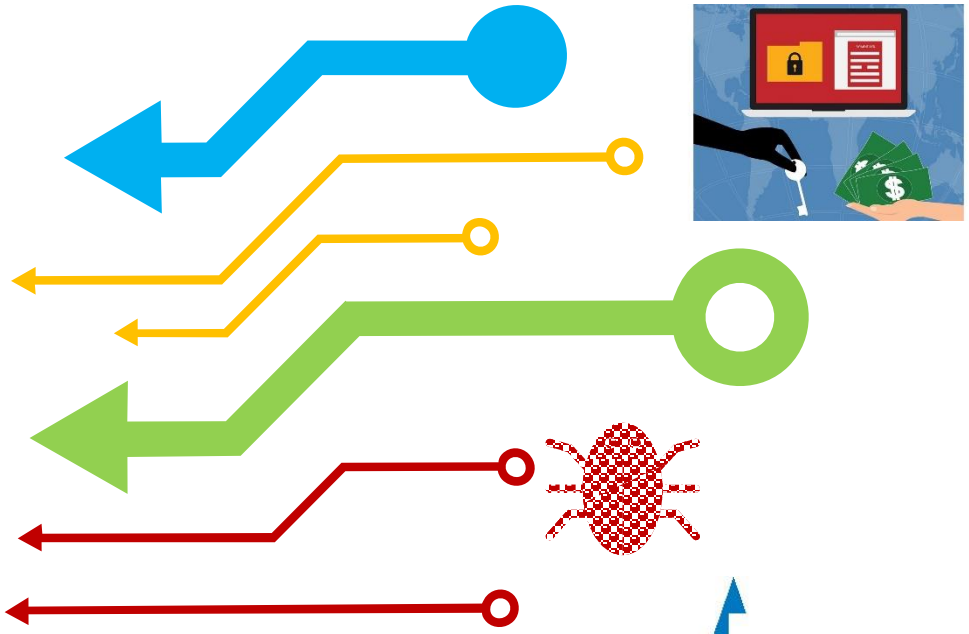
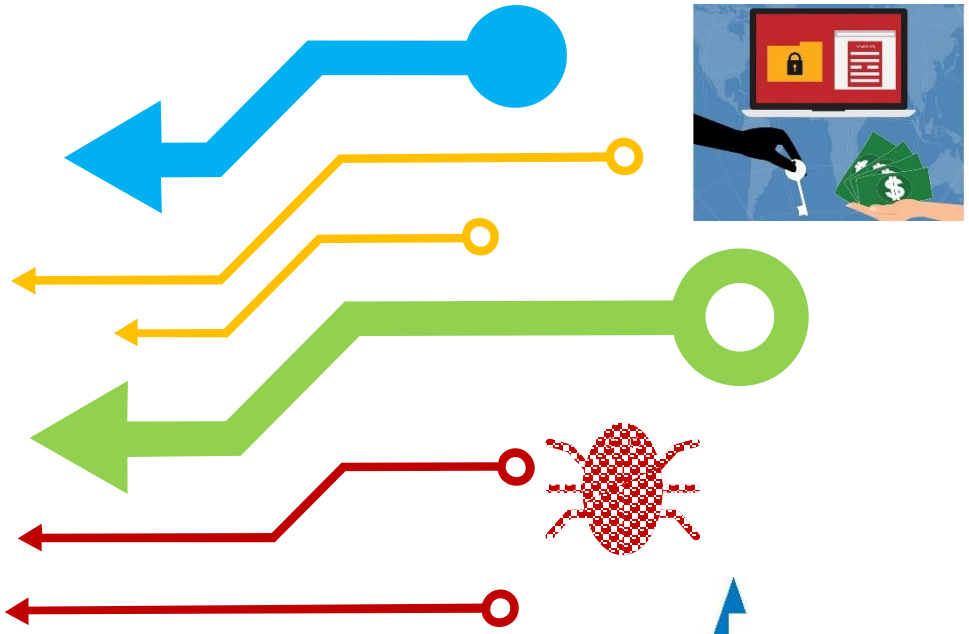
CYBER SECURITY



Presented by
Cathy Bryant
April 22, 2022

TMLT
Texas Medical Liability Trust

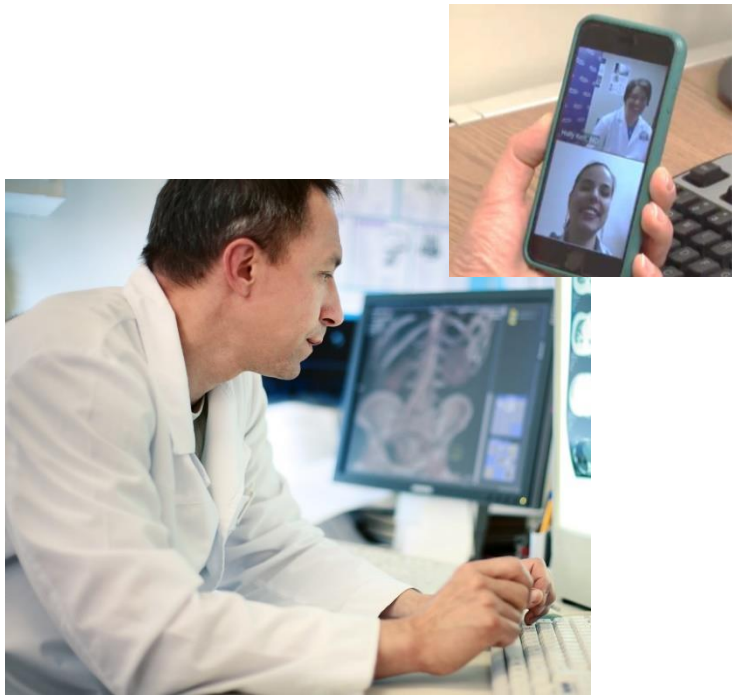
CYBER SECURITY



Presented by
Cathy Bryant
April 22, 2022

TMLT
Texas Medical Liability Trust

Protected Health Information
2003
HIPAA Privacy Rule



Electronic Protected Health Information
2005 - Present
HIPAA Security Rule

Patient care is your priority!
Cybersecurity has not been a priority in healthcare.

Why healthcare is a target?

Threat Actor

Vulnerabilities

Valuable Assets

- Physicians need access to electronic medical records during patient encounters is important
- Medical history cannot be “re-issued”
- Cybersecurity has not been a priority in healthcare

HHS 405(d)
Aligning Health Care Industry Security Approaches

10 Practices to Protect Your Organization from Cyber Threats

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram or visit our website at 405d.hhs.gov!

Email Protection Systems

Put in place email protection systems that can help thwart cyber attacks. Enable basic email protection controls, educate staff with phishing simulations, and, if possible, use multi-factor authentication as a double layer of defense.

Endpoint Protection Systems

Implement basic Endpoint Protection Controls such as antivirus software, full disk encryption, and patching. Each endpoint in your organization should be equipped with these controls and configured to update automatically.

Access Management

Clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints. Establish unique accounts for each individual and avoid using ADMIN accounts. Tailor access for each user based on the user's specific role and work requirements.

