

# Cybersecurity Woes in 2020: Protecting Patients From Evolving Threats and Lessons Learned from HHS' Wall of Shame



Yolanda Sims, JD, MHA  
Loss Prevention & Risk Management Advisor



# Today's Agenda

- Review security threat vectors that are most impactful in healthcare organizations.
- Identify risks related to cybersecurity incidents.
- Practical tips to protect against cybersecurity insider/outsider threats.



# Park DuValle Clinic Faces Blowback After Ransomware Attack

By Lisa Gillespie



Hackers held patient files at a Battle Creek doctor's office for ransom. The office didn't pay. It closed.

## Hackers Demand \$1M in Grays Harbor Ransomware Attack

The Washington-based provider initiated EHR downtime in June, but remained mum on details; a report shows hackers demanded a \$1 million ransom to unlock patient files after a cyberattack.



Brookside ENT and Hearing Center was forced to shut down after their system was hacked by a ransomware virus. (Photo: Brooks Hepp)

# Hackensack Meridian Health pays up after ransomware attack

The undisclosed sum paid by the New Jersey health system, one of the state's largest, is covered by an insurance plan that helps it cover costs related to cyber attacks, officials said.



# Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak

By [Shira Stein](#) and [Jennifer Jacobs](#)

March 16, 2020, 7:37 AM CDT *Updated on March 16, 2020, 3:35 PM CDT*

## 140K Patients Impacted in Tandem Diabetes Care Phishing Attack

Several Tandem Diabetes employee email accounts were comprised during a three-day period after a phishing attack; an insider incident, email hack, and more phishing complete this week's breach roundup.



## OCR Shares COVID-19 Cyber Scam Advice, as Hackers Impersonate WHO

Hackers are taking advantage of the COVID-19 outbreak by impersonating WHO in coronavirus phishing campaigns. In response, OCR urges providers to review DHS cyber scam advice.





## RANSOMWARE ATTACK DISRUPTS CAMPBELL COUNTY HOSPITAL SERVICES



TOM MORTON | September 20, 2019

Google Maps

The ransomware attack, according to the hospital's news release, disrupted and affected the following services:

- No outpatient lab, respiratory therapy and radiology exams or procedures.
- No new inpatient admissions
- Some surgery cancellations
- Patients presenting to the emergency department and walk-in clinic will be triaged and transferred to an appropriate care facility if needed.
- Phone systems were operational.

# IBM & Ponemon Institute Cost of a Data Breach Report (2019)

- Data breaches cost the healthcare industry \$6.5M or **\$429.00** per patient record.
- For the ninth consecutive year, the healthcare industry is the hardest hit financially by data breaches.
- The costs are directly related to legal, technical and regulatory functions such as patient notification, credit monitoring, and reputational damage.



# Let's Talk About Hackers!





# THREAT: RANSOMWARE ATTACKS



# What is Ransomware?

- Ransomware is a type of malware distinct from other malware.
- It denies you access to your information and files.
- It encrypts the data with a key known only to the hacker who deployed the malware.
- It is released when ransom is paid \$\$\$\$.



# Disruption of Services



▼ Ransomware attacks against medical, educational & governmental organizations - as reported across the US by America's 374,016 views  
[SHARE](#)

☑ Ransomware Map

- ▼ 📍 Municipality
- 📍 Medical
- 📍 Education
- 📍 Other
- 📍 Law Enforcement
- 📍 Federal Government
- 📍 Other / No data



