EMC VNX2 WITH DATA-AT-REST ENCRYPTION FOR HEALTHCARE
Controller-Based Encryption for Maximum Protection and Flexibility

INTRODUCTION
In today’s computing environment, there are a number of threats to the information collected and stored by any enterprise. The severity of these threats is much higher when an enterprise begins to store the information on the end user devices, such as laptops, tablets, smart phones, flash drives, etc. A more inherent threat with handheld or mobile devices is the loss of a device, and then subsequent loss of data accessed from an unauthorized entity or individual. If your enterprise is regulated by the federal government, your risk for data loss will cause negative publicity, along with lost revenue, lost customers, and subsequent regulatory fines.

Industries such as healthcare, financial, federal and state governments and defense regulate the disclosure of personally identifiable information, as well as other sensitive information to unauthorized parties. For example, the healthcare industry is regulated by Healthcare Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA has been revised and expanded to govern data confidentiality through the HIPAA Privacy Rule, HIPAA Security Rule, Patient Safety Rule, and the HIPAA Breach Notification Rule. The HIPAA Privacy Rule protects the privacy of individually identifiable health information, HIPAA Security Rule sets national standards for securing the electronic protected health information, Patient Safety Rule protects patient health information being used to analyze patient safety events and improve patient safety, and HIPAA Breach Notification Rule requires covered entity and their business associates, to provide notification following a breach of protected health information.

OMNIBUS RULE
The Office of Civil Rights (OCR) enforces these rules and in September of 2013 announced a final rule that implements a number of provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The new rules (also known as the OMNIBUS Rule) expands the obligations of physicians and other healthcare providers to protect patients’ protected health information (PHI). It also extends the same obligations to a number of other individuals and companies working with healthcare providers. The rule increases the penalties for violations of these obligations.

There are severe financial penalties tied to noncompliance. The healthcare industry is taking steps to protect the patient information data from its conception, usage, storage, sharing, archiving, and destroying. The patient information traverses through a healthcare provider’s network through several components, and is often shared by other entities within the healthcare industry to provide patient care.
However, at some point, all patient-related information reaches a database for storage and becomes available for future retrieval. This is most commonly referred as data-at-rest. IT experts offer several definitions for data-at-rest based on the location of the data within the network.

In any case, the healthcare information that resides within a healthcare entity must be protected through encryption methodology, which prevents data visibility in the event of unauthorized access or theft.

OCR defers to the National Institute of Standards and Technology (NIST) Special Publication 800-111 to provide the basics of storage security. The NIST Publication 800-111 can be used to assist organizations in understanding storage encryption technologies for end user devices and storage devices in planning, implementing and maintaining storage encryption solutions.

**VNX SERIES – PERFORMANCE PLATFORM WITH SECURE DATA AT REST**

EMC® VNX® Series delivers industry-leading innovation and enterprise level capabilities for file, block, and object storage in a scalable, easy-to-manage platform. The new EMC VNX2 incorporates a number of changes; including new controllers designed to work with flash storage, and enhanced utilization of multi-core processors for increased performance. The VNX2 now adds another powerful security offering to its platform – Controller-based Data-at-Rest encryption (D@RE).

**TECHNOLOGY BEHIND DATA AT REST ENCRYPTION**

EMC anticipated the need for encryption of data-at-rest for many industries, and has taken measures to include the encryption hardware on the recently released VNX2 platforms. The VNX5200, VNX5400, VNX5600, VNX5800, VNX7600 and VNX8000 storage platforms have the hardware components to support data-at-rest-encryption functionality. EMC also chose controller based encryption because it is the most optimal and secured option of releasing encryption for data-at-rest, which means that performance impact on the data I/O will be minimized. The data will be encrypted by the back-end controllers using XTS-Advanced Standard (AES) 256 encryption, AES is a Federal Information Processing Standards (FIPS) approved cryptographic algorithm used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in block of 128 bits. AES-256 means that the EMC’s solution will be using a cipher key length of 256 bits, the same algorithm which is used to protect TOP SECRET data by the United States’ government.

**HOW DOES ENCRYPTION WORK?**

Federal regulations will dictate whether a customer is required to encrypt their data-at-rest. For the customers in the healthcare industry this will be a required item, if the customer chooses to encrypt data, then the entire VNX array’s data will be encrypted. There is no option for partially encrypting your data on the VNX array. Also, once the data is encrypted at rest, customers will not be able to store the data in clear on the VNX array.
In the event the data-at-rest encryption option is turned-on and a device writes to the VNX array, data is encrypted by the back-end controller, and is placed on the storage platform in an encrypted format. Subsequently, when the data is read from the array, the back-end controller will decrypt the data and send it over to the accessing device in a clear format.

**ENCRYPTION KEY MANAGEMENT**

EMC will modify the VNX Unisphere™ functionality and add new command line interface (CLI) commands for Controller based data-at-rest encryption. All encryption keys will be randomly generated, either at the install time, enablement time, or when a RAID group is created. These random keys are assigned to each disk drive. All keys generated will be unique by virtue of a randomly generated FIPS 140-2 compliant crypto module. Key Management Server will be a new component and will be a combination of RSA® BSAFE® product and CST Lockbox. RSA BSAFE product will be responsible for generating keys when the user completes provisioning of a RAID group within the array, and CST Lockbox will be responsible for storage of the keys. Key Management Server will monitor the changes to the configuration of the array that will require changes to the key storage. Keys will be generated and or deleted in response to the notification that a RAID group has been added or removed. The Key Management Server, in conjunction with the Unisphere, will provide the ability to securely offload the keys to a remote location for the purpose of backup.

**ADVANCED ARRAY SERVICES SUPPORTED**

EMC has chosen to use controller based encryption. This means all protocols supported by the VNX array today will be supported when the data-at-rest encryption is turned on. At the same time, all types of disk drives supported by the VNX platform today, along with all capacity of the drives supported by the VNX platform today, will support the data-at-rest encryption functionality. This approach will also support all the future drive types and capacities that will be introduced on the VNX platform. Advanced data services, such as replication, snaps, FAST™, compression, deduplication, backup, etc. will be supported, and there are no changes introduced to these services. Care must be taken when using replication, the replication process reads the data from the array and writes to a remote location. The process will read the data from the encrypted array in clear and transmit the data to the replicated site in clear. If data-at-rest encryption is needed at the replication site, another VNX array with an encryption option is required at the remote location, and the data transmitted across the two sites must be encrypted through other technologies.

**IMPLEMENTING ENCRYPTION FOR VNX2**

All VNX2 models (VNX5200, VNX5400, VNX5600, VNX5800, VNX7600 and VNX8000) are currently shipping with the back-end controller capable of encrypting data. The encryption software will be released in Q3 2014. Once the VNX2 D@RE software package, a right-to-use license has been installed and turned on, customers will be able to encrypt their data-at-rest on the array.
When this functionality is turned on, and if the customer is using FAST Cache, it needs to be temporarily disabled prior to enabling encryption. Once the data has been flushed to the back-end, the FAST Cache can be turned back on. After the FAST Cache has been flushed, the customer can use the user interface or command line to turn the data-at-rest encryption feature on. Once the feature is activated, the data in place will be automatically encrypted as a background task, while the new data sent to the array will be stored encrypted.

EMC will introduce a new optional software bundle package, starting in Q3 2014, for data-at-rest encryption. Customers wanting to encrypt their data-at-rest will be required to purchase the VNX2 D@RE package as optional software. This right-to-use license will support the entire VNX2 array regardless of the raw capacity or the number of drives, and will be priced based on the VNX2 model.