Ransomware Attacks on Healthcare Organizations and How to Minimize Patient Risk

Owen Bodine
Ido Zimbelman
Christian Karabetsos

Date:

April 9th, 2023

Course title:

Public Policy Incubator PPCY 100

College:

Lake Forest College

Table of Contents

Executive Summary

Audience

This white paper looks to reach the audience that is in charge of public policy changes within the United States government. With bringing awareness to medical data breaches and offering a solution, the hope is that something will be done, legally, to make a positive change in protecting patients' private medical data.

Purpose of White Paper

This white paper looks deep into the safety, or the lack thereof, in the realm of data stored within medical organizations. The paper helps to investigate the root causes of medical data breaches and what might cause them. Medical data breaches have only been increasing in frequency, and the paper works to highlight the importance of this issue. The purposes of this white paper are to:

- Bring awareness to the issue of private and sensitive medical data being leaked and breached
- Provide a number of solutions to this issue, whilst focusing on one main solution

Findings and Conclusions

Within the research conducted for this white paper, it was found that the number of healthcare data breaches have increased dramatically over the past 10-15 years. This proposes a real issue that is at hand.

There were plenty of options the research deems plausible, when it comes to putting a halt to medical data security breaches. The options for a solution included:

- Medical organizations should ensure that all software and systems are up to date with the latest security patches and updates
- Medical Organizations should provide regular IT training to employees on cybersecurity best practices
- Create an app for users to send encrypted messages that are protected from interception and unauthorized access

Recommendation for Increasing Medical Data Security

After analyzing the possible solutions for the issue of healthcare data breaches, it is recommended that healthcare organizations should require their IT workers to meet semiannual job advancement training quotas. The training would occur twice a year, every six months. The employees would be required to partake in a four-week training course which would engage them in privacy rules and policies. They would be further instructed on technical advancements, ransomware tactics, and hackers. The training would ensure that the employees will gain practical experience, which would make them more effective workers. Due to their experience, employees would make less mistakes, which ensures greater safety for patients' data.

Furthermore, this solution is also cheap. The training program would be online, with no need for instructors that would teach in person. Instead, healthcare organizations would be able to create their own training programs with low cost because there is no need to pay for materials or for an instructor. Moreover, while employees are being trained, they would be able to keep working. It would decrease healthcare organizations' spending, whilst increasing their productivity and profits.

Addressing the Problem

(Risks of Ransomware Attacks)

In general, technological developments, such as apps, changed the world and the way people communicate. In the healthcare field, patients have increased their online communication with doctors compared to the past. For instance, telemedicine apps are being used for online communication between medical professionals and patients. These apps are not intended to replace traditional clinical visits; however, they allow patients to access pertinent information and contact medical professionals for non-emergency issues through the comfort of their phones, computers, or tablets. You no longer have to travel to a doctor in person to renew a prescription or wait on hold to schedule appointments. The simplification of telehealth communications has benefitted the general population, specifically those working full-time, having families, or living with disabilities. These technological innovations have paved the way for fewer complications and scheduling conflicts in our daily lives. Still, it has done so at a cost that might only be apparent to some who utilize and rely on healthcare applications.

If someone uses an unsecured public network for Wi-Fi or an unencrypted channel to send texts, pictures, videos, or call their healthcare provider, they risk having their information hacked. People are identified by their IP address, and when on an unsecured channel, it is easier for hackers to determine what people are searching for on the internet and what information they are giving out by entering usernames and passwords into sites. However, targeting and attacking one specific individual for medical information is difficult and time-consuming. Instead, it is easier for hackers to access patient data to sell by infiltrating a healthcare organization's server with malware. Malware allows personal information to be stolen by infecting a computer or server with a program that tracks everything someone does online and sends that information back to the hacker.[1]

Recently, several California medical groups have been notified that malware had been detected on their servers to exfiltrate the data of over 3 million patients across the state.[2] The stolen data included social security numbers, prescription data, lab test results, and diagnosis and treatment information, among other information recorded on medical organizations' servers.[3] This personal data could end up on the dark web, where hackers would sell it to the highest bidder. This fact puts innocent patients at risk of having their identity stolen or their livelihoods blackmailed.

For instance, ransomware gangs which infiltrate healthcare organizations' servers have become more prevalent in the years since the beginning of the COVID-19 pandemic. These gangs of hackers expect huge payouts from these institutions for the information that they hold hostage. They set conditions to the healthcare system that must be followed. If hospitals refuse to pay, the gangs would sell patients' information to anonymous buyers online. In 2020 alone, more than 1 in 3 healthcare organizations worldwide were hit and extorted by ransomware.[4]

Due to the extremity of hackers and ransomware extortionists, healthcare data breaches are a significant concern due to the sensitive nature of the data involved, which can include the personal and medical information of patients. The consequences of a data breach can be severe, ranging from financial losses due to fraud or identity theft to reputational damage to the organization. Furthermore, the exposure of sensitive medical information can have serious implications for patients, including loss of privacy, discrimination, and even harm to their physical or mental health. Healthcare data breaches can also result in legal consequences, such as fines or lawsuits, particularly in cases where organizations are found to have violated regulations such as the Health Insurance Portability and Accountability Act (HIPAA). Therefore, healthcare organizations must prevent and respond to data breaches to protect their patients and their own interests.