Made with Google My Maps



**Google Ransomware War Map 4.7.20**

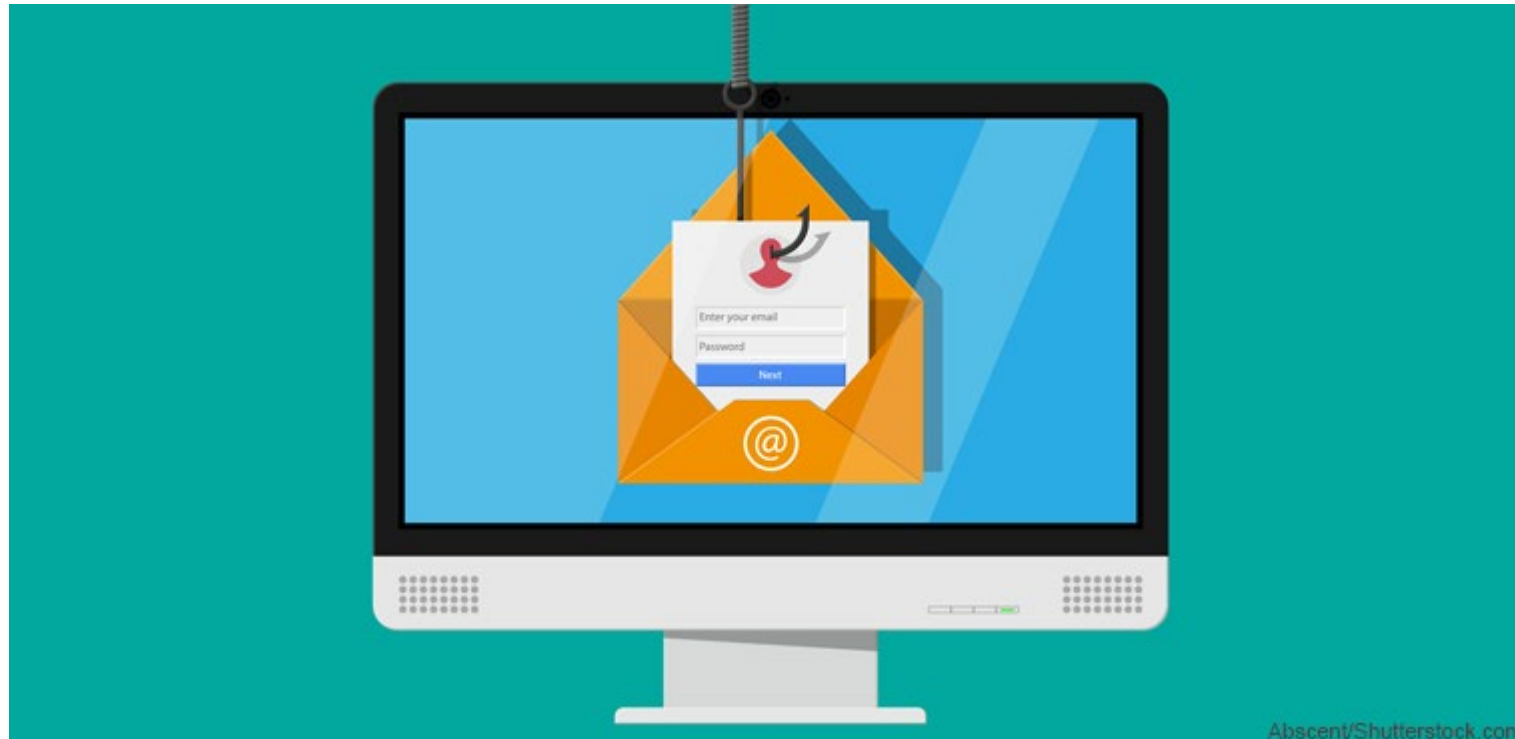
[https://www.google.com/maps/d/u/0/viewer?mid=1UE6Nko9iRG1tLci\\_AeqqsxzxGzs&ll=46.074272469861846%2C-117.53898531930452&z=4](https://www.google.com/maps/d/u/0/viewer?mid=1UE6Nko9iRG1tLci_AeqqsxzxGzs&ll=46.074272469861846%2C-117.53898531930452&z=4)



# Should You Pay the Ransom?

- Paying a ransom does not guarantee that the hacker will unencrypt or unlock the stolen or locked data.
- Law enforcement and government agencies such as the FBI, say don't pay unless you really have to.

# THREAT: Email Phishing Attacks



Abscent/Shutterstock.com

# What is Email Phishing?

Email phishing is an attempt to trick you, a colleague or someone else in the workplace into giving out information using email.

Phishing attacks rely on human tendencies, which is why email is the most common initial point of compromise for significant security incidents.

Phishing attacks may appear to come from reputable organizations or charities. Attackers take advantage of current events and certain times of the year.

