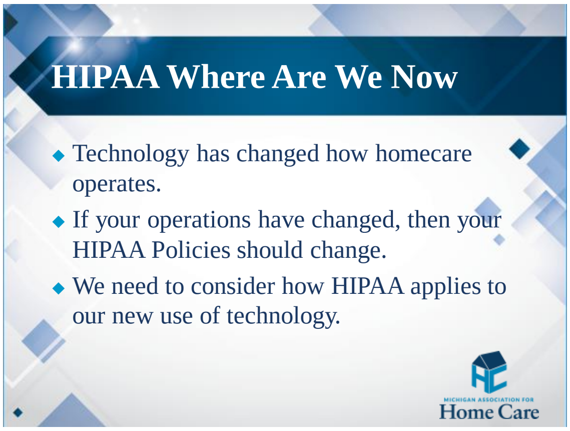


Technology and Healthcare

- Technology and healthcare means EPHI.
- EPHI means HIPAA Security Rule.
- HIPAA Security Rule means considering threats and taking action to protect EPHI.
- Your use of technology must be considered in your HIPAA policies and procedures.

MICHIGAN ASSOCIATION FOR Home Care

13

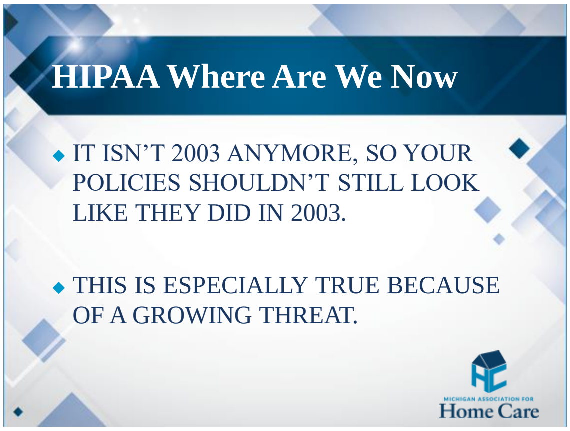


HIPAA Where Are We Now

- Technology has changed how homecare operates.
- If your operations have changed, then your HIPAA Policies should change.
- We need to consider how HIPAA applies to our new use of technology.

MICHIGAN ASSOCIATION FOR Home Care

14



HIPAA Where Are We Now

- IT ISN’T 2003 ANYMORE, SO YOUR POLICIES SHOULDN’T STILL LOOK LIKE THEY DID IN 2003.
- THIS IS ESPECIALLY TRUE BECAUSE OF A GROWING THREAT.

MICHIGAN ASSOCIATION FOR Home Care

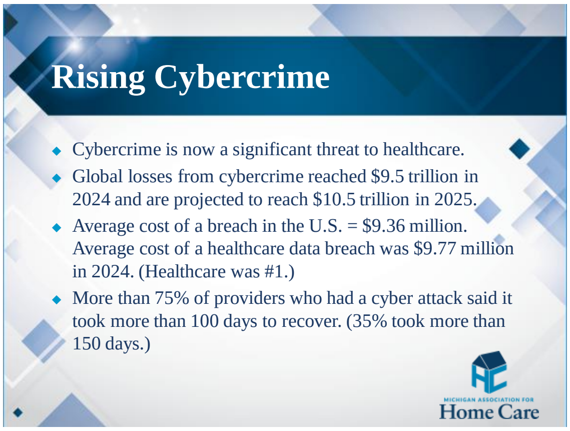
15

Cybercrime

- All of this technology allows criminals from all over the world to try to access your systems.
- Obtaining your business information or your patient information used to require a criminal to actually break into the office.
- Now, criminals from all over the world – Kazakhstan, North Korea, China, Russia, South America, Egypt, Colombia, and others – can access your systems.

MICHIGAN ASSOCIATION FOR Home Care

16

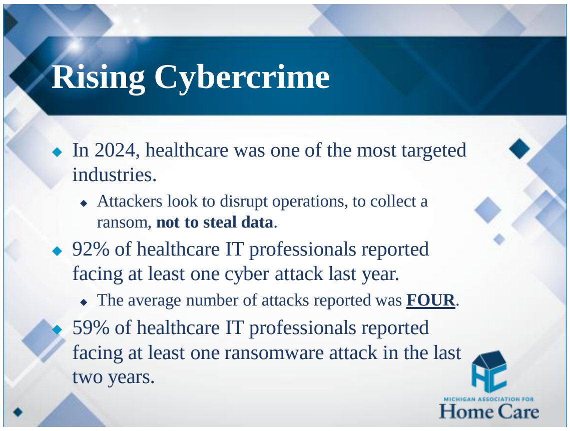


Rising Cybercrime

- Cybercrime is now a significant threat to healthcare.
- Global losses from cybercrime reached $9.5 trillion in 2024 and are projected to reach $10.5 trillion in 2025.
- Average cost of a breach in the U.S. = $9.36 million. Average cost of a healthcare data breach was $9.77 million in 2024. (Healthcare was #1.)
- More than 75% of providers who had a cyber attack said it took more than 100 days to recover. (35% took more than 150 days.)

MICHIGAN ASSOCIATION FOR Home Care

17

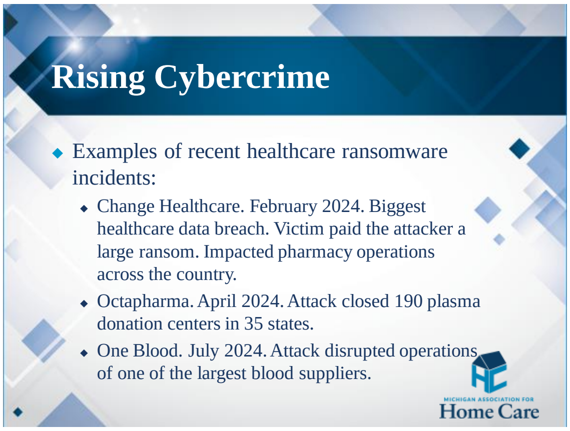


Rising Cybercrime

- In 2024, healthcare was one of the most targeted industries.
  - Attackers look to disrupt operations, to collect a ransom, **not to steal data**.
- 92% of healthcare IT professionals reported facing at least one cyber attack last year.
  - The average number of attacks reported was **FOUR**.
- 59% of healthcare IT professionals reported facing at least one ransomware attack in the last two years.

MICHIGAN ASSOCIATION FOR Home Care

18

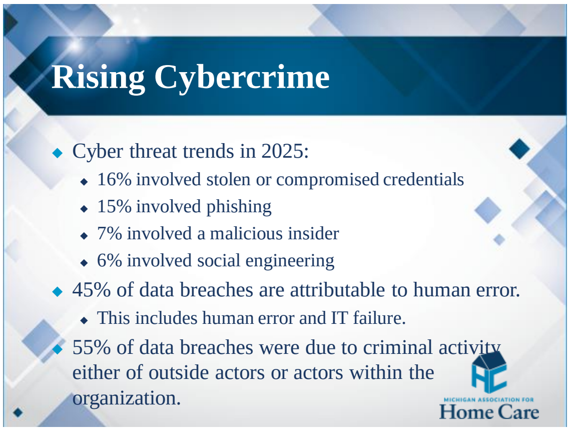


Rising Cybercrime

- Examples of recent healthcare ransomware incidents:
  - Change Healthcare. February 2024. Biggest healthcare data breach. Victim paid the attacker a large ransom. Impacted pharmacy operations across the country.
  - Octapharma. April 2024. Attack closed 190 plasma donation centers in 35 states.
  - One Blood. July 2024. Attack disrupted operations of one of the largest blood suppliers.

MICHIGAN ASSOCIATION FOR Home Care

19

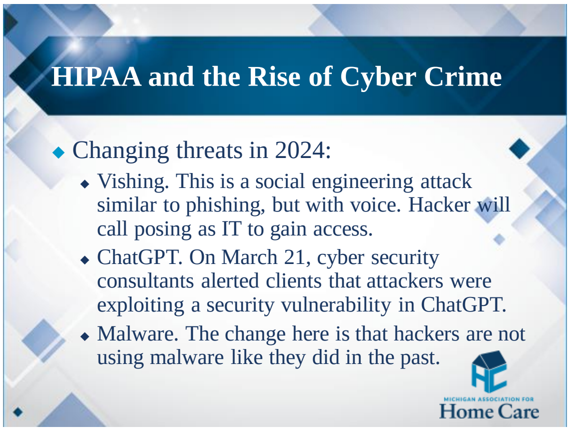


Rising Cybercrime

- Cyber threat trends in 2025:
  - 16% involved stolen or compromised credentials
  - 15% involved phishing
  - 7% involved a malicious insider
  - 6% involved social engineering
- 45% of data breaches are attributable to human error.
  - This includes human error and IT failure.
- 55% of data breaches were due to criminal activity either of outside actors or actors within the organization.

MICHIGAN ASSOCIATION FOR Home Care

20

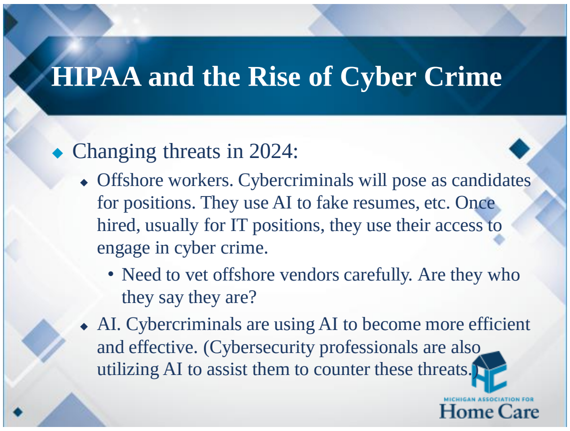


HIPAA and the Rise of Cyber Crime

- Changing threats in 2024:
  - Vishing. This is a social engineering attack similar to phishing, but with voice. Hacker will call posing as IT to gain access.
  - ChatGPT. On March 21, cyber security consultants alerted clients that attackers were exploiting a security vulnerability in ChatGPT.
  - Malware. The change here is that hackers are not using malware like they did in the past.

