Security Risks & Healthcare: How to Protect Your Practice

AND SECURE YOUR PATIENTS' DATA

lightpoint

Introduction

We've all watched reports detailing the immense strain our local healthcare workers have faced throughout 2020 and into 2021. Chances are, when you've seen or heard these sentiments, cybersecurity wasn't top of mind. Why would it be? What you and many other healthcare professionals may not realize is Covid-19 brought more than a deadly pandemic to our hospitals and clinics. It created an environment that gained still growing attention from cyberthieves who understand that information is money, and healthcare organizations today store a lot of sensitive patient data. Of course, cyber threats are nothing new to healthcare, but the deliberate targeting of smaller organizations that have proven themselves to be less protected is becoming more of a focus, and there are multiple reasons why.

Aside from the HIPAA requirements that require regular security assessments, there is no stipulation that medical practices must implement any of the resulting recommendations. By and large, this has become just a matter of checking some HIPAA boxes and nothing more. The fact is, many healthcare professionals don't want to spend their valuable time thinking about technology unrelated to patient care. The unfortunate consequence is most practices remain underprotected or without any cybersecurity at all. Even the largest healthcare organizations only devote 3 to 4 percent of their IT budgets to security, which is far below any other industry standard and speaks to why hackers are making them their new target choices.[1] When a practice is hit, it is beyond devastating and can often mean the closure of a business that took years to build. Fortunately, once we get through more of this dark tunnel of security incident awareness, there is some light waiting for you at the end.

1 https://www.fiercehealthcare.com/tech/industry-voices-how-hospitals-can-gain-upper-hand-against-hackers-amid-covid-19

The Pains of a Security Incident

Many healthcare leaders hear words like downtime or ransomware and think, "That sounds pretty bad but who would want to attack us?" First of all, when a security incident hits your operation, it can be far worse than you could have ever imagined. Secondly, cyberattacks are not the only kind of security risks your practice may face. Let's start this section by defining what a security incident is:

> Security Incident - An event that may indicate that an organization's systems or data have been compromised.[2]

These events can include a broad range of possible vulnerabilities that aren't always intentional. Still, significant incidents are especially devastating to smaller practices that aren't sitting on billions in revenue every year. A 2019 IBM Data Breach study found that medical organizations of less than 500 people suffered an average loss of $2.5 million post-breach.[3] It can be difficult to fathom how even a major security incident can add up to millions in such a short time. The reality is there are multiple factors contributing to such losses that are difficult to comprehend without going through a breach yourself. Our intention is to help you preview and anticipate threats so you never have to experience them in your organization

2 https://whatis.techtarget.com/definition/security-incident

3 https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

DOWNTIME

In healthcare, downtime takes on another level of concern apart from other industries, considering the well-being of your patients can become compromised. Because you can never predict precisely when your systems will fail, you can't exactly schedule around it. It's important to remember how much of your organization is dependent on operational security. An inability to access your electronic health record (EHR) software alone can cause multiple ongoing issues, even after you're up and running again. Worse still, when an incident occurs, there's no telling how long your practice will be out of commission. This uncertainty can shake the trust of even your most long-standing patients and can lead to losing them to other practices. Obviously, during periods of downtime, your ability to generate revenue is ground to a halt, which is where the cost of the incident begins. Unfortunately, it doesn't stop there.

RECOVERY

Another costly aspect of downtime is the recovery process. Depending on your preparedness for a security incident, your recovery time will vary. If you are handling your IT internally and have postponed implementing proper security measures, you will likely need the help of an external company to get you back online more quickly. Emergency IT repairs are far more expensive than outsourcing preventative security recommendations and maintenance to keep your operation protected from security mishaps. Even with an in-house data back-up plan in place, if the incident is some kind of unforeseen disaster you could still lose everything. Naturally, this scenario can make a complete data retrieval nearly impossible and your organization may never fully recover as a result.

CYBERATTACKS

Nothing hits harder than an intentional attack on your livelihood. Cybercriminals' methods have become more sophisticated than ever, so falling victim to a malware attack is increasingly common. As the new favorite target of cyberthieves, medical practices have been hit especially hard in recent years. Since 2010, healthcare organizations suffered losses 60 percent higher than any other industry for nine years running.[4] Often, the goal is to deploy malware to steal patient data and hold it for ransom, thus the term ransomware. When information is successfully stolen, the security incident turns into a data breach and that's where the costs really begin to multiply. The point may not be to use the data for other malicious purposes, but instead bilk the practice for a certain dollar amount per file stolen. Of course, there's always a chance the hacker has time to do both as happened to a number of Florida patients in 2019.[5] The cyberthieves not only sent ransom demands to the medical organization but they also tried to extort the patients themselves with threats to release photos and personal information. That is exactly the kind of nightmare that can annihilate the reputation of a healthcare practice and shut its doors permanently.