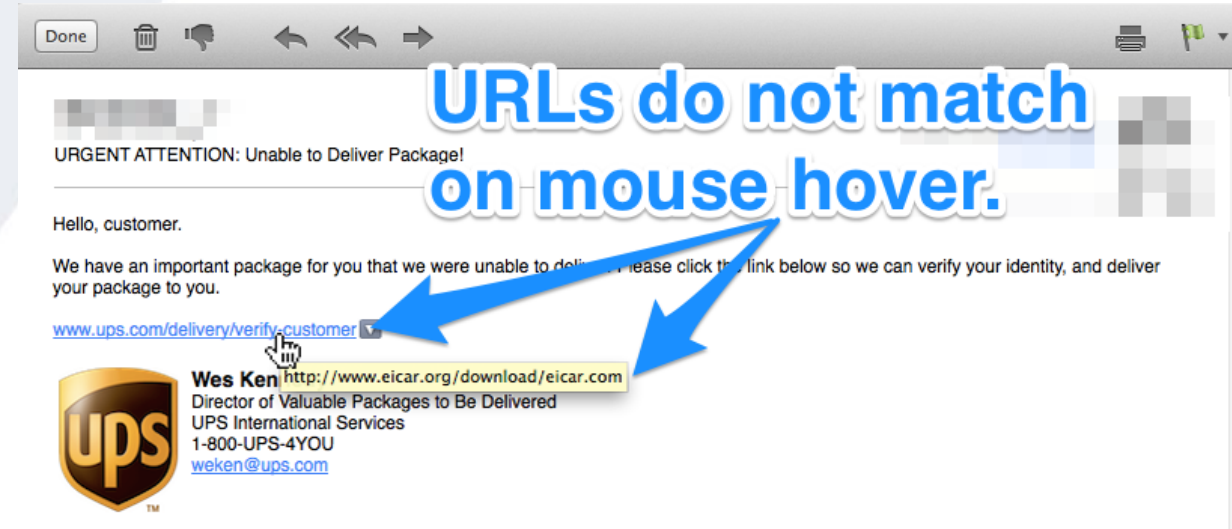
# What are Common Indicators of Phishing Attempts?

- Suspicious sender's address
- Generic greetings and signature
- Spoofed hyperlinks and websites
- Spelling and layout
- Suspicious attachments



# Always Hover

- Before clicking any links in the email, hover your mouse over the link and the actual URL will appear.
- Double check to make sure the real URL is leading you to the right place.
- You don't want to click a link to [juspandoo.de/82359/index.html](http://juspandoo.de/82359/index.html).
- Hackers will also try to spoof the URL to look like the legitimate address.



- Investigate to make sure the domain is the same as the sender of the email.

# Email Phishing Don'ts

- Don't copy and paste the link into the URL section of your browser to check it. That's the same as clicking the link.
- Don't forward a suspected malicious email to other people.
- Don't open the malicious email on your mobile devices. They are not immune to malware and viruses.
- Don't solely rely on antivirus software. Antivirus protects against known signatures, but are susceptible to new malware that goes undetected.

# Boost Your Phishing IQ: Use Critical Thinking Skills

Don't take everything at face value. Before you open and click an email go through these questions:

- Is the email from someone I recognize?
- Am I expecting the email?
- Are the requests of the email reasonable?
- Is the email using emotional gauges like fear or urgency to entice an action?

# SCAM ALERT FROM HHS

April 3, 2020

## Alert: Individual Posing as OCR Investigator

It has come to OCR's attention that an individual posing as an OCR Investigator has contacted HIPAA covered entities in an attempt to obtain protected health information (PHI). The individual identifies themselves on the telephone as an OCR investigator, but does not provide an OCR complaint transaction number or any other verifiable information relating to an OCR investigation.

HIPAA covered entities and business associates should alert their workforce members, and can take action to verify that someone is an OCR investigator by asking for the investigator's email address, which will end in [@hhs.gov](mailto:@hhs.gov), and asking for a confirming email from the OCR investigator's [hhs.gov](mailto:hhs.gov) email address. If organizations have additional questions or concerns, please send an email to: [OCRMail@hhs.gov](mailto:OCRMail@hhs.gov).