MICHIGAN ASSOCIATION FOR Home Care

21

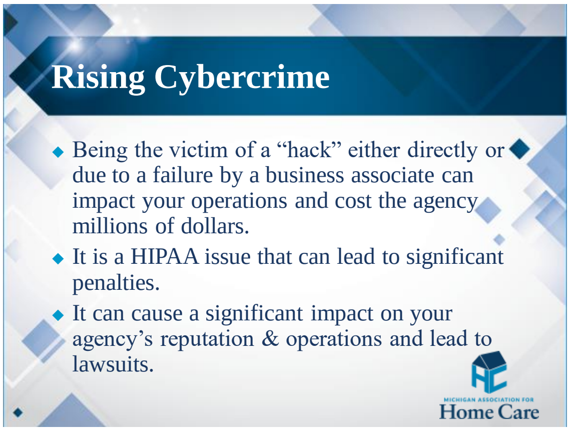


HIPAA and the Rise of Cyber Crime

- Changing threats in 2024:
  - Offshore workers. Cybercriminals will pose as candidates for positions. They use AI to fake resumes, etc. Once hired, usually for IT positions, they use their access to engage in cyber crime.
    - Need to vet offshore vendors carefully. Are they who they say they are?
  - AI. Cybercriminals are using AI to become more efficient and effective. (Cybersecurity professionals are also utilizing AI to assist them to counter these threats.)

MICHIGAN ASSOCIATION FOR Home Care

22

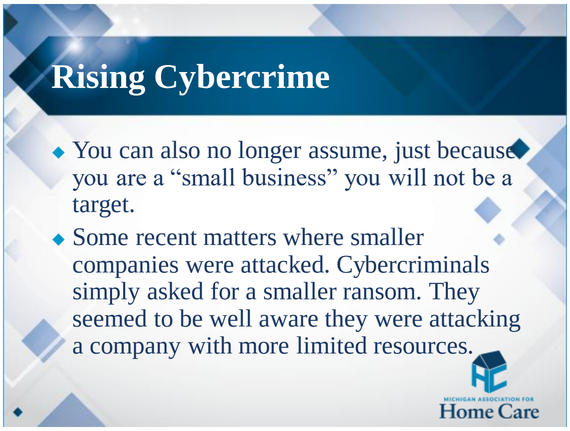


Rising Cybercrime

- Being the victim of a "hack" either directly or due to a failure by a business associate can impact your operations and cost the agency millions of dollars.
- It is a HIPAA issue that can lead to significant penalties.
- It can cause a significant impact on your agency's reputation & operations and lead to lawsuits.

MICHIGAN ASSOCIATION FOR Home Care

23

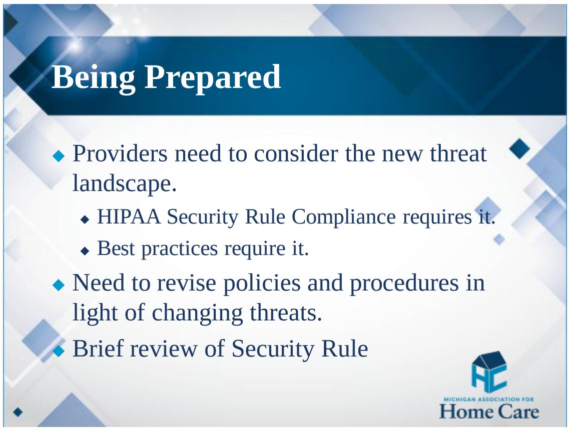


Rising Cybercrime

- You can also no longer assume, just because you are a "small business" you will not be a target.
- Some recent matters where smaller companies were attacked. Cybercriminals simply asked for a smaller ransom. They seemed to be well aware they were attacking a company with more limited resources.

MICHIGAN ASSOCIATION FOR Home Care

24

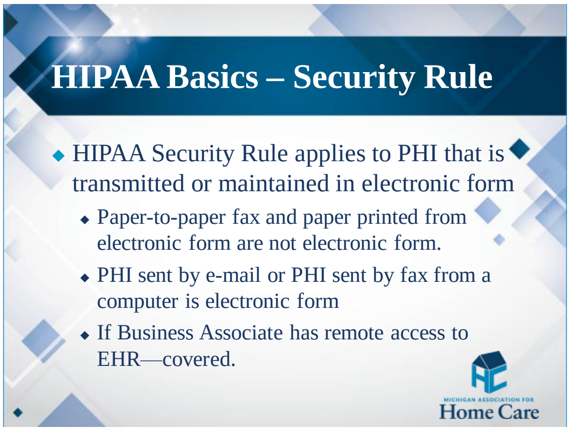


Being Prepared

- Providers need to consider the new threat landscape.
  - HIPAA Security Rule Compliance requires it.
  - Best practices require it.
- Need to revise policies and procedures in light of changing threats.
- Brief review of Security Rule

MICHIGAN ASSOCIATION FOR Home Care

25

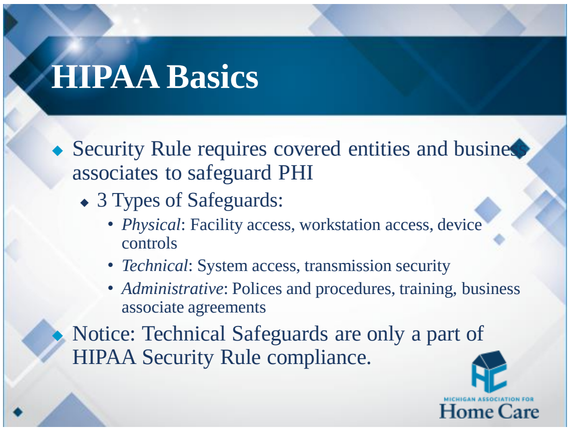


HIPAA Basics – Security Rule

- HIPAA Security Rule applies to PHI that is transmitted or maintained in electronic form
  - Paper-to-paper fax and paper printed from electronic form are not electronic form.
  - PHI sent by e-mail or PHI sent by fax from a computer is electronic form
  - If Business Associate has remote access to EHR—covered.

MICHIGAN ASSOCIATION FOR Home Care

26

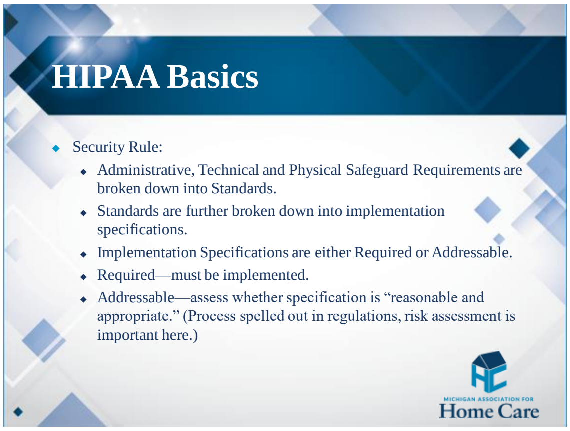


HIPAA Basics

- Security Rule requires covered entities and business associates to safeguard PHI
  - 3 Types of Safeguards:
    - *Physical*: Facility access, workstation access, device controls
    - *Technical*: System access, transmission security
    - *Administrative*: Polices and procedures, training, business associate agreements
- Notice: Technical Safeguards are only a part of HIPAA Security Rule compliance.

MICHIGAN ASSOCIATION FOR Home Care

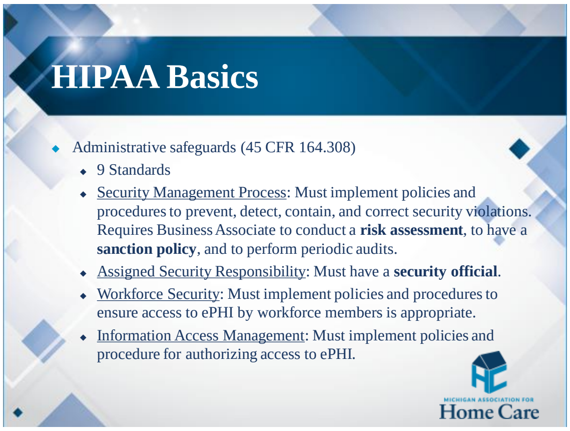
27



HIPAA Basics

- Security Rule:
  - Administrative, Technical and Physical Safeguard Requirements are broken down into Standards.
  - Standards are further broken down into implementation specifications.
  - Implementation Specifications are either Required or Addressable.
  - Required—must be implemented.
  - Addressable—assess whether specification is "reasonable and appropriate." (Process spelled out in regulations, risk assessment is important here.)

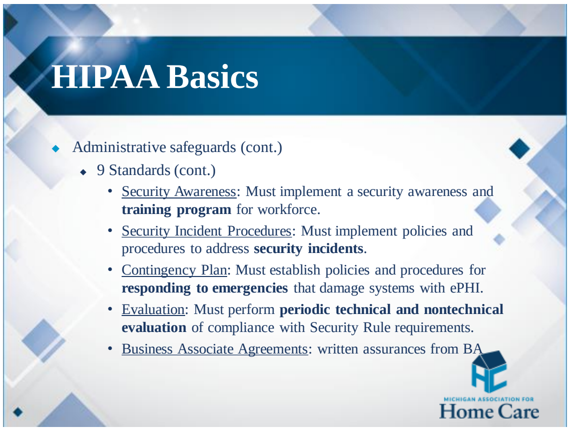
28



HIPAA Basics

- Administrative safeguards (45 CFR 164.308)
  - 9 Standards
  - Security Management Process: Must implement policies and procedures to prevent, detect, contain, and correct security violations. Requires Business Associate to conduct a **risk assessment**, to have a **sanction policy**, and to perform periodic audits.
  - Assigned Security Responsibility: Must have a **security official**.
  - Workforce Security: Must implement policies and procedures to ensure access to ePHI by workforce members is appropriate.
  - Information Access Management: Must implement policies and procedure for authorizing access to ePHI.

