Attachment 3 (B); Security Exhibit

As of March 29, 2016

UVA Medical Center (UVaMC) Security Requirements

The term “System” shall mean computer equipment, peripheral equipment, system software, application software, or embedded or included third party software provided to UVaMC.

Systems containing EPHI (electronic protected health information) must meet or exceed all current regulatory requirements including those emerging from the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009.

The Vendor warrants their application software is free of any requirements that would, if followed, create a potential security risk, e.g., requiring accounts without passwords or with non-complex or widely published/generic passwords.

The Vendor will provide the System in a condition that allows it to be connected to the UVaMC network without exposing the network to risk of security compromise. The vendor will allow UVaMC to place a firewall between the system and the Internet without breach of contract.

The Vendor will participate in the UVaMC security evaluation and certification program and will perform any needed remediation before System is accepted and placed into production. The UVaMC security evaluation and certification program is an ongoing process which periodically requires System security remediation. UVaMC reserves the right to modify, replace, upgrade, or remove any software or security practice as is deemed appropriate by UVaMC.

For Systems involving Application System Providers, the UVaMC Cloud Risk Assessment process must be completed before purchase of the System.

The Vendor accepts all terms defined within this document without voiding or negating any performance warranties.

I. Group Policy

All Windows based servers must be members of the Medical Center’s existing Microsoft Domain and utilize domain baseline group policy. Acceptable Business needs must be presented to enable features locked-down by this policy.

Other operating systems must also run UVaMC standard baseline security standards. These are consistent with the Center for Internet Security (CIS) Critical Security Controls.

II. VPN Support Connectivity/Secure Data Transfer

Vendor access will be achieved using Cryptocard VPN tokens, Firepass SSL Web Access, Cisco client software, and Microsoft Remote Desktop.

Point to Point/Site to Site VPN's are required to be limited to specific port(s) access as well as a finite number of vendor IP addresses.

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Guides for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations recommends using 256 bit encryption or stronger. Any data transferred via the Internet will be encrypted with no less than 256 bit encryption methods.

III. Encryption

As recommended by NIST SP 800-52 system does not prevent the use of hardware or software based full disk encryption technologies or must include data at rest encryption capabilities.

IV. Administrative Rights/Principle of Least Privilege

UVaMC adheres to the information security best practice of Least Privilege. This approach minimizes the privileges available to a user to those that are critical to performing specific tasks. This approach minimizes risk exposure for both UVaMC and the vendor, shows due diligence in protecting data and the UVaMC customer base, and demonstrates the separation of duties.

Initial Installation of System/Application

1. UVaMC staff will use their existing security access to assist the vendor/application administrator with the initial installation.

   Or

2. A local vendor/application administrator account will be created on the server with local administrator privilege. This account will only be enabled when a vendor/application administrator needs access to the system; it will be disabled at all other times. While the vendor/application administrator is working on the system his/her session will be monitored/reviewed by a UVaMC Technical Services staff member via Terminal Services or other technology to review the actions that are being performed. This is commonly referred to as the information security best practice of the "two man approach".

Vendors must review their application to identify the least privileges required for their application to operate successfully. Services/processes will only be permitted to run with administrator privileges if the program cannot be successfully operated otherwise and UVaMC has determined that this operation does not impose a security risk. In such cases the account password to the service/process will be retained by UVaMC and the vendor/application administrator must contact UVaMC LAN staff to enable access.

Ongoing System / Application Support

1. Most modern application vendors supply administrative programs for their applications that run from the Application Administrator's pc. In this case all necessary access is provided through this program and additional server privileges are not granted.

2. For applications that require direct server access to be managed, UVaMC will provide system access to a locked down desktop on the server on which only the necessary programs/access have been made available. This will provide the application administrator direct day-to-day access to managing/troubleshooting the application without the need for additional assistance from UVaMC Technical Services staff. If access is required to additional items that are not available then UVaMC Technical Services staff should be contacted for assistance or to review for possible addition.

V. Operating System Security Patches

Microsoft Security Patches are applied using Microsoft Windows Update Server. Test servers receive updates on their release on the 2nd Tuesday of the month. If no problems present themselves by the end of the following business day, production servers are then patched according to the scheduled downtime established for each server. This process normally occurs within 7 days of patch release from UVaMC. For all released patches to be installed, Vendors will provide approval within 7 days of Microsoft patch release or provide specific documentation as to why a specific patch cannot be installed and when and how the patch can be installed. UVaMC reserves the right to install patches at any time in order to maintain the overall security of the Medical Center and Health System.

Application vendor will test and approve all Microsoft Service Packs within 3 months of Microsoft release dates. All Microsoft Service Packs will be installed within 6 months of Microsoft release dates.