Data Protection and Loss Prevention

Put in place data classification policies that clearly define how sensitive data is to be handled at your organization. Instill proper procedures that outline the distribution method, encryption level, storage, and removal of all types of data.

IT Asset Management

Keep a full and accurate inventory of all IT equipment at all times. This also includes implementing procurement processes that encompass the lifecycle of each IT Asset. Also, if your organization allows the use of personal devices, establish integration with network access control procedures to ensure protection to your systems.

Secure your Organization from the Top 5 Threats Facing the Healthcare and Public Health Sector

Healthcare continues to be one of the top industries targeted by cyber attacks. Organizations of all sizes, small, medium, and large, continue to fall victim to attacks that directly affect patient safety. Our number one goal as healthcare organizations is to continue protecting patients and delivering care. So, don't let a cyber attack stop you from your mission! To protect your organization from these top five cyber threats, utilize and implement these ten mitigating practices and always remain cyber vigilant.

Network Management

Use Network Segmentation to configure networks to restrict access between devices to that which is required to successfully complete work. An effective network management strategy also includes the deployment of firewalls and network profiles to enable proper access inside and outside the organization.

Vulnerability Management

Consistently schedule and conduct vulnerability scans on servers and systems under your control to proactively identify technology flaws. Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software.

Incident Response

The Incident Response Process coupled with an Incident Response Plan allows users to discover cyber attacks on the network and prevent them from causing a data breach or loss. An Incident Response strategy is established and implemented so that you and all your employees are prepared in the event of an attack. Practice this plan to ensure success.

Medical Device Security

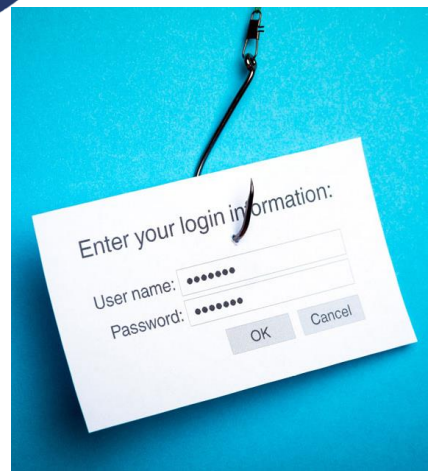
Much of Medical Device security can be accomplished by treating the devices as IT equipment. Just as you would for a computer, establish endpoint protections, proper inventory, regular software patching, and implement access management procedures.

Cybersecurity Policies

For organizations of all sizes, cybersecurity policies should include consistent education and awareness, proper roles and responsibility guidelines, incident reporting, IT equipment use policies, and guidance of personal device use.

TMLT Texas Medical Liability Trust

Threats Facing Your Practice



Phishing

Vishing
SMShing

Social engineering is the art of manipulating people, so they give up confidential information.

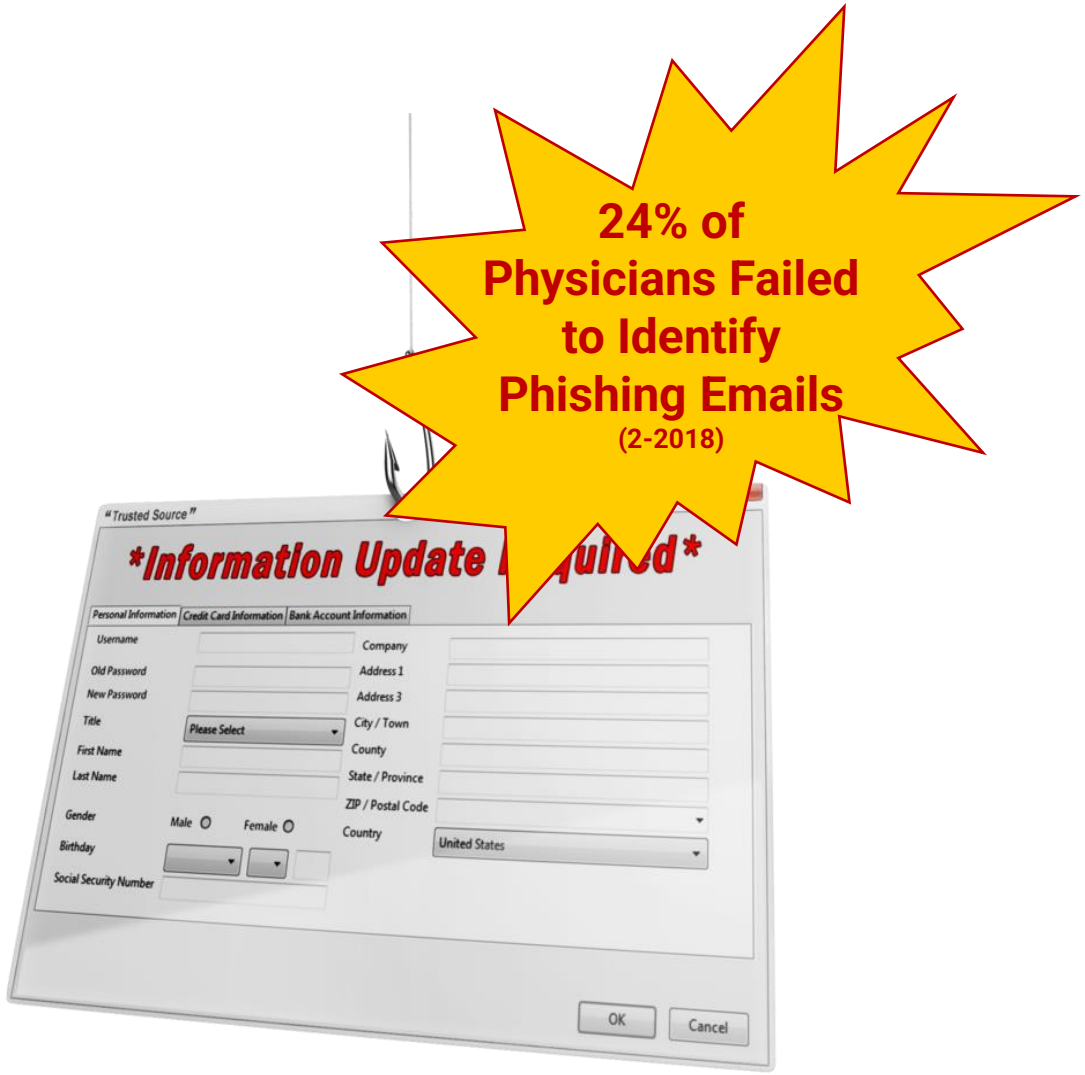
The types of information these criminals are seeking can vary, but when individuals are targeted, the threat actors are usually trying to trick you into giving them your passwords or access your computer to secretly install malicious software–that will give them access to your passwords and medical records as well as giving them control over your computer.

