Maintaining a Production VistA EHR: Security Issues, and Mitigation and Remediation Strategies

Prepared by:

VistA Security Technical Working Group (TWG)

under

VA Contract Number: VA118-16-C-0841

Version 1.0
April 18, 2017
# Table of Contents

## 1 Foreword

1.1 VistA Security TWG

1.2 Purpose and Organization of Paper

1.3 Acknowledgments

## 2 Network and Infrastructure Security

2.1 Physical Access Controls

2.1.1 Facility Access for Employees

2.1.2 Visitor Control

2.1.3 Additional Physical Security Controls at Datacenters

2.1.4 Workstation/Workforce Separation

2.2 Configuration Management

2.2.1 Asset Management

2.2.2 Change Management

2.2.3 Patch Management

2.3 Connectivity

2.3.1 Internet Connectivity

2.3.2 Partner Connectivity

2.3.3 Wireless Connectivity

2.3.4 Internal Firewalls and Defense in Depth

2.4 Embedded Systems and the Internet of Things

2.5 BYOD

2.6 Log Files and Auditing - Host Level

2.7 Vulnerability and Risk Assessments

## 3 System and Process Security

3.1 Confidentiality

3.1.1 Encryption

3.1.2 User Authentication – Access/Verify Codes

3.1.3 Non-Person Authentication

3.1.4 Restriction of Access to Patient-Sensitive Information

3.1.5 Media/PHI Management and the Final Disposition of Data
1 Foreword

It can be argued that VistA is an exceptionally secure electronic health record system. Tightly integrated design based on M technology constricts the number of direct external threats to the core system to a small number. Additionally, VistA runs behind a tightly secured firewall both within Department of Veterans Affairs (VA) facilities and at many open source sites.

However, VistA also relies increasingly on interoperability with internally and externally networked device and systems for data and multimedia acquisition, storage and reporting. This reliance expands the perimeter of exposure to external threat. Moreover, resolution of internal operating and user vulnerabilities is essential to the safe and secure operation of any system, particularly one responsible for the real-time and long-term needs of millions of healthcare consumers.

We therefore offer this volume as a checklist of possible vulnerabilities to VistA installations and suggestions for risk mitigation. Readers are encouraged to adapt these strategic suggestions to the needs of their particular VistA implementation, and to suggest additional topics for discussion.

Most importantly, we welcome constructive feedback about any errors or omissions in this document. Please address any comments or questions to security-twg@groups.osehra.org.

1.1 VistA Security TWG

The VistA Security Technical Working Group (TWG) was the first to be established by the Open Source Electronic Health Record Alliance (OSEHRA) under VA contract VA118-16-C-0841, Open Source Technical Support and Working Group Services for VA Vista. This contract called for the establishment of technical working groups that would increase communication between VA and the open source community, elaborate on VA requirements, and solicit feedback from the community on how to improve those requirements.

Because of the increasing emphasis on information security across the community, as well as previous success in collaboration on security vulnerabilities, the Vista Security TWG was established as the prototype group. The criticality of this topic brought immediate participation from multiple key members of the community, including developers, security specialists, certification organizations, and VA stakeholders. At the initial meeting, the group decided to begin their collaboration by producing a strategy document that could serve as a focal point for discussion on Vista security. Following the publication of this document, the group will continue to collaborate on specific security issues, including policies and actual technical vulnerabilities.

1.2 Purpose and Organization of Paper

This paper was written to provide VistA implementers a high-level overview of the salient security issues associated with operating a VistA instance, along with practical recommendations for
mitigation/remediation. The authors are aware that most instances of VistA address many (or even most) of these issues. However, it is rare that all of these issues are adequately addressed, and the attacker’s advantage lies in the fact that any exploitable vulnerability is sufficient to begin exploration and possible compromise.

Sections 2 and 3 contain the bulk of the specific issues. Section 2 focuses on network and infrastructure which, if not properly designed, implemented, and maintained, can nullify many of the application-level security precautions currently in use. It also offers suggestions on network topology that, to the best of our knowledge, have not yet been implemented in VA facilities. Section 3 addresses systems and processes, including application-level security. This section is structured to correspond with the three major cybersecurity areas: confidentiality, integrity, and availability.

