National University Redesignated as National Center of Academic Excellence in Cyber Defense

The nonprofit university is one of only six four-year institutions in California to receive the prestigious designation from the National Security Agency

Healthcare and Cybersecurity

The number of reported healthcare breaches is significant, and even just one breach of a person's confidential medical records could reasonably be considered alarming. In 2019 there were 41.2 million healthcare records exposed, wrapped up in 505 data breaches that crossed industries and regions. The cost of each breach, according to an IBM report, was nearly $6.5 million — more than double the average non-healthcare data breach. This statistic doubles when looking specifically at the United States.

What's more, according to the US Department of Health and Human Services' Office for Civil Rights, overall breaches stand at an increase of 36 percent in 2019, from 371 in 2018 to 505.

It's a problem that's not going away and is increasingly getting more attention from healthcare organizations looking to secure their infrastructure and protect patients' data. And, of course, to provide peace of mind for all involved.

HIPAA and Cybersecurity

HIPAA is the Health Insurance Portability and Accountability Act, passed by the U.S. Congress in 1996. It was signed into law as a measure to "improve the portability and accountability of health insurance coverage" for employees between jobs. But in cybersecurity, it's largely recognized for its security policies and standard in which security is measured against. Compliance with HIPAA and its healthcare cybersecurity regulations is a top priority for many organizations.

Among other actions, the law — which has been amended several times since first passed — reduces healthcare fraud and puts the onus on healthcare providers and insurance companies to protect patients' health information, referred to in the industry as PHI, or protected health information.

Upon its introduction, whether through explicitly stated policies or incentives, the law marked a transition to electronic billing and other digital processes. It further developed the larger policy that business conducted should only use necessary health information for business purposes, and those dealing with PHI, whether physically or electronically, must prove an ability to control access to it and provide protection for it.

This, of course, has enormous implications for cybersecurity and healthcare, as protecting patient information from modern hacks and scams becomes paramount. Those responsible for management of this information can face criminal charges from the Department of Health and Human Services' Office for Civil Rights, under certain conditions.

Healthcare Cybersecurity Issues

There are several concerns with cybersecurity in healthcare. Chief among them—particularly as it pertains the cybersecurity-HIPAA dynamic — are the following:

- **Ransomware.** Criminals may use ransomware or malware to shut down devices, servers, and networks. Ransomware is software designed to block access to files until a sum is paid; it typically spreads through phishing emails or visits to sites with ride-along downloads. This is more broadly known as malware or "spyware." The ultimate mission is to extract data to gain leverage against an organization, like a hospital, insurance company, or any of their business associates.
- **Data breaches.** The healthcare industry receives more data breaches than any other sector, according to the Ponemon Institute and Verizon Data Breach Investigations Report. This is, quite simply, because PHI sells at a high price. These breaches might target a laptop or specifically seek out credentials. Notably, though, this is not always through malware or phishing — it can also be an employee who discloses information. A breach of more than 500 records, by HIPAA law, must be reported.

- **Encryption inefficiencies.** Blinds spots and human error can sometimes cause encryptions — as highly recommended as they are — to still lead to a breach. This can be because a hacker simply devoted enough resources to the project of revealing the files, or because data was stolen while being decrypted or as encryption keys are being made. There are also possible holes in files stored in the cloud, which can feature varying degrees of encryption.
- **Medical device hacks.** A growing area of concern is the possibility of software-enabled medical devices, like a pacemaker, that can be susceptible to hacking. These hacks are difficult to detect. While there are no known hacks of medical devices, the Food and Drug Administration (FDA) has identified 11 cybersecurity holes in commonly used operating systems.

Healthcare Cybersecurity Solutions

Fortunately, healthcare cybersecurity issues are not without solutions. While technology can be used to breach records, it can also be used to safeguard sensitive information by focusing on a few simple, yet effective practices.

- **Healthcare cybersecurity best practices for employees.** Part of developing a secure system for an organization is simply cultivating an employee culture of best practices. Employees should be trained to identify suspicious emails and update software as needed. In general, they should understand the responsibilities they share, and the risks associated with mishandling of patient data. Healthcare cybersecurity best practices start with a strong, united workforce.
- **Employment of cybersecurity professionals.** The easiest step to take is to hire people tasked with securing health information. And, more importantly, to make hiring them a priority. Give them the authority to oversee the architecture of a security system and administer its use as necessary. These are practiced professionals who are tasked with encryption processes and ensure employees are sufficiently carrying out their duties in a secure way.
- **Passwords.** Weak passwords are a notoriously easy way for cyber criminals to access sensitive information. Passwords should be strong, be changed regularly and, ideally, require two-step authentication.

- **Limits on installations.** Employees should not have access to software downloads without the consent of the organization.
- **Physical access.** HIPAA requires that physically stored data also be secured. Simply put, any device or folder with private information should be carefully stored in a locked area.

National University offers a Bachelor of Science degree in Cybersecurity, preparing aspiring professionals for a career as a security analyst, computer network defender, or computer incident responder. Skills acquired in the program lend themselves well to the healthcare industry and beyond.

Join the over 180,000 NU Alumni and be sure to mention your scholarship code, **EDCOR**!

To learn more about degree programs, visit: NU.edu. For additional information, visit the Edcor partnership page or email WESCorp@nu.edu