TMLT
Texas Medical Liability Trust

Phishing

A form of social engineering that uses email or malicious websites (among other channels) to solicit personal information from an individual or company by posing as a trustworthy organization or entity

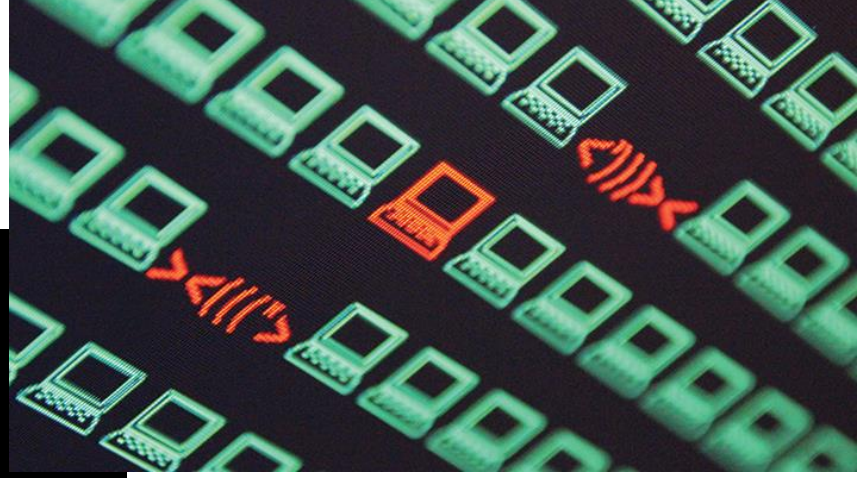
The goal of a phishing attempt is to trick the recipient into taking the attacker's desired action, such as providing login credentials or other sensitive information.



91% of all malware attacks come from phishing attempts using different variations of social engineering techniques.

TMLT
Texas Medical Liability Trust

How to Identify Phishing



- Phishing is most often initiated through email communications
- There are ways to distinguish suspicious emails from legitimate messages
- Training employees on how to recognize these malicious emails is essential
- The following may be indicators that an email is a phishing attempt rather than an authentic communication from the company it appears to be.

What can you do?

Educate Workforce

- ✓ **Phishing Awareness Training**
- ✓ **Conduct Phishing – SMiShing campaigns.**
- ✓ **Be suspicious of unsolicited phone calls, visits, or email messages.**
- ✓ **Do not provide personal information or information about your organization.**
- ✓ **Pay attention to the URL of a website.**
- ✓ **Technical Safeguards: anti-virus software OR end-point protection, firewalls, and email filters to reduce some of this traffic.**

Ransomware is a form of malware that accesses your electronic data files, passes them through an encryption function, and then stores the resulting encrypted copies in their place.

PHI and other sensitive data in your computer are now under the control of a cyber criminal who demands a ransom in exchange for giving access.

Ransomware itself is mutating and becoming more sophisticated, as more advanced threats occur.

Ransom Attacks

Ransom Attacks Cyber Incidents Reported to TMLT

- First reported incident 2012 – resolved in 2016
- Continue to be one of the most frequent security incidents reported to cyber insurance
- More than one claim exceeded their policy limits in a few months

Anatomy of a ransom attack . . . learned from Forensics

1. First, the threat actor infiltrates a physician practice's network
2. Now, the threat actor has unlimited access to network files
   - ✓ Patient records
   - ✓ Financials
   - ✓ Physician credentials, DEA numbers
   - ✓ Employee SS# and other personal data
3. Threat actor know your network better than perhaps you do, what your backup process is and if it is attached to the network
4. Confident that the practice will need to pay the ransom
5. **The threat actor launched the ransom attack**
6. **Ransom Payment Made by the Practice to recover data**

Phishing

Hacking

Open RDP Port

TMLT
Texas Medical Liability Trust

Example of Ransomware Notice

What to Do If Infected with Ransomware

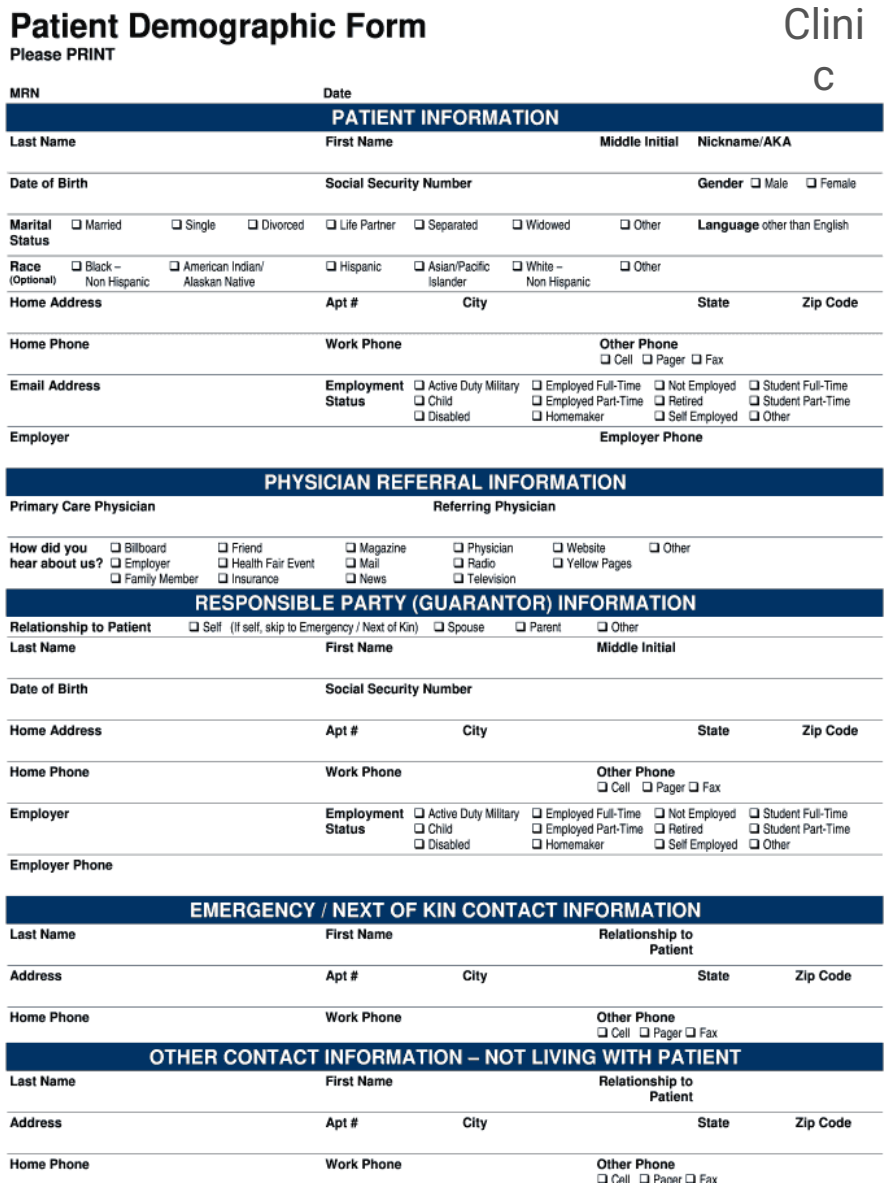
Should preventive measures fail, have a response plan if you become infected with ransomware:

1. Isolate the infected computer immediately. Infected systems should be removed from the network as soon as possible to prevent ransomware from attacking network or share drives. Do NOT power off, this can destroy forensic evidence.
2. Isolate affected devices that have not yet been completely corrupted. This may afford more time to clean and recover data, contain damage, and prevent worsening conditions.
3. Immediately secure backup data or systems by taking them offline. Ensure backups are free of malware.
4. Notify your Cyber Insurance carrier.
5. Contact law enforcement immediately.