Other UVaMC approved operating systems will be patched on a monthly basis. Application vendor will test and approve all operating system and operating system vendor distributed patches for other modules within 30 days of release. UVaMC reserves the right to install patches at any time in order to maintain the overall security of the Medical Center and Health System.

VI. 3rd Party Software Patches

Vendors must report and provide security patch remediation to address all security issues with base products and 3rd party products as vulnerabilities are discovered/disclosed by UVaMC or 3rd party scanning tools. The primary application vendor must address and remediate any publicly known vulnerability that may exist with base product or 3rd party products that the primary application may utilize. These vulnerabilities must be addressed within 30 days of request from UVaMC. UVaMC reserves the right to install patches at any time in order to maintain the overall security of the Medical Center and Health System.

VII. Antivirus

UVaMC has implemented Symantec as the Antivirus solution on all servers and is placed into a managed policy. As new virus definitions become available they are applied to the servers. The Vendor agrees to allow UVaMC to add this software without being in Breach of Contract. Antivirus definitions are downloaded if available from Symantec, and updated on an hourly basis.

VIII. Passwords

All passwords are required to be complex, i.e., each should consist of at least eight (8) characters with upper and lower case letters, numbers, and/or special characters. Passwords must not be a word found in a dictionary. Vendors will provide documentation detailing the process for changing service account passwords. Password must not be in clear text while in network transit or while at rest within the storage of the application.

The Vendor warrants to the best of Vendor's knowledge that all software and code delivered does not contain any Trojans, backdoors, time bomb code, time outs, or other lock-out features which will restrict UVaMC's use of this system. Vendor further agrees that the System does not send any information back to the vendor without knowledge and consent of UVaMC.

IX. Authentication

Applications are required to authenticate against UVaMC Microsoft Active Directory. This can be accomplished by using integrated Windows authentication via normal desktop authentication, Active Directory Federation Services or by using LDAP Authentication against Microsoft Active Directory within the application.

Usage of Microsoft Active Directory allows for single/simplified sign on ability within the domain and also allows for usage of Microsoft Active Directory Groups for Access Control. UVaMC Computing Services LDAP requirements are attached.

X. Vulnerability Checks

UVaMC uses 3rd Party scanning software to perform security scans against servers in the DMZ and internal networks. This scanning includes, but is not limited to, port, operating system, application, and web application scanning. Servers residing on the DMZ will receive daily scanning, and servers within internal networks will receive not less than weekly scanning.

All servers must pass a security scan before they are added to the domain. Additional security scans are run immediately after applications updates and as part of an enterprise scheduled scan. Vulnerabilities will be reviewed and addressed with the vendor, preventive measures may be taken depending on the risk associated with the vulnerability. All Microsoft and 3rd Party patches must be installed as previously defined.

XI. Monitoring

UVaMC has implemented numerous monitoring systems including, but not limited to Microsoft System Center Operations Manager (SCOM), HP Insight Manager, Netbotz environmental monitoring and Integrated Research's Prognosis. The Vendor agrees to allow UVaMC to add this software without being in Breach of Contract.

XII. Documentation

Vendor will supply UVaMC with detailed installation instructions as Microsoft Word documents or Adobe PDF files for all applications including 3rd party applications required by the primary application. Vendor provided documentation will be added to that developed by UVaMC.

Vendor will supply UVaMC with appropriate documentation on how to properly backup and recover the System.

To maintain proper Change Management, modifications to the System must be reviewed and accepted by UVaMC prior to implementation.

XIII. Backup and Recovery

Server data must be backed-up at least daily. Application vendor must provide adequate documentation for proper back-up and recovery processes. All backups will be monitored on a minimum daily basis. Failed backups will be re-processed if feasible.

System State Backup

UVaMC performs System State Level backups on a daily basis for all Windows server systems.

XIV. Databases

UVaMC Computing Services preferred database provider is Microsoft SQL 2014 databases.

SQL servers are backed-up using one of two methods. The first involves configuring maintenance plans for all databases within the SQL Server followed by the back-up of the live SQL data to a flat file SQL Backup located on the server. UVaMC will then backup these files to the UVa backup system.

The second method, typically used by larger SQL implementations, involves using the advanced SQL client provided by the backup vendor. The advance option using the same SQL APIs that are used for the maintenance plan, the difference being that the data is backed up directly to UVa backup system, bypassing the production of flat files.

Non-SQL databases (e.g., Oracle, Access, MySQL, InterSystems Cache, and others) are to include a Vendor-provided export function that will export the data into a flat file format using a scheduled process.

XV. Operating System / Hardware Standards

UVaMC uses Microsoft Windows Server 2012 R2 Hyper V Server to improve hardware efficiency and reduce hardware costs on Windows server systems. Servers that require an isolated OS environment and that do not have heavy I/O demands are good candidates for Virtualization.