Currently, healthcare organizations are heavily dependent on the capability and proficiency of their IT department, which can prove increasingly costly as new technological innovations and ways to secure them arise. However, paying attention to the investment in proper training and relying on IT in the healthcare sector can prove even more costly. Along with losing money for stolen data, healthcare organizations can also receive severe financial penalties from HIPAA. When data violations persist or when there is systemic non-compliance with HIPAA, medical institutions can suffer from multi-million-dollar fines.[5] So, to enact a policy that regulates and enforces the specific use of data encryption on all medical information, multi-step authentication for personal accounts, and routine network and unauthorized open port checks will not only greatly benefit the livelihoods of patients but also save medical care facilities time, hassle, and money in the long run.

The phenomenon of telehealth communication has been increasing during the last few years.[6] Sometimes talking to the doctor online is much more financially profitable and saves time. Everyone loves more efficient innovations, so people would expect that their data will be secured through every aspect of healthcare service just like it would be to go to an appointment in person. However, while hospitals protect patients' date, most online apps are not protected. When people communicate with their doctors about personal health care issues, the information may reach third parties. Healthcare information contains personal data which not every patient would like to share.

The leaking of medical and personal data might decrease people's trust in the healthcare system. How can people share personal data with a system that is getting hacked so often? When less people trust the system, fewer patients would use healthcare services, and the companies would lose money.

Furthermore, a patient shortage would inevitably hurt healthcare organizations and third-party businesses associated with them. The information that would leak from the online apps could influence insurance contracts. When past diseases, injuries, and accidents of the public are available to everyone, insurance companies may use this information to cancel or change existing contracts. For instance, if an insurance company realized that one of its customers faced unknown health issues, the company could cancel the agreement between the customer and them or increase the bill that they must pay. This scenario might lead to far-reaching consequences and harm the current situation of some customers.

In addition, there are chats with doctors containing personal data that may harm patients' lives if said data is leaked. For example, in gender-related treatments, some patients have information-sensitive backgrounds. This can include families who do not accept their child's sexual identity. Some patients may face severe consequences if their gender identity is made known. Some of the possible consequences might be ostracization or sanctioning, and social abandonment. This scenario is the reality for a lot of people in the U.S., and a potential threat over every American.

Another form of personal data is mental health data. "19.86 % of adults are experiencing a mental illness. Equivalent to nearly 50 million Americans." [7]Almost 1 of 5 adults face this issue in the U.S. Due to a lack of protection, the healthcare system is not able to protect their patients' privacy.

People who have their data hacked might face the issues of being fired, facing differing insurance regulations, and may experience a worsening of their mental state. This scenario might influence 20% of the U.S. adult population. One in five adults. This issue might lower the economic state of patients, while increasing their taxes and fees charged with different services, and can change the life of every American.

While telehealth communications have provided many conveniences and many considerable benefits for its users, there are many effects that the faults of the communication services may cause. If users' data were to be hacked, leaked, and exposed, it might lead to far-reaching consequences. The exposure of data will cause countless interpersonal and individual complications among the general population of the U.S.

Implications of Maintaining the Status Quo

The status quo should not be maintained under any circumstance. The first and most surface-level consequence of personal medical data being leaked would be a widespread loss of trust amongst the general population towards many medical apps. This is the primary response to a leak of extremely sensitive medical data. People entrust confidential information to medical institutions, hospitals, and many telehealth communications apps. A direct result of this information being stolen when it was expected to be confidential would be an immediate loss of trust. People might be more hesitant to request or provide information online in the future if they were to be exposed in such a way. This may negatively affect medical institutions and those that must retrieve their data online consistently, whether due to a family situation, a work situation, or otherwise.

Beyond the loss of trust from users of telehealth communications apps, the exposure of personal medical data may have troubling effects on people's relationships, whether in the household or the workforce. Looking at the household, people may be viewed differently by their spouses or parents if some sensitive data is leaked or revealed. If a family finds out their child is attempting a gender transition, for example, some parents may not take this lightly. The parents now know information that was supposed to be private to the child, which can fracture the parent-child relationship. This is why confidentiality and security when communicating medical data are vital.

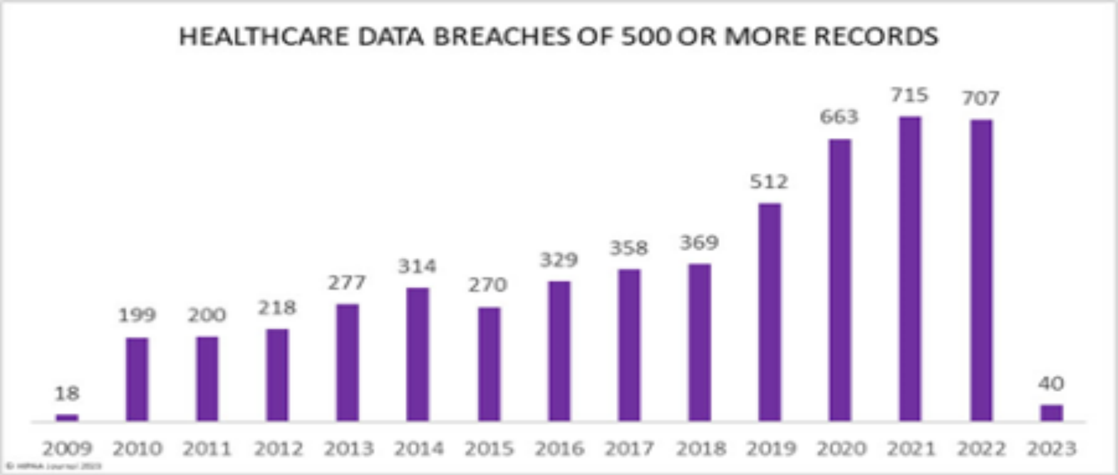
Furthermore, one can focus on how a leak of medical data may affect one's position in their job. If it is revealed that they have a specific condition or disease that is viewed negatively regarding productivity, an employer can avoid hiring this person. Most states recognize "at-will" employment, meaning they do not need to provide a specific reason for hiring or firing someone. Therefore, employers may discreetly discriminate based on one's conditions, diseases, or gender identities.