TMLT
Texas Medical Liability Trust

Good morning, your network is unavailable …

Three weeks before data was restored



Patient Demographic Form
Please PRINT

Clini
c

MRN | Date

PATIENT INFORMATION

Last Name | First Name | Middle Initial | Nickname/AKA

Date of Birth | Social Security Number | Gender ❑ Male ❑ Female

Marital Status ❑ Married ❑ Single ❑ Divorced ❑ Life Partner ❑ Separated ❑ Widowed ❑ Other | Language other than English

Race (Optional) ❑ Black – Non Hispanic ❑ American Indian/ Alaskan Native ❑ Hispanic ❑ Asian/Pacific Islander ❑ White – Non Hispanic ❑ Other

Home Address | Apt # | City | State | Zip Code

Home Phone | Work Phone | Other Phone ❑ Cell ❑ Pager ❑ Fax

Email Address | Employment Status ❑ Active Duty Military ❑ Child ❑ Disabled ❑ Employed Full-Time ❑ Employed Part-Time ❑ Homemaker ❑ Not Employed ❑ Retired ❑ Self Employed ❑ Student Full-Time ❑ Student Part-Time ❑ Other

Employer | Employer Phone

PHYSICIAN REFERRAL INFORMATION

Primary Care Physician | Referring Physician

How did you hear about us? ❑ Billboard ❑ Employer ❑ Family Member ❑ Friend ❑ Health Fair Event ❑ Insurance ❑ Magazine ❑ Mail ❑ News ❑ Physician ❑ Radio ❑ Television ❑ Website ❑ Yellow Pages ❑ Other

RESPONSIBLE PARTY (GUARANTOR) INFORMATION

Relationship to Patient ❑ Self (If self, skip to Emergency / Next of Kin) ❑ Spouse ❑ Parent ❑ Other

Last Name | First Name | Middle Initial

Date of Birth | Social Security Number

Home Address | Apt # | City | State | Zip Code

Home Phone | Work Phone | Other Phone ❑ Cell ❑ Pager ❑ Fax

Employer | Employment Status ❑ Active Duty Military ❑ Child ❑ Disabled ❑ Employed Full-Time ❑ Employed Part-Time ❑ Homemaker ❑ Not Employed ❑ Retired ❑ Self Employed ❑ Student Full-Time ❑ Student Part-Time ❑ Other

Employer Phone

EMERGENCY / NEXT OF KIN CONTACT INFORMATION

Last Name | First Name | Relationship to Patient

Address | Apt # | City | State | Zip Code

Home Phone | Work Phone | Other Phone ❑ Cell ❑ Pager ❑ Fax

OTHER CONTACT INFORMATION – NOT LIVING WITH PATIENT

Last Name | First Name | Relationship to Patient

Address | Apt # | City | State | Zip Code

Home Phone | Work Phone | Other Phone ❑ Cell ❑ Pager ❑ Fax

Front desk script:
"We are updating our computer files. Please complete a new demographic form for me. I will also need to make a copy of your photo ID and insurance card."

Office encounter was documented by hand on the back of the demographic sheet.

If a patient cancels an appointment, write it on a calendar.

You are developing a list of available appointments

What can you do to protect against a ransom attack?

- Make real-time backups and store offline.
- Have your IT dept. employ technology that prevents unapproved software from running. Restrict users' ability to install and run software applications. User access vs. admin access.
- Keep your operating system and all software applications up-to-date.
- Maintain your antivirus/antimalware software.
- Endpoint protection

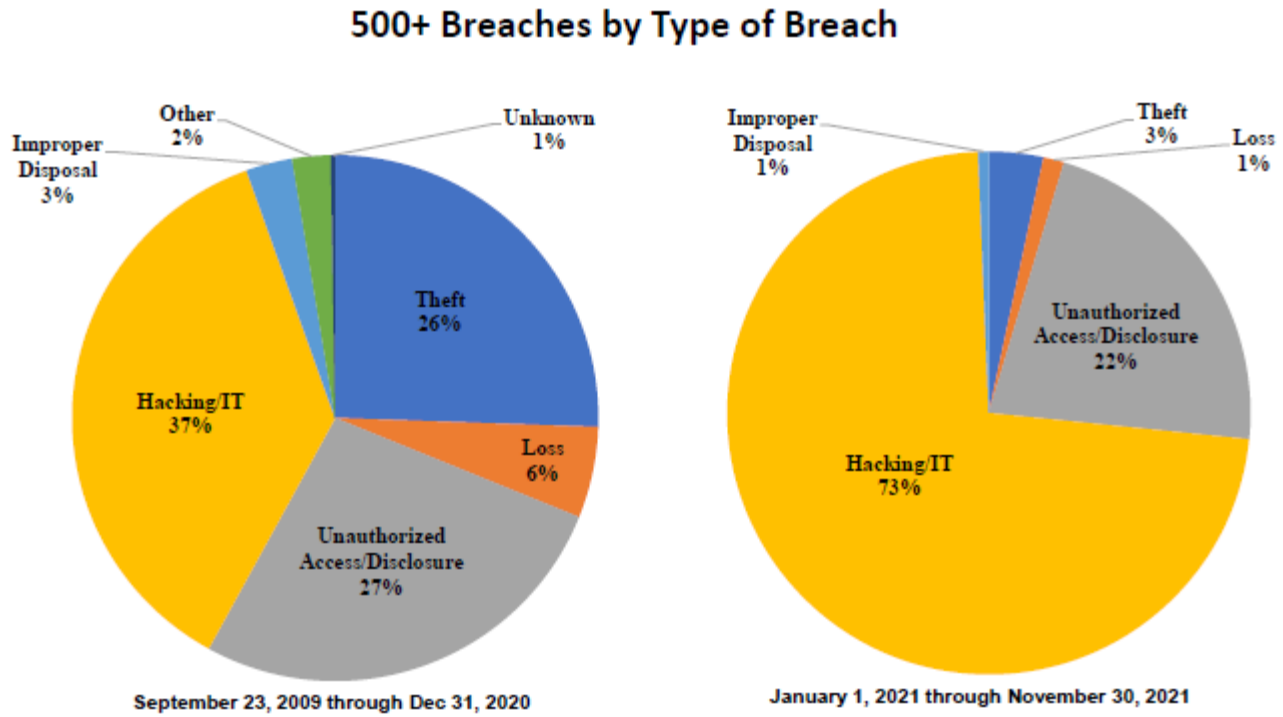
TMLT
Texas Medical Liability Trust

What can you do … continued?

- Don’t enable macros from email attachments.
- Develop policies and procedures on the safe handling of email attachments.
- Educate your workforce.
- Report the ransom attempt to the cyber insurance carrier, local police and FBI.
- Have a data recovery plan and test it.