INCREASED FUTURE RISK

Because nothing is fair about the consequences of a security breach, once a hacker has successfully infiltrated your systems, you become an even bigger future target. Just as a previously robbed corner store can gain the reputation of being an easy mark by local thieves, your organization will be known by cybercriminals. It is not uncommon for the same practice to have to ward off hackers for months after a successful cyberattack. If a healthcare facility is fortunate enough to survive a major breach, they will find themselves investing in all the security measures they put off prior to the attack just to fend off further attempts. We've all experienced moments of reflection where we know we could have done something differently, but hopefully not to a massive scale with millions of dollars lost.

4 https://www.ibm.com/security/digital-assets/cost-data-breach-report/#

5 https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats

Identifying Risks

Before you can begin to protect your organization by mitigating risk factors, you need to understand what they look like. As mentioned above, security incidents vary in scale and aren't always malicious. Sometimes an organization is left vulnerable through no fault of their own and the prevention lies in how you've secured your data. Other times, there may indeed be criminals targeting you and that takes further preparation to guard against. This section will underscore the difference between a security incident versus a data breach and identify common risks for each.

Security Incidents

Risks that may compromise the security of your data are plentiful and sometimes don't involve human error in any way. While many of these threats are less common, they do occur in multiple medical practices each year and should be addressed. The important takeaway here is to identify some less reported risks that still warrant simple preventative measures.

NATURAL DISASTERS

Living in the Pacific Northwest (PNW) is beautiful and most of us wouldn't want to be anywhere else. Because so much of our terrain is set directly on top of the Cascadia fault line, protecting against the possibility of natural disaster driven security incidents is a wise decision. We've all experienced the steady increase in wildfires and saw how affected urban areas were this last Summer and Fall. Flooding is also an increasing risk in many areas of the PNW with erratic rainfall and melting mountain tops. And let's not forget all the massive trees that loom over buildings and might topple under certain conditions, like an ice storm. If your practice happens to be in the path of mother nature acting out, this would certainly constitute a security incident because all of your patient data becomes vulnerable and may be compromised.

REGULAR DISASTERS

Security incidents are more likely to be caused by common disasters rather than giant environmental events. Fires happen for a variety of reasons that cannot be predicted or necessarily prevented. There may be wiring issues or other electrical mishaps that can lead to a medical building succumbing to fire. Pipes burst and other plumbing issues routinely cause flooding and can stop a practice in its tracks. No matter what form a regular disaster takes, it is still a disaster and definitely poses an underlying threat to your patient data.

POOR SERVER STORAGE

Healthcare organizations are focused on treating patients and always want to maximize their space with that goal in mind. Often, that means server storage can become an annoying necessity that requires creativity to find room. We've seen it all. Servers get stuffed inside closets with water heaters, utility rooms next to mop sinks, or directly in the path of automatic sprinklers systems, just to name a few. This kind of storage decision can pose a serious threat to patient data because it only takes a small mishap to cause massive damage to your servers and associated data.