Suspected incidents of individuals posing as federal law enforcement should be reported to the Federal Bureau of Investigation (FBI). The FBI issued a public service announcement about COVID-19 fraud schemes at: <https://www.ic3.gov/media/2020/200320.aspx>.



# THREAT: Loss or Theft of Equipment or Data



# Loss or Theft of Equipment or Data

Every day, mobile devices such as laptops, tablets, smartphones, and USB/thumb drives are lost or stolen.

The threat is far worse if the lost device was not appropriately safeguarded or password protected.

- Loss or malicious use of unsecured PHI may result in business disruption and compromised patient safety.
- May trigger regulatory obligations and notification to patients.

Ex: a physician stops for a coffee. As he leaves the table momentarily to pick up his coffee, a thief steals the laptop. He returns to find the laptop gone.

# Do you know your organization's policy on removing equipment from the workplace?

Ask the following:

- Can I travel with my equipment?
- Can I take my equipment offsite to work remotely?
- Are USB or other portable storage devices allowed?
- Is the information on my computer or device encrypted?
- Is there a secure VPN that I can use, along with secure, password-protected Wi-Fi to log into the network and work?

# Vulnerabilities of Mobile Device

## Bring Your Own Device (“BYOD”)

- Hospital issued vs Employee owned
- Personal use on Hospital-owned devices
- PHI on devices? Remote Access?
- Policies regarding use
- Ability to remotely wipe
- Mobile Device Management Software



# THREAT: Insider, Accidental or Intentional Data Loss



# Insider Threats: Accidental or Intentional Data Loss

Human error is a significant initial point of compromise, which is why insider threats are so prevalent.

- An accidental insider threat is unintentional loss caused by honest mistakes or a degree of negligence.
- An intentional insider threat is malicious loss or theft with the objective of personal gain or inflicting harm to the organization or another individual.

Ex: An attacker impersonating a staff member of a physical therapy center contacts a hospital employee and asks to verify patient data. Pretending to be hospital staff, the imposter acquires the entire patient health record.

# Insider Threats vs. Outsider Threats

Insider Threats: Employees, contractors, or partners can commit fraud, espionage or theft of intellectual property.

- Insider threats are successful with the use of ransomware, malware, business email compromise, phishing scams etc.

Outsider Threats: Cyberterrorists, hackers

- Data breach, denial of service attacks, cybersquatting etc.

# THREAT: Medical Device Attacks



# Medical Device Attacks

IT experts are concerned that recent trends will convince cybercriminals to target medical devices such as pacemakers or Intensive Care Unit (ICU) respirators.

- Know your organization's protocols in case of a potential shutdown or attack against medical devices.
- That means asking: 1) How do we notify patients if medical devices are compromised? 2) How do patients notify us if they suspect their medical device is compromised?
- Engage vendors or manufacturers of medical devices to understand vulnerabilities, risks and appropriate protection and response measures.

# What is the Real Cost of a Data Breach?

## Detection and Escalation

- Forensics and investigative services, crisis team management

## Notification Costs

- Letters, emails and outbound calls to notify the person their information has been compromised

## Post Data Breach Response

- Credit monitoring, legal expenditures, regulatory fines.

## Lost Business Cost

- Cost of business interruption, revenue loss and reputation loss



# HIPAA Compliance

The HIPAA Security Rule & Meaningful Use incentives require physicians to conduct a security risk analysis.

Covered Entities have an obligation to implement administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of protect health information.

OCR is increasing their enforcement efforts in this area. No organization, big or small is exempt.

If you fail to comply, you may be the next covered entity listed on the OCR Breach Portal (“Wall of Shame”).



