CYBERSECURITY & HEALTHCARE PROVIDERS

SAFEGUARDING YOUR HEALTHCARE ASSETS AGAINST CYBERATTACKS

The UAE healthcare market is projected to reach $19.5 billion (Dh71.56 billion) by 2020, achieving an annual average growth of 12.7 per cent, marginally higher than the GCC growth average. The region is also the world's fastest growing medical tourism hub and poised to become the world's top destination by 2021. This growth projections has led to more adoptions of world-class healthcare infrastructure and services – driven by technology.

This is not limited to hospitals alone. For example, in order to provide more efficient access to critical health information, healthcare providers are using web-based applications and online portals that give physicians, nurses, medical staff as well as administrative employees more access to electronic Protected Health Information (ePHI). Providers are also using clinical applications such as computerized physician order entry (CPOE) systems, electronic health records (EHR), and radiology, pharmacy, and laboratory systems. There are considerable benefits in using these technology innovations in providing outstanding patient experiences.

However, this increases the threat landscape of healthcare providers and their exposure to cybersecurity breaches. It also raises further data privacy issues with regulations such as the General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) as customer records are increasingly at risk.

Security breaches in the health sector have devastating consequences because they could render an entire system or network inoperable, creating a life or death situation that needs immediate attention. A recent study by the *Identity Theft Resource Center* found that healthcare accounted for 36 percent of all breaches which occurred worldwide in 2016.

Healthcare records are extremely attractive targets for cybercriminals as it contains sensitive information like patient's sensitive records and other ePHI. The most recent form of attacks to hit healthcare organizations are Ransomware; where healthcare provider networks and patient records are hacked, infected with malware, encrypted and subsequently locked down until a ransom is paid.

> A recent study found that healthcare accounted for **36%** of all breaches that occurred worldwide in 2016.

BDO UAE TECHNOLOGY ADVISORY

BDO UAE's Technology Advisory practice consists of seasoned technology advisors who come from diverse backgrounds and cover a range of specialist skill sets in: Cybersecurity, IT Audit, Governance, Risk and Compliance(GRC), Forensics and Security Awareness and Training. Our passion is to see organizations extract the best value from a resilient and secure technology environment.

CONTACT US:

RICHARD UHUNMWAGHO
Senior Manager
Technology Advisory Services

Tel: +971 4 436 3500
Mobile: +971 55 810 7750
richard.uhunmwagho@bdo.ae

BDO UAE
www.bdo.ae

Recently, the UAE Government developed the National Cyber Security Strategy (NCSS), a roadmap for protecting national infrastructure including the healthcare sector. The UAE Information Assurance Standard (NESA Standard) was also created to provide guidance to entities across the UAE for implementing cybersecurity programs.

However, two critical questions still linger – *"Are our healthcare facilities secure against cyber breaches?"* and "*Is the NESA Standard streamlined to provide healthcare providers the necessary guidance for addressing data security and privacy issues pertaining to their industry?*"

BDO recommends these critical activities which healthcare providers can take to help safeguard their assets including rules on privacy, security, breach notification to safeguard healthcare provider's critical data and systems:

- **Providers must develop and implement policies and procedures to protect the security of ePHI they create, receive, maintain, or transmit.** Risks to ePHI in their environment should be analyzed to protect against reasonably anticipated, impermissible uses or disclosures and create solutions appropriate to address these risks.
- **Assign responsibilities and train staff on cybersecurity.** Hackers have become much more creative when launching phishing campaigns. Providers need to ensure that employees are constantly educated on phishing attacks and how to spot and avoid these attacks. Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email or downloading attachments from unknown senders. Every hospital staff member needs to be educated on how to identify cyber threats. It is easier to train staff on cybersecurity when it is presented in a practical way.
- **Employ a data backup and recovery plan for critical information.** Perform and test regular backups to limit the impact of data or system loss, and to speed up the recovery process. Data should be kept on a separate device/system, test should take place at least quarterly and backups stored offline.
- **Assess IT workflow and people to identify potential system vulnerabilities.** A breach of data-reliant treatment areas would cause clinical problems, since patients' past and recent medical records would be unavailable. Creating secure IT perimeters makes it possible to shut down data-reliant treatment areas to protect them from infiltration until the attack is addressed.
- **Restrict users' ability to access critical health records; installation and running applications.** This could be achieved by applying the principles of Least Privilege and Need-to-Know to systems and information. Doing so may prevent the execution of malware or at least limit its capability to spread whilst restricting unauthorized access to ePHI.
- **Implement effective preventive measures.** As vulnerable systems are identified, hospitals may choose to introduce new resources to their prevention and response protocols including security incident procedures and contingency plans. A variety of early detection systems and technologies are already in use in other industries to identify malware and intrusions that have gained access to IT systems. Hospitals can contain these infiltrators by identifying them early on and preventing them from accessing ePHI.
- **Implement Privacy Rule which gives patients important rights with respect to their health information.** This includes patients' rights to examine and obtain a copy of their health records in the form and manner they request (electronic, oral, or paper form) and to ask for corrections to their information in a secure manner.
- **Develop a cybersecurity framework.** This helps providers prepare so that if and when they do get hacked, they can prevent further infiltration, minimize the damage and quickly redirect staff to practiced protocols so patient care is not compromised. It also encompasses access controls, security monitoring, data privacy, and the selection and implementation of security tools.

Healthcare providers that empower themselves to respond to breaches will have a good sense of what is going on and what needs to be addressed – as opposed to those who are caught off guard and can merely react as they try to figure out the problem and how to resolve it.

BDO assists healthcare facilities in conducting ongoing security risk assessments, testing of Cybersecurity controls and implementing cybersecurity risk management programs, strategy and governance.

For more on Cybersecurity services provided by BDO, please visit our page on:
http://www.bdo.ae/en-gb/services/advisory/technology-advisory-services/cybersecurity-services