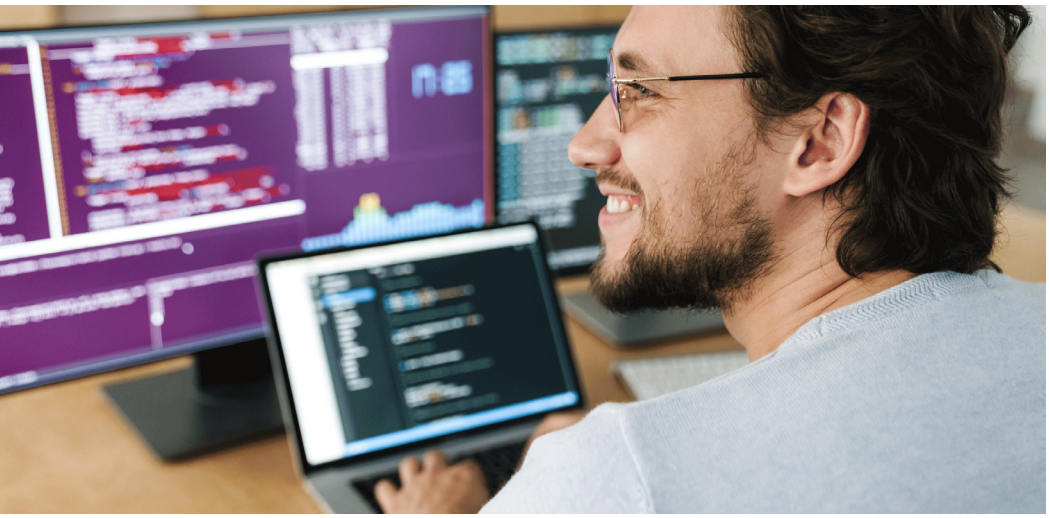
When Security Incidents become a Breach

While every breach is considered a security incident, not every security incident will become a breach. A breach is determined to have occurred when your data has been compromised long enough for encryption efforts to advance. Generally speaking, there are several indicators like those listed in the "Pains of a Security Incident" section that can identify in real time if a breach has taken place. There are incidents, however, in which a hacker may gain access to your network for only a short time before other security measures intervene to protect your data. This would likely not be considered a breach because the cyberthieves didn't have an opportunity to do more harm. That said, If there is an incident in which data may have been accessed and you're not certain if encryption was possible, your practice must assume the worst and treat it like a breach. The extent to which your data has been breached may result in various reporting requirements which are extremely taxing in their own right. This section will give you a peek inside some common cyberattack concerns so you can keep it from happening to your practice.

PHISHING

Most of us know enough these days not to open an email sent by a Saudi Royal Prince trying to give us money. While that is certainly a move in the right direction, attacks have become far more sophisticated and damaging. Cyberthieves are just searching for any low-hanging fruit they can find to lure an unsuspecting employee into clicking the wrong link. Today, we see phishing emails that look very official by taking on the form of popular brands with logos that are easy to recognize and not at all threatening. Because cyberattacks are so much more efficient, ransomware incidents are rising at a rapid rate. Hacking was the cause of 58 percent of the total number of breaches in 2019, impacting 36.9 million patient records.[6] It's important to remember that not every malicious link you click will lead to a data breach, but a lot of that depends on what preventative steps are taken before-hand.

6 https://www.fiercehealthcare.com/tech/number-patient-records-breached-2019-almost-tripled-from-2018-as-healthcare-faces-new-threats



OPEN REMOTE ACCESS

Like most industries, healthcare organizations have had to expand their remote work capabilities due to Covid-19. Even prior to this, there were some positions like administrators, accountants, or even doctors working after hours who may have accessed their organization's systems from home or the local coffee shop. Unfortunately, this can pose a serious security risk. When multiple parties rely on open remote access to work from outside the office, a potential door is unlocked for cybercriminals. Part of the reason is the security at the home of remote users may be lax so without additional measures in place to secure your environment, your organization may be a sitting duck for hackers.

