CASE STUDY

Seeding Safe Collaboration

Though data security poses problems in every industry, the financial world has the advantage of being able to lock up its customer information in the modern equivalent of Fort Knox. But the health care industry doesn't have the same advantage of this strict privacy. Doctors, nurses, insurance companies and others have to share data among themselves and with patients.

Trustwave®
Smart security on demand

CLIENT SPOTLIGHT

This health care system consists of 14 hospitals, 36 minor-injury units (with 13,000 beds), nearly 500 general practices, more than 700 pharmacies—and a mind-boggling 65,000 healthcare providers. Staff send and receive more than four million emails each and every month.

THE CHALLENGE

Email is one of the most flexible and efficient ways to collaborate, but it can be challenging to secure. This health system needed an email security solution that would not only protect it from spam and malicious attachments but one that would also identify and protect patient data. Precise filtration rules to recognize sensitive patient information in their varied forms was required, and these rules needed to be customizable. Inadvertently exposing patient data put the health system at risk of incurring fines that go as high as hundreds of thousands of dollars per incident. But the email security solution also needed the flexibility to allow medical providers to override the security restrictions during a patient emergency.

"By imposing this stringent testing regime, we are confident that every effort has been made to ensure that no personally identifiable or confidential information is being passed by email without the correct level of protection in place."

– Hospital system security manager

THE SOLUTION

Trustwave Secure Email Gateway (SEG) initially helped the client control malware and spam. Based on this success, a more in-depth highly customized security protocol was established that gave individual hospitals some autonomy while still maintaining a base level of safety across the entire system. Data loss prevention rules scan email in real-time to check for the presence of personally identifiable details, which help keep communication safe without hampering medical professionals' work.

INDUSTRY THREAT

Consider this grim statistic: By 2024, everyone in the U.S. will have had their health care data compromised if online theft keeps accelerating at the current pace. Health records, which can contain U.S. Social Security, drivers' license and payment card numbers in addition to insurance information, go for four figures or more on the dark web. And so the average size of a data breach keeps growing, to more than 24,000 records each.

"Our team now has peace of mind knowing that we won't get fined for loss of data."

– Hospital system security manager

Trustwave®

Smart security on demand

CS-HEALTHCARE_2-0118