Another possible complication that could be a direct result of medical data being leaked or exposed is the possibility of harassment, both online and in person. This can affect both everyday people and large-scale celebrities. Many people are already bullied for their disabilities and illnesses, and keeping this information private, if possible, is vital to many. It is essential to reduce negative engagement and attention. If someone owns a popular online account and has sensitive information about them leaked, it can affect their reputation and how their followers view them. This is yet another reason it is so essential to protect medical information and data that is flowing through various apps.

Other more extraneous worries that could arise from unsafe and unprotected telehealth communication apps include the effect on targeted advertising or an impact on insurance rates. Marketers take advantage of any benefit they can find and will be open to advertising products to those who may find them more useful. If an inhaler company gets a hold of all people with asthma in an area, for example, they can target advertisements for those in this area. This is using sensitive medical data for monetary gain. The same can be said about insurance rates. If an insurance company finds out someone is more susceptible to passing away, they may raise their insurance rates on this person. Many effects emerge from telehealth communication apps with little protection for patients' medical data and information. There are no benefits to less medical security other than cost-cutting, therefore encouraging the upscale of cybersecurity.

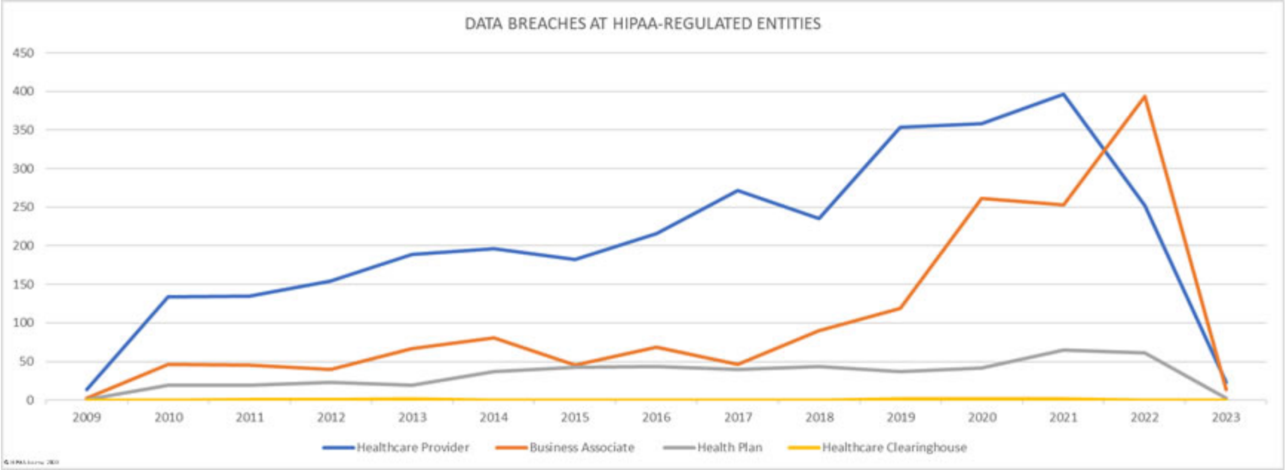
Statistics Regarding Data Breaches

As the graph below shows, every year, there are more cases of hacking. This is except for 2023, because data was only recorded at the beginning of the year (HIPPA Journal, *Healthcare Data Breaches of 500 or More Records* 2023).[8] Over the past three years alone, there have been 1,042,500 healthcare data breaches that have jeopardized the information of millions of innocent people. Evidently, the current system that the public relies on to store and maintain their health records is not being managed well enough. Clients should be protected more securely.