# Common HIPAA Violations Revealed in OCR Investigations

- Impermissible uses and disclosures of PHI
- Lack of safeguards of PHI
  - Encryption
  - Ability to remotely wipe a hard drive
- Use or Disclosure of more than the minimum necessary rule
- Lack of administrative safeguards
- Lack of Business Associate Agreement (BAA)



# Civil Monetary Penalty Maximums Lowered

Table 2—Penalty Tiers Under Notification of Enforcement Discretion

<b>Culpability</b>	<b>Minimum penalty/violation</b>	<b>Maximum penalty/violation</b>	<b>Annual limit</b>
No Knowledge	\$100	\$50,000	\$25,000
Reasonable Cause	1,000	50,000	100,000
Willful Neglect— Corrected	10,000	50,000	250,000
Willful Neglect— Not Corrected	50,000	50,000	1,500,000

# HHS' WALL of SHAME SECURITY INCIDENTS



# OCR's First Settlement Case of 2020

## Health Care Provider Pays \$100,000 Settlement to OCR for Failing to Implement HIPAA Security Rule Requirements

The practice of Steven A. Porter, M.D., has agreed to pay \$100,000 to the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) and to adopt a corrective action plan to settle a potential violation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Dr. Porter's medical practice provides gastroenterological services to over 3,000 patients per year in Ogden, Utah.

OCR began investigating Dr. Porter's medical practice after it filed a breach report with OCR related to a dispute with a business associate. OCR's investigation determined that Dr. Porter had never conducted a risk analysis at the time of the breach report, and despite significant technical assistance throughout the investigation, had failed to complete an accurate and thorough risk analysis after the breach and failed to implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

"All health care providers, large and small, need to take their HIPAA obligations seriously," said OCR Director Roger Severino. "The failure to implement basic HIPAA requirements, such as an accurate and thorough risk analysis and risk management plan, continues to be an unacceptable and disturbing trend within the health care industry."

In addition to the monetary settlement, Dr. Porter will undertake a corrective action plan that includes two years of monitoring. The resolution agreement and corrective action plan may be found at:

<https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/porter/index.html>.

# HHS' "WALL OF SHAME"

U.S. Department of Health and Human Services  
Office for Civil Rights

Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information

Under Investigation

Archive

Help for Consumers

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. The following breaches have been reported to the Secretary:

## Cases Currently Under Investigation

This page lists all breaches reported within the last 24 months that are currently under investigation by the Office for Civil Rights.

[Show Advanced Options](#)

Breach Report Results							
Expand All	Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
	Golden Valley Health Centers	CA	Healthcare Provider	39700	03/20/2020	Hacking/IT Incident	Email
	Hawaii Pacific Health	HI	Business Associate	836	03/19/2020	Loss	Paper/Films
	Hawaii Pacific Health	HI	Business Associate	3772	03/17/2020	Unauthorized Access/Disclosure	Electronic Medical Record
	Lifesprk	MN	Healthcare Provider	9000	03/17/2020	Hacking/IT Incident	Email
	Tandem Diabetes Care, Inc.	CA	Healthcare Provider	140781	03/17/2020	Hacking/IT Incident	Email
	Lakewood Health System	MN	Healthcare Provider	1415	03/16/2020	Hacking/IT Incident	Email
	Hao Rong DDS Inc dba Genuine Care Dental	CA	Healthcare Provider	2190	03/14/2020	Theft	Network Server
	Randleman Eye Center	NC	Healthcare Provider	19556	03/13/2020	Hacking/IT Incident	Network Server

# WALL of SHAME Continued.....

0	TriHealth Cancer Institute	OH	Healthcare Provider	912	03/13/2020	Unauthorized Access/Disclosure	Paper/Films
0	The Prudential Insurance Company of America	NJ	Health Plan	1945	03/11/2020	Hacking/IT Incident	Network Server
0	OneDigital Health and Benefits	GA	Business Associate	22894	03/06/2020	Theft	Laptop
0	Torrance Memorial Medical Center	CA	Healthcare Provider	3448	03/06/2020	Unauthorized Access/Disclosure	Network Server
0	Stephan C Dean	CA	Business Associate	70000	03/04/2020	Hacking/IT Incident	Desktop Computer, Electronic Medical Record, Email
0	Elk Ridge Dentistry	CO	Healthcare Provider	2793	03/02/2020	Theft	Other Portable Electronic Device
0	Alameda Alliance for Health	CA	Health Plan	500	02/28/2020	Hacking/IT Incident	Network Server
0	Walgreen Co.	IL	Healthcare Provider	6681	02/28/2020	Unauthorized Access/Disclosure	Other Portable Electronic Device
0	Ozark Orthopaedics, PA	AR	Healthcare Provider	15240	02/28/2020	Hacking/IT Incident	Email

