# HEALTHCARE CYBERSECURITY

## ADDRESSING THE IMMEDIATE ISSUE TODAY

CHT

WORLD CLASS HEALTHCARE COMPLIANCE

# Introduction

Healthcare facilities are not without risk when it comes to cyber attacks. Theft of medical records is so common, that by 2024 (if online theft keeps accelerating at the current pace),”everyone in the U.S. will have had their healthcare data compromised.”

Threats will only continue to increase in volume and in sophistication. Securing healthcare data is a top priority. As a healthcare facility manager, knowing the ins and outs of healthcare cybersecurity will leave your facility less vulnerable to attacks.

This guide is to provide an overview of healthcare cybersecurity including but not limited to: terminology, breaches, trends, challenges and prevention.

# Chapters

Chapter 1

# Cybersecurity Terminology: The Good, The Bad and The Ugly

Healthcare cybersecurity  is growing. You need the ability to protect or defend the use of cyberspace from the cyber attacks.

I pulled together a list of relevant terms healthcare professionals should know, with the help of the National Institute of Standards and Technology, Glossary of Key Information Security Terms.

**Breach:** Violation to a company's security system. Can happen within or outside of an organization. Involves the misuse of data, applications, and network systems.

**Cyberattack:** An attack on a computer network that disrupts, steals, disables, or destroys the operations of a susceptible organization. Results in the loss of financial, corporate, and personal information.

**Encrytion:** Algorithms that can be used to protect private data and information.

**File Encryption:** Encrypting individual files from being read, copied, or deleted by unauthorized people.

**Hacker:** A skilled computer user who attempts to or gains access to an information system and steals important data.

**Internet Protocol (IP):** Standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.

**Malicious Code:** Software or firmware that enter network drives and have adverse impact on the confidentiality, integrity, or availability of an information system. Some examples of malicious codes are virus, worm, Trojan horse, or other code-based entity that infects a host.

**Malware:** A computer program that infects a system with the intent of inflicting harm on the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

**Passive Attack:** This type of attack is similar to eavesdropping because the attacker intercepts data transmission between the claimant and verifier, but does not alter the information in any way.

**Phishing:** Online scam where the hackers send an email that appears to be from a legitimate company. The email usually requests sensitive personal information or directs a user to a fake website.

**Recovery Procedures:** The process by which information systems and computational capability are restored after a destructive cyber attack or failure.

**Risk Assessment:** Identifying risks that arise inside information systems. During this process, potential risks are assessed and evaluated in order to create better security networks.

**Threat:** Any circumstance or event that has the potential to negatively affect computer information operations.

## Chapter 2

# Breaches/Threats: Detection has Become a Must for the Industry

“Breach”, “Hack”, “Threat” are terms used interchangeably in regards to digital compromises. The fact remains, no healthcare facility wants to be compromised.

Breach detection has become a must for your facility as the attackers are not slowing down.

HealthcareIT News curated the biggest healthcare data breaches of 2018 (so far). The list is extensive.

Here’s a few healthcare cybersecurity articles on breaches that continue to be a problem for the healthcare sector:

“270,000 patient records breached in Med Associates”. A hacker accessed an employee workstation.

“42,000 patients impacted by 2016 breach of Michigan provider”. An unauthorized user accessed a patient database as far back as 2016, but concealed the extent of the intrusion until just recently.

“Phishing hack on Ohio provider breaches data of 42,000 patients for a month”. Email accounts were hit by one of the most common attacks, phishing attacks.

### Healthcare Cybersecurity Tip

Block email traffic that comes from a  brand new domain. Counltess phishing scams come from newly created domains (just a few days old).

HIPAA Journal chimed in with their May 2018 Healthcare Data Breach Report.

“The largest healthcare data breach reported in May 2018 – by some distance – was the 538,127-record breach at the Baltimore, MD-based healthcare provider LifeBridge Health Inc. The breach was reported in May, although it occurred more than a year and a half earlier in September 2016, when malware was installed on its server that hosts electronic health records.”

The threats are nothing new. The number of healthcare cybersecurity breaches is no doubt on the rise.

Becoming aware that security breaches continue to be problematic for the healthcare industry, will be one of its solutions.

## Chapter 3

# How Hackers Gain Access to Healthcare Facilities [Trends]

There are numerous ways attackers will try and gain access to your data. Some of the common practices are malware, ransomware and phishing.

1. **Malware** - a piece of malicious code/software intended to damage computers and computer systems. Malware can include viruses, worms, and spyware.

2. **Ransomware** - malicious code that attacks your computer systems. Your data is held ransom so to speak for money. It prevents a user's access to their computer system.

Malware is used to encrypt data and demand a ransom (or payment) for the decryption. It's always good to back up your systems but most attacks have happened (without you knowing) and you are not able to recover all your data from backups.

3. **Phishing (email)** - Attackers are clever. Phishing is a tool used by hackers to con you into providing your personal information or gain access to account data.

Hoala Greevy, founder and CEO of Paubox; a provider of HIPAA-compliant email services, wrote an article "Don't get phished: 3 email security lessons for healthcare companies". In the article, he identifies mistakes healthcare facilities make to leave them so vulnerable.