Sections 4 and 5 provide more strategic future guidance. Section 4 reflects current discussions regarding cloud implementation, open architecture, and further COTS acquisitions. Section 5 provides useful references to other large providers, as well as ongoing standards work at NIST.

Three appendices are included: two policy templates (one for Personal Health Information, and the other for operating with a Cloud Service Provider), as well as a glossary of terms.

1.3 Acknowledgments

This strategy document was developed by the VistA Security Technical Working Group (TWG), established by the Open Source Electronic Health Record Alliance (OSEHRA) in hopes to encourage a robust security strategy for the VistA Community, including the U.S. Department of Veterans Affairs (VA). OSEHRA thanks all members of the VistA Security TWG as well as the Co-Chairs Mike Henderson of Document Storage Systems, Inc. (DSS) (formerly a member of the OSEHRA staff) and Terry Luedtke of VA. OSEHRA would like to acknowledge contributions made by group members from VA, DSS, the Electronic Healthcare Network Accreditation Commission, PatchAdvisor, Inc., and SAFE BioPharma. The VistA Security TWG members, and their organizational affiliations include:

| Peter Alterman | Samuel Giles | Mike Lotas |
| SAFE BioPharma | ASM Research | Intelligent Waves LLC |
| Lee Barrett | Chris Goggans | Terry Luedtke |
| EHNAC | PatchAdvisor, Inc. | VA |
| Dirk Barrineau | Walter Grant | Mark McLaughlin |
| Liberty IT Solutions | VA | EHNAC |
| Eddie Brito | Mike Henderson | Lee Miller |
| DSS, Inc. | DSS, Inc. | DSS, Inc |
| Conrad Clyburn | Don Hewitt | Joe Ortman |
| EHNAC | OSEHRA | VA |
| Keith Cox | Lynda Joseph | Steve Oster |
| VA | DSS, Inc. | VA |
| Mark Cummings  
*Liberty IT Solutions* | Alan Leung  
*Horizon Blue Cross* | Shelley Williams  
*Apex Data Solutions* |
|------------------------|------------------------|------------------------|
| **Guy Francois**  
*DoD/VA IPO* | **Alberto Llanes**  
*HHS* | **Marc Wine**  
*VA* |
2 Network and Infrastructure Security

2.1 Physical Access Controls

The relationship between physical access controls and information security is sometimes overlooked, because the responsibilities often reside in separate organizations. However, there is little point in implementing extensive software measures for confidentiality and availability if an attacker can simply unplug a server and remove it from the premises. Properly securing an instance of VistA begins with fundamental physical security as described below.

2.1.1 Facility Access for Employees

All facility employees should be identifiable via an access badge compliant with HSPD-12. This badge should be displayed by the employee at all times, and should also function with the facility access control system. Like any access control system, the facility’s physical access control system should be configured to allow the minimum required access for any individual. It should also provide logs of all access. Processes for on-boarding and dismissal should ensure prompt revocation of any badge reported missing or whose owner terminates employment for any reason.

For further information, facility access using PIV IDs is addressed in the NIST Special Publication 800-94, titled “A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS).”

2.1.2 Visitor Control

Visitor control is an important aspect related to physical security safeguards to be put in place within any organization housing Protected Health Information (PHI). PHI should be managed on a need-to-know basis for workforce members and should be kept even more private from those non-workforce members that stop by the office for whatever reason. Visitor control should include the following as best practice:

1. Visitor logs – Visitors should be required to sign a log capturing the following information: date of visit, check in time, name of visitor, company visitor is representing, who the visitor is there to see, check out time.
2. Badges assigned – Visitors should be required to wear a badge that clearly identifies them as a “Visitor” so workforce members may challenge them if they are un-escorted within the facility.
3. Escorts - Visitors should be escorted at all times when within the facility to ensure the minimal amount of incidental contact with PHI will occur.
4. Optional item to include - Photographs of the visitor upon check in – This allows the picture to be printed on a temporary badge and worn as an alternate form of identification to the standard visitor badge.

Often, the most overlooked part of the process is getting the visitor to return the badge and sign out; however, signing out is just as important as the sign in process because the visitor log can
be used to determine what non-workforce members are in the building in the event of an emergency such as a fire. Having a completely reliable and accurate visitor log will save time looking for someone who may have already left the facility.

