HITECH / HIPAA Compliance & XCrypt™ Data Encryption Software Solutions

Data within distributed cloud and data center environments is fluid, as data is replicated in many places and moves as needed. Security must be consistently applied and enforced across a distributed computing environment. The Zettaset XCrypt™ Data Encryption Platform has been designed from the ground up to address the unique big data security challenges presented by these complex, distributed computing environments.

Two key pieces of US Federal legislation define security compliance requirements for healthcare providers to protect data at rest:

- HITECH – Health Information Technology for Economic and Clinical Health (HITECH) act - enacted as a part of the American Recovery and Reinvestment Act (ARRA) of 2009
- HIPAA – The US Health Insurance Portability and Accountability act (HIPAA) of 1996

HITECH Act (Health Information Technology for Economic and Clinical Health)

The HITECH Act was enacted under Title XIII of the American Recovery and Reinvestment Act of 2009 to promote and expand the adoption of health information technology.

The HITECH Act set meaningful use of interoperable EHR (Electronic Health Record) adoption in the health care system as a critical national goal and incentivized EHR adoption. Health information exchange (HIE) has emerged as a core capability for hospitals and physicians to achieve "meaningful use" and receive stimulus funding. Healthcare vendors are pushing HIE as a way to allow EHR systems to pull disparate data and function on a more interoperable level. Since 2015, hospitals and doctors have been subject to financial penalties under Medicare if they are not using electronic health records.

Meaningful Use Incentive Categories

The meaningful use of EHRs intended by the US government incentives is categorized as follows:

- Improve care coordination
- Reduce healthcare disparities
- Engage patients and their families
- Improve population and public health
- Ensure adequate privacy and security
  - » The Zettaset XCrypt Data Encryption Platform specifically addresses the incentive category "Ensure adequate privacy and security" designated under the HITECH Act.

Meaningful Use Core Requirements (Stage 1)

Stage 1 contains 25 objectives/measures for Eligible Providers (EPs) and 24 objectives/measures for eligible hospitals. The first steps in achieving meaningful use are to have a certified electronic health record (EHR) and to be able to demonstrate that it is being used to meet the requirements.

- » The Zettaset XCrypt Data Encryption Platform specifically addresses the core requirement: "Protect electronic health information (privacy & security)".

The HITECH Act requires HIPAA covered entities (see HIPAA-related section, below) to report data breaches affecting 500 or more individuals to HHS and the media, in addition to notifying the affected individuals.

This subtitle extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities. This includes the extension of newly updated civil and criminal penalties to business associates. These changes are also required to be included in any business associate agreements with covered entities. On November 30, 2009, the regulations associated with the new enhancements to HIPAA enforcement took effect.

Another significant change brought about in Subtitle D of the HITECH Act is the new breach notification requirements. This imposes new notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities if a breach of unsecured protected health information (PHI) occurs.

On April 27, 2009, the Department of Health and Human Services (HHS) issued guidance on how to secure protected health information appropriately. Both HHS and the Federal Trade Commission (FTC) were required under the HITECH Act to issue regulations associated with the new breach notification requirements. The HHS rule was published in the Federal Register on August 24, 2009, and the FTC rule was published on August 25, 2009.

HIPAA (Health Insurance Portability and Accountability Act)

The HIPAA Act of 1996 deals with the privacy, security, and transmission of medical information. Title II of HIPAA defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information as well as outlining numerous offenses relating to health care and sets civil and criminal penalties for violations

Per the requirements of Title II, the U.S. Department of Health & Human Services has promulgated five rules regarding Administrative Simplification: the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule.

The "HIPAA Omnibus Rule" of 2013 formally holds business associates liable for compliance with the HIPAA Security Rule.

The Zettaset XCrypt Data Encryption Platform assists IT departments in healthcare organizations (provider and payer) with HIPAA compliance in the following categories:

1. Privacy Rule - The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.) The Privacy Rule requires covered entities to notify individuals of uses of their PHI. Covered entities must also keep track of disclosures of PHI and document privacy policies and procedures.
2. Security Rule - The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications.

Meeting Data-at-rest Encryption Requirements for HIPAA HITECH Act Compliance

Zettaset XCrypt Data Encryption Platform provides HIPAA encryptions and HITECH encryption solutions that help organizations meet HIPAA Security Rule and HITECH compliance requirements transparently - without changes to operational processes and the daily work of healthcare professionals.

Zettaset XCrypt Protects ePHI

XCrypt provides data-at-rest encryption for multiple data environments along with integrated, secure encryption key management that meets HIPAA encryption compliance requirements to separate keys and encrypted data. Access controls and data access monitoring information extend protection from data breaches by limiting data access to only personnel and programs authorized to do so, and provide the security intelligence information required to identify accounts that may represent a threat because of a malicious insider, or a compromise of account credentials by malware.

