NYC Health + Hospitals
Information Security & Risk Management:

Vendor Security Requirements

NYC HEALTH + HOSPITALS

Document Control

Author: ISRM Risk Management

History

Created on: 8/17/2018

Revision History

Version	Date	Notes
1.0	9/5/2018	1st Draft
2.0	1/23/2019	Revised authentication requirements
3.0	2/20/2019	Tabulated requirements
3.1	3/25/2020	No changes required, other than the review interval.
4.0	1/5/2021	Add requirement to change default passwords
5.0	9/7/2022	Add requirements for PFS-capable ciphers and interface to PPM system. Tweaked the control audit requirement.

*To be reviewed ANNUALLY

NYC HEALTH + HOSPITALS

Contents

1.0 Purpose

This document has been created to highlight NYC Health + Hospital's (the System) security requirements which should be met by the vendor(s) during the selection process.

2.0 Scope

This document should be used for the purpose of understanding NYC Health + Hospital's minimal security requirements during the vendor selection process. It does not replace the requirement to complete a security review during the new business or project initiation request process (i.e. Project In-Take).

3.0 Security Requirements

The Security requirements have been divided into 3 high level sections – Business, Infrastructure, and Application. Details on each are described below.

Requirements stated as MUST or MUST NOT are **mandatory**.

Requirements stated as SHOULD or SHOULD NOT are strongly preferred practices. If they cannot be met, the vendor(s) must provide compensating controls.

Please enter an 'X' to designate the *Yes* or *No* response on each row in the following sections. If a requirement is not currently met, then in addition to denoting the 'X' in the *No* column for that row, a comment should be included describing why the control is not met as well as your roadmap for compliance. For controls stated as "SHOULD" also include any compensating controls.

3.1 Business

Requirement	Yes	No	Comment
Any vendor handling ePHI MUST sign the System's BAA (Business Associate Agreement).	○	○	
The vendor SHOULD follow industry best practices for security governance and training (e.g. ISO 27001:2013).	○	○	
The vendor MUST allow the System to assess their data security controls or make scheduled audit reports available (as needed given new scope, upgrades, etc.).	○	○	

3.2 Infrastructure

Requirement	Yes	No	Comment
The (on-premise) application MUST support either the current or immediate prior version of the operating system.	◯	◯	
The version of the operating system used MUST still be under active vendor support.	◯	◯	
All data transfers SHOULD use one of the System's approved methods, either SFTP through the System's KiteWorks server or a site-to-site VPN.	◯	◯	
Internet-facing web servers MUST use trusted certificates issued by a Certificate Authority (CA) that is in the default Trusted CA list of all major browsers (IE, Edge, Chrome, Firefox).	◯	◯	
Internal-facing web servers MUST be capable of using a certificate issued by the System's internal CA.	◯	◯	
Any external infrastructure hosting the System's applications or data SHOULD only be hosted in the USA.	◯	◯	
Applications MUST use a standard method of authentication or federation so that users' credentials in the System's Active Directory (AD) are used for authentication and group permissions.	◯	◯	
Standard federation or integration protocols (e.g. SAML 2.0, LDAP, or Kerberos) SHOULD be used for AD authentication.	◯	◯	
Any Wi-Fi connectivity for the application MUST be provided by the System's infrastructure according to our standards (currently WPA-2 Enterprise).	◯	◯	
All external hosting providers SHOULD adhere to established governance framework(s) involving data security controls such as HIPAA, PCI, SOC 2 (type I & II), ISO 27001:2013, NIST800-144 etc. In addition, cloud providers SHOULD adhere to Cloud Security Alliance (CSA) standards and certifications.	◯	◯	
External hosting providers SHOULD have capabilities to detect leakage of sensitive or confidential data.	◯	◯	
Externally hosted applications SHOULD implement virtual network segmentation and zoning across tiers.	◯	◯	
The vendor SHOULD provide end-to-end encryption for data-in-transit using TLS 1.2 with a cipher suite supporting perfect forward secrecy (PFS).	◯	◯	

3.3 Application

Requirement	Yes	No	Comment
Application SHOULD be designed to defend against the OWASP Top 10 and SANS Top 25 vulnerabilities.	◯	◯	
Default passwords MUST be changed on installation.	◯	◯	
Default password change SHOULD be enforced by installation scripts.	◯	◯	
Applications hosting ePHI MUST be encrypted at rest (locally and in the cloud) using an approved encryption algorithm and key length (currently AES-256).	◯	◯	
Proprietary cryptographic algorithms MUST NOT be used.	◯	◯	
Application running on-premise MUST use only domain service accounts (or group-managed service accounts) for started services and scheduled tasks.	◯	◯	
Application SHOULD use RBAC (Role Based Access Control) to determine each user's type and level of access, both within the application and the database.	◯	◯	
End user components of the application MUST NOT require local administrator rights for normal operation.	◯	◯	
Authentication dialogs between client and server SHOULD be encrypted with TLS 1.2 or higher using a cipher suite that supports PFS.	◯	◯	
Applications hosting ePHI that are used for patient care SHOULD support an approved Break-the-Glass process.	◯	◯	
Application MUST record every user activity, authentication, authorization process including user name, date and time in the event logs. In addition, changes to protected / sensitive information including user, date and time in the event logs MUST be recorded.	◯	◯	
Application SHOULD be capable of exporting log data to the System's Patient Privacy Monitoring (PPM) system.	◯	◯	
System SHOULD protect against tampering of audit logs by a System Administrator or other users.	◯	◯	
Applications SHOULD follow a three-tier design (Presentation – Application Logic – Data).	◯	◯	

Requirement	Yes	No	Comment
The data layer MUST NOT be exposed to the Internet.	◯	◯	
The application MUST NOT require writing to an unencrypted USB (or other removable) storage device for routine operation.	◯	◯	
The application MUST be compatible with the System's standard commercial off the shelf (COTS) virus scanning software products for removal and prevention of malicious code.	◯	◯	
The application MUST be certified to perform as intended with security updates to the operating system and other helper applications (such as service packs and hotfixes). There SHOULD be a process for customer notification after each patch release.	◯	◯	
Data used for development or testing MUST either be dummy data or production data that has been appropriately masked.	◯	◯	
Source code MUST be appropriately protected against unauthorized changes.	◯	◯	