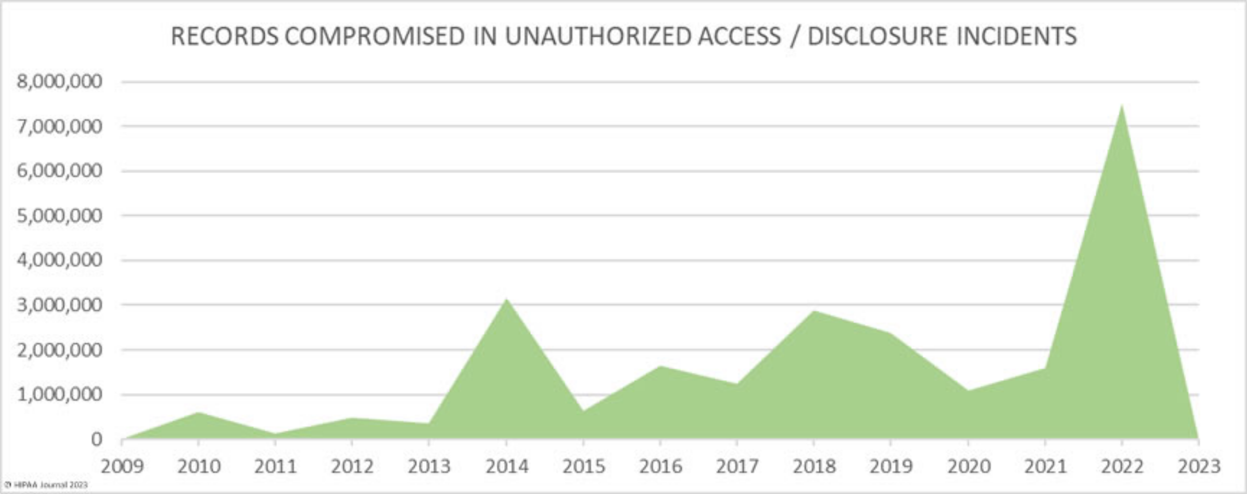


In the top 34 largest healthcare data breaches between 2009 and 2023, 23 were due to "Hacking/IT Incident." Furthermore, 14 of the 23 data breaches occurred at a business associate of a healthcare organization.[9] According to HIPPA's "Privacy Rule," a business associate to a healthcare organization is "a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity."[10] The data presented by the HIPPA journal shows that hacking incidents are the leading cause for healthcare data breaches over the past decade. Security awareness training at healthcare organizations has been getting better at reducing data breaches, but records that have been compromised in unauthorized access/disclosure incidents were at an all-time high since 2009 last year.[11]

Some of the most important training needed in the healthcare cybersecurity department is securing the supply chain.[12] Since a majority of data breaches have occurred with business associates, it is of the upmost importance for healthcare provides to diligently conduct reviews of their vendors and how they are conducting themselves in the accordance to the HIPPA Security Rule. In 2022, data breaches amongst business associates exceed those that happened at healthcare organizations in the last 14 years.[13]

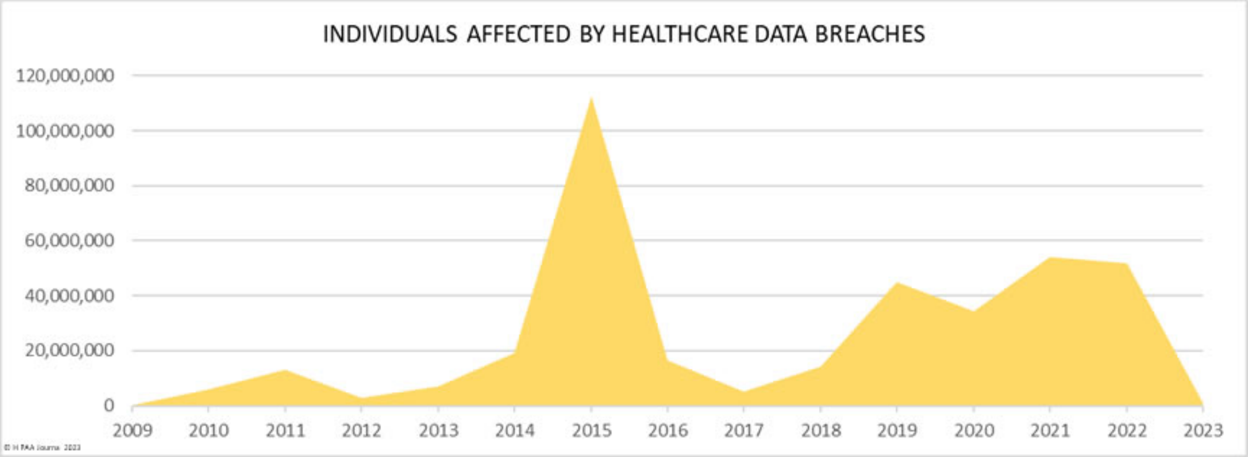


In 2020, there were approximately 1 million reported records compromised due to unauthorized access and disclosure incidents, and as of 2022, that number jumped to over 7 million. Unauthorized record access and disclosure incidents can pose significant risks to healthcare organizations and their patients. When confidential patient information is accessed or disclosed without proper authorization, it can lead to a breach of trust between the organization and its patients. This breach of trust can have profound consequences, including legal and financial penalties, loss of reputation, and erosion of patient confidence. Patients may become reluctant to share their personal health information with healthcare providers, which can hinder the delivery of quality healthcare services.



© HIPAA Journal 2023

Additionally, unauthorized record access and disclosure incidents can result in identity theft, insurance fraud, and other types of cybercrime. There has been a general upward trend in the number of records exposed each year, with a massive increase in 2015.[14] When sensitive patient information, such as social security numbers, medical histories, and insurance information, falls into the wrong hands, it can be used to commit fraud or other criminal activities. This can harm patients and result in financial losses for the organization. Healthcare organizations must take proactive steps to protect their patient data from unauthorized access and disclosure, including implementing robust security protocols, providing regular employee training, and conducting thorough risk assessments to identify potential vulnerabilities.



