CASE STUDY

PKWARE®

PKWARE's Smartcrypt Enhances Protection for Sensitive Medical Data

A GROWING THREAT

The Centers for Medicare & Medicaid Services (CMS) is responsible for safeguarding sensitive patient data, and also secures information exchanged between hundreds of partners at the federal and state level, as well as with universities and private businesses. As a result, there is zero tolerance for security breaches, and CMS must comply with ever-changing regulatory requirements.

CMS faced public pressure for privacy which led to internal agency directives and heightened concern from program members. CMS realized it needed to address support issues with partners who may not have had the expertise or skillset necessary to manage installations. As the rate of data exchange and the number of external partners continued to increase, CMS grew concerned about its exposure to potentially catastrophic data breaches and identified the critical need to enhance its data protection.

OUTDATED PROTECTION

While it has historically maintained an excellent record for data security, CMS's strategy had been focused on securing networks and devices, not the data itself. It now recognized the need to implement data-level encryption that would protect health care recipients' personal information at rest and in motion, regardless of IT platform, point of origin, or destination.

The agency's move toward encryption was given further urgency by the need to maintain compliance with data protection standards mandated by federal laws including the Federal Information Security Management Act and the Health Insurance Portability and Accountability Act.

PAIN POINTS

NO PROTECTION OF DATA EXCHANGED WITH FEDERAL, STATE AND EXTERNAL BUSINESS PARTNERS

FEDERAL MANDATES FOR SECURE DATA TRANSFER

INCREASING VOLUME OF DATA EXCHANGE

SOLUTION

SINGLE AGENCY-WIDE ENCRYPTION POLICY

MORE THAN 6,000
ENDUSER BUSINESS INSTALLATIONS

MORE THAN 250
EXTERNAL BUSINESS PARTNER IMPEMENTATIONS

100%
COMPLIANCE WITH FISMA, HIPAA, AND FIPS 140 DATA EXCHANGE REQUIREMENTS

PKWARE'S SMARTCRYPT

Before selecting a data encryption solution, CMS developed an extensive list of capabilities that the solution would be required to provide:

- AES256 strong encryption
- Support for PKI certificates
- Complex password support
- Policy key management capabilities
- Support for all enterprise platforms and operating systems

In addition, it was critical that all of its partners react favorably to the solution and adopt it into their daily processes. An extensive evaluation process revealed that PKWARE's Smartcrypt was the only data encryption solution that could deliver persistent data-level protection while providing support for all of the platforms used by the agency's internal departments and external partners.

CMS installed the Smartcrypt application on desktops, laptops, and mobile devices for more than 6,000 employees, in addition to implementing Smartcrypt protection for data exchange with more than 250
partner organizations.

As expected, PKWARE's Smartcrypt solution met every requirement defined by the agency and brought its data exchange procedures into compliance with all federal and industry guidelines for secure storage and exchange of sensitive health information.

LOOKING AHEAD

In addition to making CMS's data exchange more secure, Smartcrypt has greatly improved data transfer times, as the solution uses PKWARE's industry-leading data compression technology to reduce file sizes
before encryption.

Smartcrypt is now an essential component of the agency's information collection and exchange procedures. CMS continues to increase its Smartcrypt install base and usage internally and with new business partners.

The Smartcrypt technology received a Designation as a Qualified Anti-Terrorist Cyber Security Technology by the Safety Act Commission administered by the Department of Homeland Security.