Find out why attackers are continuing to target the healthcare industry in this video created by IBM Watson Health.will sound again when another signal is activated. Some alarms can be programmed to resume sounding if the out of spec condition continues.

# 5 Cybersecurity Trends in Healthcare 2018

**Trend #1** Connected devices will be targeted by Ransomware

**Trend #2** Insider education will minimize threats

**Trend #3** Healthcare investments in cybersecurity will rise

**Trend #4** The machine learning arms race will heat up

**Trend #5** Patients will change providers following data breaches

Is your facility doing all that can be done to tackle the challenges now and in the future?

# Chapter 4
# Challenges From a Healthcare Perspective

Patient information is being shared all over the internet. Here's just a few spots to mention:

- patient portals
- insurance companies
- emails

Think about this...

It's getting **harder for organizations to spot when they've even been breached**.

Hackers spend 200+ days inside systems before discovery

IBM Security Senior Threat Researcher John Kuhn told HealthITSecurity.com,

"Always backup, have a backup plan, and have backups of these systems. You need to have knowledge of how to restore this system in the amount of time required to not impact someone's health or impact your business at all. And that's where healthcare is struggling a little bit."

**Additional Challenges for the Healthcare Industry**

1. Breaches are taking longer to find and longer to resolve.

2. Patient care is always a top priority, so sometimes "security measures are dialed down or updates are delayed so they do not interfere with patient care."

3. The Internet of Things (IoT) makes everything a moving target. Nearly every object we know will be connected to the internet. This can make lives easier, but will at the same time increase risk.

4. Health data / (Big Data) allows physicians to build better patient profiles and predictive models. However all the data sharing can be compromised if precautions are not in place.

## Chapter 5

# Gain Control - Plans, Prevention, and Safeguards

It’s time to conduct a risk analysis.

- Identify the risks - could be as simple as strengthening your passwords. And change them regularly.
- Be wary of mobile devices. Different apps on different devices can spell trouble. There should be some type of mobile device management.
- Know what types of data are flowing in and out of your network.
- Employees should use their own devices to access their personal emails, etc.

“Organizations must have defined security procedures that address how staff access and interact with the technology in their facilities. Where possible, implementing two-factor identification to further assure privacy is protected adds another level of protection.” [source]

Risk analysis should be an ongoing process.

> An effective risk analysis is one that is comprehensive in scope and is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data. [source]

The risk assessment should review physical, technical, and administrative safeguards. When potential vulnerabilities are found, covered entities must make applicable changes to keep data secure.

# 10 Tips For Cybersecurity In Healthcare

1. Establish a Security Culture
2. Protect Mobile Devices
3. Maintain Good CPU Habits
4. Use a Firewall
5. Install & Maintain Anti-Virus Software
6. Plan for the Unexpected
7. Control Access to Protect Info
8. Strong Passwords & Change Them Regularly
9. Limit Network Access
10. Control Physical Access

## Chapter 6

# Highly Functional & Operationally Efficient Heathcare Facility

The healthcare cybersecurity landscape continues to be faced with emerging challenges. As technology continues to grow, so will cybersecurity attacks. Medical identity fraud usually takes longer to detect than other types of fraud. And unfortunately, cyber attackers are becoming extremely savvy in their attack approaches and use of malware.

Healthcare facilities need to take action to protect themselves. Prevention is worth the alternative. In today's high tech, high pressure industry, healthcare facilities are faced with more than just online scares.

Healthcare infections, environmental pollutants and emergency preparedness are just a few on an exhaustive list. Behind the scenes are the medical gases and the systems used to sustain life.

As in cyberattack prevention, there is much scrutiny over the use of medical gases and ways to prevent failure or in extreme cases death. Your medical gas systems need to be inspected annually.

Adhering to proper maintenance standards will allow your facility to avoid unnecessary risks and delays. Reliable medical gas and vacuum systems are at the crux of patient care and safety. The ongoing maintenance of medical gas systems is essential for patients.

A hospital or healthcare facility need to assess risk based on risk to patient.

Here's what I mean...

"Risk based assessment assigns a value to each asset by their use and their potential to be harmful to the patients or staff. For example, an oxygen outlet in an emergency room would have the highest urgency while the outlet in the storeroom would have the lowest priority."

The categories are subsequently defined by threat. A category 1 would fall into the need for a highly functional system; failure may cause death or serious injury. A category 4, patients are not adversely affected.

## Conclusion

The importance of safety and security falls under the consistent, dedicated monitoring and testing of a healthcare facility's medical gas and stable and resilient cyber safety.

If you have questions concerning the best ways to keep any medical gas working at their optimum rates, contact your CHT representative.

Medical gas testing, software and inspection will provide you with a safe, cost-efficient hospital. It's important more than ever, that organizations develop effective risk management strategies.

Looking for a partner to
help you achieve
medical gas compliance?

# We Can Help With That

*Yes, really.*

***Talk to the right person today!***

*Click the button above to contact the CHT Account Manager nearest to you and start saving on your medical gas compliance costs today.*

CHT

World Class Healthcare Compliance