Options to Ease the Increase of Ransomware Attacks

IT workers can take several measures to avoid hacking occurrences and protect their organization's data and systems. Healthcare organizations should ensure that all software and systems are up to date with the latest security patches and updates. Outdated software can leave vulnerabilities that hackers can exploit. Additionally, they should encourage employees to use strong passwords and two-factor authentication to access sensitive data. Strong passwords should be unique, long, and complex, and employees should avoid using the same password across multiple accounts.

Moreover, IT workers should conduct regular security audits to identify potential vulnerabilities and take steps to address them. They should provide regular training to employees on cybersecurity best practices, such as how to recognize phishing emails and how to avoid clicking on suspicious links. IT workers should also implement access controls to restrict access to sensitive data to only those employees who need it to perform their job duties. This can help to prevent unauthorized access to data. Moreover, they should monitor network activity for unusual or suspicious activity, which could indicate a hacking attempt. It is important to recognize that cybersecurity threats are constantly evolving, and IT workers should stay up to date on the latest threats and best practices for protecting against them. By implementing these measures and staying vigilant, IT workers can help to prevent hacking occurrences and protect their organization's data and systems.

Healthcare practitioners already have a standard amount of continuing education units depending on the state where they are employed. The same should go for those who work in the IT department for hospitals. Ransomware attacks on healthcare serves have only gotten more intricate as time goes on, and with continual updated education courses for IT professionals it will be easy to detect potential threats. Standard training hours can also keep employees sharp and remind them of basic practices that can sometimes be overlooked by natural human error. For instance, in 2020 there were over 500,000 records exposed in improper disposal incidents, like records not being sent to shredding and data abandonment.[15] Through research, nothing could be found that states there are current training hours required of IT managers and technicians. By setting a workplace standard for required training hours per quarter completed by healthcare organizations' IT departments, it could lessen potential data breaches and data disposal leaks. Regular training can help aid in the protection of patient data through "routine network and unauthorized open port checks and eliminating Shadow IT environments developed as workarounds."[16] Simple cyber security diligence will not only greatly benefit the livelihoods of patients but also save medical care facilities time, hassle, and money in the long run.

Some organizations and companies like HIPPA, “the Health Insurance Portability and Accountability Act of 1996 set national standards for protecting patient privacy,” had established encrypted methods to communicate with doctors. Doctors might use encrypted systems wrong, or respond to their clints on text messages, which is an unencrypted system. “In general, text messages are not encrypted, which means that they can be intercepted and read by unauthorized parties. Additionally, text messages can be sent over public Wi-Fi, which is not a secure network. This makes text messaging a risky way to transmit sensitive patient information.”[17] For instance, “iPlum,” which “allows users to send encrypted messages that are protected from interception and unauthorized access.” This app could be the solution to this problem. The iPlum app ensures the encryption of the patients’ data. When data is encrypted, it is much harder to hack it.

However, the most common cause for hacking, as appears from the following graph, is employee mistakes.[18] It is this team’s assumption that enacting a standard of training hours for staff that handle sensitive patient information will decrease a substantial portion of healthcare data breaches. It is recommended that IT workers in the healthcare field should be required to meet semiannual job advancement training quotas. Twice a year, these employees will partake in a four-week training course where they will be briefed on surface-level issues to be aware of and instructed on upcoming technical advancements and ransomware tactics. Employees will gain more practical experience and can learn how to perform their job duties effectively and efficiently by practicing them on the job, which ensures greater safety for patient data. On-the-job training can also be cost-effective for healthcare organizations because there is no need to pay for materials or an instructor, and employees can continue to work while they are being trained.

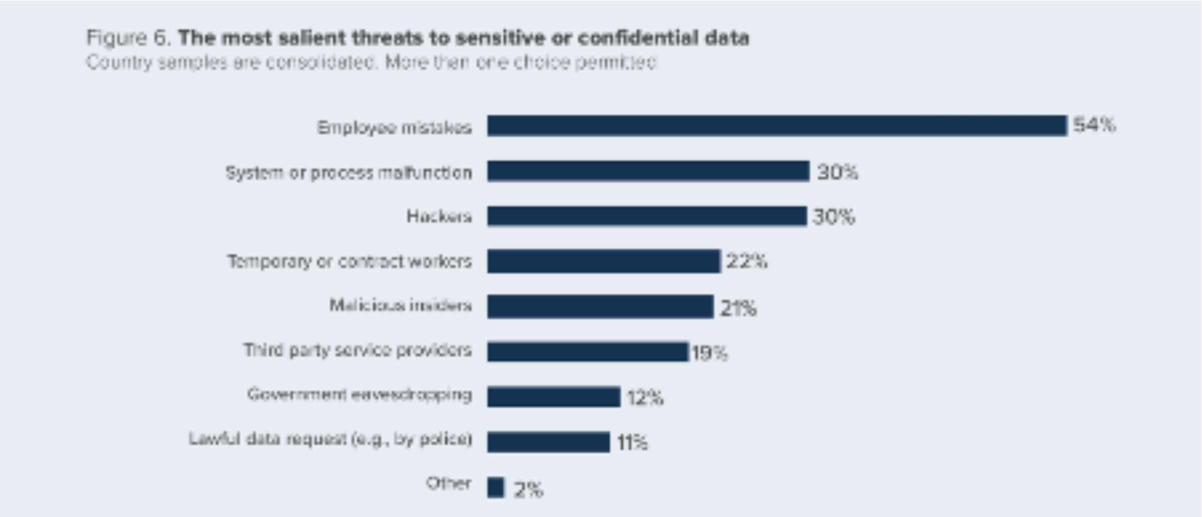


Figure 6. **The most salient threats to sensitive or confidential data**

Country samples are consolidated. More than one choice permitted

One cannot expect the public to be aware of the risks that are mentioned. There are too many people with diverse backgrounds, so the ambition to educate them is not realistic. However, this can inform the doctors about these risks and make sure they are not communicating with their patients by text or any other potentially vulnerable system.