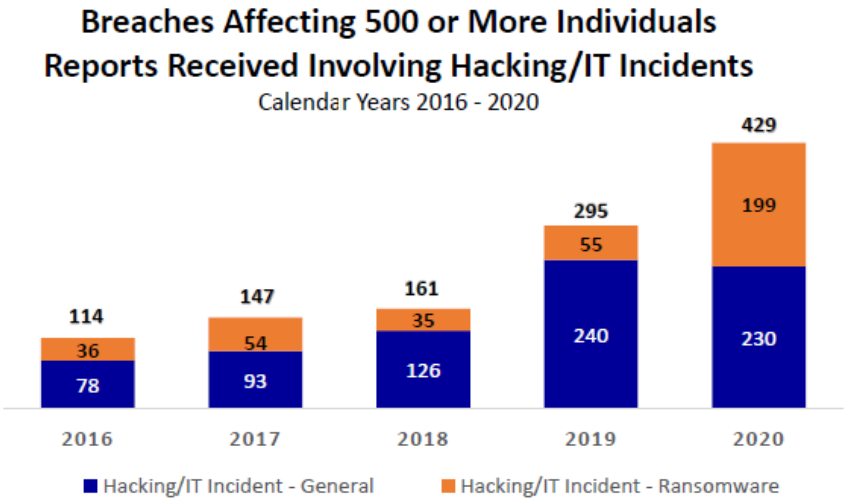
Loss or Theft of Equipment or Data

- Significant decrease in the number of large breaches by theft/loss



Insider, Accidental or Intentional Data Loss

Attacks Against Medical Devices



Medical Devices Increasingly Vulnerable to Cyberattacks In Compliance

January 27, 2022

Despite ongoing publicity around the need to secure systems and equipment against the threat of cyberattacks, a new report suggests that cyber vulnerabilities continue to be a major source of concern for connected medical devices.

- 53% of connected medical devices in hospitals have a known critical vulnerability. Potentially more concerning when it comes to patient safety, a third of bedside connected devices used in healthcare settings have an identified critical risk.
  - Outdated operating system software
  - Default passwords
  - IV pump vulnerabilities

HHS 405(d)
Aligning Health Care Industry Security Approaches

10 Practices to Protect Your Organization from Cyber Threats

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram or visit our website at 405d.hhs.gov!

Email Protection Systems

Put in place email protection systems that can help thwart cyber attacks. Enable basic email protection controls, educate staff with phishing simulations, and, if possible, use multi-factor authentication as a double layer of defense.

Endpoint Protection Systems

Implement basic Endpoint Protection Controls such as antivirus software, full disk encryption, and patching. Each endpoint in your organization should be equipped with these controls and configured to update automatically.

Access Management

Clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints. Establish unique accounts for each individual and avoid using ADMIN accounts. Tailor access for each user based on the user's specific role and work requirements.

Data Protection and Loss Prevention

Put in place data classification policies that clearly define how sensitive data is to be handled at your organization. Instill proper procedures that outline the distribution method, encryption level, storage, and removal of all types of data.

IT Asset Management

Keep a full and accurate inventory of all IT equipment at all times. This also includes implementing procurement processes that encompass the lifecycle of each IT Asset. Also, if your organization allows the use of personal devices, establish integration with network access control procedures to ensure protection to your systems.

Secure your Organization from the Top 5 Threats Facing the Healthcare and Public Health Sector

Healthcare continues to be one of the top industries targeted by cyber attacks. Organizations of all sizes, small, medium, and large, continue to fall victim to attacks that directly affect patient safety. Our number one goal as healthcare organizations is to continue protecting patients and delivering care. So, don't let a cyber attack stop you from your mission! To protect your organization from these top five cyber threats, utilize and implement these ten mitigating practices and always remain cyber vigilant.

Network Management

Use Network Segmentation to configure networks to restrict access between devices to that which is required to successfully complete work. An effective network management strategy also includes the deployment of firewalls and network profiles to enable proper access inside and outside the organization.

Vulnerability Management

Consistently schedule and conduct vulnerability scans on servers and systems under your control to proactively identify technology flaws. Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software.

Incident Response

The Incident Response Process coupled with an Incident Response Plan allows users to discover cyber attacks on the network and prevent them from causing a data breach or loss. An Incident Response strategy is established and implemented so that you and all your employees are prepared in the event of an attack. Practice this plan to ensure success.

Medical Device Security

Much of Medical Device security can be accomplished by treating the devices as IT equipment. Just as you would for a computer, establish endpoint protections, proper inventory, regular software patching, and implement access management procedures.

Cybersecurity Policies

For organizations of all sizes, cybersecurity policies should include consistent education and awareness, proper roles and responsibility guidelines, incident reporting, IT equipment use policies, and guidance of personal device use.

HHS 405(d)
Aligning Health Care Industry Security Approaches

10 Practices to Protect Your Organization from Cyber Threats

Cybersecurity Policies

For organizations of all sizes, cybersecurity policies should include consistent education and awareness, proper roles and responsibility guidelines, incident reporting, IT equipment use policies, and guidance of personal device use.

Data Protection and Loss Prevention

Put in place data classification policies that clearly define how sensitive data is to be handled at your organization. Instill proper procedures that outline the distribution method, encryption level, storage, and removal of all types of data.

Email Protection Systems

Put in place email protection systems that can help thwart cyber attacks. Enable basic email protection controls, educate staff with phishing simulations, and, if possible, use multi-factor authentication as a double layer of defense.

IT Asset Management

Keep a full and accurate inventory of all IT equipment at all times. This also includes implementing procurement processes that encompass the lifecycle of each IT Asset. Also, if your organization allows the use of personal devices, establish integration with network access control procedures to ensure protection to your systems.

Endpoint Protection Systems

Implement basic Endpoint Protection Controls such as antivirus software, full disk encryption, and patching. Each endpoint in your organization should be equipped with these controls and configured to update automatically.

Network Management

Use Network Segmentation to configure networks to restrict access between devices to that which is required to successfully complete work. An effective network management strategy also includes the deployment of firewalls and network profiles to enable proper access inside and outside the organization.

Access Management

Clearly identify all users and maintain audit trails that monitor each user's access to data, applications, systems, and endpoints. Establish unique accounts for each individual and avoid using ADMIN accounts. Tailor access for each user based on the user's specific role and work requirements.

Vulnerability Management

Consistently schedule and conduct vulnerability scans on servers and systems under your control to proactively identify technology flaws. Conduct routine patching of security flaws in servers, applications (including web applications), and third-party software.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram or visit our website at 405d.hhs.gov!

HHS 405(d)
Aligning Health Care
Industry Security Approaches

10 Practices to Protect Your Organization from Cyber Threats

Incident Response

The Incident Response Process coupled with an Incident Response Plan allows users to discover cyber attacks on the network and prevent them from causing a data breach or loss. An Incident Response strategy is established and implemented so that you and all your employees are prepared in the event of an attack. Practice this plan to ensure success.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram or visit our website at 405d.hhs.gov!

Practice downtime procedures

- ✓ Develop a computer “crash cart”.
- ✓ Create an emergency contact list of companies and phone numbers you may need.
- ✓ Keep **copies** of forms you needed to operate if you could not access your EHR.
- ✓ Practice how the clinic would function, document care, communicate with patients, place orders, and bill for services.