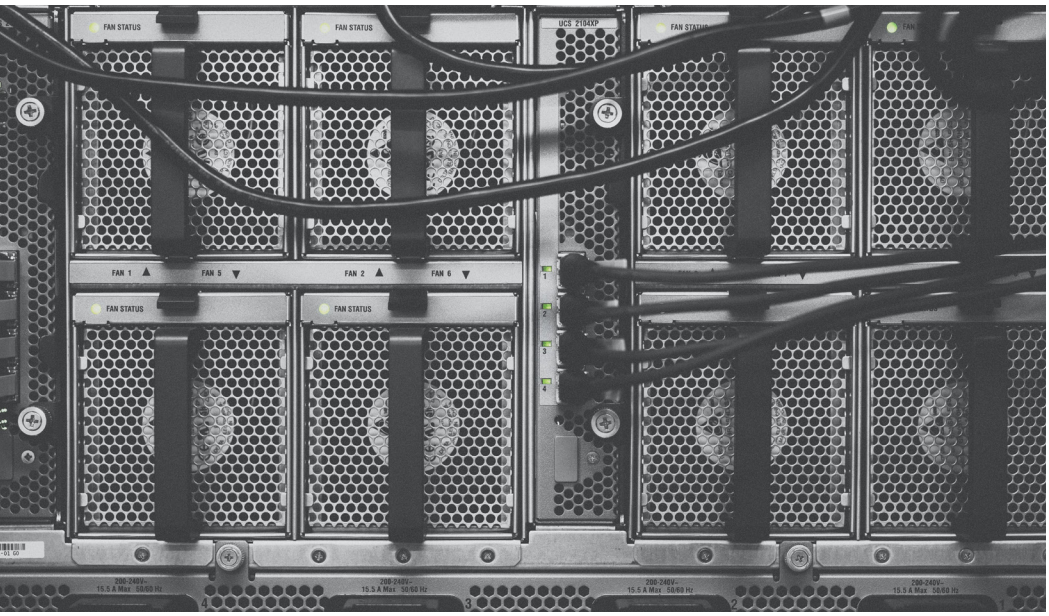
INAPPROPRIATE SECURITY PERMISSIONS

This is an all too common occurrence within multiple organizations trying to handle their IT needs internally. When a new staff member joins your team, the process by which you give them permissions to access your networks may open you up to major security issues. Should a new employee be onboarded with broad permissions that are linked to multiple files and departments operating outside their role, a hacker can do extensive damage. If that staff member finds one of those sophisticated phishing emails waiting in their inbox, one click could mean your whole system is not only down but compromised. This is far from hyperbole. For example, there is a prominent ransomware campaign called REvil that actively exploits this kind of vulnerability. Once their attacks have breached the network via a single staff member, they steal credentials, elevate privileges, and move laterally across the system before installing malware to maximize impact.[7] Ensuring your staff has only appropriate permissions helps to mitigate this threat dramatically.

7 https://www.fiercehealthcare.com/tech/microsoft-warns-hospitals-sophisticated-ransomware-attacks-targeting-remote-workforce

Reporting Requirements

On top of all the other pains associated with a breach, there is the HIPAA Breach Notification Rule.[8] Depending on the severity of the event, the requirements become more cumbersome. To start, a breach is defined by the Department of Health and Human Services (HHS) as "an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information."[9] Under every circumstance, the patient must be notified that their private data has been accessed by an unauthorized party and detail what information was included in the breach. If the stolen data impacts more than 500 people, you must then report it to relevant media outlets for the area impacted and to the HHS Secretary. From there, HHS will investigate and determine if any fines will be incurred but this process is not a quick one. There are currently over 22,000 health organizations under investigation by HHS for incurring a breach of 500 or more patients.[10] Not only is this a horrible embarrassment for you as a healthcare entity, but your organization may face stiff penalties if the investigative process finds you knew the risk and didn't do enough to prevent the breach. There is no real bright side to lean on when a breach happens so it's best to do everything possible to make sure it doesn't.



8 https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

9 https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

10 https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

lightpoint

Security Solutions

Finally! We've reached that light at the end of the tunnel you've been waiting for. The good news is, there are security solutions available for every risk we've covered and then some. In fact, that HIPAA risk assessment requirement is a good place to start. Some providers see it as an intrusive regulatory process with limited value for their operation. However, this policy is intended to protect your practice as much as your patients because the consequences of a major security incident can be so severe. The assessment leads to developing a plan and incorporating tools that will help keep your practice protected. We can't really speak for how every provider conducts their risk assessments. To give you an idea how it should go, we will breakdown our LightPoint process in greater detail.

Security Risk Assessments

Medical organizations usually undergo an annual risk audit to evaluate the security of their patient information as part of a HIPAA compliance requirement. Since healthcare has adopted so much technology to serve their patients over the years, organizations really need an IT professional evaluating systems to get the full picture. We run a three-part risk assessment that includes a technical, physical and administrative category with several practical components measured within each one and HIPAA recommendations interwoven throughout. Our methodology begins with the technical piece by identifying and documenting the location of the current electronic protected health information (ePHI) and running a network scan to flag vulnerabilities. Then we want to determine how data is stored, received, maintained, and transmitted, so we can detect any vulnerabilities and potential threats. For example, we use an assessment tool that can track every user's role-based permissions to make sure their access is appropriate and within HIPAA guidelines. While HIPAA gives no specific technological guidance on permissions, the healthcare organization must decide based on their risk audit if they are acting in compliance with the Security Rule. As for the physical

and administrative sections, we perform a manual review of all written security policies and advise recommendations to ensure they are also in line with regulations. Often, our IT expertise combined with our extensive knowledge of HIPAA allows for a clearer decision-making process. This assessment as a whole helps us to calculate the likelihood of a security incident and what the potential impact could be on your practice. All of the data we gather comes from your systems, staff, and even vendors when necessary.

The documentation you receive includes these specific areas of analysis:

Administrative

- Security Responsibility policy
- Training policies
- Mobile Device policies
- Business Associate Agreements
- User access policies
- Sanction policies
- Hiring policies (background checks, references)
- User termination policies
- Workstation use policies
- Emergency Mode Operation plan
- Physical Security plan
- Media disposal/reuse policies
- Workstation security policies
- Password policies
- Auditing/System Access Review policies
- Risk assessment policy
- Risk management policy
- Disaster Recovery plan

Physical

- Building and Office Alarms/Security Patrols
- Key Card Systems
- Security Cameras
- Server and Backup Security
- Front Desk Security
- Workstation Security
- Workstation Location
- Monitor Orientation
- Workstation Use
- Hardware Inventory Tracking