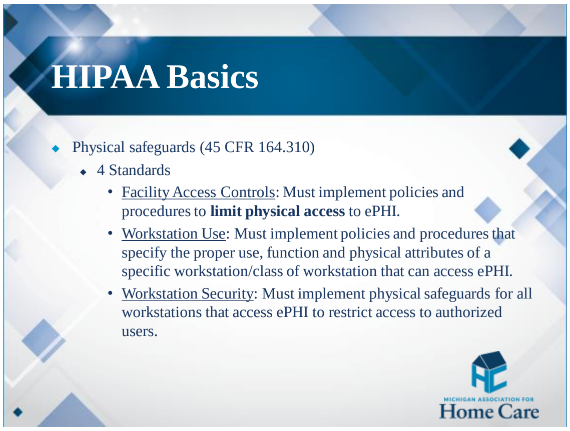
29



HIPAA Basics

- Administrative safeguards (cont.)
  - 9 Standards (cont.)
    - Security Awareness: Must implement a security awareness and **training program** for workforce.
    - Security Incident Procedures: Must implement policies and procedures to address **security incidents**.
    - Contingency Plan: Must establish policies and procedures for **responding to emergencies** that damage systems with ePHI.
    - Evaluation: Must perform **periodic technical and nontechnical evaluation** of compliance with Security Rule requirements.
    - Business Associate Agreements: written assurances from BA

30

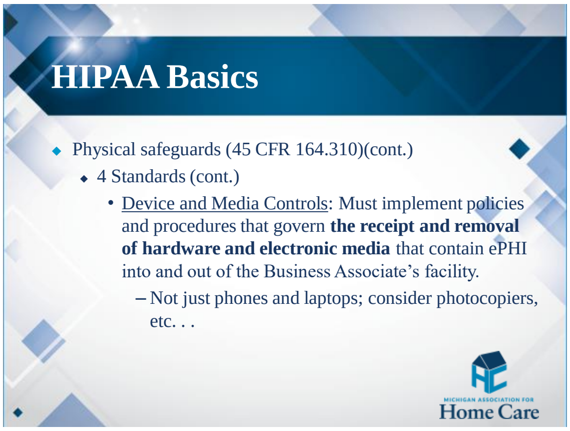


HIPAA Basics

- Physical safeguards (45 CFR 164.310)
  - 4 Standards
    - Facility Access Controls: Must implement policies and procedures to **limit physical access** to ePHI.
    - Workstation Use: Must implement policies and procedures that specify the proper use, function and physical attributes of a specific workstation/class of workstation that can access ePHI.
    - Workstation Security: Must implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.

MICHIGAN ASSOCIATION FOR Home Care

31

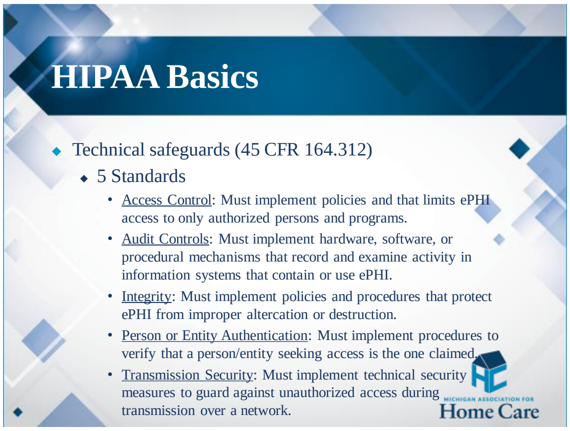


HIPAA Basics

- Physical safeguards (45 CFR 164.310)(cont.)
  - 4 Standards (cont.)
    - Device and Media Controls: Must implement policies and procedures that govern **the receipt and removal of hardware and electronic media** that contain ePHI into and out of the Business Associate's facility.
      - Not just phones and laptops; consider photocopiers, etc. . .

MICHIGAN ASSOCIATION FOR Home Care

32

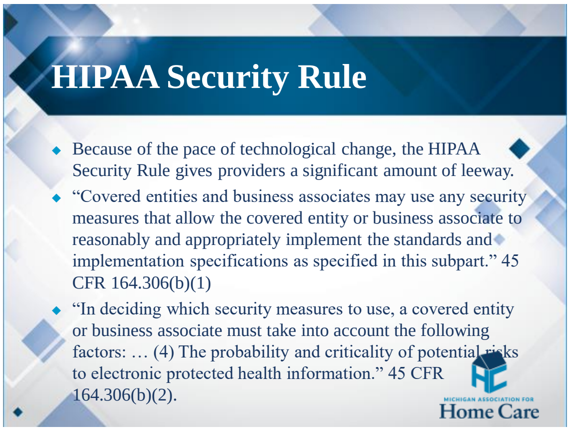


HIPAA Basics

- Technical safeguards (45 CFR 164.312)
  - 5 Standards
    - Access Control: Must implement policies and that limits ePHI access to only authorized persons and programs.
    - Audit Controls: Must implement hardware, software, or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
    - Integrity: Must implement policies and procedures that protect ePHI from improper altercation or destruction.
    - Person or Entity Authentication: Must implement procedures to verify that a person/entity seeking access is the one claimed.
    - Transmission Security: Must implement technical security measures to guard against unauthorized access during transmission over a network.

MICHIGAN ASSOCIATION FOR Home Care

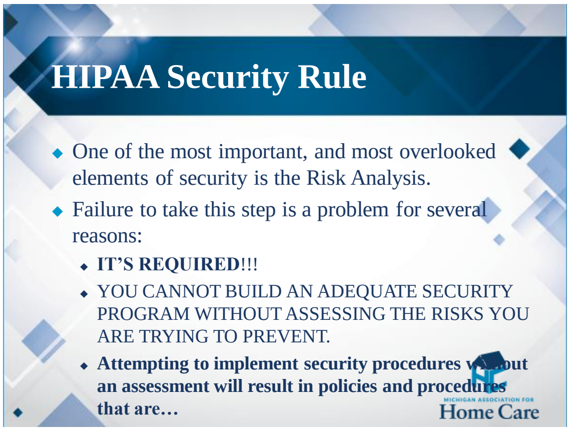
33



HIPAA Security Rule

- Because of the pace of technological change, the HIPAA Security Rule gives providers a significant amount of leeway.
- "Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." 45 CFR 164.306(b)(1)
- "In deciding which security measures to use, a covered entity or business associate must take into account the following factors: … (4) The probability and criticality of potential risks to electronic protected health information." 45 CFR 164.306(b)(2).

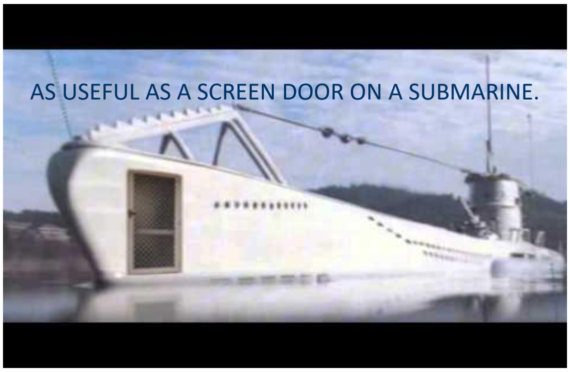
34



HIPAA Security Rule

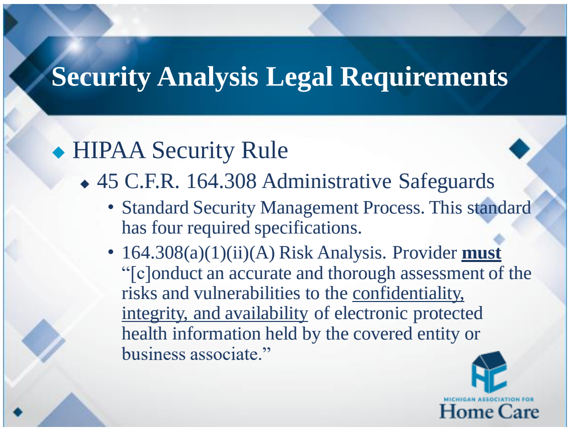
- One of the most important, and most overlooked elements of security is the Risk Analysis.
- Failure to take this step is a problem for several reasons:
  - **IT'S REQUIRED**!!!
  - YOU CANNOT BUILD AN ADEQUATE SECURITY PROGRAM WITHOUT ASSESSING THE RISKS YOU ARE TRYING TO PREVENT.
  - **Attempting to implement security procedures without an assessment will result in policies and procedures that are…**

35



AS USEFUL AS A SCREEN DOOR ON A SUBMARINE.

36

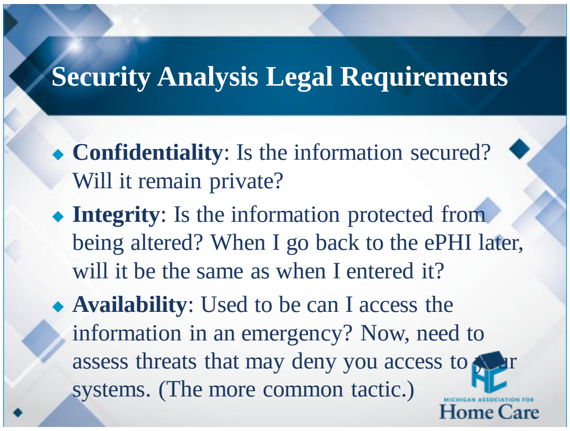


Security Analysis Legal Requirements

- HIPAA Security Rule
  - 45 C.F.R. 164.308 Administrative Safeguards
    - Standard Security Management Process. This standard has four required specifications.
    - 164.308(a)(1)(ii)(A) Risk Analysis. Provider **must** "[c]onduct an accurate and thorough assessment of the risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate."

MICHIGAN ASSOCIATION FOR Home Care

37

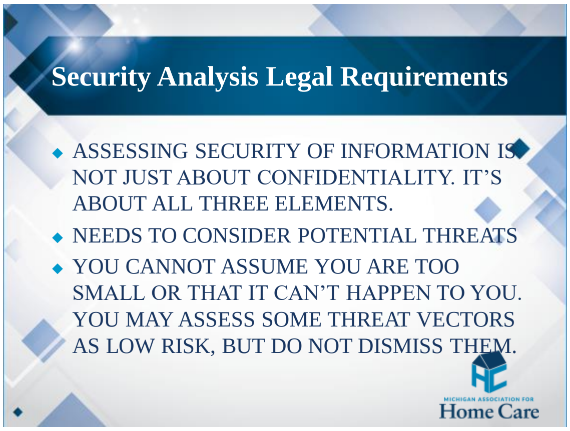


Security Analysis Legal Requirements

- **Confidentiality**: Is the information secured? Will it remain private?
- **Integrity**: Is the information protected from being altered? When I go back to the ePHI later, will it be the same as when I entered it?
- **Availability**: Used to be can I access the information in an emergency? Now, need to assess threats that may deny you access to your systems. (The more common tactic.)