### 2.1.3 Additional Physical Security Controls at Datacenters

Datacenters typically have multiple layers of physical security to safeguard the infrastructure of their customers. These safeguards are in place to restrict access to physical components of a datacenter to only those with legitimate access needs. Physical security control best practices for datacenters include:

1. Gated parking lots – Visitors or workforce members must either utilize a key card/key pin pad to enter the gate or buzz to the security desk for entry;
2. Front door to the facility – Protected by key card, key pin pad, or biometric readers for those with authorized entrance to the facility. Visitors must be buzzed in via the security desk for entry to the lobby.
3. External to the facility – CCTV cameras are placed at each corner of the building and other strategic locations such as the generators, shipping docks, and water cooling tanks. Generators and cooling tanks should be enclosed with fencing or walls to prevent visitor access without authorization. Generators should also be locked in housing cabinets surrounding the generator.
4. Inside lobby – The inside lobby is protected from entry to the datacenter floor by securely locked doors. Security guards sit behind bullet-proof glass and require government id and a ticket in the visitor tracking system prior to assigning a visitor badge. Visitor badges have no access control built in but are rather used for easy identification of a visitor within the datacenter itself. Security guards also monitor the CCTV camera feeds throughout the facility. Datacenter floor doors typically require key card or key pin pad in conjunction with some form of biometric scanning device. Entry through the door from the lobby to the datacenter floor is managed through a man trap. The man trap doors typically require the lobby door be closed prior to allowing entry into the datacenter floor area. Often, more sensitive man trap doors do not allow more than one person at a time through the man trap. This feature may be overridden by security personnel in the event visitors need to be allowed access.
5. Datacenter floor – Once inside the datacenter, CCTV cameras are present at each and every exit door as well as showing views down each aisle of cages. Camera feeds are typically kept for 90 days. Cages housing the computer cabinets are locked by key locks or key card/key pin capability sometimes also including biometrics. Once inside the cage, the computer cabinets themselves are also locked and require either a key or a key pin code entry to unlock them.
6. Shipping dock – Monitored by CCTV, this area is secured from the datacenter floor by requiring key card/key pin pad or biometric reader to regain entry to the datacenter. All equipment shipped to the datacenter must be unpacked in the shipping area prior to being located on the datacenter floor to remove the fire hazard of cardboard boxes being contained within the datacenter itself.
2.1.4 Workstation/Workforce Separation

Physical workstation separation is required by HIPAA when members of the workforce have diverse access controls related to Protected Health Information (PHI) meaning some workforce members have access to PHI and others do not. Policies and procedures should be created to fully define an organization’s stance in handling the physical workspace of workforce members.

In order to limit incidental exposure to PHI the following guidelines may be followed:

1. Segregate the physical workspace – If possible, create a physically segregated workspace and restrict access (i.e. key card access) to keep those without PHI access from entering the restricted area.
2. Restrict incidental contact - If it is not possible to create a segregated workspace or restrict access to the area where PHI is handled, additional effort should be given to protect against the viewing of PHI. Additional protections include:
   - Privacy screens on computers;
   - High cube walls;
   - Screen lock timeouts;
   - Policies to require placing computers in sleep mode when leaving the workstation.

2.2 Configuration Management

For purposes of this document, configuration management includes the identification of all hardware and software assets connected to the operational network, along with established processes to control additions, changes, and deletions to the system configuration. Configuration management is critical to all aspects of information security, and is perhaps the most underrated security countermeasure. When assessing vulnerability and risk, it is essential to know what addressable devices exist on the network and what software is resident on those hosts. For example, most zero-day vulnerabilities are announced with information regarding what target hardware/software configuration is susceptible to the attack. Without an accurate list of hardware and software running on a given network, it would be impossible to determine whether the vulnerability was relevant. This is one of the principal reasons that standard images must be used on PCs authorized for use on the network, and that end users should not be given software installation privileges.

Since most changes to production configurations are managed as patches, configuration management is divided below for discussion purposes into asset management and patch management.

2.2.1 Asset Management

Any VistA instance will include a suite of hardware and software, and will operate across one or more local networks. Every addressable host on the underlying network(s) is a potential attack platform, and every external connection is a potential attack vector (see Connectivity, below).

Asset tracking must include:
• A database containing information on every addressable host connected to the network. This information should include, at a minimum, the hardware type, location, operating system (including version), all applications (including versions), the person responsible for the system, system criticality, and whether the system is authorized to contain sensitive information or PHI.