The Zettaset Virtual Enterprise Key Manager (V-EKM) enables centralized management of encryption keys for other environments and devices including existing KMIP-compliant hardware from multiple vendors. The Zettaset Virtual Hardware Security Module (HSM) provides additional key management security and is compatible with existing PKCS#11-compliant HSMs.

This unified software-based solution to multiple HIPAA/HITECH encryption compliance requirements helps organizations meet compliance and data breach security needs with low TCO and an easy-to-deploy, centrally managed solution set.

Key features and benefits include:

- **Encryption and Access Controls:** ePHI can be encrypted for files and volumes, and file- and volume-level access is controlled and logged
- **High Performance:** Optimized for scalability in distributed computing architectures with high data volumes, resulting in minimal impact on SLAs and application latency
- **Auditing and Monitoring:** Log data is available for easy integration with auditing tools and Security Information and Event Management (SIEM) systems
- **Broad Database and Cloud Coverage:** Supports Relational, Object, NoSQL, and Hadoop, data environments; Deployable in the cloud or on-premises
- **Fast and easy deployment:** An all-software approach to encryption simplifies implementation and eases expansion in elastic cloud and extended enterprises, helps meet audit deadlines, and minimize deployment costs

Zettaset XCrypt Data Encryption Platform - Support for HIPAA Compliance Rules

The following table outlines specific areas within the HIPAA Privacy and Security rules where the Zettaset XCrypt Data Encryption Platform can assist healthcare organizations to achieve compliance with HIPAA regulations.

HIPAA Requirement	Regulation Reference	Zettaset XCrypt Platform Capabilities
Administrative Safeguards	164.308 (a)(1)(ii) • Risk Analysis • Risk Management	Automated integration with Security Information and Event Management (SIEM) systems can provide both data on unauthorized access attempts and identification of anomalous access patterns by authorized accounts – making risk analysis and reduction possible.
Access Management Provide authorization of access to users, authentication and de-registration of users when appropriate	164.308 (a)(4)(ii)(B,C) 164.308 (a)(5)(ii)(C) 164.312 (a)(2)(i) 164.312 (a)(2)(ii) 164.312 (a)(2)(iii) 164.312(c)(1,2) • Access Authorization, Establishment, Modification • Login Monitoring • Unique User IK • Emergency Access Procedure • Automatic logoff • Integrity and authenticity of ePHI	Zettaset XCrypt supports access management with access controls on top of native operating system capabilities for both local system roles and directory services – it decrypts information only for authorized access, allowing privileged users to perform their work without seeing data. Detailed audit and access data supports login/logout, policy creation, deletion or edits, backups, and user administration.
Encryption and Decryption While not specifically required by HIPAA, some organizations require that data be encrypted to meet certain standards. Some organizations provide "safe harbor" to their partners when data remains in the encrypted state.	164.312 (a)(2)(iv) 164.312 (e)(2)(ii) 164.312(e)(2)(i) 164.312(c)(2) • Encryption and Decryption • Encryption • Integrity • Mechanism to Authenticate electronic health information	Zettaset supports file level and volume level encryption with XCrypt Full DIsk and XCrypt Hadoop. Zettaset manages access to the encrypted data independent from the operating system's access control. While integrated with a customer's LDAP or Active Directory for authentication, access to decrypted data is based upon rules managed and administered within the XCrypt Data Encryption Platform.
Key Management Effective key management and protection must be demonstrated to support the encrypted state of data.	164.312 (a)(2)(iv) 164.312 (e)(2)(i) • Encryption and Decryption • Integrity Controls	Zettaset's Virtual Enterprise Key Manager (V-EKM) is designed for strong key management using a secure console. Administrators never see keys, access policies governing key management or separation of duties. XCrypt encryption products are also compatible with existing KMIPcompliant key managers.
Logging – Audit Controls Audit trails of access to data must be created and maintained. Monitoring Organizations are required to ensure that access to PHI/PII data is appropriate.	164.312 (b) • Audit Controls 164.308 (a)(1)(ii)(D) • Information System Activity Review	Zettaset XCrypt provides logging of access at the File System and Volume level. All read/write requests to sensitive data are tracked with compliant audit records. Reporting tools provide the ability to analyze logs.
Security Incident Management	164.308 (a)(6)(ii) • Response and Reporting	

For more information, please contact us at +1.650.314.7920 or sales@zettaset.com

Zettaset
465 Fairchild Drive, Suite 234, Mountain View, CA 94043 // USA: +1.650.314.7920 // Fax: +1.650.314.7950
sales@zettaset.com // www.zettaset.com

© 2018 Zettaset. All rights reserved. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. – AB.HITCH.EN-US.180122