ENCRYPTICS®

{Case Study}

Protecting PII in Healthcare

Large Hospital Group/Texas

Why Choose Encryptics?

Highly Secure
- End-to-end data protection
- Encryption at the device level
- Data Rights Management

Cost Effective
- Software-based solution
- No additional hardware needed

Easy to Use
- Compatible with any email service
- Convenient Add-In for Outlook®
- Supported on mobile devices

"HGT is able to provide state-of-the-art medicine in world-class facilities due to the support of hundreds of doctor-investors, and we must regularly communicate confidential information via email and attachments. Encryptics provides device-level encryption and Data Rights Management that helps us ensure end-to-end data security and control, from inception and transit to its use and ultimate storage on any recipient device. We can communicate critical information with the knowledge and confidence that only authorized recipients are able to gain access to it.

Chief Information Officer

visit us on the web
ENCRYPTICS.COM
talk with us
512.649.8185

After successfully deploying Encryptics for Email, a large Hospital Group in Texas (HGT) decided to implement Encryptics Command Line Interface (CLI) to automate the protection and delivery of surgery schedules to their expansive network of doctors and nurses.

Technical Situation

HGT automatically generated doctor-specific surgery schedules on a daily basis and needed to deliver that data to numerous facilities that are outside of their IT department's control. Manually securing and sending this data daily via email was time consuming and inefficient. In addition, the schedule is useful for just one day, and the ability to open and use the previous day's schedule could create confusion for the doctors and nurses.

Security Challenge

Utilizing regular email to send surgery schedules that contains patient PII leaves information vulnerable to would be hackers. Information sent via email travels across unsecured networks and rests indefinitely on cloud-based email systems and servers. HGT needed a way to satisfy HIPAA requirements, secure patient PII, reduce the liability involved with sharing surgery schedules, and preventing unauthorized access.

Encryptics CLI and Email Solutions

HGT sought a proactive solution that would automatically protect the patient PII contained in the surgery schedules and enable them to control the usage and access rights of the data after it left their secure network. With Encryptics CLI, the HGT IT staff was able to quickly and easily create a script for automatically generating surgery schedules, defining authorized recipient lists, and setting usage rights to limit access to the data for the day specified. These secure schedules are automatically emailed to the doctors and nurses at designated facilities, who use Encryptics for Email to gain access and utilize the surgery schedules as allowed by HGT.

Result

Armed with our comprehensive security solution, HGT is able to safeguard its patients, doctors, and nurses from the vulnerabilities inherent in email communication. By taking a proactive approach to protect privacy, HGT is reducing liability and engendering trust throughout itsorganization and network of doctors.

About Encryptics Technology

Encryptics solutions utilize our Trusted Peer-to-Peer™ platform and .SAFE technology to eliminate common security gaps and ensure true end-to-end data protection. This means private data is secured at the device level — before a transfer takes place — so there is never a vulnerable point where a breach could occur. Plus, our powerful Data Rights Management (DRM) tools allow authors to control the usage and availability of their data even after it leaves their possession.