**Sahm Ahmed**

**Montclair State University**

**CSIT 100\_12**

**April 7, 2025**

**Cybersecurity in the Healthcare Industry: Protecting Patient Data**

The healthcare industry has followed the pace of technology. From internet-based health websites to smart appliances measuring heartbeats and sleep rhythms, medicine is growing more digital every day. Hospitals, clinics, and private practitioners today depend on technology for almost everything - from patient data storage to procedure scheduling, disease diagnosis, and even consulting other doctors. It makes healthcare easy and accessible but vulnerable to as dangerous as cyber attacks. Information is as currency or even more valuable in the current era. All this renders medical information an unmatched target of cybercrime attack.

Medical records also hold every kind of personal, medical, and financial information that can be used by hackers as a means of identity theft, insurance fraud, or blackmail. A stolen credit card number can be revoked and replaced. But a medical record? Information like that goes with a person for life. This renders patient data one of the most lucrative information on the black market of the internet. Consequently, healthcare cybersecurity is not just a technology issue - it's a public health issue. When a hospital network is breached, people's personal data can be stolen, treatments delayed, surgeries postponed, and trust in the healthcare system lost. This essay will address why cybersecurity is so important in healthcare, the types of threats hospitals face, real examples of cyberattacks, and how to protect patient information. Start with the most apparent: health information is private.

It contains names, addresses, Social Security numbers, insurance data, medical history, and even mental health history. That's gold for anyone looking to steal someone's identity or create false claims for fake insurance. Cybersecurity experts estimate one electronic health record can sell on the dark web for hundreds of dollars - dozens of times what a credit card number will fetch. And beyond that, clinics and hospitals are sitting ducks since many of them lag behind the times when it comes to cybersecurity. Healthcare workers would rather attend to patients than invest in upgrading their IT systems.

It is not really surprising, patient care must come first, but by doing so it does provide these establishments with the look of low-hanging fruit for the hackers. Certain healthcare providers still use antiquated software or lack adequate firewalls, making it more convenient for hackers to get in. There are a variety of cybersecurity threats that healthcare providers should know about. Some are industry-independent, and others are more specific to healthcare. Below are some of the most significant ones:

1. Ransomware: One of the most crippling types of attack. During a ransomware attack, hackers encrypt the data of a hospital - patient information, test results, and schedules - and demand payment (usually in cryptocurrency) to decipher it. A ransomware attack hit the University of Vermont Health Network in 2020, which burned for weeks. They had to reschedule treatments and revert to paper records.

2. Phishing Attacks: Phishing is when a hacker gets someone to click on a malicious link or open a malicious attachment, usually through email. The second it's clicked, the hacker is into the hospital's network. Physicians, nurses, and administrative personnel are bombarded with hundreds of emails every day, so it's easy to unknowingly click on something that looks real but isn't. One click can cause a serious breach.

3. Insider Threats: Not all threats are always from the outside. Sometimes an insider already working within the hospital - whether as an employee or contractor - abuses their position. It may be intentional, i.e., selling out patient information, or unintentional, such as clicking the link to access a phishing message. Either way, insider threats may be equally destructive as those hacking attempts.

4. Legacy Systems: Most of the hospitals possess aged systems that don't receive routine update or security patches. Those vulnerable systems possess loopholes which the hackers target. Most healthcare organizations possess blends of old and new technology, and this further complicates protecting the system.

These threats aren't theoretical - they've occurred. The largest health care cyber breach took place in 2015, when hackers invaded Anthem Inc., which is among the largest health insurance companies in the United States. They accessed nearly 80 million people's personal data, including names, dates of birth, Social Security numbers, and employment information. Anthem incurred a massive penalty and paid millions of dollars for victim identity protection.

And then in 2017, there was another huge attack with the global WannaCry ransomware attack. The cyber attack affected hundreds of organizations across over 150 countries, worst being the UK's National Health Service. The hospitals canceled thousands of appointments, redirected ambulances, and even closed down entire departments. The NHS was targeted because it was using old operating systems that were not being updated. These cases just go to show how calamitous healthcare cyberattacks can be. They not only cost money, they also jeopardize patients' lives, too. When people hear the word "cyberattack," they think of money. And indeed, data breaches are extremely costly to hospitals. But the damage does not end there. If the infrastructure of a hospital breaks down, then it can postpone surgery, hamper treatments, or result in misdiagnosis. Physicians cannot readily call up patient records or test results, and that would degrade the quality of care. Patients already sense something horrific is happening to them might now have to experience that additional fear of their private information becoming public. A number of studies have established that once trust has been lost, it is difficult to regain momentum. Health care professionals are also impacted. Doctors and nurses must contend with the aggravation of having to work within a dysfunctional system. IT personnel must scramble to repair the damage. The entire organization is impacted.

There are regulations in the United States to protect patient data. The most recognized one is the Health Insurance Portability and Accountability Act (HIPAA). HIPAA establishes the standards that the patient data should be treated by healthcare providers. HIPAA mandates organizations to have physical, network, and process security. One can be fined heavily or even incarcerated for breaching HIPAA.

HITECH Act, yet another milestone legislation, prompted health-care providers to opt for electronic records and strengthened HIPAA regulations further. It increased the fine for data breaches and mandates them to report such incidents to their patients in the event of such breach with regard to patients' data.

Such standards are required but will only apply if they are being adhered to by the organizations. Healthcare professionals must be serious about taking cybersecurity into account and not thinking of it as a tick-in-the-box type of scenario.

