Using Dell Data Encryption for HIPAA HITECH

DirectDefense's analysis of Dell Encryption Enterprise & Dell Data Guardian on Windows Desktops and Servers attests that the products meets all of the HIPAA Security Rule requirements for encryption solutions as defined in §164.312(a)(2)(iv) which addresses data protection by encryption.

Background

If an organization processes, stores, or transmits EPHI, it must comply with the HIPAA Security Rule. The HIPAA Security Rule is separated into six main sections written to define a minimum level of security protections that an organization must implement. The implementation specification provides a detailed description of the approach to be used to meet a standard and is defined as required (R) or addressable (A). Addressable implementation specifications indicate covered entities must perform an assessment to determine whether the implementation specification is a reasonable and appropriate safeguard for implementation in the covered entity's environment.

The table that follows lists the six sections that all covered entities must comply with to meet the HIPAA Security Rule:

§164.306 Security Standards – General Rules	General requirements for all covered entities and business associates.
§164.308 Administrative Safeguards	Administrative actions and policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's and business associate's workforce in relation to the protection of that information. 5(ii) – "*Implementation Specifications"* (B) - "*Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software."*
§164.310 Physical Safeguards	Physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
§164.312 Technical Safeguards	The technical policy and procedures that protects electronic protected health information to control access, integrity and maintain audit controls. **Encryption requirements are defined here under 164.312.**
§164.314 Organizational Requirements	Standards for business associate's contracts or other arrangements between covered entities and business associates.
§164.316 Policies, Procedures and Documentation Requirements	Requires implementation of reasonable and appropriate policies and procedures to comply with the standards and implementation specifications.

The specific HIPAA Security Rule regarding encryption states:

***§164.312(a)(2)(iv) Encryption and decryption* (Addressable).**
Implement a mechanism to encrypt and decrypt electronic protected health information.

In summary HIPAA ensures that electronic patient health information (EPHI) is secured with due diligence and due care effectively with strong encryption.

DirectDefense Testing of Dell Encryption Enterprise & Dell Data Guardian Encryption:

To properly gauge the accuracy of the **Dell Encryption Enterprise & Dell Data Guardian** solution, DirectDefense tested the encryption capabilities of the platforms. Tests were run on servers and workstations to ensure that strong encryption was being implemented in a well-managed, easy to use manner.

Testing was performed using NMAP, Wireshark, HxD, file read and write code, and code written by DirectDefense to hook the Windows Kernel to monitor all activity at the Kernel level during the file encryption and decryption processes. Test cases were run for varying roles and rights, with differing levels of access (owner vs other users), different types of files. Files were also tested with progressive pattern analysis to ensure that recognizable patterns are not possible to be obtained.

DirectDefense also tested key security and generation capabilities of the products. New keys were generated. The security of their storage was reviewed. Re-encryption of data scenarios were performed. Failover processes were tested and reviewed to ensure that the risk of data loss is minimized while maintaining security.

Conclusions

In conclusion DirectDefense attests that Dell Encryption Enterprise & Dell Data Guardian is 100% compliant with HIPAA HITECH encryption requirements for protection of PHI and reporting requirements when it has been properly deployed within the Electronic Healthcare Records (EHR) environment.

Dell Encryption Enterprise & Dell Data Guardian exceeds the HIPAA HITECH compliance requirements which are only “addressable” meaning that they are assessable. Dell Encryption Enterprise & Dell Data Guardian adds a layer of security and due care that stops data breaches from occurring in the case that a system containing EPHI is compromised by an attack. Even with full access to the system the attacker, who could be an internal employee, still would not be able to access the sensitive EPHI data because it is strongly encrypted with strong access controls.

Litigation is a large concern for all healthcare organizations. Using Dell Encryption Enterprise & Dell Data Guardian to protect EPHI it demonstrates the highest possible level of due diligence and due care which is of great importance in the case of disputes. Not only is your data more secure with strong encryption but it shows the extra efforts being taken to protect data.

Signed:  Date: 4/11/2017

Jim Broome, CEO DirectDefense