• A continuous inventory validation process to ensure that the asset database is current and accurate.

• A data and application criticality analysis to determine which systems should be restored first in an emergency. The results should be captured in the asset database, and used in planning disaster recovery.

### 2.2.2 Change Management

Control of the system configuration is essential to establish and maintain the security of both the network and the resident applications. This control may be intramural, or may be part of a larger change management system administered by a central authority. In either case, a formal local change management framework and procedures must be implemented to ensure all system software changes are controlled in line with this framework. This includes both operating system and application patches, and should extend to all devices on the network. One or more test platforms should be maintained to test proposed changes prior to installation on production systems. Once the need for an addition, change, or deletion to the system configuration is confirmed, the patch management system can be used to manage deployment.

### 2.2.3 Patch Management

Patch management and password management are arguably the two most important components of any information security program. Network vulnerability assessments continue to show that, notwithstanding zero-day exploits, the vast majority of serious vulnerabilities (i.e., those that lead to massive host compromise) are caused by poor password discipline (see section 4.1.2 below) or failure to maintain patch levels on operating systems or applications.

Patch management is critically dependent upon asset management, since identifying all network hosts and the software running on each host is a prerequisite for determining the required patch levels. After implementing an asset management process as described above, due diligence requires that effective patch management be implemented. This requires:

• Formal policies and procedures for enterprise patch management. The policy must cover all addressable equipment on the network, including leased equipment and equipment under outside maintenance contracts. The procedures must include continuous identification of vulnerabilities and required patches applicable to any equipment/software in the inventory.

• An automated system to track the patch level of each host’s operating system and applications, including specialized devices and embedded posts.
A process for patch distribution and installation. Note that this process has several inherent challenges. While the preference would obviously be to “push” updates from a central patch management system, many commercially available systems do not recognize the wide variety of software likely to be implemented in a VistA facility environment. Ideally, the patch management system would be integrated with the asset management system to ensure that all software and hosts are addressed. Timing is also an issue, since machines must be powered on to receive updates. If patch distribution is limited to off hours, many personal desktops or notebooks may not be on the network, and may return to the network unpatched during business hours.

Further details on the importance, challenges and technologies regarding patch management are specified outlined in NIST’s (SP 800-40) “Guide to Enterprise Patch Management Technologies.”

2.3 Connectivity

In order to adequately protect the system from external attack, all points of external connectivity must be identified and properly secured. Several major categories of potential external attack must be addressed, as discussed below.

2.3.1 Internet Connectivity

All Internet points of access must be identified and properly restricted by firewalls. The network architecture should incorporate a “DMZ” so that externally-addressable hosts are isolated from the internal network. A rule set (including inbound and outbound connections) should be developed and then implemented in the firewall at each access point. It is advised that the NIST Special Publication 800-52r1, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations” be followed for securing transport layer connections.

2.3.2 Partner Connectivity

Partner connectivity includes Internet, VPN, and direct connections to specific business partners, whether initiated by the VistA facility or by the outside partner. For example, a credit card processing device may be connected to the internal network, or an embedded system may be set up to connect to a contractor maintenance system. In every case where business partner connectivity exists, the following actions should be taken:

- Document the connectivity and the required access/privileges.
- Limit access to the minimum necessary hosts, using MAC addresses if possible. If access will traverse a firewall, incorporate the requirements into the firewall rule set to provide the maximum possible restrictions in each direction.

NIST SP 800-47 also known as the “Security Guide for Interconnection Information Technology Systems,” explains the security aspects of planning, establishing, maintaining and disconnecting a system interconnection.
2.3.3 Wireless Connectivity

Wireless connectivity can be a major threat to system security. In addition to commercially available personal wireless access points, many devices such as printers have the capability to set up their own wireless access. The result is that there are often more accidental wireless access points within a facility than planned ones. Wireless security strategy should include:

- Specific authorization of all wireless access points in the facility, and implementation of a policy strictly prohibiting the setup of any unauthorized wireless access. The policy must be enforced through recurring physical checks to detect any unauthorized wireless broadcasting (whether broadcasting an SSID or not). Unauthorized wireless networks must be immediately shut down.