<input checked="" type="checkbox"/>	The Prudential Insurance Company of America	NJ	Health Plan	1945	03/11/2020	Hacking/IT Incident	Network Server
<b>Business Associate Present:</b> Yes							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	OneDigital Health and Benefits	GA	Business Associate	22894	03/06/2020	Theft	Laptop
<b>Business Associate Present:</b> Yes							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	Conagra Brands Welfare Benefit Wrap Plan	IL	Health Plan	1713	03/06/2020	Unauthorized Access/Disclosure	Paper/Films
<b>Business Associate Present:</b> No							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	Torrance Memorial Medical Center	CA	Healthcare Provider	3448	03/06/2020	Unauthorized Access/Disclosure	Network Server
<b>Business Associate Present:</b> No							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	Stephan C Dean	CA	Business Associate	70000	03/04/2020	Hacking/IT Incident	Desktop Computer, Electron Record, Email
<b>Business Associate Present:</b> Yes							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	Elk Ridge Dentistry	CO	Healthcare Provider	2793	03/02/2020	Theft	Other Portable Electronic
<b>Business Associate Present:</b> No							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	Alameda Alliance for Health	CA	Health Plan	500	02/28/2020	Hacking/IT Incident	Network Server
<b>Business Associate Present:</b> No							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	Walgreen Co.	IL	Healthcare Provider	6681	02/28/2020	Unauthorized Access/Disclosure	Other Portable Electronic
<b>Business Associate Present:</b> No							
<b>Web Description:</b>							
<input checked="" type="checkbox"/>	Ozark Orthopaedics, PA	AR	Healthcare	15240	02/28/2020	Hacking/IT Incident	Email



# The Three P's

## Policy: THE WHAT

- Timely
- Relevant
- Defend against the current threat landscape.

## Procedures: THE WHO

- You must be able to demonstrate that you have procedures in place based on the policies.

## Practice: THE PROOF

- Evidence that you practice those procedures.



# Cyber Hygiene: Practical Tips to Mitigate Cyber Threats





# Tip 1: Establish a Cybersecurity Policy

You can start with the National Institute of Standards and Technology (NIST) Cybersecurity framework.

- Visit [www.nist.gov](http://www.nist.gov)
- Establish a policy that will define all cyber roles and responsibilities throughout the organization.



Function
Identify
Protect
Detect
Respond
Recover

- Describes desired outcomes
- Understandable by everyone
- Applies to any type of risk management
- Defines the entire breadth of cybersecurity
- Spans both prevention and reaction

# Tip 2: Conduct Security Risk Assessments



Use security risk assessment results to take actions and further enhance your cybersecurity efforts.

- First, start with a GAP analysis.
  - Identify threats and vulnerabilities and their potential impact.
- Maintain a complete, accurate and current asset inventory profile to ensure you know where PHI resides.
  - Including laptops, USB drives and mobile devices.

# Tip 3: Conduct Phishing Tests and Simulated Attacks

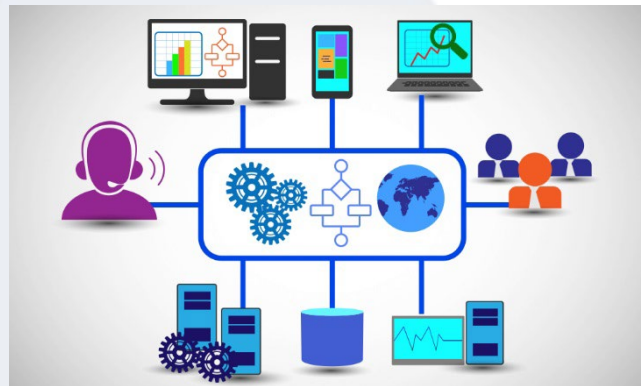
Do you know your phishing click rate at your practice or facility?

- Routinely launch “fake phishing scams”, use click bait to test your workforce’s awareness.
- Raise the collective phishing IQ of everyone.
- Train workers to trust their instincts and use common sense.