UVaMC reserves the right to use Microsoft virtualization technology in order to more efficiently utilize physical server hardware. Specific I/O requirements may be requested by the vendor from UVaMC in order to properly evaluate.

UVaMC utilizes HP server hardware for Windows and Redhat server systems. Specific models of hardware must be reviewed and accepted by UVaMC in order to meet UVaMC standards.

UVaMC supports other Operating Systems as well, these include: AIX and RedHat.

XVI. Auditing

The Health Information Portability and Accountability Act (HIPAA) Security Rule § 164.308 Administrative safeguards (ii) (D) Information system activity review (Required) states: "*Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking*". Vendor application will provide the means by which UVaMC can monitor and audit for user access including successful and failed logins, as well as data access auditing as required by HIPAA or other regulations, legislation, and statutes.

XVII. Additional Requirements for Vendors Providing Support

All employees or agents will pass an industry-standard background check.

All vendor employees will have access removed immediately upon termination.

Vendor will be able to produce a list of who has physical and logical access to system.

Vendor will maintain antispyware hardware/software.

Vendor will provide documentation on how log files are reviewed.

Exhibit C1

University of Virginia Health System
Active Directory/LDAP Integration

Integration:

The primary objective of integration with the Health Systems' Microsoft Windows 2012R2 Active Directory infrastructure is to enhance and simplify the overall end user experience.

This can be achieved by:

1) Utilizing the user id and password contained within the Active Directory.
   This process provides Authentication for the end user without having to require the end user to remember multiple user ids or passwords.

2) Utilizing the group memberships of the user id to provide Access Control to Application resources.

Description of Health System LDAP (Lightweight Directory Access Protocol):

The Health Systems' LDAP servers are supplied by the LDAP services provided within the Microsoft Windows 2012R2 Active Directory infrastructure. The current schema is the default schema provided with Windows 2012R2 and has been extended with Microsoft Exchange 2013 Server extensions.

Microsoft's LDAP service is based upon the X.500 hierarchy. As such, user objects may be contained within any Organizational Unit within the X.500 hierarchy.

The primary purpose of the LDAP server is to provide user authentication and access control. **It is not intended to be an overall database repository for miscellaneous data fields.**

Requirements of integration:

1) Vendor supplied application must support the X.500 hierarchy of the Microsoft Windows 2012R2 Active Directory.

This entails being able to locate the distinguished name of the user object within any Organizational Unit within the X.500 Hierarchy

2) Vendor supplied application must support multiple LDAP servers in order to prevent single point of failure. The application should be able to dynamically switch over to the alternate LDAP server in the event that service is disrupted on the primary LDAP server.

3) Vendor supplied application must support using SSL with LDAP (Port 636). This requirement is to provide encryption of sensitive data that is passing over the network.

Additional LDAP Integration Requirements and Validation:

The following list details additional exception handling that a Vendor supplied application should provide.

1) **Successful Login**
   a) Test Description: Attempt to login using a valid user id and password.
   b) Pass/Fail Criteria: Login to the application was successful. Repeat the test several times to make sure it the login process is done in a reasonable time.
2) **Wrong Password**
   a) Test Description: Attempt to login using a valid user id and a wrong password.
   b) Pass/Fail Criteria: On failure, an error message similar to “Username or Password is incorrect” should be displayed.
3) **User Account does not exist**
   a) Test Description: Attempt to login using a user id which does not exist.
   b) Pass/Fail Criteria: On failure, an error message similar to “Username or Password is incorrect” should be displayed.
4) **User does not have application access privileges**
   a) Test Description: Attempt to login using a valid user id and password to an application which the user does not have access to.
   b) Pass/Fail Criteria: On failure, an error message similar to “User XXXX does not have permissions to access this application.” should be displayed.
5) **Disabled user account**
   a) Test Description: Disable a user on the LDAP server and try to login using that user id.
   b) Pass/Fail Criteria: On failure, an error message similar to “User XXXX is locked. Please contact System Administrator.” should be displayed.
6) **Expired Password**
   a) Test Description: Expire a user password on the LDAP server and try to login using that user id.
   b) Pass/Fail Criteria: On failure, an error message similar to “Account password has expired, please change the password.” should be displayed.

Example of Typical LDAP Usage:

1) Application performs a simple BIND to the LDAP server using a predefined user id that is created at the top level of the X.500 hierarchy.

2) Application searches the X.500 hierarchy for the distinguished name of the user object by performing a recursive whole tree search by using the SAMACCOUNTNAME attribute.

Note: The distinguished name may contain backslashes, commas, and other characters.

3) Application attempts to perform a Simple Bind using the distinguished name and password collected from the application. This step provides “Authentication”.

4) Application searches for the filtered Group and Member attributes of the distinguished name of the user object. This will return the groups that the user id is a member of.

5) Application verifies that the returned values contain the necessary group for security clearance. This step provides “Access Control”.