MSK Vendor Information Security Requirements

Introduction

This document establishes the minimum requirements expected of Third-Party Vendors and Business Associates ("Vendors") which access, process, or store MSK Data; as well as any Vendors developing Information Systems ("Systems") designed to do the same. As part of their Information Security Program, Vendors must maintain controls at least as rigorous as those set forth in this document where appropriate and applicable. These controls must be implemented in addition to requirements set forth by any applicable laws and governing standards which may include, but is not limited to, the Health Insurance Portability and Accountability Act ("HIPAA") or the Payment Card Industry Data Security Standards ("PCI DSS").

Definitions

"MSK Data" has the same definition ascribed to it in applicable governing agreements, provided that in the absence of such definition, as used herein the term includes any data supplied by or on behalf of MSK or its affiliates to Vendor.

"MSK Sensitive Data" means any MSK Data which, in the event of its unauthorized use, disclosure, access, alteration, or destruction, could i) by law or regulation require notice to affected individuals or governing bodies; or ii) have a material adverse impact on MSK, its operations, or workforce members.

"Information System" ("System") means any discrete set of information resources (such as hardware, software, and associated information technology services) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of MSK Data.

Requirements

1. **Vendor Information Systems.** For non-MSK managed Systems used by Vendor, its employees, contractors, or agents to access, process, or store non-public MSK Data, Vendor must ensure:
   - 1.1. User Access Management. Formal, documented procedures must be followed for access authorization, provisioning, review, and revocation based on the principle of "least privilege" permitting access only to the systems, functionality, and data required for its workforce members to perform their duties.
     - 1.1.1. User access to non-public MSK Data must be uniquely authenticated and individually attributable.
     - 1.1.2. Access rights of any Vendor employee, contractor, or agent must be revoked promptly upon termination or change in job role which eliminates the requirement for continued access.
     - 1.1.3. Provisioned access rights must be reviewed at least annually to ensure continued least privilege.
   - 1.2. Passwords and Authentication. Passwords used to authenticate access must be at least eight (8) characters in length and be constructed of mixed case letters, numbers, and symbols.

1.2.1. The requirement for symbols and numbers may be waived for passwords with an enforced length of at least twelve (12) and sixteen (16) characters, respectively.

1.2.2. Passwords suspected to have been compromised or shared must be changed promptly upon discovery.

1.3. Password Storage. Passwords must only be stored hashed, utilizing a salting mechanism, with an algorithm that implements a work factor (such as PBKDF2, bcrypt, or scrypt). Authenticators used in multi-factor authentication mechanisms (such as PKI or biometrics) must be afforded the same secure storage protections.

1.4. Encryption. Non-public MSK Data must be encrypted while at rest, when written to removable devices, and while in transit using industry standard platform and data-appropriate encryption in non-deprecated, open/validated formats, and standard algorithms. Where applicable and commercially reasonable, such encryption solutions must utilize cryptographic modules which have been issued a Federal Information Processing Standards (FIPS) 140-2 validation certificate. Whenever Vendor does not utilize validated modules solely due to commercial reasonableness, Vendor will disclose the factors of that decision to MSK.

1.4.1. Removable media and/or mobile devices must not be used to store or transport MSK Sensitive Data unless explicitly authorized, in writing, by MSK.

1.5. Data Storage. Storage media within Vendor control (whether magnetic, optical, non-volatile solid state, paper, or otherwise capable of retaining information) that captures MSK Sensitive Data must be sanitized in accordance with the most recent release of National Institute of Standards and Technology (NIST) SP 800-88, or comparable industry standard, prior to its repurposing or disposal.

1.5.1. Upon termination of applicable governing agreements with MSK, Vendor must delete all copies of non-public MSK Data in such a way as to make them forensically unrecoverable. In such an event, Vendor must provide an attestation of destruction upon MSK's reasonable request.

1.6. Vulnerability and Patch Management. Formal, documented procedures must be followed governing the identification, distribution, and application of security patches. *Note that FDA-governed medical devices are not exempt from this requirement.*

1.6.1. Applicable security patches must be deployed in a timeframe commensurate with their severity, not to exceed thirty (30) days after publication for Critical and High impact vulnerabilities.

1.7. Anti-Virus/Anti-Malware. Appropriate anti-virus/anti-malware solutions must be implemented where an acceptable solution is available, in accordance with the most recent release of NIST SP 800-83, or comparable industry standard.

1.8. Logging and Monitoring. Sufficient administrator and event logs must be generated and retained to allow for the investigation and non-repudiable attribution of suspicious or malicious activity.

1.8.1. Any access, modification, and deletion of MSK Sensitive Data must be captured in relevant logs.

1.8.2. In the event of a security incident suspected to impact the confidentiality, availability, or integrity of non-public MSK Data, appropriate and relevant log information must be shared with MSK upon reasonable request.

2. **Vendor Developed Systems.** For Systems developed by Vendor, its employees, contractors or agents intended to access, process, or store non-public MSK data, Vendor must ensure:
   2.1. Secure Design. Systems must be designed in such a way to allow for (i.e., does not preclude) the implementation of the technical and procedural controls mentioned in above Section 1, irrespective of the party managing said Systems (e.g., Vendor-managed, MSK-managed, etc.) or performing referenced actions.
   2.2. Secure Coding Practices. Formal, documented secure software engineering and coding practices must be followed to address common security risks.
   2.3. User Authentication. Systems must support MSK Active Directory integration or Single-Sign-On (SSO) for MSK user authentication and authorization.
3. **Network Security.** For Systems hosted by Vendor, its contractors, or agents which access, process, or store non-public MSK Data, reasonable protections must be implemented at the network and/or host level designed to detect and prevent unwanted or hostile network traffic.
4. **Physical Security.** For facilities which Vendor controls, appropriate physical security measures, including visitor access controls, must be maintained to ensure the protection of company assets and non-public MSK Data.
5. **Remote Access.** In the event that Vendor requires remote access to MSK's internal network (including access to any Vendor provided equipment thereon), Vendor must ensure that it exclusively occurs using an MSK provisioned and managed solution.
6. **Awareness and Training.** Vendor must ensure all employees, contractors, or agents receive regular security awareness training, including any laws and contractual obligations that govern personal information and customer data, and instruction on safeguarding such data against loss, misuse, or other security events.

Contact Information
For more information regarding these requirements, contact the MSK Information Security Office.

Effective Date:	01/01/2013
Revision Dates:	03/18/2016
	05/16/2018
	07/15/2019
	6/11/2020