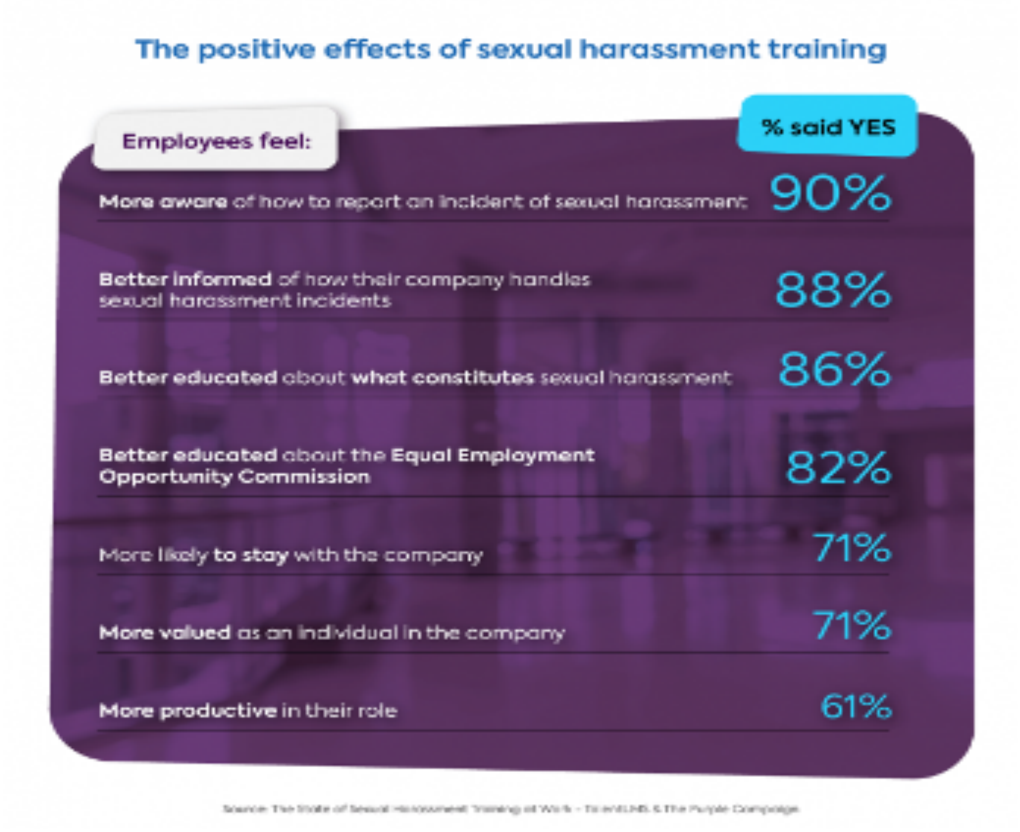
Recommended Solution to Decrease Healthcare Data Breaches

This solution is intended to build a proficient level of training for doctors. Healthcare IT has revolutionized healthcare organizations by creating a system designed to store, share, and analyze data that has been collected. It has also opened the door for an ever increasingly critical position of IT technician. Millions of people rely on healthcare IT to keep their data protected; medical records are safely stored within the organization's confines, including their servers. Many healthcare organizations offer apps that their patients can use which will transfer their medical and personal information directly to the organization's healthcare data collection system. Since patient information is stored digitally now, and that since the pandemic hacking event have been steadily increasing, it is pertinent to require standard IT training hours and continuing education opportunities for healthcare organizations and its business associates.

Most of the training hours could be completed and taken online. Online IT training has become increasingly popular due to its flexibility, convenience, and accessibility. The technical employees would be able to complete their training anywhere- their homes, offices, and even vacations. Online IT training can be scaled to meet the needs of many employees. Organizations can train all their employees at the same time, without having to worry about space limitations or scheduling conflicts. Online IT training can be customized to meet the unique needs of an organization or employee which means that training can be tailored to the specific skills and knowledge required to identify potential hacking risks. The training would include relevant information to avoid healthcare employees’ future mistakes regarding the privacy of their patients. The plan is to enforce it by legislation, passing a bill.