Emergency Contact List	
Physician(s)	
Administrator	
Key Staff	
IT	
EHR	

Patient Demographic Form
Please PRINT

Patient Name:_____Nickname/AKA:_____
Date of Birth:_____ Social Security Number_____Sex:_____
Home Address:_____
City:_____ State:_____ Zip Code:_____
Home #:_____ Cell #:_____ Work #:_____
Preferred method of contact: (circle one) Phone Email Letter
Marital Status: Married____ Single ____ Divorced _____ Separated____ Widowed____
Language (other than English):_____ Race:_____ Ethinicity:_____
Email address:_____ Employer:_____
Spouse/Parent:_____ Phone #:_____
Emergency Contact:_____ Phone #:_____
How did you hear about us:_____

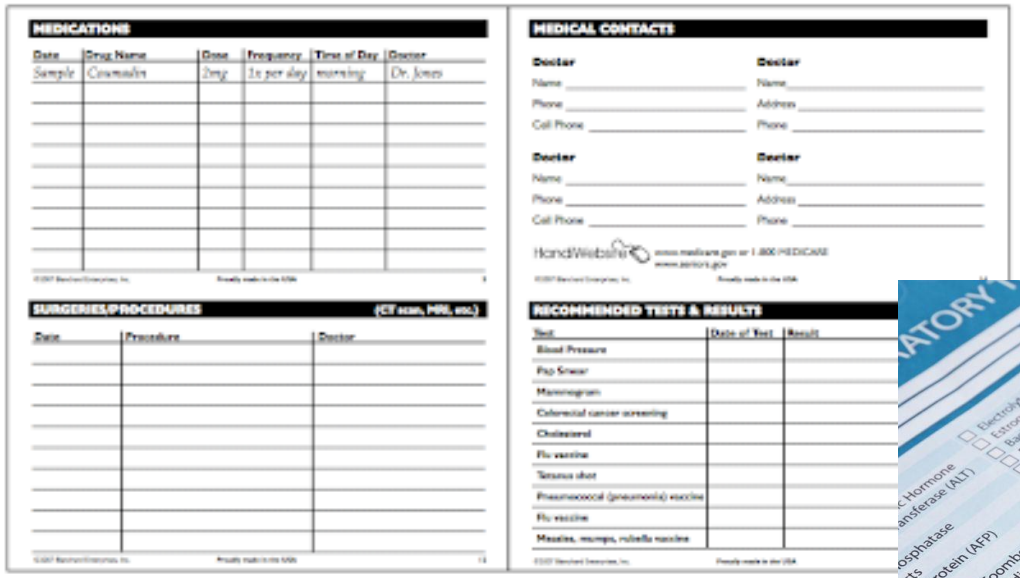
INSURANCE INFORMATION

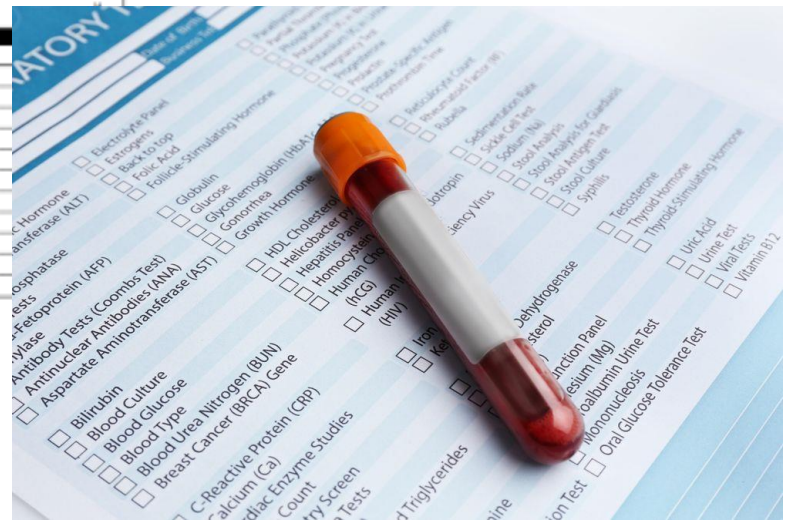
Ins Co Name:_____ Policy/ Member ID #:_____
Patient Relation to Insured: Self:_____ Spouse:_____ Child:_____ Other:_____
Policy Holder:_____ Sex:_____
Address:_____City:_____ Zip Code:_____
Home #:_____ Date of Birth:_____
Employer:_____

SECONDARY INSURANCE

Ins Co Name:_____ Policy/ Member ID #:_____
Patient Relation to Insured: Self:_____ Spouse:_____ Child:_____ Other:_____
Policy Holder:_____ Sex:_____
Address:_____ City:_____ Zip Code:_____
Home #:_____ Date of Birth:_____
Employer:_____

What forms do you need to run the clinic for a day? A week? Longer?