- Placement of boundaries on internal wireless networks via internal firewalls. Access from any given wireless network should be constrained to the minimum operating requirements. The best possible encryption (currently WPA2) should be implemented on all authorized wireless networks. If possible, internal wireless networks should be configured to suppress broadcast of SSID. Authorized users can be provided with the network name as required.

- If necessary, a guest network may be provided for visitors. Visitors should never be given the credentials to utilize an internal network other than a guest network. The guest network should be structured so that it provides Internet access but no access to any part of the internal network. Guest networks may broadcast a guest SSID, but should still be encrypted with a password that is changed periodically.

2.3.4 Internal Firewalls and Defense in Depth

The concept of defense in depth is based upon the paradigm of layered military defenses. Network security often focuses on securing the perimeter against outside attacks, but neglects to place appropriate limitations on internal connectivity. The result is a two-fold problem: first, any successful perimeter breach results in broad internal access; second, there is little defense against an authorized user exceeding authorized access within the network. To address these problems, the facility network should be examined to determine the functional access required from each host (or group of hosts). For example, it is unlikely that a scheduling PC would require access to a robotic surgery device. However, unless the network is segmented to restrict internal access, all that would be required would be the appropriate IP address.

Network administrators should take the following steps:

- Utilize the asset management inventory to determine the functionality of each host on the network, and the minimum connectivity requirements. This may also be integrated with the criticality survey described under Asset Management above.

- Define an appropriate set of network segments consistent with the connectivity requirements, and implement firewall or router rule sets to limit connectivity.

- Utilize MAC addresses where possible to limit critical communications.
Covering areas of network segregation and defense in depth architecture; it is recommended that the NIST SP 800-82r1 "Guide to Industrial Control Systems Security," be used to secure internal and external connectivity.

2.4 Embedded Systems and the Internet of Things

While there are many industries and technology settings that involve embedded processors, hospitals are arguably at or near the top when it comes to networked embedded processors. Medical devices such as CAT scanners, MRI machines, and other monitoring/measurement devices are routinely networked so that they can transmit information to clinicians or, in some cases, post information directly into the system of record. Such devices are often driven by sophisticated onboard computers, containing processors, primary and secondary memory, extensive executable programming, and communications/networking capability. These computers rely on commercially available operating systems, often some UNIX variant such as Linux or IRIX. VA has already addressed a number of critical issues relating to these medical devices in a new Design Pattern.¹

These embedded computers are, from a network perspective, full-fledged hosts. If the operating system and act application software on these machines are not maintained at current patch levels, they are vulnerable to takeover. If compromised, they can be used as platforms from which to attack other network hosts. Depending upon the machine in question, simple compromise could be disastrous if used to interfere with normal operation. For example, if the embedded processor in a CyberKnife or similar system is compromised and shut down during surgery, the result could be fatal.

For all such embedded systems that they are attached to the network, the following guidelines apply:

- **When purchased, the purchase agreement / maintenance contract should clearly identify who is responsible for maintaining the operating system and applications contained on the device at current patch levels.** The IT department must then either apply the appropriate updates or ensure that the seller applies them, depending upon who is responsible.

- The equipment must be added to the asset management system as a network host, and the versions of operating system/application software on the device recorded in the tracking database (see Asset Management).

- The equipment should be added to the Patch Management system to monitor patch levels.

For more information on the internet of things, many specifics are covered in the NIST Special Publication 800-183, titled "Networks of Things." Additionally, the Food and Drug Administration offers industry guidance for the Postmarket Management of Cybersecurity in Medical Devices.

¹ VA Enterprise Design Patterns: Privacy and Security Medical Device Security, VA Office of Information and Technology (OI&T), Version 0.5, November 2016. Executive Summary available.
2.5 BYOD

Given the ubiquity of smartphones, tablets and other mobile computing devices, most organizations are faced with demands from their user community to provide some level of network access to personally-owned mobile computing devices. The risks from PHI or other sensitive data leakage from these devices, if unmanaged, far outweighs any possible benefits.

Since there is no easy way to enforce corporate security controls on employee-owned hardware, healthcare organizations should take a more conservative approach to the BYOD problem. Personally-owned devices should always be treated as inherently insecure and granted only limited network access. The preferred strategy would be to create specific network segments for these devices, and allow only outbound Internet access. Any access to the internal network would be treated as external Internet. Due to the variability of BYOD, it is advised that NIST SP 800-46r2 (Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security) be supplemented when considering BYOD security matters.