MICHIGAN ASSOCIATION FOR Home Care

38

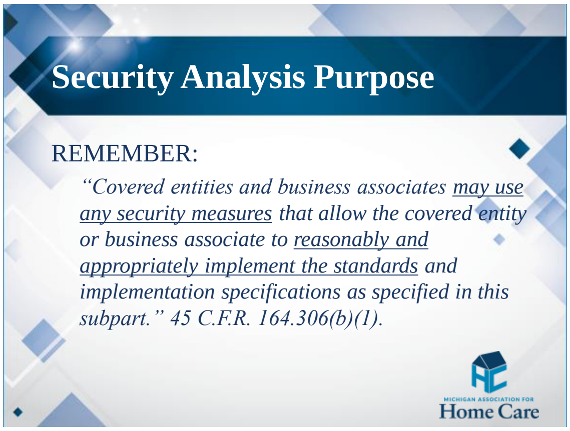


Security Analysis Legal Requirements

- ASSESSING SECURITY OF INFORMATION IS NOT JUST ABOUT CONFIDENTIALITY. IT'S ABOUT ALL THREE ELEMENTS.
- NEEDS TO CONSIDER POTENTIAL THREATS
- YOU CANNOT ASSUME YOU ARE TOO SMALL OR THAT IT CAN'T HAPPEN TO YOU. YOU MAY ASSESS SOME THREAT VECTORS AS LOW RISK, BUT DO NOT DISMISS THEM.

MICHIGAN ASSOCIATION FOR Home Care

39



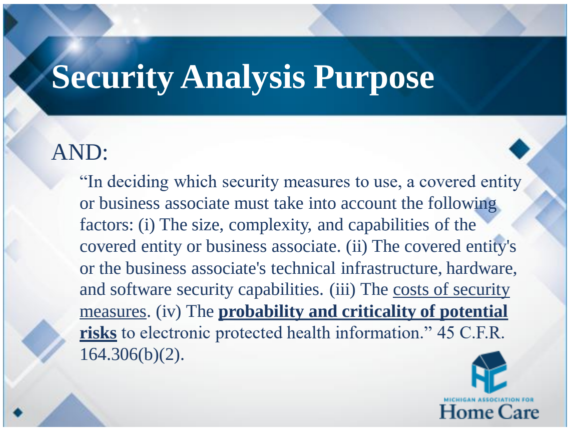
Security Analysis Purpose

REMEMBER:

"Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart." 45 C.F.R. 164.306(b)(1).

MICHIGAN ASSOCIATION FOR Home Care

40



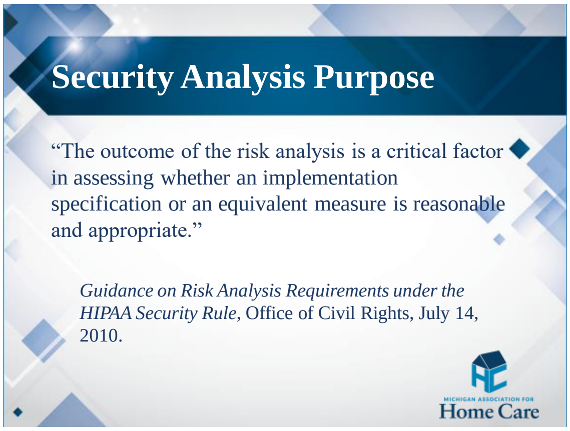
Security Analysis Purpose

AND:

"In deciding which security measures to use, a covered entity or business associate must take into account the following factors: (i) The size, complexity, and capabilities of the covered entity or business associate. (ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities. (iii) The costs of security measures. (iv) The **probability and criticality of potential risks** to electronic protected health information." 45 C.F.R. 164.306(b)(2).

MICHIGAN ASSOCIATION FOR Home Care

41



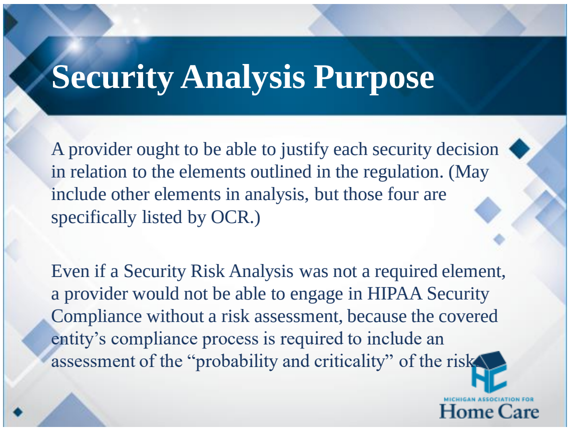
Security Analysis Purpose

"The outcome of the risk analysis is a critical factor in assessing whether an implementation specification or an equivalent measure is reasonable and appropriate."

Guidance on Risk Analysis Requirements under the HIPAA Security Rule, Office of Civil Rights, July 14, 2010.

MICHIGAN ASSOCIATION FOR Home Care

42

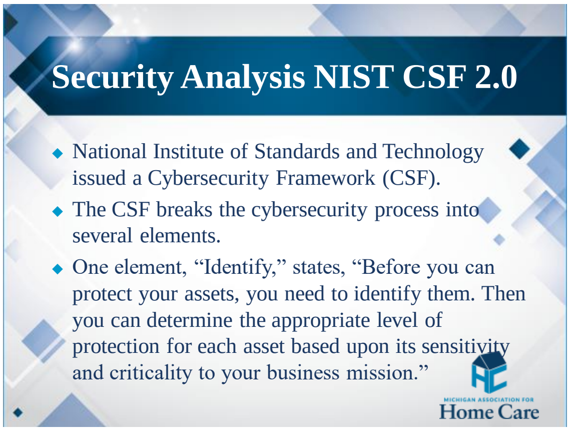


Security Analysis Purpose

A provider ought to be able to justify each security decision in relation to the elements outlined in the regulation. (May include other elements in analysis, but those four are specifically listed by OCR.)

Even if a Security Risk Analysis was not a required element, a provider would not be able to engage in HIPAA Security Compliance without a risk assessment, because the covered entity's compliance process is required to include an assessment of the "probability and criticality" of the risk.

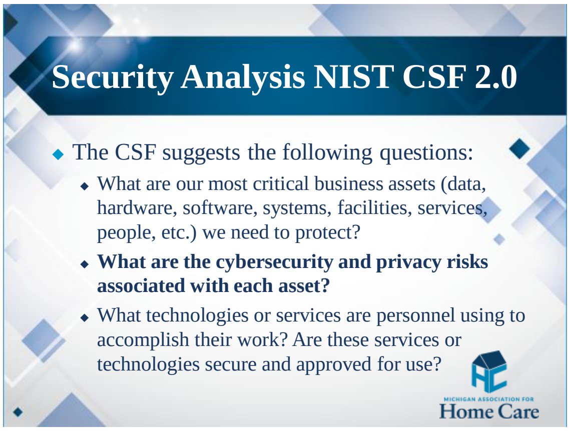
43



Security Analysis NIST CSF 2.0

- National Institute of Standards and Technology issued a Cybersecurity Framework (CSF).
- The CSF breaks the cybersecurity process into several elements.
- One element, "Identify," states, "Before you can protect your assets, you need to identify them. Then you can determine the appropriate level of protection for each asset based upon its sensitivity and criticality to your business mission."

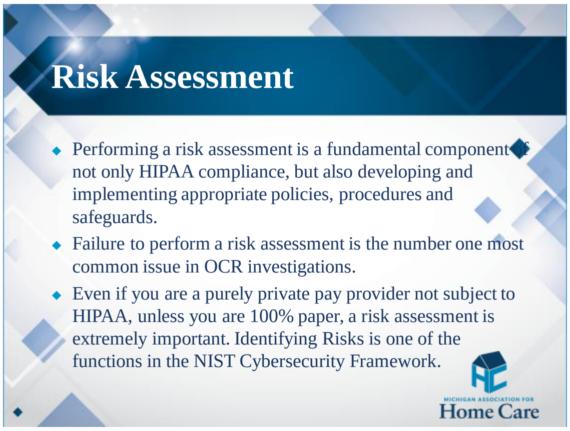
44



Security Analysis NIST CSF 2.0

- The CSF suggests the following questions:
  - What are our most critical business assets (data, hardware, software, systems, facilities, services, people, etc.) we need to protect?
  - **What are the cybersecurity and privacy risks associated with each asset?**
  - What technologies or services are personnel using to accomplish their work? Are these services or technologies secure and approved for use?

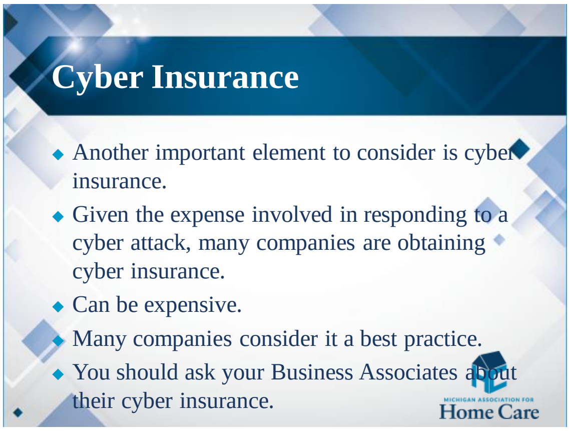
45



Risk Assessment

- Performing a risk assessment is a fundamental component of not only HIPAA compliance, but also developing and implementing appropriate policies, procedures and safeguards.
- Failure to perform a risk assessment is the number one most common issue in OCR investigations.
- Even if you are a purely private pay provider not subject to HIPAA, unless you are 100% paper, a risk assessment is extremely important. Identifying Risks is one of the functions in the NIST Cybersecurity Framework.

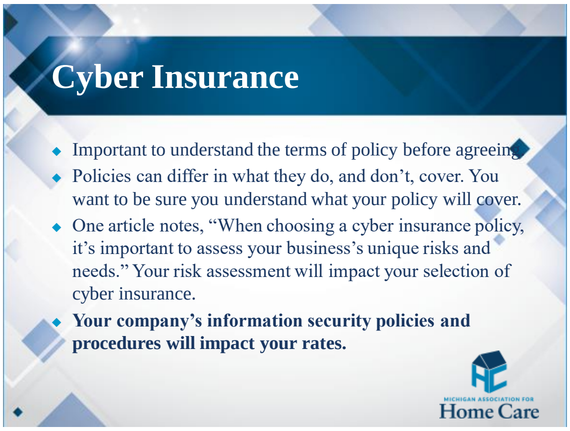
46



Cyber Insurance

- Another important element to consider is cyber insurance.
- Given the expense involved in responding to a cyber attack, many companies are obtaining cyber insurance.
- Can be expensive.
- Many companies consider it a best practice.
- You should ask your Business Associates about their cyber insurance.