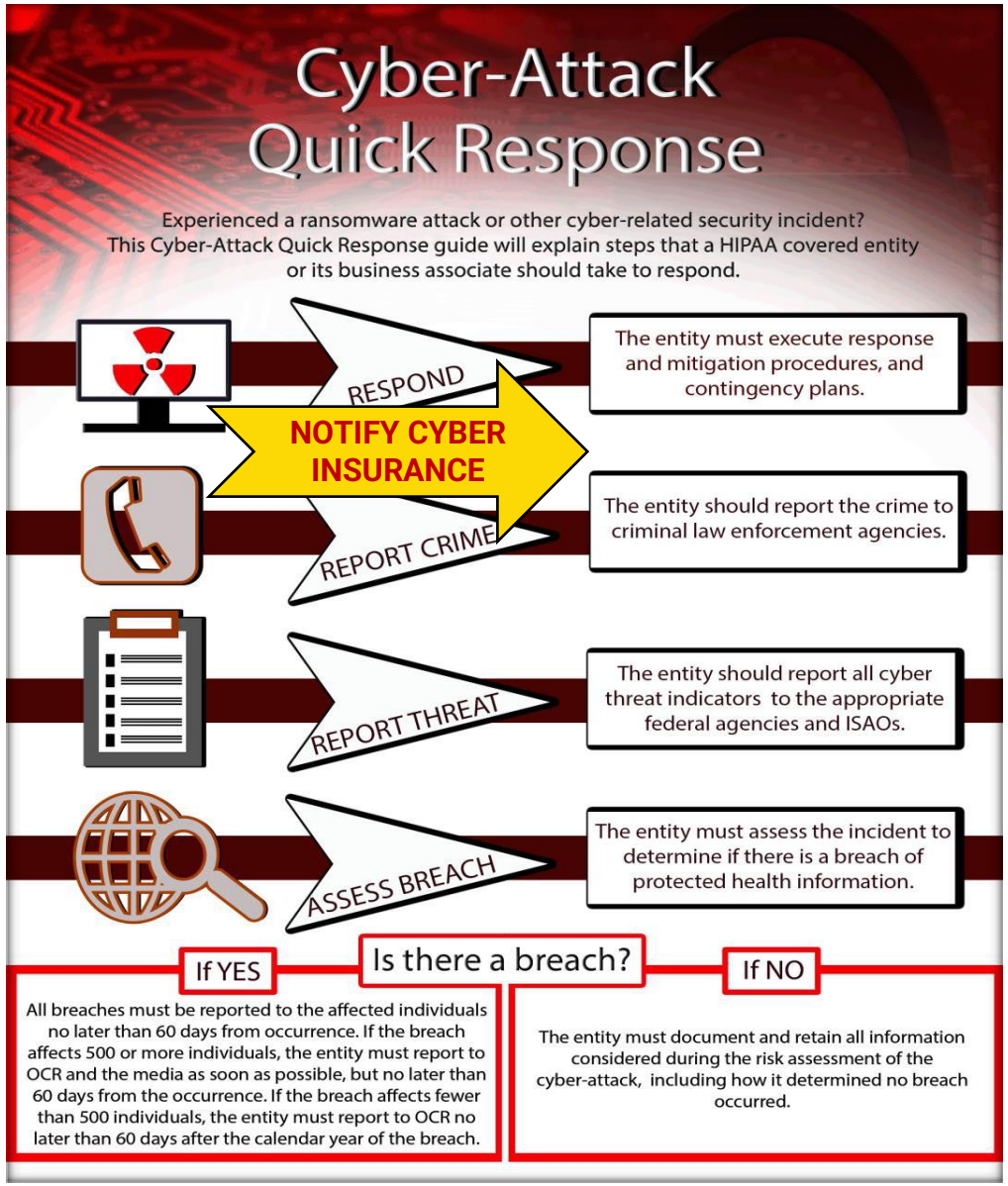
IMAGING

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

My entity just experienced a cyber-attack! What do we do now?

A Quick-Response Checklist from the HHS, Office for Civil Rights (OCR)

Has your entity just experienced a ransomware attack or other cyber-related security incident,[i] and you are wondering what to do now? This guide explains, in brief, the steps for a HIPAA covered entity or its business associate (the entity) to take in response to a cyber-related security incident. In the event of a cyber-attack or similar emergency an entity:



Source: Health and Human Service – Office for Civil Rights

HHS 405(d)
Aligning Health Care
Industry Security Approaches

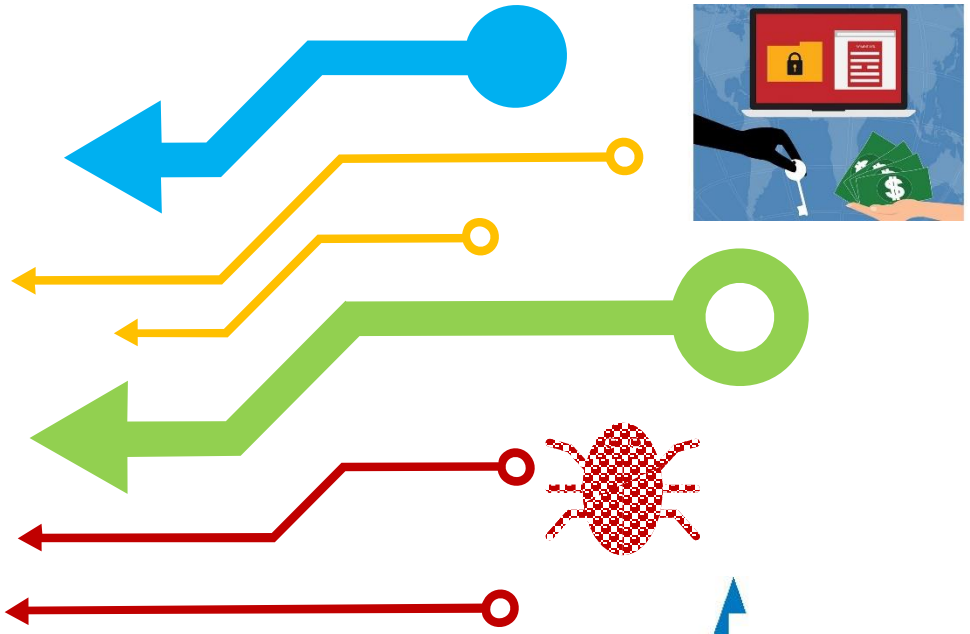
10 Practices to Protect Your Organization from Cyber Threats

Medical Device Security

Much of Medical Device security can be accomplished by treating the devices as IT equipment. Just as you would for a computer, establish endpoint protections, proper inventory, regular software patching, and implement access management procedures.

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram or visit our website at 405d.hhs.gov!

CYBER SECURITY



TMLT

Texas Medical Liability Trust

What is your source for emerging cyber threat information?

i.e. RDP – Emergency Directive to Mitigate known Vulnerability

An official website of the Department of Homeland Security

cyber.dhs.gov

Home

20-03 - Mitigate Windows DNS Server Vulnerability from July 2020 Patch Tuesday

20-02 - Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday

Background

Emergency Directive 20-02

January 14, 2020

Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday

This page contains a web-friendly version of the Cybersecurity and Infrastructure Security Agency's Emergency Directive 20-02, "*Mitigate Windows Vulnerabilities from January 2020*

HHS Office for Civil Rights in Action

January 15, 2020

Cyber Notice: Emergency Directive to Mitigate Windows Vulnerabilities

OCR is sharing the following update from the HHS Critical Infrastructure Protection Public-Private Partnership with our listserv:

TMLT
@TMLT_TMIC

HHS has issued a Cyber Notice: Emergency Directive to Mitigate Windows Vulnerabilities notifying the public of a number vulnerabilities identified in Microsoft Windows operating systems. Read it here: cyber.dhs.gov/ed/20-02/