# Tip 4: Monitor the Monitors

- Limit access to people who need it to perform their job duties, but be wise, snooping still exists.
- Security settings should monitor for unauthorized access or access attempts at every level.



# Tip 5: Encryption, Encryption, Encryption

Extensive encryption is a huge cost saving measure.




# Tip 6: Workforce Training



- Provide security awareness training and education for all staff.
- Define the mechanisms that will be used to train workforce on cybersecurity practices, threats and mitigations.
  - Ensure that education includes common cyberattacks, lost/stolen devices and methods for reporting suspicious behavior on their computers.
  - The user base should be all users and a dedicated cybersecurity department or individual.

# Tip 7: Pay Attention to Third Party Vendors, Contractors and Consultants

- Look at risks that involve third party partners.
- Always review their Business Associate Agreement (BAA) on an annual basis.



Note to Self:  
Pay Attention

# Tip 8: Protect Yourself from Ransomware

Backup your data and use the 3-2-1 backup rule

- Have 3 copies of your data, 2 copies on different media types and 1 copy offsite.

Patch/Update your software

- Develop a regular patch update program and make someone responsible for implementing it.

Use Anti-Virus Software

- Use from a reputable source and keep it updated.



# Tip 9: Have An Incident Response Team & Test Your Incident Response Plan

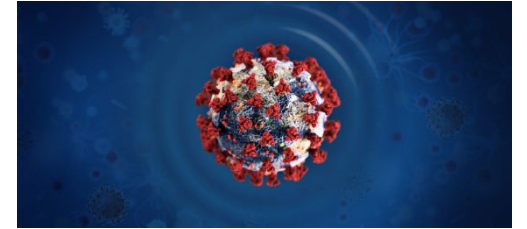


- Create a ransomware recovery playbook.
- Conduct several tabletops or demonstrations throughout the year.
- Cyber threats are ever evolving, extensive training will help ensure you are ready to respond when it happens.

# TIP 10: Stay Ready!



# Additional Tips in Light of COVID-19



- Secure systems that enable remote access. Ex: VPN
- Implement multi-factor authentication
- Enhance system monitoring to receive early detection and alerts on abnormal activity.
- Remind employees to be aware of potential phishing attacks during the pandemic.
- Increase awareness of IT support mechanisms for employees who work remotely.
- Update incident response plans to consider workforce changes in a disrupted environment.

[https://www.cisa.gov/sites/default/files/publications/20\\_0306\\_cisa\\_insights\\_risk\\_management\\_for\\_novel\\_coronavirus.pdf](https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus.pdf)

# Final Takeaways



1. Adopt a security framework
  - NIST, HHS, HIMSS
2. Develop cybersecurity plans and policies
  - HHS guidance is a great starting point
3. Insure against remaining threats
  - Purchase cybersecurity coverage

# References

U.S Department of Health and Human Services Office for Civil Rights. Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information. 2019. <https://ocrportal.hhs.gov/ocr/breach/breachreport.jsf>. Accessed April 7, 2020.

Chase, M and Mohs, A. Thinking Inside the Box: How to Identify and Tackle Insider Cyber Threats. Baird Holm LLC Aug. 12, 2019

HHS Task Force Document: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

HHS Fall 2019 OCR Cybersecurity Newsletter <https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity-newsletter-fall-2019/index.html>. Accessed December 2019

HHS Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations

2019 HIMSS Cybersecurity Survey

Ponemon Institute Report 2019, available at <https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years>

R, Luna et al. Cyber threats to health information systems: A systematic review. Technology and Health Care 24 (2016) 1-9

Healthcare and Cybersecurity Clark Schaefer Consulting September 2017

Avoiding Social Engineering and Phishing Attacks March 2020 Cybersecurity and Infrastructure Security Agency CISA

Ransomware: What it is and What To Do About It, available at <https://www.fbi.gov/contact-us/field/listingbystate>



# Any Questions?

Yolanda Sims, JD, MHA

Loss Prevention &  
Risk Management Advisor

[ysims@kammco.com](mailto:ysims@kammco.com)

800.232.2259