47



Cyber Insurance

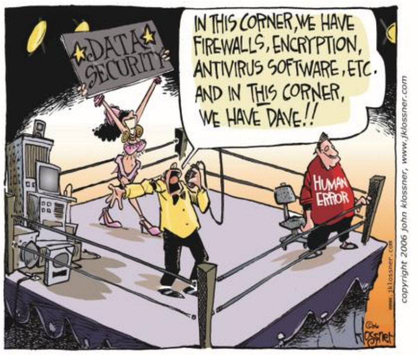
- Important to understand the terms of policy before agreeing
- Policies can differ in what they do, and don't, cover. You want to be sure you understand what your policy will cover.
- One article notes, "When choosing a cyber insurance policy, it's important to assess your business's unique risks and needs." Your risk assessment will impact your selection of cyber insurance.
- **Your company's information security policies and procedures will impact your rates.**

48

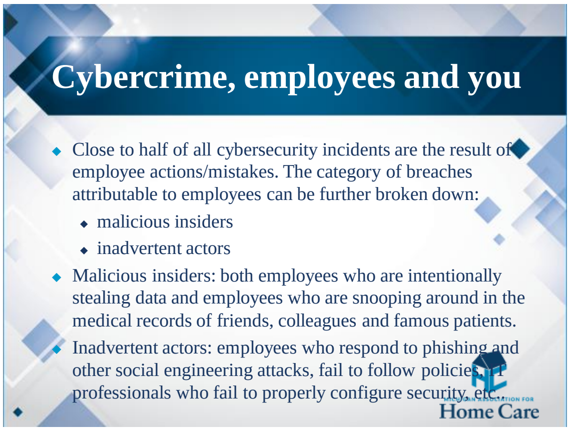
Preventing Threats

MICHIGAN ASSOCIATION FOR Home Care

49


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
copyright 2006 john klossner, www.jklossner.com
www.jklossner.com
©06 klossner

50

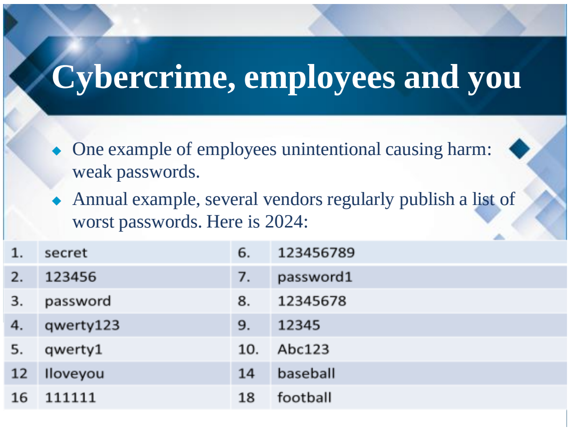


Cybercrime, employees and you

- Close to half of all cybersecurity incidents are the result of employee actions/mistakes. The category of breaches attributable to employees can be further broken down:
  - malicious insiders
  - inadvertent actors
- Malicious insiders: both employees who are intentionally stealing data and employees who are snooping around in the medical records of friends, colleagues and famous patients.
- Inadvertent actors: employees who respond to phishing and other social engineering attacks, fail to follow policies, IT professionals who fail to properly configure security, etc.

MICHIGAN ASSOCIATION FOR Home Care

51

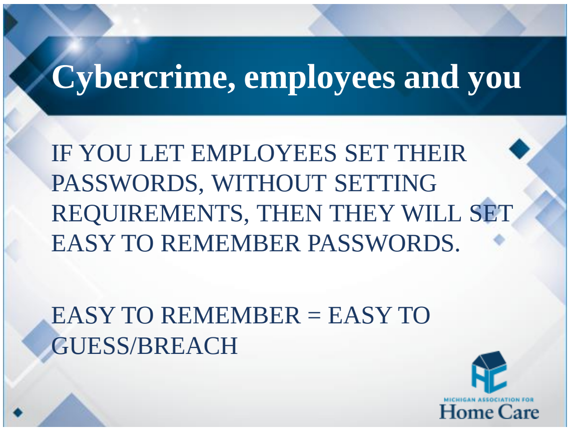


Cybercrime, employees and you

- One example of employees unintentional causing harm: weak passwords.
- Annual example, several vendors regularly publish a list of worst passwords. Here is 2024:

1.	secret	6.	123456789
2.	123456	7.	password1
3.	password	8.	12345678
4.	qwerty123	9.	12345
5.	qwerty1	10.	Abc123
12	Iloveyou	14	baseball
16	111111	18	football

52



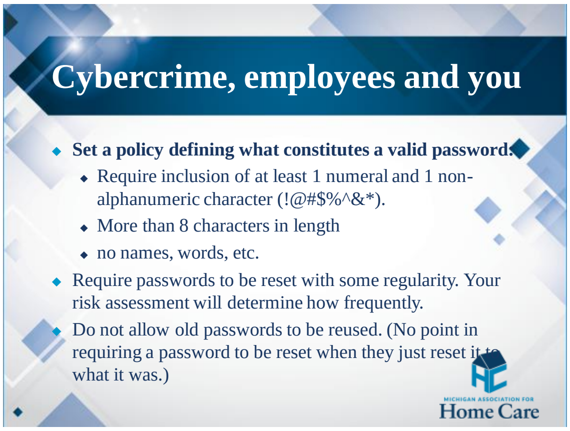
Cybercrime, employees and you

IF YOU LET EMPLOYEES SET THEIR PASSWORDS, WITHOUT SETTING REQUIREMENTS, THEN THEY WILL SET EASY TO REMEMBER PASSWORDS.

EASY TO REMEMBER = EASY TO GUESS/BREACH

Michigan Association for Home Care

53

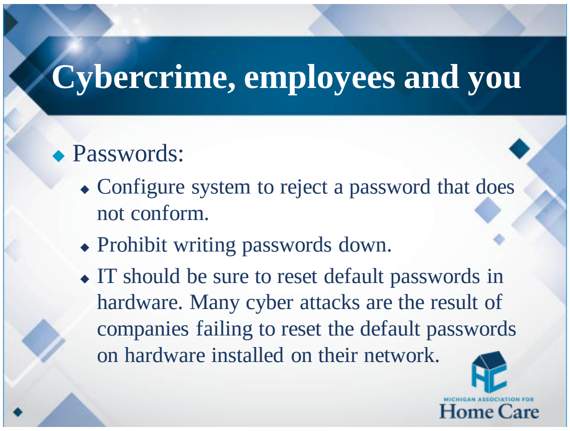


Cybercrime, employees and you

- **Set a policy defining what constitutes a valid password.**
  - Require inclusion of at least 1 numeral and 1 non-alphanumeric character (!@#$%^&*).
  - More than 8 characters in length
  - no names, words, etc.
- Require passwords to be reset with some regularity. Your risk assessment will determine how frequently.
- Do not allow old passwords to be reused. (No point in requiring a password to be reset when they just reset it to what it was.)

Michigan Association for Home Care

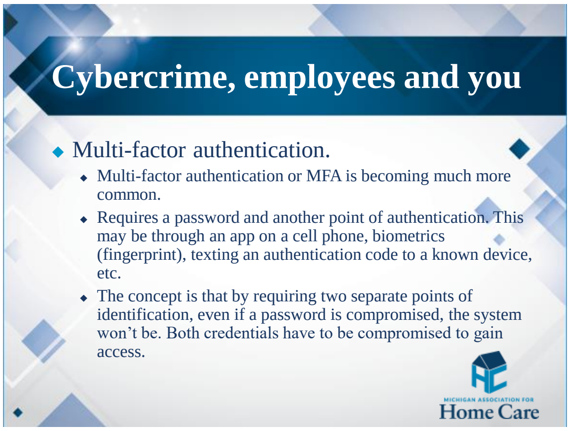
54



Cybercrime, employees and you

- Passwords:
  - Configure system to reject a password that does not conform.
  - Prohibit writing passwords down.
  - IT should be sure to reset default passwords in hardware. Many cyber attacks are the result of companies failing to reset the default passwords on hardware installed on their network.

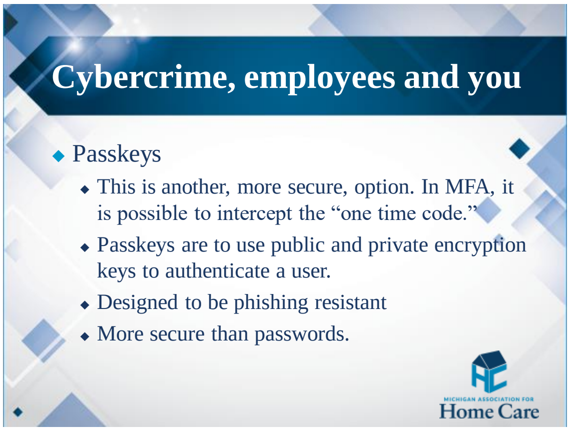
55



Cybercrime, employees and you

- Multi-factor authentication.
  - Multi-factor authentication or MFA is becoming much more common.
  - Requires a password and another point of authentication. This may be through an app on a cell phone, biometrics (fingerprint), texting an authentication code to a known device, etc.
  - The concept is that by requiring two separate points of identification, even if a password is compromised, the system won’t be. Both credentials have to be compromised to gain access.

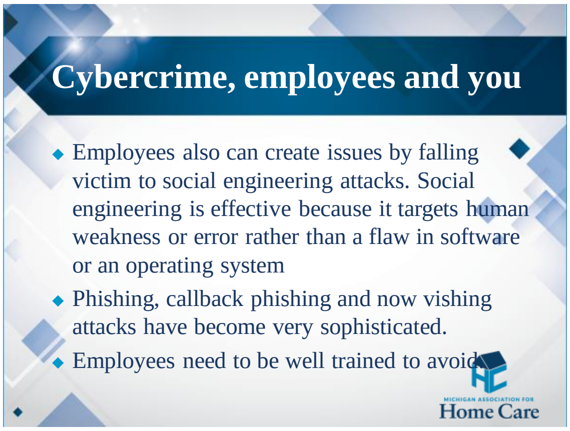
56



Cybercrime, employees and you

- Passkeys
  - This is another, more secure, option. In MFA, it is possible to intercept the “one time code.”
  - Passkeys are to use public and private encryption keys to authenticate a user.
  - Designed to be phishing resistant
  - More secure than passwords.