If there is an overwhelming demand from the user community to support mobile computing, or a compelling business case, then the organization should provide those users with mobile devices owned and managed internally.

2.6 Log Files and Auditing - Host Level

Log files and other audit trail datasets represent an important part of any organization’s information security program. Ready access to the information contained in these files can make the difference between a quick resolution to a potential security issue and a multi-day nightmare scenario wrought with confusion. Beyond the obvious forensic benefits, healthcare organizations may need to show adequate log files retention to meet compliance with various governance and auditing processes.

Components on modern computer networks can generate many gigabytes of data per day, ranging from authentication logs (who logged into what, and when they did it) to tracking actual exploit attempts against a given network resource. For these logs to be useful they should be saved in a central repository so they can be easily recovered. Many organizations opt for more robust log consolidation in a Security Information and Event Management (SIEM) product. While the specific feature sets may vary by vendor, the basic features in nearly all SIEM products include data aggregation, event correlation, and automatic alerting.

Examples of the types of data that should be saved in an enterprise SIEM include:

- UNIX/Linux Syslog data
- Web server access logs
- Router and Switch NetFlow data
- Intrusion Detection System logs
- Windows Event Logs
Along with a plethora of external sources, the NIST’s SP 800-92, “Guide to Computer Security Log Management” clearly explains the critical aspects of security log management.

2.7 Vulnerability and Risk Assessments

Risk exists at the juncture of four distinct elements, as shown in the figure below. Three of the four elements are relatively subjective:

- **Threat**, which must be estimated from available data and is subject to the judgement of the assessor;
- **Likelihood**, again an estimated value, based upon all available data on a particular threat and analysis/judgement of the motivation of the potential attacker;
- **Impact**, which involves a valuation of data, estimate of recovery costs (including legal costs), and often an estimate of intangible damages such as loss of public confidence.

![Figure 1. Four Distinct Elements of Risk](image)

The fourth item, **Vulnerability**, can (and should) be more objective. While no testing template is perfect (and none can anticipate all zero-day exploits), it is possible to develop and maintain a test methodology that is comprehensive enough to satisfy the requirements of due diligence. This methodology must include more than scanning tools – it must include an emulation of attackers operating inside and outside of the enterprise. Despite the increasing sophistication of automated scanning tools, human attackers combine externally-obtained information (e.g., userids or even exposed passwords used elsewhere on the Internet) and known vulnerabilities in ways that automated tools cannot. Ideally, the emulation of “real” attackers also includes social engineering. It is better for an employee to be embarrassed by simulated social engineering than victimized by the real thing.
Assessments should be performed by an independent third party (both for objectivity and for a better emulation of external attacks), and should be performed both from the standpoint of an outside entity (external assessment) and an insider attempting to exceed authorized access (internal assessment). Note that vulnerabilities are not necessarily classed as internal or external, since the discovery of any perimeter vulnerability that gets an outsider into the network means that all of the “internal” vulnerabilities are accessible to the outsider.

Vulnerability assessments are fundamental to enterprise information security, and essential for developing risk assessments. As shown in Figure 2 below, ascertaining the vulnerability of assets is the first step in the Risk Assessment process. A vulnerability assessment should document all discovered vulnerabilities across network hosts, and prioritize them for remediation. Prioritization is critical, as some vulnerabilities, such as a poor administrator password on a server, will “domino” into widespread compromise very quickly in a real attack. Experience has shown that the classic “80/20” rule applies here. Addressing 20% of the identified vulnerabilities (if they are properly prioritized) is likely to reduce overall vulnerability on the order of 80%. The term “Penetration Testing” is sometimes used synonymously with vulnerability assessment. However, care should be taken that the penetration testing methodology is not a “capture the flag” strategy where the process ends with successful access to any internal network resource. All discoverable vulnerabilities and exploit strategies must be documented and prioritized in order for the results to drive a valid risk assessment and remediation strategy.

