Allscripts Enterprise

INFORMATION PRIVACY & SECURITY POLICIES:

ENCRYPTION STANDARDS FOR PUBLIC CLOUD ENVIRONMENTS

Revision:	1.0 – FINAL
Approval Date:	December 01, 2015
Security Policy:	S-10-01
Approval Authorities:	CPSC & CSO

Reproduction and distribution of this document without the express written permission of Allscripts Healthcare Solutions, Inc. is strictly prohibited. The methodology and models presented herein are proprietary with copyrights, Allscripts Healthcare Solutions, Inc. (Allscripts).

Summary of Changes

Date	Version	Summary of Changes	Author
12/01/15	1.0	Policy Initiation	Compliance Team

Approval Log

Date	Version	Authority
12/01/15	1.0	CPSC & CSO

CONFIDENTIAL

1.0 Contents

CONFIDENTIAL

2.0 Purpose and Scope

- The purpose of this **Encryption Standards for Public Cloud Environments** is to outline the key requirements for Allscripts Healthcare Solutions, Inc. and its subsidiaries (Allscripts) to create, store, or process Confidential and Proprietary information, Protected Health Information (PHI), Personally Identifiable Information ("PII"), Personal Information ("PI"), Personal Data ("PD"), and/or other sensitive information (collectively, "Sensitive Information") in a Public Cloud environment.
- All members of the Allscripts workforce, including permanent full or part-time employees, agents, and independent contractors, shall abide by this Policy.
- Contractors who may collect, process, use, disclose, access, store, transmit, transfer, or create Sensitive Information shall also abide by this Standard.

3.0 Requirements & Examples

3.1 Information that has no PHI/PII or other Sensitive Data

- *Requirement*: Encryption not required except for the storage of credentials, in which case the passwords must be stored as hashed [i] values.
- *Example*: publically available information, newsletters, ACE announcements, etc.

3.2 Company Confidential Information without PHI/PII/other Sensitive Data or with PHI/PII/other Sensitive Data

- *Requirement*: Encryption by at least one of the following: hardware disk encryption; file level encryption (e.g., TDE encryption).
- *Example*: product development environments; testing/QA environments.

3.3 Any system/application/database/file with PHI, PII, or PD whether for production, development, or any other use.

- *Requirement*: Encryption to Safe Harbor standards by at least one of the following: hardware disk encryption (e.g., Self-Encrypting Drives or SEDs); file level encryption (e.g., TDE encryption); or field-level [i] encryption of all PHI/PII/PD data elements. Additionally, from a defense in depth approach, data that have heightened protections such as social security numbers, or similar national identifier numbers, shall be encrypted at the field level. [i]
- *Example*: hosted client applications; Allscripts corporate applications/databases with PII or other Sensitive Data.

3.4 Data in Transit [ii]

- *Requirement*: TLS over the Internet or encrypted communication link, e.g., VPN or dedicated circuit.

CONFIDENTIAL

- *Example*: any data that is moving into or outside of an Allscripts controlled data center via public or “untrusted” networks such as the Internet.

3.5 Credential Protection

- *Requirement*: The use of hashed [i] passwords is mandatory regardless of the type of information involved.
- Any exceptions must be approved by the Chief Security Officer, Chief Privacy & Security Counsel, and SVP Solutions Development Organization before deployed.

---

[i] When implementing encryption or hashing, the use of cryptography must at least be compliant with the Federal Information Processing Standards (FIPS) 140-2 Annex A list.

[ii] Encryption of data in transit must comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection, Configuration and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs

CONFIDENTIAL