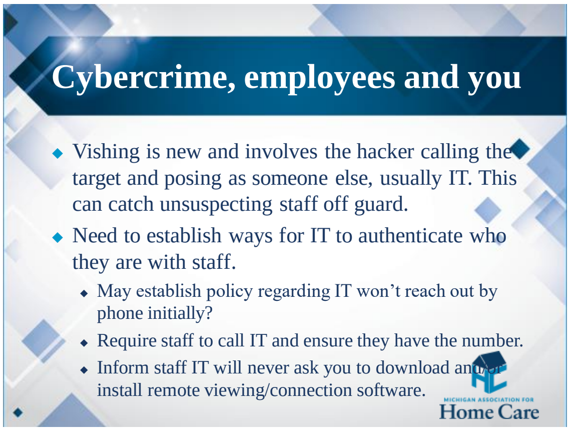
57



Cybercrime, employees and you

- Employees also can create issues by falling victim to social engineering attacks. Social engineering is effective because it targets human weakness or error rather than a flaw in software or an operating system
- Phishing, callback phishing and now vishing attacks have become very sophisticated.
- Employees need to be well trained to avoid

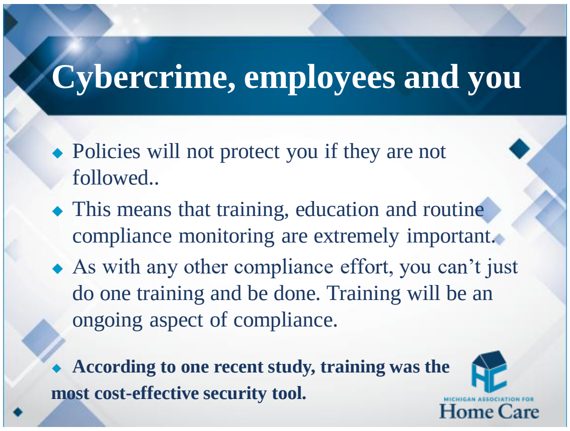
58



Cybercrime, employees and you

- Vishing is new and involves the hacker calling the target and posing as someone else, usually IT. This can catch unsuspecting staff off guard.
- Need to establish ways for IT to authenticate who they are with staff.
  - May establish policy regarding IT won't reach out by phone initially?
  - Require staff to call IT and ensure they have the number.
  - Inform staff IT will never ask you to download and/or install remote viewing/connection software.

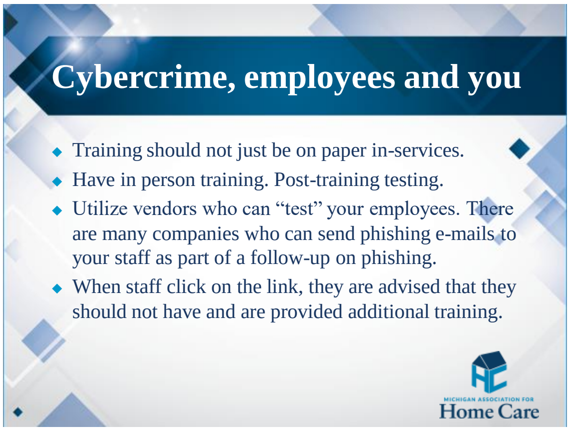
59



Cybercrime, employees and you

- Policies will not protect you if they are not followed..
- This means that training, education and routine compliance monitoring are extremely important.
- As with any other compliance effort, you can't just do one training and be done. Training will be an ongoing aspect of compliance.
- **According to one recent study, training was the most cost-effective security tool.**

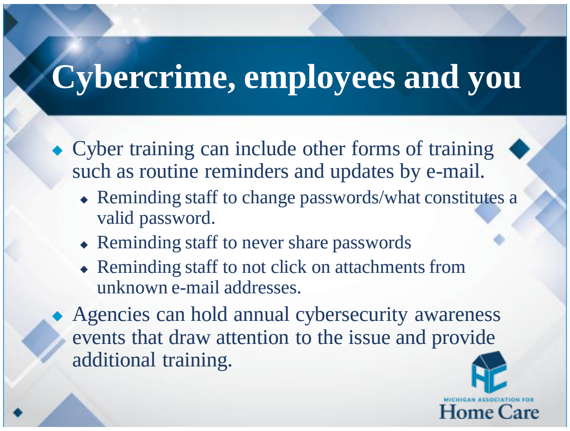
60



Cybercrime, employees and you

- Training should not just be on paper in-services.
- Have in person training. Post-training testing.
- Utilize vendors who can “test” your employees. There are many companies who can send phishing e-mails to your staff as part of a follow-up on phishing.
- When staff click on the link, they are advised that they should not have and are provided additional training.

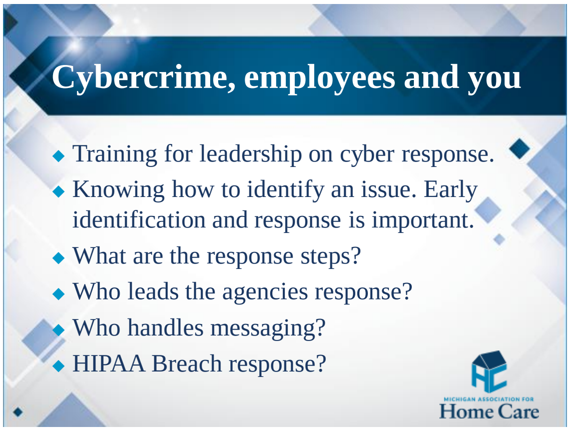
61



Cybercrime, employees and you

- Cyber training can include other forms of training such as routine reminders and updates by e-mail.
  - Reminding staff to change passwords/what constitutes a valid password.
  - Reminding staff to never share passwords
  - Reminding staff to not click on attachments from unknown e-mail addresses.
- Agencies can hold annual cybersecurity awareness events that draw attention to the issue and provide additional training.

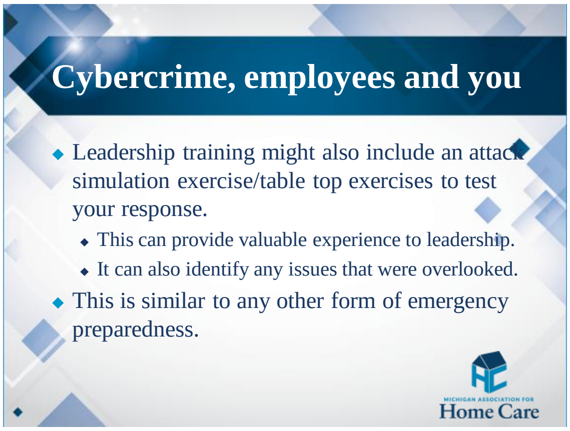
62



Cybercrime, employees and you

- Training for leadership on cyber response.
- Knowing how to identify an issue. Early identification and response is important.
- What are the response steps?
- Who leads the agencies response?
- Who handles messaging?
- HIPAA Breach response?

63

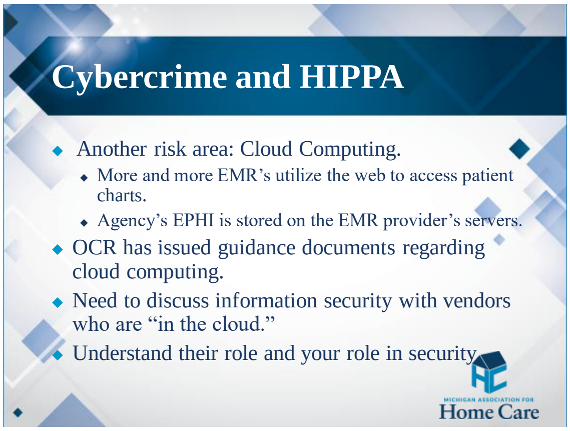


Cybercrime, employees and you

- Leadership training might also include an attack simulation exercise/table top exercises to test your response.
  - This can provide valuable experience to leadership.
  - It can also identify any issues that were overlooked.
- This is similar to any other form of emergency preparedness.

MICHIGAN ASSOCIATION FOR Home Care

64

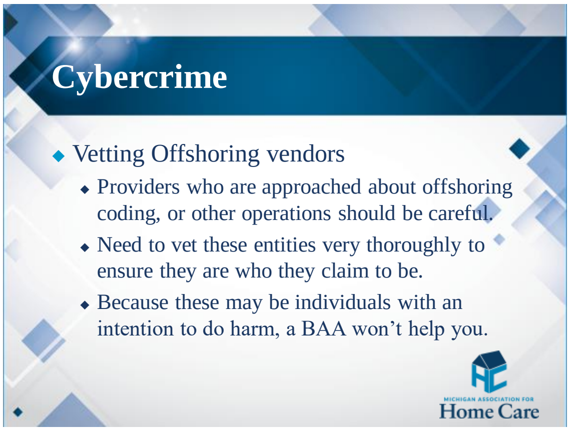


Cybercrime and HIPPA

- Another risk area: Cloud Computing.
  - More and more EMR's utilize the web to access patient charts.
  - Agency's EPHI is stored on the EMR provider's servers.
- OCR has issued guidance documents regarding cloud computing.
- Need to discuss information security with vendors who are "in the cloud."
- Understand their role and your role in security.

MICHIGAN ASSOCIATION FOR Home Care

65

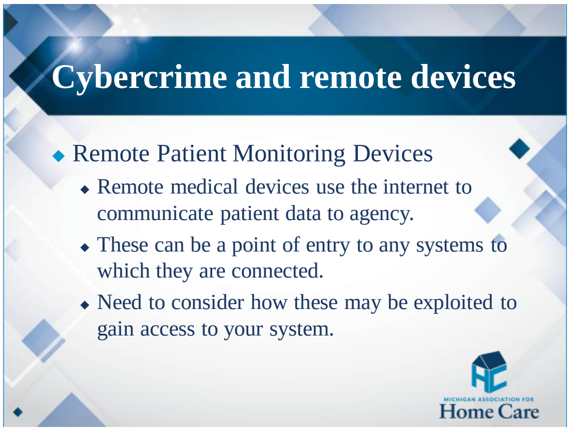


Cybercrime

- Vetting Offshoring vendors
  - Providers who are approached about offshoring coding, or other operations should be careful.
  - Need to vet these entities very thoroughly to ensure they are who they claim to be.
  - Because these may be individuals with an intention to do harm, a BAA won't help you.

