Government agency handles billions of files containing private health information

The Challenge Improve security and data exchange across a complex partner network

The numbers were staggering...years worth of sensitive data about every Medicare and Medicaid recipient exchanged with hundreds of partner organizations with zero tolerance for security breaches. This posed a significant challenge for the Centers for Medicare & Medicaid Services (CMS) in attempting to comply with the regulatory requirements of OMB M-06-16 and FIPS 140-2. In addition to changing regulations, public pressure for privacy meant new internal agency directives coupled with heightened concern from program members.

CMS also needed to address the support issues with its partners who may not have the expertise or skill set necessary to manage the installation. Recognizing its own resource limitations and time constraints, CMS wanted experience and commitment from a vendor who could bridge the gaps.

CMS encountered major interoperability challenges, as their large partner network had multiple operating platforms ranging from z/OS® mainframes to Windows® desktops. Data needed to be sent--and readily used--across a wide variety of technology platforms, applications and data formats. Current methods of electronic transfer, tapes and CD storage presented immense administrative and logistical burdens as well as increased security risks.

CMS safeguards sensitive patient data & secures information exchanged between hundreds of partners. ***As a result, there is zero tolerance for security breaches.***

Under intense scrutiny, *CMS needed to overhaul traditional methods of shipping more than 20,000 cartridges a year, reduce administrative burdens & minimize security risks.*

There were also numerous variables among the diverse group of partners...several did not have funds to purchase a decryption tool or a budget for integrating new software and many lacked an IT support staff.

It was critical that all the partners react favorably to the solution chosen by CMS and adopt it into their daily processes. Up against an ever-changing mix of partners and environments, CMS needed to present a true "no cost" solution to its extended enterprise without a cumbersome implementation process or compromised security.

With an existing IT Infrastructure support relationship with PKWARE, CMS leveraged that contract to investigate a variety of solutions. The PKWARE Solution was the standout choice—meeting every one of the CMS's requirements.

The PKWARE Solution

The only complete system for reducing, securing, moving and storing data across the extended enterprise

Only the PKWARE Solution provides total interoperability, integrated with file-level security and compression to optimize data center service delivery. PKWARE offsets network strain from taxed resources, growing amounts data and stronger security requirements. For over two decades, PKWARE has reduced the overall data footprint across applications, operating systems and platforms with as much as a 90% reduction in elapsed time for the consistent achievement of SLAs/SLOs.

CMS must translate and secure data so it can be easily shared with partners.

Our platform-neutral, highly portable data container securely encrypts and reduces usage needs by up to 95%. With incredibly efficient data "in motion," huge amounts of information travel faster, improving critical transmission times associated with operational and Service Level Agreements. And, PKWARE protects data irrespective of transport protocol or network security.

The PKWARE Solution stands alone in securely supporting the sharing of information across a wide variety of system platforms, applications, data formats and all transport protocols. And, PKWARE is the only solution that provides a consistent set of file encryption applications for all major enterprise platforms, achieving inherent compliance with industry-driven regulations. The advantages of this low risk, high performance solution met all of CMS's requirements, including the following capabilities:

- Encrypt data onto mainframe tapes
- Create CDs and DVDs on the mainframe as well as on Solaris® and Windows Server® systems
- Utilize the mainframe encryption coprocessor
- Support the AES encryption standard
- Decrypt all encrypted files on the mainframe as well as on Solaris and Windows Server systems
- Provide free decryption software to the CMS trading partners or create self-extracting files
- Provide contingency capabilities for CMS to decrypt files if a user's key or password is unknown
- Support data compression before or during encryption so that the resulting file is not larger than the source file
- Support encryption using either PKI certificates or passwords, determined on a case-by-case basis

PKWARE also guarantees that its ease of implementation is the best in the industry, production ready within just hours of implementation. It also yields easy integration and support advantages for the existing CMS infrastructure, which enables daily operations with partners to continue without interruption.

The Results

PKWARE raised CMS to a new standard in the secure, efficient exchange of critical business information

RISK MANAGEMENT

CMS is now safeguarding medical data and patient records at the file level, making it impregnable to anyone but authorized staff -- whether the data is at rest or in transit among CMS's numerous partner organizations. The solution's use of strong encryption and its ability to run in "FIPS mode" ensures compliance with FIPS 140-2 and OMB M-06-16.

PKWARE offers the only totally integrated solution for data compression, encryption and authentication in a single secure portable data container.

COMPLETE INTEROPERABILITY

CMS deployed the PKWARE Solution at three data centers on multiple mainframes and multiple open systems environments, including HP-UX® and Windows®. The PKWARE solution instilled confidence and equipped CMS with high performance at low risk, while eliminating the need for several diverse solutions. It also yielded easy integration and support advantages for the existing CMS infrastructure, which enabled daily operations with partners to continue without interruption. PKWARE also offered direct technical and engineering support to CMS's partner organizations.

COST REDUCTION

PKWARE proprietary technology allowed a multiplatform approach to compress (at a rate of approximately 80%) and encrypt very large datasets resulting in less required storage and more efficient transfer to partners, regardless of their operating environment.

DATA-CENTRIC SECURITY

What's more, because the PKWARE Solution is transport-independent, it can package encrypted data for transmission via EFT as well as encrypting data onto mainframe tapes and other forms of data movement, like CD and DVD. The PKWARE Solution creates the encrypted .zip archives that then can be transferred to the media of choice via the standard method of writing. It also utilizes the mainframe encryption coprocessor and supports the AES encryption standard. In this way, it provides cross-platform security -- encryption, digital signing and authentication -- both within and outside the IBM hardware cryptographic environments.

CMS and its partners are able to encrypt, decrypt, compress and decompress data—with complete security and guaranteed recoverability—across all platforms at no cost to the partner organizations.

Looking Ahead Continuous security and more efficient exchange for enormous data sets

Not only is CMS exchanging information securely with current partners, but the agency also distributes unlimited number of free partner licenses to new partners as they are added – making it a true "no-cost" solution. Praised for its responsiveness, PKWARE developed a repeatable standard procedure to introduce new partners to the technology.

While CMS is able to encrypt data exchanged with partners, it is also able to utilize an unlimited number of contingency keys that can be added to any encrypted .zip file created on any platform. These contingency keys open access to the encrypted archives if the primary key or passphrase is lost or compromised. The PKWARE Solution also supports the use of PKI certificates that comply through the X.509 certificate standard. Passwords or passphrases can be added, in conjunction with digital certificates.

PKWARE easily integrated CMS's unique mix of partners and IT environments with and support options proving its adaptability for dynamic infrastructures. CMS has implemented a sustainable cost-effective solution that promises to be both easy to launch and easy to use, with little, if any, interruption at origin or endpoints.

CMS can count on smooth adoption by partners— including implementation without interruption— reduced costs and lower operational overhead.

ABOUT PKWARE: **PKWARE, the industry leader in enterprise data security products, has a history rooted in innovation, starting with the creation of the .ZIP file in 1986. Since then, PKWARE has been at the forefront of creating products for reducing and protecting data — from Mainframes and zLinux to servers to desktops and into virtual and cloud 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

Learn more on the web at pkware.com • Have questions? Call 1.800.219.7290