opentext™ | Cybersecurity

CASE STUDY

Memorial Hermann easily secures protected health information with Webroot™ Email Encryption powered by Zix™

MEMORIAL HERMANN

AT A GLANCE

Company

Memorial Hermann Health System

Industry

Healthcare

Products

Webroot™ Email Encryption powered by Zix™

Key Findings

- Thousands of HIPPA compliant messages are sent and received securely every day
- The ease-of-use of Webroot Email Encrytion keeps the communication flowing securely and maintains productivity
- Use of TLS via the custom Secure Portal to commuciate securely with organizations not using Webroot Email Encryption

Background

Memorial Hermann is an integrated health system with 5,500 affiliated physicians and more than 26,000 employees who practice evidence-based medicine with a relentless focus on quality and patient safety. As one of the largest not-for-profit health systems in Southeast Texas, Memorial Hermann has nearly 20 hospitals, including 14 hospitals owned and operated by Memorial Hermann and 5 through joint ventures.

Memorial Hermann operates one of the nation's busiest Level I trauma centers and also serves as the primary teaching hospital for McGovern Medical School at UTHealth.

In serving its patients, Memorial Hermann makes sure to take the necessary measures needed to protect patient privacy, including securing protected health information in email.

Challenge

Memorial Herman needed to juggle the need for privacy and regulations with the importance of keeping communication flowing smoothly between physicians, nurses, staff, patients and outside healthcare organizations. The top challenge in their search for email encryption centered on the user experience. Securing email is complex, but in order for email encryption to be effective, the solution needed to be as simple to adopt and use as regular email.

"When communicating protected health information or personally identifiable information outside of Memorial Hermann, it's critical that we have a secure yet seamless means of emailing other doctors, clinics and hospitals," said Patrick Santiamo, Cyber Security Analyst – Cyber Security for Memorial Hermann Health System."

Solution

That put them on lookout for a trusted partner in cybersecurity that had an easy-to-use solution, proven automatic policies and exceptional support. Their search brought them to Webroot™ Email Encryption powered by Zix™.

> ***"Nurses, physicians and even patients understand why we need email encryption and our organization really likes the Webroot solution."***
>
> - Patrick Santiamo, Cyber Security Analyst
> Cyber Security for Memorial Hermann
> Health System

Results

For Memorial Hermann, nearly 75 percent of its encrypted emails are exchanged transparently to customers that share the same solution, allowing more than 1,750 outside organizations to access encrypted email right from their inbox with no extra steps or passwords. With this unrivaled ease of use, email messages and their attachments are secured when leaving Memorial Hermann's network and then automatically decrypted at the recipient organization's network, requiring no unnecessary hassle.

For other organizations that don't use Webroot Email Encryption powered by Zix, Memorial Hermann sets up TLS connections for expanded transparency when sending secure emails. A mobile-friendly, custom-branded portal enables recipients without Webroot to easily access encrypted email. In less than two steps, recipients can quickly read, reply and reply-all to encrypted emails.

Just as encrypted email is convenient to receive, it is also convenient to send. With out-of-the-box automatic policies for Health Insurance Portability and Accountability Act (HIPAA), Social Security numbers and financial information, Memorial Hermann has confidence that emails with sensitive information in the message or attachment are protected. When a policy is triggered, emails can be encrypted, blocked or quarantined depending on the content, sender or recipient, or other policies.

"Webroot email encryption and policies are a way for us to meet our HIPAA requirements and automatically prevent spillage for everyone in our organization. It serves as a cost saving measure, keeping us from facing fines related to a breach," said Santiamo.