QI EXPRESS

HEALTH TECH
ACCESS ALLIANCE

Current Vulnerabilities and Threats Affecting Healthcare

Week of November 11, 2019

Healthcare Data Breaches

In 2019, nearly 4 out of 5 cybersecurity breaches were targeted toward healthcare organizations. Since 2016, more than 93% of healthcare organizations have experienced a data breach and 57% have had more than 5 breaches during the same timeframe. Since 2015, more than 300 million records have been stolen. The estimated cost of a data breach for healthcare organizations in 2019 averaged at $423 per record. Data breaches are projected to cost healthcare $4 billion by the end of 2019. In 2020, data breach costs are expected to increase significantly. Thus, organizations must take action to enhance their security measures.

Misconfiguration Errors

Texas Health is a faith-based health system with hospitals and clinics in over 16 counties and serving over 7 million patients each year. In August 2019, Texas Health Resources reported a misconfiguration error in their billing system that compromised the data of 82,000 patients. The IT team investigated this misconfiguration error that sent billing information to the wrong recipients for a period of 3 months. Proper development, implementation, and testing strategies would help avoid this risk.

Breach Remediation Efforts

Data from over 3000 hospitals for years 2012-2016 was analyzed to estimate the relationship between breach remediation efforts and patient care quality. They found a shocking increase in 30-day mortality rate for heart attacks, meaning 36 additional deaths per 10,000 heart attacks per year and they kept increasing for 3 more years after the breach. They also had an unsettling impact on the time it took for staff to hook up a patient to an EKG in the emergency room and time-to-EKG rose by 2.7 minutes following a breach. While an incident is investigated and security updates are applied, this post-breach delay is also negatively contributing to these time-sensitive processes and patient outcome measures. Security solutions against breaches should focus on usability assessments ensuring providers the access they need when they need it most.

Failing to Comply with HIPAA Rules

The University of Rochester Medical Center in New York has agreed to pay a penalty of $3 million for violating HIPAA rules. The fine was imposed for two data breaches that occurred in 2013 and 2017. In 2013, a data breach was reported following the loss of an unencrypted flash drive that contained patients' protected health information (PHI). In 2017, URMC reported another breach after an unencrypted personal laptop of one of its surgeons was stolen from a treatment facility which contained PHI of patients. URMC failed to conduct an enterprise-wide risk analysis and failed to employ a mechanism to encrypt and decrypt electronic PHI when needed. Failing to encrypt electronic devices puts patients' health information at risk.

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