Technical

- Windows user accounts
- Windows file and folder permissions
- Windows password policies
- Windows session timeouts (auto-logoff)
- Physical location/security of systems
- Network Design
- Antivirus
- Auditing

Risk Management Plan

After the risk assessment is complete, a healthcare organization must draft a plan to address the findings within the security audit. You can either handle this internally or delegate this task to an MSP like LightPoint who can efficiently document any ePHI security weaknesses. Choosing the latter will further breakdown vulnerabilities into priority levels and give specific recommendations for how to mitigate risk and who within your organization can assist. This option also includes a suggested timeframe that reflects the urgency associated with each recommendation. LightPoint will not only show you what your practice should stop doing or change, we will explain exactly why. In our experience, most healthcare organizations do not request a professional risk management plan despite the level of risk involved. We can only surmise that this reflects a habitual rolling of the dice that so far has worked for you. Unfortunately, it only takes one successful hacker to blow up this false sense of security.

Mitigating Risk

There are multiple methods you can implement to keep your ePHI better protected. Some healthcare practices resist adding another expense, especially when it doesn't appear directly linked to patient care. After reading through the various "effects of a security incident" above, you no doubt have a good idea what a positive investment these tools really are. There is no way to measure how many breaches are averted by incorporating recommended IT security. We do, however, have data to track how medical organizations fare in the rare event hackers access networks even with regular monitoring. Research has found that small to midsize companies that fully deployed security technologies experienced half the cost of a breach. That's a difference of $2.65 million on average.[11] This savings can mean the difference between saving your practice and closing down for good. What investment could be more worthwhile?

11 https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

TOOLS AND METHODS

Managed IT Service Providers are instrumental in keeping healthcare organizations safe from would-be cyberthieves. While it is possible for a practice to handle some security measures internally, there are many software tools that are not accessible to small entities due to their size. MSPs are able to provide these premium tools and associated processes due to their scale.

Here are some of the cybersecurity perks Managed IT Services can provide:

Managed Security: MSPs provide 24/7/365 monitoring of your systems to detect any potential virtual intruder. Contracting with Managed IT Services allows you to pay a predictable monthly fee that is scalable to your needs and receive a team of IT experts to keep your patient data secure.

Backup: Data backup does what the name implies and is essential for any healthcare practice. It is literally a copy of your patient data stored somewhere else so that, in the event that data loss occurs, you are able to more quickly restore your systems to working order.

Cloud Migration: Migrating your mission critical application to the Cloud allows you to retain your data despite a ransomware attack. This greatly decreases downtime and helps expedite the recovery process which is the number one goal following any security incident.

Recovery: To ensure you meet your recovery time objective (RTO), which is an acceptable amount of time your systems can go down during an incident, you need professional IT assistance. MSPs have a large team of experts to tackle the issue that most small practices do not.

Staff Training: Because phishing attempts are so much harder to identify than ever before, your employees need ongoing training to teach them what to avoid and how to react if it happens to them. This is part of what Managed IT Services can deliver for you so you can just relax and let them handle it.

Phishing Tests: Beyond the regular training routines, MSPs perform phishing tests for your staff members to make sure they haven't forgotten what to look out for. This process keeps their awareness elevated and reduces the risk of an employee driven breach.

In Closing

Even though cybersecurity isn't always top of mind for a healthcare organization, we are living through a time in which attacks against medical practices are more aggressive and widespread than ever before. HIPAA requires that your leadership remain aware of any ePHI security risks within your network. Why not use that to your advantage? Investing in Managed IT Services to manage annual security risk assessments, plan your risk management and implement recommendations with their own tools just makes sense. You may never know how many millions of dollars you will have saved in the long run, but you will have peace of mind knowing your practice is protected. Even better, you can put all of your energy into caring for your patients and leave the technology concerns to your own team of IT experts.

LightPoint has been providing exactly this kind of high level security for healthcare practices for 20 years. We are known for our personal touch. Support calls are answered by a live person who helps resolve your issue right away. Serving thousands of users across 300+ locations means that our support model is proven, and is easily scalable to meet the needs of your practice. The most important thing to our team at LightPoint is to provide stellar service all day, everyday, so you can focus on what matters to your healthcare organization's future.

WE'D LOVE TO HELP

We aren't your typical IT team. We are highly motivated to be proactive, and to quickly resolve problems and leave you with a smile. We hire talented individuals with great communication skills and a desire to learn and grow, but most importantly, provide a stellar customer experience. We stand behind our service with a Money Back Guarantee and no annual contracts. Contact us today at info@lightpointnw.com to learn more.