MICHIGAN ASSOCIATION FOR Home Care

66

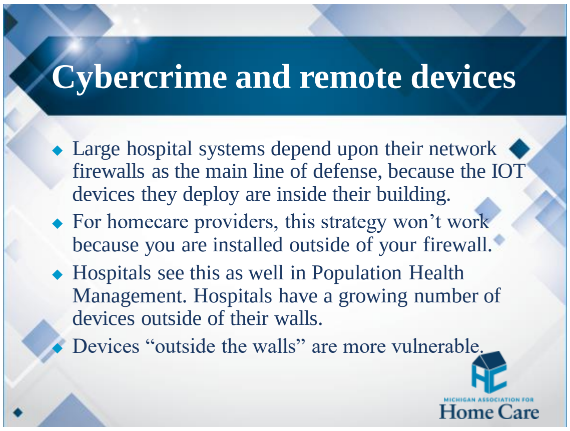


Cybercrime and remote devices

- Remote Patient Monitoring Devices
  - Remote medical devices use the internet to communicate patient data to agency.
  - These can be a point of entry to any systems to which they are connected.
  - Need to consider how these may be exploited to gain access to your system.

MICHIGAN ASSOCIATION FOR Home Care

67

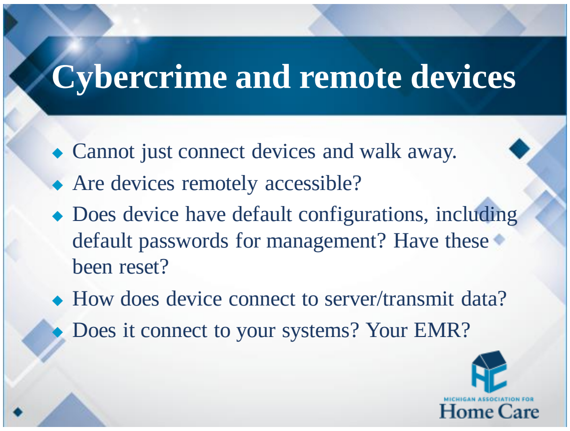


Cybercrime and remote devices

- Large hospital systems depend upon their network firewalls as the main line of defense, because the IOT devices they deploy are inside their building.
- For homecare providers, this strategy won’t work because you are installed outside of your firewall.
- Hospitals see this as well in Population Health Management. Hospitals have a growing number of devices outside of their walls.
- Devices “outside the walls” are more vulnerable.

MICHIGAN ASSOCIATION FOR Home Care

68

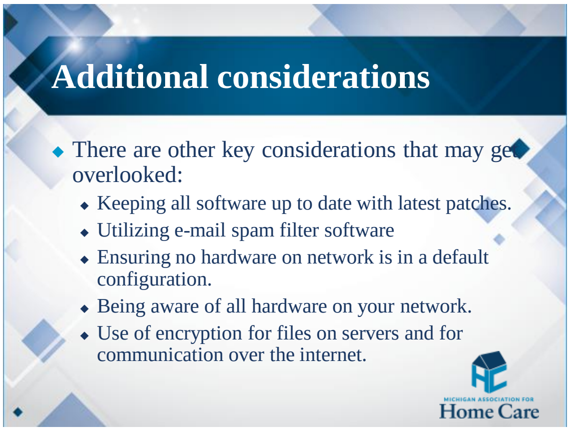


Cybercrime and remote devices

- Cannot just connect devices and walk away.
- Are devices remotely accessible?
- Does device have default configurations, including default passwords for management? Have these been reset?
- How does device connect to server/transmit data?
- Does it connect to your systems? Your EMR?

MICHIGAN ASSOCIATION FOR Home Care

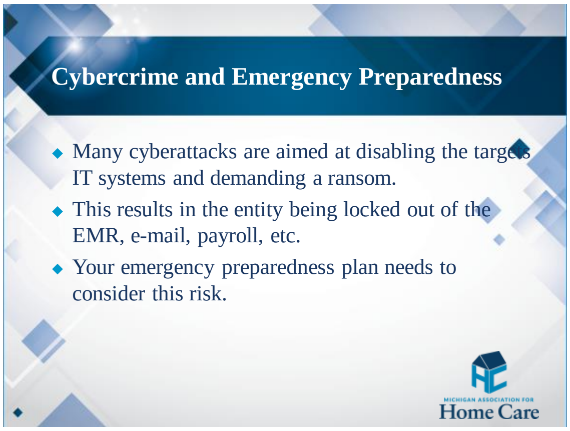
69



Additional considerations

- There are other key considerations that may get overlooked:
  - Keeping all software up to date with latest patches.
  - Utilizing e-mail spam filter software
  - Ensuring no hardware on network is in a default configuration.
  - Being aware of all hardware on your network.
  - Use of encryption for files on servers and for communication over the internet.

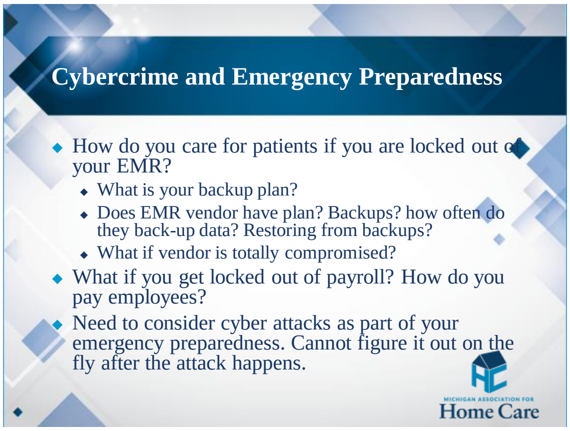
70



Cybercrime and Emergency Preparedness

- Many cyberattacks are aimed at disabling the targets IT systems and demanding a ransom.
- This results in the entity being locked out of the EMR, e-mail, payroll, etc.
- Your emergency preparedness plan needs to consider this risk.

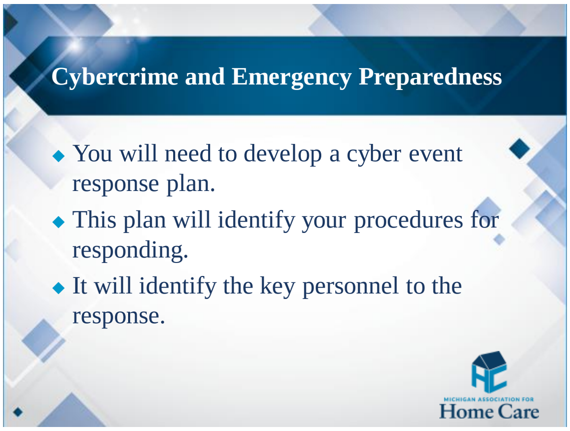
71



Cybercrime and Emergency Preparedness

- How do you care for patients if you are locked out of your EMR?
  - What is your backup plan?
  - Does EMR vendor have plan? Backups? how often do they back-up data? Restoring from backups?
  - What if vendor is totally compromised?
- What if you get locked out of payroll? How do you pay employees?
- Need to consider cyber attacks as part of your emergency preparedness. Cannot figure it out on the fly after the attack happens.

72

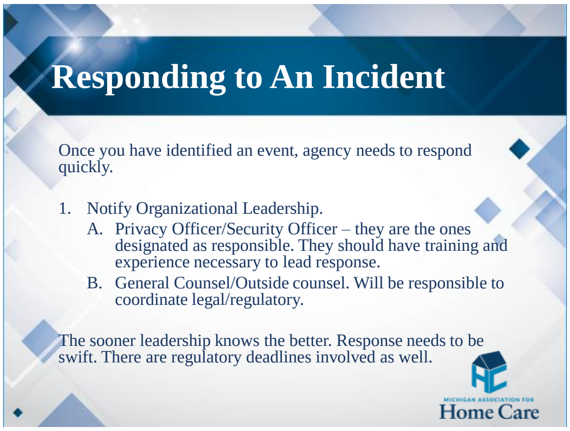


Cybercrime and Emergency Preparedness

- You will need to develop a cyber event response plan.
- This plan will identify your procedures for responding.
- It will identify the key personnel to the response.

MICHIGAN ASSOCIATION FOR Home Care

73



Responding to An Incident

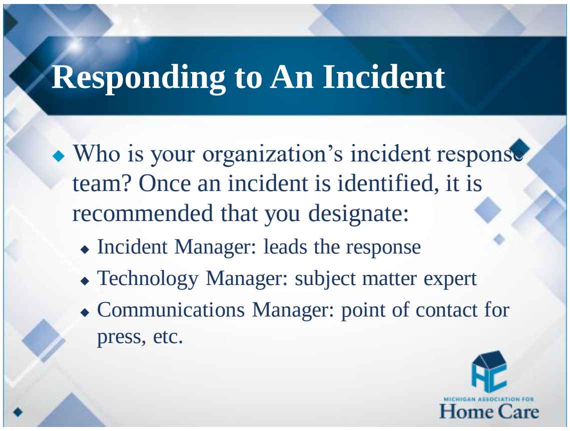
Once you have identified an event, agency needs to respond quickly.

1. Notify Organizational Leadership.
   A. Privacy Officer/Security Officer – they are the ones designated as responsible. They should have training and experience necessary to lead response.
   B. General Counsel/Outside counsel. Will be responsible to coordinate legal/regulatory.

The sooner leadership knows the better. Response needs to be swift. There are regulatory deadlines involved as well.

MICHIGAN ASSOCIATION FOR Home Care

74

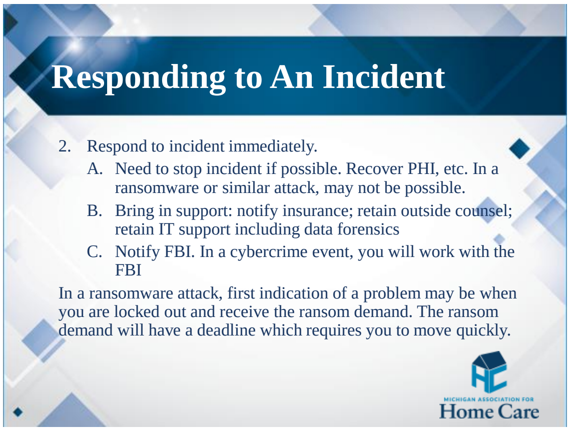


Responding to An Incident

- Who is your organization’s incident response team? Once an incident is identified, it is recommended that you designate:
  - Incident Manager: leads the response
  - Technology Manager: subject matter expert
  - Communications Manager: point of contact for press, etc.