How IT Advancement Training Can Benefit Organizations, Employees, and Patients

There are many examples of workplaces that use training programs to educate and prevent behaviors and phenomena of the employees. For instance, Sexual Harassment Prevention Training Program. As it appears from the following graph, training program has a positive impact on the employees:



The positive effects of sexual harassment training

Employees feel:	% said YES
More aware of how to report an incident of sexual harassment	90%
Better informed of how their company handles sexual harassment incidents	88%
Better educated about **what constitutes** sexual harassment	86%
Better educated about the **Equal Employment Opportunity Commission**	82%
More likely **to stay** with the company	71%
More valued as an individual in the company	71%
More productive in their role	61%

Source: The State of Sexual Harassment Training at Work – TalentLMS & The Purple Campaign

“With more than 80% of employees saying that their sexual harassment training left them better informed about how their company handles sexual harassment, better educated about what constitutes sexual harassment, and feeling safer at work, this survey demonstrates that training is a powerful way for employers to reduce instances of sexual harassment by establishing shared norms and improving understanding about the type of conduct that is acceptable in the workplace.”[19] Job training can be incredibly beneficial for employees, as it provides them with the knowledge and skills they need to perform their job duties effectively. When employees receive job training, they become more confident in their abilities, which can lead to increased job satisfaction and motivation. Additionally, job training can provide employees with the opportunity to acquire new skills and knowledge, which can lead to career advancement opportunities and increased job security. By improving their job performance, employees can also contribute to the overall success of the organization, which can lead to increased job stability and growth opportunities.

Another way that job training can help employees is by reducing stress in the workplace. When employees feel confident in their abilities to perform their job duties, they are less likely to experience stress and anxiety related to work. Additionally, job training can provide employees with the tools and resources they need to manage their workload effectively, which can help to prevent burnout and other types of stress-related health problems. By investing in job training for their employees, organizations can help to create a healthier and more productive work environment, which can benefit everyone involved.

Healthcare IT is a rapidly evolving field, and to keep up with the latest advancements and technologies, IT professionals in this industry must undergo continuous training and development. By investing in IT training programs, healthcare organizations can ensure that their IT staff is equipped with the necessary skills and knowledge to stay up-to-date and proficient in their roles. “Employees who receive high quality training from their organization also work in organizations that are significantly more likely to provide a work environment conducive to helping retain staff (Table 4).”[20] Providing IT training can also help healthcare organizations retain their IT employees by offering them a clear path for career development and advancement. Employees who feel that their employer is invested in their professional growth and development are more likely to remain with the organization and be motivated to perform their job duties to the best of their abilities.

Moreover, IT training programs can also help healthcare IT employees feel more engaged and satisfied with their work. Learning new skills and technologies can be challenging and rewarding, and the sense of accomplishment that comes with mastering new concepts can be a powerful motivator. IT employees who are engaged and satisfied with their work are more likely to stay with their organization, reducing employee turnover and related costs. Overall, investing in IT training programs is a smart strategy for healthcare organizations looking to retain their IT talent, remain competitive in the industry, and ensure that they are providing the best possible patient care.

Costs of Implementing IT Training Standards

Implementing IT training for healthcare employees can be a significant investment for healthcare organizations. The costs associated with IT training can include expenses such as the development and delivery of training materials, hiring trainers, and providing time off for employees to attend training sessions. Additionally, healthcare organizations may need to invest in new software or hardware to support the training, such as simulation software or hardware to simulate electronic health records. The costs can also include indirect expenses such as lost productivity during the training period, as employees may need to take time off from their regular duties to attend training sessions. Despite these costs, healthcare organizations must recognize that the long-term benefits of IT training, including increased employee retention and improved patient care, outweigh the initial investment in IT training programs. By investing in the development of their IT staff, healthcare organizations can stay competitive and keep up with the ever-changing landscape of healthcare IT.

Any change or implementation of workplace advancement will result in costs, that might lead to opposition. However, the solution does not necessarily require a lot of money. A quick search of "healthcare IT training courses," will bring up a plethora of cost-effective sources to better educate IT staff. Online IT training can be an affordable option for healthcare organizations, as it eliminates the need for travel and accommodations associated with traditional in-person training. Additionally, many online training programs offer flexible payment options, such as pay-per-course or subscription-based models, which can be more cost-effective than traditional training programs. Furthermore, online training can help to reduce the need for hiring external IT consultants or experts, as IT staff can develop the necessary skills and knowledge in-house. Also, it is possible to create a training program based on the specific topic and values. By investing in online training for their IT staff, healthcare organizations can improve their overall cybersecurity posture and ensure that their staff have the skills and knowledge required to effectively protect their patients' sensitive data.

How to Evaluate the Success of Standard IT Training Hours

While all of this information is useful for understanding the scope and nature of the problem, one must look at how the effectiveness of measures to prevent and respond to data breaches can be evaluated. One way to do so is through the analysis of incident response plans and their implementation. Incident response plans outline the steps that an organization will take in the event of a data breach, and evaluating the effectiveness of these plans can help to identify areas for improvement. For example, organizations can conduct simulations or tabletop exercises to test their incident response plans and identify any weaknesses or gaps that need to be addressed.

Another way to evaluate the effectiveness of measures to prevent and respond to data breaches is through the analysis of security controls and risk management practices. Organizations can conduct regular security assessments and audits to identify vulnerabilities in their systems and processes and implement controls to mitigate these risks. Additionally, organizations can monitor their systems for suspicious activity and implement advanced security technologies such as intrusion detection and prevention systems. Evaluating the effectiveness of these measures can help organizations to identify areas for improvement and ensure that their systems and processes are secure and resilient.

Finally, the effectiveness of measures to prevent and respond to healthcare data breaches can be evaluated through the analysis of compliance with regulations and standards such as HIPAA. Compliance with these regulations and standards is essential for protecting patient data and avoiding legal consequences. Organizations can conduct regular audits and assessments to ensure that they are in compliance with these regulations and standards and implement corrective actions when necessary. By evaluating compliance with regulations and standards, organizations can ensure that their data security practices are up-to-date and effective in protecting patient data.

