A Cure for Healthcare Data Security, Sharing and Compliance

How an emerging Midwestern healthcare software provider secured a nationwide network of patient data with SecureZIP Toolkit for Windows®

HEALTHCARE ENCRYPTION, COMPLIANCE & PORTABILITY: THE DETAILS

PKWARE's SecureZIP Toolkit for Windows® was selected by this healthcare specialty vendor to incorporate strong encryption in its Electronic Health Records (EHR) software. PKWARE enabled the company to achieve Meaningful Use and reliable data transfers by providing the following capabilities:

- Encryption that safeguards PHI at rest and in motion with persistent security that stays with the data itself, regardless of storage location or transfer method.
- Complete portability across all major operating systems and the ability to share data with partners regardless of platform, application or format.
- Embedded security that didn't interrupt the user experience.

The prognosis was grim for Ron's healthcare products. As CIO for a growing, Midwest-based healthcare specialty software vendor, Ron* faced increasing demand from his hospital system customers to add encryption for enhanced security and sharing in its Electronic Health Records (EHR) applications. Without guarantees on federal data compliance for Meaningful Use and FIPS, Ron couldn't even get a call back from potential customers.

The healthcare software and applications vendor needed a booster shot of security and compliance to stay ahead of its rivals – and a "devastating" security event.

"Loss of data security and personal health information would be devastating for our business, not to mention our customers and their patients. We needed to build stronger security for personal health information moving across our network of healthcare providers that hit government compliance benchmarks and, just as importantly, created confidence for users of our software product," he said.

Early on, Ron realized that building their own encryption amounted to a significant dedication of time and skills. For one, Ron's products would have to meet FIPS encryption standards. It typically takes developers anywhere between two months to one year to evaluate and create encryption that satisfies FIPS. Then, there is up to six months of lag time while the product is judged for government FIPS certification. These weren't optimistic timelines for a product Ron's managers expected to release in a matter of months. It would also take up all the developer resources on Ron's team of three, none of whom had extensive previous expertise in security, encryption or crypto libraries.

- Compliance with the encryption requirements of HIPAA and protocols such as HIE, HITECH and HITRUST along with PHI regulatory standards and FIPS 140-2 certification.
- Introduction of industry-standard encryption and security elements within weeks.
- Bypass the typical 8-to-18 month development and approval cycle for FIPS certification.

Instead of crafting their own offering, Ron worked with our developer toolkit to strengthen their healthcare offerings in a matter of weeks. Rather than testing and waiting on encryption certification, Ron could plug in industry-recognized encryption that satisfied FIPS and other federal standards. Encryption woven into the EHR software also enables healthcare providers to move and store sensitive PHI in accordance with HIPAA, HITECH and the ARRA stimulus requirements. This allowed Ron's customers to be eligible for the government's Meaningful Use funding and incentives.

The upgraded software also allows portability across all major operating systems and secure data sharing with partners regardless of platform, application or format. Upgrades and applications were rolled out to customers with no surprises. A developer agreement opened the door to include encryption as a vital element in another healthcare application that was released later in the year.

A few months after the development of the EHR software, Ron says there's been an uptick in new customers. He's also gained a conversation starter with potential customers as secure data exchanges become the norm. Existing customers have also found piece of mind—but no disruptions—with the way they work with medical information.

"When a patient comes in for a check-up, the process for the healthcare provider and the patient hasn't changed. We use the software in the same way," said Bethanny, a medical group physician using the enhanced healthcare software product. "Knowing there is a layer of encryption behind the scenes gives us confidence that we're meeting our security expectations."

* THIS IS A PRO FORMA CASE STUDY. THE NAMES HAVE BEEN CHANGED AND SOME FACTS ALTERED TO PROTECT THE IDENTITY OF THE CUSTOMER.

PKWARE **provides security technologies with performance that help organizations protect their critical information assets as data moves beyond the enterprise. PKWARE invented the ZIP file standard in 1986 and continues to develop innovative solutions used by more than 30,000 global customers. We support all major computing platforms from IBM mainframes to distributed systems, servers, desktops, mobile devices and now the cloud and virtual environments.**

PKWARE®

CORPORATE HEADQUARTERS
648 N. Plankinton Ave.
Suite 220
Milwaukee, WI 53203
1.800.219.7290

UK / EMEA
Building 3 Chiswick Park Chiswick High Road,
London W4 5YA
United Kingdom
+44 (0) 208 899 6060

Find out more about our customers and solutions at pkware.com