HEALTH TECH ACCESS ALLIANCE

QI EXPRESS

Current Vulnerabilities and Threats Affecting Healthcare

Week of October 21, 2019

Data Leaks in Healthcare

WizCase recently discovered database leaks from several unsecured medical websites that didn't require a password to be accessed, leaving millions of patients' data vulnerable. This was mainly because these medical databases are managed by third-party organizations who might not fully understand the implications of handling sensitive medical data. This should alert these companies to have proper privacy and security measures in place.

Email Attacks

Fraudulent emails are affecting the industry's ability to care for patients. They hijack patients' trust with scams that exploit your organization's brand equity. Healthcare workers are tricked into opening an unsafe attachment or a questionable link that leads to malware. The largest volume of these imposter emails arrived during weekdays between 7AM and 1PM. In the first quarter of 2019, 77% of email attacks on the healthcare industry used malicious URLs and an average of 65 staff members were attacked for each targeted organization.

Health Sector Breaches

Data breaches are having bigger impacts and hijackers have managed to stay undetected for years due to a lack of proper security measures in place. For Mission Health, a health services provider based in North Carolina, their payment portal became a target of cyber attackers for a period of 3 years, from March 2016 to June 2019. The portal was compromised for the purpose of data theft and was subject to skimmer malware or scripts.

After the Breach - Impacts

The Florida-based healthcare provider Jackson Health System (JHS) violated the Health Insurance Portability and Accountability Act (HIPAA) multiple times between 2013 and 2016. In 2016, JHS notified that 1,436 patient records were lost. JHS determined that an employee had accessed and sold patients' electronic medical records. JHS failed to conduct risk analyses and failed to restrict employees' access to PHI. Office for Civil Rights imposed a fine of $2.15 million which JHS agreed to pay for the multiple HIPAA violations.

The most common HIPAA violations that have resulted in fines are due to the failure to perform an organization-wide risk analysis. Risk analysis must be performed regularly in order to identify vulnerabilities that may be of high threat. HIPAA violation fines can range from $100 to $50,000 per violation with a maximum penalty of $1.5 million per year for each violation. Organizations need to restrict access to medical records in order to reduce risk and prevent financial penalties.

Our mailing address is:
11140 Rockville Pike, Suite 400
Rockville, MD 20851
301-200-9776