Conclusion

Healthcare organizations can benefit greatly from implementing on the job training for their IT workers. With the ever-evolving nature of technology, it is essential for IT workers to stay up to date with the latest skills and knowledge required to effectively protect their organization's data and systems from security threats. On the job training can help IT workers to develop these skills and stay current with industry best practices, while also providing opportunities for them to apply their learning in a real-world setting.

By investing in on-the-job training, healthcare organizations can improve their overall cybersecurity posture and reduce the risk of data breaches and other security incidents. Additionally, providing training opportunities can help to increase employee satisfaction and retention, as IT workers will feel more valued and invested in their role within the organization.

Overall, the implementation of on-the-job training for IT workers is a critical step towards ensuring the security and success of healthcare organizations in today's digital age. By prioritizing training and investing in their IT workforce, healthcare organizations can better protect their patients' sensitive data and maintain the trust and confidence of their stakeholders.

Works Cited

[1] Looper, Christian de. "How Hackers Are Really Getting Your Data, and What You Can Do to Keep It Safe." TechRadar. TechRadar, June 20, 2016. https://www.techradar.com/news/internet/how-hackers-are-really-getting-your-information-and-what-you-can-do-to-keep-it-safe-1323706

[2] Hardcastle, Jessica Lyons. "Ransomware Crooks Steal 3M+ Patients' Sensitive Info." The Register® - Biting the hand that feeds IT. The Register, February 11, 2023. https://www.theregister.com/2023/02/11/ransomware_regal_medical_group/.

[3] Hardcastle, Jessica Lyons

[4] Weiner, Stacy, and Senior Staff Writer. "The Growing Threat of Ransomware Attacks on Hospitals." AAMC, July 20, 2021. https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals.

[5] "Healthcare Data Breach Statistics." HIPAA Journal, February 3, 2023. https://www.hipaajournal.com/healthcare-data-breach-statistics/.

[6] Ryan, Benjamin. "Emailing Your Doctor May Carry a Fee." The New York Times. The New York Times, January 24, 2023. https://www.nytimes.com/2023/01/24/health/emails-billing-doctors-patients.html.

[7] "Adult Data 2022." *Mental Health America*, https://mhanational.org/issues/2022/mental-health-america-adult data.

[8] Healthcare Data Breach Statistics. (2023, March 22). Retrieved April 08, 2023, from https://www.hipaajournal.com/healthcare-data-breach-statistics/

Healthcare Data Breaches of 500 or More Records

[9] "Healthcare Data Breach Statistics," HIPAA Journal, February 23, 2023, https://www.hipaajournal.com/healthcare-data-breach-statistics/, *Largest Healthcare Data Breaches (2009-2023).*

[10] Office for Civil Rights (OCR), "Business Associates," HHS.gov, June 28, 2021, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html.

[11] "Healthcare Data Breach Statistics," HIPAA Journal, February 23, 2023, https://www.hipaajournal.com/healthcare-data-breach-statistics/, *Records Compromised in Unauthorized Access/Disclosure Incidents.*

[12] Healthcare Data Breach Statistics," HIPAA Journal, February 23, 2023, https://www.hipaajournal.com/healthcare-data-breach-statistics/, *Healthcare Data Breaches by HIPAA-Regulated Entity Type.*

[13] Healthcare Data Breach Statistics," HIPAA Journal, February 23, 2023, https://www.hipaajournal.com/healthcare-data-breach-statistics/, *Data Breaches at HIPPA-Regulated Entities.*

[14] "Healthcare Data Breach Statistics," HIPAA Journal, February 23, 2023, https://www.hipaajournal.com/healthcare-data-breach-statistics/, *Individuals Affected by Healthcare Data Breaches*

[15] "Healthcare Data Breach Statistics," HIPAA Journal, February 23, 2023, https://www.hipaajournal.com/healthcare-data-breach-statistics/, *Records Exposed in Improper Disposal Incidents.*

[16] "Healthcare Data Breach Statistics," HIPAA Journal, February 23, 2023, https://www.hipaajournal.com/healthcare-data-breach-statistics/, *How can healthcare organizations mitigate data breaches?*

[17] Staff, K. (2023, March 31). Secure messaging apps: The future of HIPAA-compliant communication in healthcare. Retrieved April 09, 2023, from https://knowtechie.com/secure-messaging-apps-the-future-of-hipaa-compliant-communication-in-healthcare/

[18] Chris Brook on Monday August 22, Mullins, C., Fischer, T., & Brook, C. (n.d.). 45 percent of orgs have encryption plans in place. Retrieved April 08, 2023, from https://www.digitalguardian.com/blog/45-percent-orgs-have-encryption-plan-place

[19] The state of employee sexual harassment training - 2021 survey. (2022, April 18). Retrieved April 09, 2023, from https://www.talentlms.com/employee-harassment-training#h-the-facts-about-sexual-harassment-training-who-what-and-how-often

[20] Acton, T., & Golden, W. (2002, June). Training: The Way to Retain Valuable IT Employees? Retrieved April 08, 2023, from https://www.researchgate.net/profile/Thomas-Acton-2/publication/228695288_Training_The_way_to_retain_valuable_IT_employees/links/00b49519f29d74f2ee000000/Training-The-way-to-retain-valuable-IT-employees.pdf