The good news is that a few options are available to protect patient data. Yet, it involves effort, funds, and organization. Following are some of the steps that must be done by healthcare professionals:

1. Training Staff

Each organizational member - doctors, nurses, administrative staff - should receive training on detecting cyber attacks. That implies detection of phishing e-mails, protection of passwords, and notification of suspicious stuff.

2. Multi-Factor Authentication

Incorporating MFA adds one more layer of security. Even if the password is compromised, it is impossible for the perpetrator to gain access without a second form of identification, like a code sent through text to a phone.

3. Encrypt Data

Encryption makes information unreadable without a unique key. Encrypting patient information, both storage and transmission, makes it worth less to hackers if they obtain it.

4. Update Systems

Patches and software updates are continually being issued to close security loopholes. Failure to update systems is equivalent to leaving the front door open to hackers.

5. Restrict Access

Not all employees require access to all. Role-based access controls restrict workers to the data they require to perform their function.

6. Have a Security Incident Response Plan

The hospital must have a plan in place for what to do if a cyber attack occurs. That will trigger a response and reduce the damage.

Most people believe that cybersecurity is someone else's responsibility, the IT department's, but the reality is, it's everybody's job. Sure, IT staff are definitely in the trenches, but they architect and implement secure systems, scan for anything abnormal, and react when something does occur.

They also need to make sure security technologies don't get in the way of patient care. For example, if a procedure is ungainly or too slow, physicians will somehow get around it in a manner that will be generating more security issues. It's one of the toughest aspects of healthcare IT: finding a balance between usability and security.

Technology doesn't stay still, nor do threats in the virtual world. And that is the same reason that new tools are being built to combat them. Artificial Intelligence and Machine Learning are also becoming part of play in identifying irregular action that might foreshadow a cyberattack.

It's able to sense patterns that can fly under the radar of people. Blockchain is even on the drawing board. It's an approach to documenting data that is extremely secure and very difficult to tamper with. Blockchain even has some thinkers hoping that it will be the key to safely keeping health records. And then there's the Internet of Medical Things - smart, networked medical devices such as insulin pumps or wearable heart monitors. They're incredibly valuable, but they need robust cybersecurity because they can be easily hacked just like a computer. Another threat to healthcare cybersecurity is the growing practice of telemedicine. With the COVID-19 pandemic, it became the norm to visit doctors through video calls. Although it was very convenient for patients who could not physically be at the clinic, it also opened new doors to hackers. Video calls, online websites, and digital prescriptions all need secure links. Without a secure telemedicine platform, private conversations between doctors and patients would be vulnerable. It's critical that as telemedicine continues to expand, cybersecurity continues to follow.

Healthcare organizations also must share more. Cybersecurity cannot be solved by one hospital by itself. By disclosing intelligence on new threats, security reactions, and lessons from previous attacks, other sites can avoid making the same mistakes. Governments and private enterprise need to collaborate as partners to build more formidable defenses. Some of these hackers are coordinating their efforts in groups within nations, so it makes sense that healthcare systems need to be doing the same.

Collaboration is the key to a safe healthcare system for all. The other significant aspect of healthcare cybersecurity that is typically neglected is patient awareness.

Whereas much attention is being put on hospitals, physicians, and IT staff, patients too must do their part in securing their health information. Few individuals are aware of how much personal information they are giving when they fill out online surveys, utilize health apps on their phones, or even post about their health on Twitter. For instance, there are applications that require access to calendars, locations, and contacts - none of which have any overt bearing on health but which may nonetheless be misused against them if this kind of information is accessed by the wrong party. Patients should be encouraged to ask questions regarding how their information is stored and by whom it may be accessed. Healthcare workers can also provide patients with advice on how to protect themselves, such as using good passwords on internet sites, identifying phishing messages, and being cautious with apps they install. Just like people are instructed on how to be healthy or how to exercise, they can also be instructed on how to protect their health information. If patients are more educated and activated, they can be the front line of defense instead of being passive victims.

Better patient education equates to better cybersecurity for the entire health system. Healthcare cybersecurity is no longer merely an IT concern, nor a concern in the future. It is something that is current. The question is now no longer one of HIPAA or HITECH but how to keep people private and trusting in a patient-provider relationship, so the hospitals do not close their doors. Since the cyber threat is constantly changing, healthcare organizations must get a jumpstart. That includes investing in secure systems, educating their staff, and preparing for the worst. It also means embracing new technology, like AI and blockchain, but making sure it's safe to use. Healthcare is not about hurting people, it's about assisting them. That's why cyber security must be at the top of the list - because ultimately doing no harm also means safeguarding patient information.

**Works Cited**

American Hospital Association. (2020). "Cybersecurity and Hospitals." Retrieved from <https://www.aha.org/cybersecurity>

HealthIT.gov. (2023). "Understanding Cybersecurity in Health IT." Retrieved from [https://www.healthit.gov](https://www.healthit.gov/)

HIPAA Journal. (2022). "Healthcare Data Breach Statistics." Retrieved from [https://www.hipaajournal.com](https://www.hipaajournal.com/)

National Institute of Standards and Technology (NIST). (2023). "Cybersecurity Framework for Healthcare." Retrieved from [https://www.hipaajournal.com](https://www.hipaajournal.com/)

Ponemon Institute. (2021). "Cost of a Data Breach Report." Retrieved from [https://www.hipaajournal.com](https://www.hipaajournal.com/)

U.S. Department of Health & Human Services (HHS). (2023). "HIPAA for Professionals." Retrieved from <https://www.hhs.gov/hipaa/for-professionals/index.html>