Healthcare Cyber Security Guide

EdgeWave™

The Healthcare Cyber Challenge

Our world has been radically transformed by digital technology – smart phones, tablets, and web-enabled devices have altered our daily lives and the way we communicate. Medicine is an information-rich enterprise, and the flow of electronic health records (EHRs) improves the way care is delivered. But digital technology introduces risks as well.

An Identity Theft Resource Center survey determined that healthcare organizations suffered 43 percent of all data breaches reported in 2016, significantly higher than the business sector (education, government and others), which suffered 34 percent.

According to Verizon's *2016 Data Breach Incident report* (DBIR), web application attacks and unauthorized data transfer continue to be most widespread types of data loss. Phishing through malicious email, installing crime-ware, and exploiting weak or stolen credentials are the most effective ways criminals gain access to information assets. In fact, 30% of phishing messages were opened by the target across all campaigns, a significant increase from 2015.

Changes to HIPAA under the HITECH act of 2009 require healthcare providers to notify the Department of Health and Human Services of any data loss affecting more than 500 patients. Organizations that suffer breaches are listed publicly and face fines of up to $1.5 million on top of mitigation costs. Healthcare IT departments are now required by law to "exercise reasonable diligence" to protect patient health information (PHI), and to analyze security risks under Stage 1 of the HITECH "meaningful use" of electronic healthcare software definition.

From a crime standpoint, stolen medical records are more lucrative for thieves because PHI can be used not only to open credit lines, but also for insurance, Medicare and prescription fraud. This greater value will continue to attract entrepreneurial hackers to target healthcare organizations.

The Solution

With more complete patient information, providers improve their ability to make well-informed treatment decisions quickly and safely. But you are responsible for taking the steps needed to protect the confidentiality, integrity, and availability of electronic health information and to comply with HIPAA and meaningful use requirements.

The four key components of a solid internet and data security program include:

- Advanced Threat Defense
- Education of Staff, Patients, Vendors and Associates
- Data Protection Services
- Endpoint Security

Advanced Threat Defense

Email is a primary threat vector by which hackers access your electronic patient data. It's easier for a hacker to send out an email than to hack a firewall – it takes just one unsuspecting staff member to open the wrong email or click a bad link to punch a hole in your network defense. EdgeWave's ePrism Email Security Suite includes the powerful tools you need to assure the protection of private data belonging to your patients and staff, and the efficient delivery of legitimate mission-critical email. ePrism offers fully hosted in-the-cloud services that require minimal management, are affordable, and can scale easily to fit any size network.

ePrism includes a multi-layered approach that stops emerging threats before they can get near your network. EdgeWave cybersecurity solutions combines human threat review and automated intelligence to identify and stop advanced threats in real time. Humans can identify the intent of inbound threats in a way an algorithm can't – that's why every cybersecurity plan must include human analysis. In the first quarter of 2016 alone, our human review process has blocked over 100 million malicious emails per day with human-written rules and analysis. The 2016 Verizon Data Breach Report promised "We may be able to reduce the majority of attacks by focusing on a handful of attack patterns." EdgeWave leads the market with this capability.

Data Protection Services

Data Loss Protection (DLP) - ePrism includes a content analysis and policy engine that uses proprietary technology to detect private information transmitted via outgoing email. This data protection technology analyzes data in motion, and using compliance-based rules, detects and blocks any sensitive private data trying to leave your network. This solution is easily managed from the ePrism Central Dashboard giving you the powerful tools you need to comply with government regulations such as HIPAA and others.

Encryption - EdgeWave Email Encryption assures the secure delivery of email to anyone outside your network, with next-generation technology that eliminates the cost and complexity associated with many traditional encryption services. As a completely hosted service, there is no hardware or software to implement and encryption can be easily enabled on a per user basis or as part of an automated routing policy. In addition, because it is integrated into the ePrism Hosted Email Security and Data Loss Protection services, your outgoing email is inspected for malware, viruses, inappropriate content, compliance breaches and violations of your acceptable use policy (AUP). You can manually encrypt messages or configure to automatically encrypt per a variety of factors; such as sender, recipient, or when DLP problems are detected.

Endpoint Security

Mobile devices such as tablets, phones, and laptops have found their way into your healthcare organization whether you like it or not. Doctors want immediate access to PHI and personal devices are the future for instant retrieval. Nurses and other staff need separate access levels so they can only see what is appropriate for their positions.

iPrism Web Security can help you mitigate endpoint risk with Cloud-Based Remote Web Filtering and Mobile Device Security. These security solutions employ proprietary technology to bring powerful Enterprise Web Filtering to all staff and devices, even outside the network. You receive comprehensive protection from web-based threats, granular policy controls, and selective data wiping -- all with centralized administration and reporting. Suitable for both corporate and BYOD devices, iPrism provides anytime, anywhere any device security for iPads, iPhones, Android devices, Windows laptops and MacBooks.

Education of Staff, Patients, Vendors and Associates

The internet and data security technologies described above are only as effective as the training and policies that enforce their use. Here are 5 steps to get you started on the path to ensuring your organization will support your security efforts:

1. Integrate a security strategy with every plan and initiative. Security is no longer an afterthought, especially in healthcare
2. Empower employees with intensive, regular security policy and procedure education. Training must include knowledge of federal HIPAA regulations, state and local rules regarding privacy
3. Implement and enforce strong organizational/IT policies regarding social media and portable devices.
4. Ensure all employees -- not just those who see patients -- know exactly what PHI can be shared and which needs their utmost discretion. Require a signed and sealed agreement of understanding and adherence from all parties with PHI access, possibly in the form of a special certification
5. Employ an agile, robust, platform-agnostic, advanced threat detection system that includes encryption

EdgeWave's award winning solutions have helped thousands of healthcareorganizations protect their data and networks. EdgeWave offers cloud-based services as well as on premise appliances for email and Web security services that require minimal management, are affordable, and can scale easily to fit any size network. To learn more about EdgeWave and its powerful solutions, please visit https://www.edgewave.com/.