MICHIGAN ASSOCIATION FOR Home Care

75

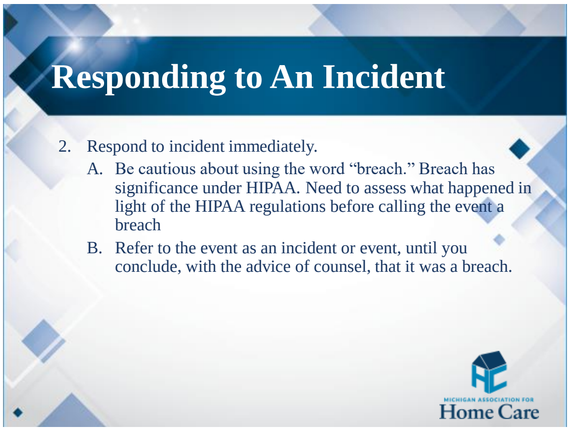


Responding to An Incident

2. Respond to incident immediately.
   A. Need to stop incident if possible. Recover PHI, etc. In a ransomware or similar attack, may not be possible.
   B. Bring in support: notify insurance; retain outside counsel; retain IT support including data forensics
   C. Notify FBI. In a cybercrime event, you will work with the FBI

In a ransomware attack, first indication of a problem may be when you are locked out and receive the ransom demand. The ransom demand will have a deadline which requires you to move quickly.

76

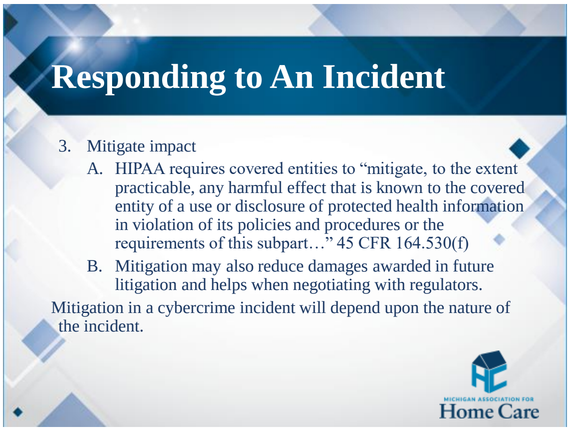


Responding to An Incident

2. Respond to incident immediately.
   A. Be cautious about using the word “breach.” Breach has significance under HIPAA. Need to assess what happened in light of the HIPAA regulations before calling the event a breach
   B. Refer to the event as an incident or event, until you conclude, with the advice of counsel, that it was a breach.

MICHIGAN ASSOCIATION FOR
Home Care

77

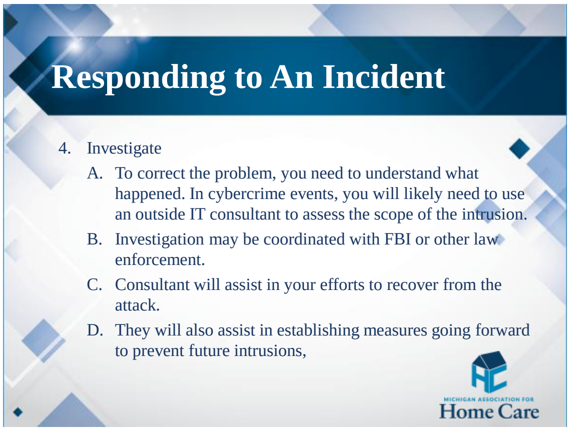


Responding to An Incident

3. Mitigate impact
   A. HIPAA requires covered entities to “mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart…” 45 CFR 164.530(f)
   B. Mitigation may also reduce damages awarded in future litigation and helps when negotiating with regulators.

Mitigation in a cybercrime incident will depend upon the nature of the incident.

78

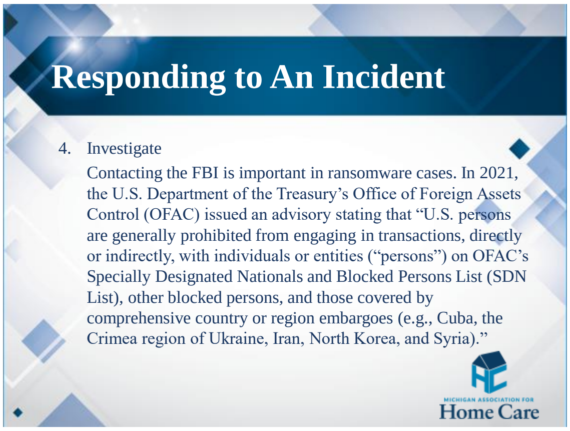


Responding to An Incident

4. Investigate
   - A. To correct the problem, you need to understand what happened. In cybercrime events, you will likely need to use an outside IT consultant to assess the scope of the intrusion.
   - B. Investigation may be coordinated with FBI or other law enforcement.
   - C. Consultant will assist in your efforts to recover from the attack.
   - D. They will also assist in establishing measures going forward to prevent future intrusions,

Michigan Association for Home Care

79



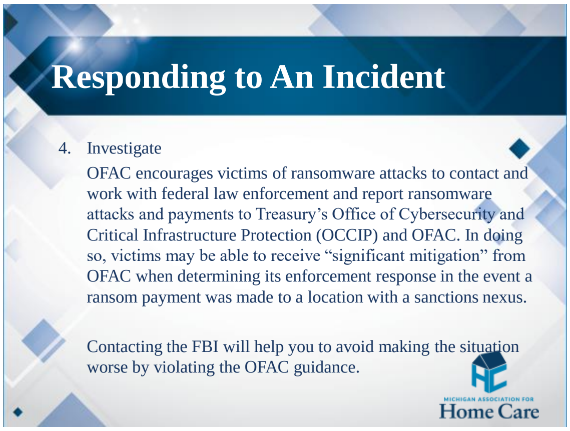
Responding to An Incident

4. Investigate

Contacting the FBI is important in ransomware cases. In 2021, the U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) issued an advisory stating that “U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities (“persons”) on OFAC’s Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria).”

Michigan Association for Home Care

80



Responding to An Incident

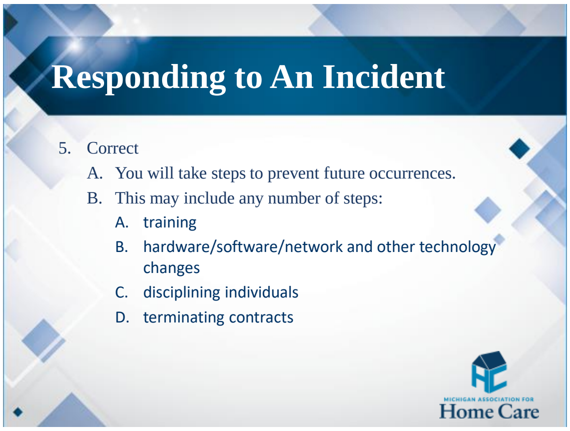
4. Investigate

OFAC encourages victims of ransomware attacks to contact and work with federal law enforcement and report ransomware attacks and payments to Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) and OFAC. In doing so, victims may be able to receive “significant mitigation” from OFAC when determining its enforcement response in the event a ransom payment was made to a location with a sanctions nexus.

Contacting the FBI will help you to avoid making the situation worse by violating the OFAC guidance.

Michigan Association for Home Care

81

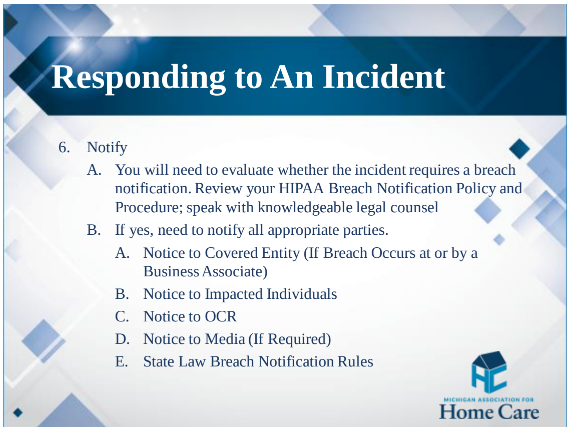


Responding to An Incident

5. Correct
   A. You will take steps to prevent future occurrences.
   B. This may include any number of steps:
      A. training
      B. hardware/software/network and other technology changes
      C. disciplining individuals
      D. terminating contracts

MICHIGAN ASSOCIATION FOR Home Care

82

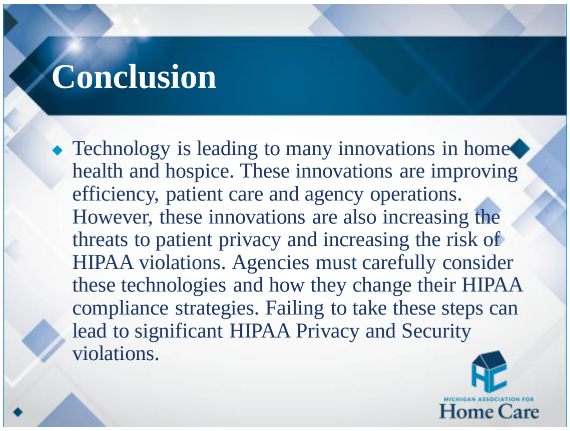


Responding to An Incident

6. Notify
   A. You will need to evaluate whether the incident requires a breach notification. Review your HIPAA Breach Notification Policy and Procedure; speak with knowledgeable legal counsel
   B. If yes, need to notify all appropriate parties.
      A. Notice to Covered Entity (If Breach Occurs at or by a Business Associate)
      B. Notice to Impacted Individuals
      C. Notice to OCR
      D. Notice to Media (If Required)
      E. State Law Breach Notification Rules

MICHIGAN ASSOCIATION FOR Home Care

83



Conclusion

- Technology is leading to many innovations in home health and hospice. These innovations are improving efficiency, patient care and agency operations. However, these innovations are also increasing the threats to patient privacy and increasing the risk of HIPAA violations. Agencies must carefully consider these technologies and how they change their HIPAA compliance strategies. Failing to take these steps can lead to significant HIPAA Privacy and Security violations.

MICHIGAN ASSOCIATION FOR Home Care

84

The End

Michigan HomeCare & Hospice Association

85