10:02 AM · 1/16/20 · Sprout Social

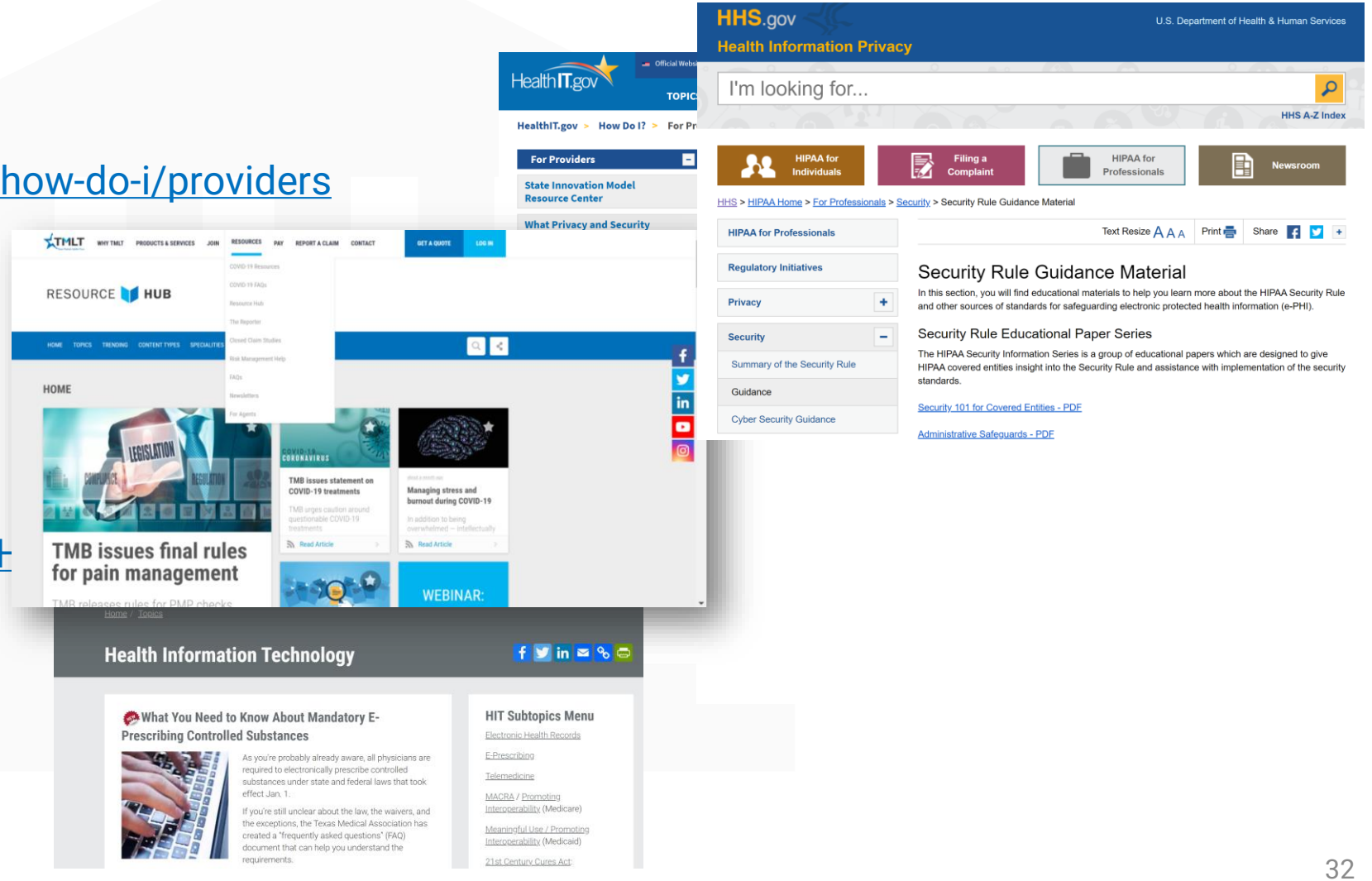
Resources

OCR
Resource: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Office of National Coordinator
Resource: https://www.healthit.gov/how-do-i/providers

TMLT
Resource: https://www.hub.tmlt.org

TMA
Resource: https://www.texmed.org/H



Resources

OCR Cyber Awareness Newsletters

In 2019, OCR moved to quarterly cybersecurity newsletters. The purpose of the newsletters remains unchanged: to help HIPAA covered entities and business associates remain in compliance with the HIPAA Security Rule by identifying emerging or prevalent issues, and highlighting best practices to safeguard PHI. Visit our Cybersecurity Newsletter Archive page to view previous newsletters from 2016.

- Summer 2019 OCR Cy
- Spring 2019 OCR Cyb
  Vulnerabilities
- Fall 2019 OCR Cybers
  Mitigating and Respon
- Summer 2020 OCR Cy

HHS Office for Civil Rights in Action

March 17, 2022

OCR Cybersecurity Newsletter: Defending Against Common Cyber-Attacks

Throughout 2020 and 2021, hackers have targeted the health care industry seeking unauthorized access to valuable electronic protected health information (ePHI). The number of breaches of unsecured ePHI reported to the U.S Department of Health and Human Service's Office for Civil Rights (OCR) affecting 500 or more individuals due to hacking or IT incidents increased 45% from 2019 to 2020.[i] Further, the number of breaches due to hacking or IT incidents accounted for 66% of all breaches affecting 500 or more individuals reported to OCR in 2020.[ii]

Although some attacks may be sophisticated and exploit previously unknown vulnerabilities (*i.e.,* zero-day attack), most cyber-attacks could be prevented or substantially mitigated if HIPAA covered entities and business associates ("regulated entities") implemented HIPAA Security Rule requirements to address the most common types of attacks, such as phishing emails,[iii] exploitation of known vulnerabilities, and weak authentication protocols. If an attack is successful, the attacker often will encrypt a regulated entity's ePHI to hold it for ransom, or exfiltrate the data for future purposes including identify theft or blackmail. Cyber-attacks are especially critical in the health care sector as attacks on ePHI can disrupt the provision of health care services to patients. This newsletter explores preventative steps regulated entities can take to protect against some of the more common, and often successful, cyber-attack techniques.

Source: https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html

Breach

Don’t use the

word

unless you have to – HIPAA requires all breaches must be reported to the federal government

- A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. An impermissible use or disclosure of protected health information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised
- Following a breach of unsecured protected health information, covered entities must provide notification of the breach to **affected individuals, the Secretary**, and, in certain circumstances, **to the media**. In addition, business associates must notify covered entities if a breach occurs at or by the business associate.

Develop a “best practices” strategy against cyber attacks

- Data backup plan
- Access controls
- Close any open remote desk ports
- Add multi-factor authentication
- Secure email
- Add endpoint protections
- Establish a process for ongoing threat detection
- Secure vendors
- Have an incident response plan including data recovery and contingency plans

UHS lost $67M from malware attack

King of Prussia, Pa.-based **Universal Health Services** lost $67 million from a malware attack last year, which caused patients to go elsewhere for care and incurred expenses to restore its operating and IT systems, according to a Feb. 26 Wall Street Journal report.

Five things to know:

1. UHS experienced the cyberattack from Sept. 27, 2020, into October 2020; **the health system said it was forced to divert patients to competitor facilities, saw steep increases in labor expenses to restore its networks, and experienced administrative functions such as coding and billing delayed into December.**

2. These factors had "**a negative impact on our operating cash flows during the fourth quarter of 2020**," UHS said in financial documents released Feb. 25.

3. UHS said the breach had an **unfavorable pretax effect of $67 million, with $55 million in the fourth quarter of 2020 and $12 million in the third quarter of 2020.**

4. UHS **didn't pay a ransom**, and a health system spokesperson told the Journal that UHS believed it would be entitled to recoup costs through insurance.

5. During the cyberattack, UHS **shut down computer systems for medical records, labs and pharmacies across 250 U.S. facilities**. This caused disruptions including ambulance diversions and sending patients to different surgeons for care, UHS CFO Steve Filton told investors in January, according to the report.

"I think, intellectually, you know that we're very reliant on our information technology," Mr. Filton said, "but you don't really realize how much you are until something disrupts that."

Providers Need Expert Guidance

As the forms of connected technology used by healthcare providers increases—so will their cybersecurity risks.

Therefore, providers will need assistance in mitigating the proliferation & diversity of cyber risks, including help with their:

- ✓ **IT Systems;**
- ✓ **HIPAA Privacy and Security Risk Assessments;**
- ✓ **Staff Privacy Training; and**
- ✓ **Risk Transfer (cyber insurance).**

Cathy Bryant
Manager, Cyber Consulting Services

512-425-5910

cathy-bryant@tmlt.org
cyber@tmlt.org

TMLT
Texas Medical Liability Trust