<table>
<thead>
<tr>
<th>ID.RA-1: Asset vulnerabilities are identified and documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>• CCS CSC 4</td>
</tr>
<tr>
<td>• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04</td>
</tr>
<tr>
<td>• ISA 62443-2-1:2009 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12</td>
</tr>
<tr>
<td>• ISO/IEC 27001:2013 A.12.6.1, A.18.2.3</td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12</td>
</tr>
<tr>
<td>• ISO/IEC 27001:2013 A.6.1.4</td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 PM-15, PM-16, SI-5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID.RA-3: Threats, both internal and external, are identified and documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>• COBIT 5 APO12.01, APO12.02, APO12.03, APO12.04</td>
</tr>
<tr>
<td>• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12</td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 RA-3, SI-5, PM-12, PM-16</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID.RA-4: Potential business impacts and likelihoods are identified</th>
</tr>
</thead>
<tbody>
<tr>
<td>• COBIT 5 DSS04.02</td>
</tr>
<tr>
<td>• ISA 62443-2-1:2009 4.2.3, 4.2.3.9, 4.2.3.12</td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-9, PM-11, SA-14</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>• COBIT 5 APO12.02</td>
</tr>
<tr>
<td>• ISO/IEC 27001:2013 A.12.6.1</td>
</tr>
<tr>
<td>• NIST SP 800-53 Rev. 4 RA-2, RA-3, PM-16</td>
</tr>
</tbody>
</table>
Vulnerability assessments do not consider the value of information or the impact of compromise. They catalog weaknesses across the network (generally by IP address). This is an important concept since, from an attacker's perspective, a seldom-used test system that can be compromised and used as an undetected long term attack platform within the network may ultimately be more valuable than the highly protected (and noticeable) server containing sensitive information. Vulnerability assessments should objectively catalog all weaknesses across the network. As shown in ID.RAs 2 through 5 in Figure 2, the objective vulnerability information is combined with threat, likelihood, and impact (value) information to create a risk assessment.

Third-party vulnerability assessments should be conducted annually at every facility, either individually or as part of a combined larger assessment (such as a regional assessment). The results should be used in two ways: first, for immediate remedial action on critical vulnerabilities; second, as input to a risk assessment and a larger plan for ongoing remediation and network/host maintenance.

For supplemental guidance on how to prepare for a risk assessment or for more information on the assessment itself, review the NIST SP 800-30 “Guide for Conducting Risk Assessments.”
3 System and Process Security

Having established the foundational security requirements in the underlying physical, network, and operating system infrastructure, a context has been established for operating application-level software and processes. This section discusses system and process security from three perspectives: confidentiality, integrity, and availability.

3.1 Confidentiality

3.1.1 Encryption

The US Government, the European Union, and the International Organization for Standardization, among others, have identified the transmission of data across the Internet as one of the most vulnerable vectors for identity theft, data theft and other malicious interference in e-commerce and provision of e-government services. This is one reason why most online e-commerce sites have implemented SSL/TLS encryption of the transactions between their servers and end user web browsers, and why e-government services are increasingly implementing the same protections.

End-to-end encryption, local Kerberos services, sMIME, VPNs and mutual SSL/TLS (in which both the server and the end user’s web browser identify themselves to the other with secure cryptographic tokens) are all well-established approaches in which data originating at one node is encrypted and transmitted in that transformed state across the Internet to only the intended receiver, where it is decrypted and made readable. This process protects the data in transit from a number of potential attacks enumerated in ISO standard 29115 (ITU-T X.1254 “Entity authentication assurance framework” Clause 10) and in comparable NIST special publications, especially NIST SP 800-52 Rev. 1, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.”

While encrypting data is a powerful protection method, it is not by itself a panacea. Data encryption itself is vulnerable to a number of attacks. If the encryption method is not sufficiently robust it can be broken by attackers who then have full access to the encrypted data. This happened to the TLS schemes lower than the current version 1.2, to the MD5 encryption suite and to Secure Hash Algorithm 1. As the compute power of malicious actors – including hostile governments – inevitably increases over time, encryption suites and even whole encryption methods must evolve to remain useful.

Another risk is that if the data is encrypted by a fraudulent service provider, then that bad actor will have full access to any data that uses it. Generally speaking, providers who register their SSL/TLS services with the CA/Browser Forum, participate in its deliberations and ensure that their offerings conform to and are registered under the Forum’s Extended Validation (EV-SSL) guidelines may be relied upon to provide encryption services that satisfy current cybersecurity needs. The European Telecommunications and Standards Institute has adopted the CA/Browser
Forum EV-SSL guidelines as its policy reference for digital signatures identifying legal persons (organizational entities) and their devices on the Internet.

That said, even legitimate encryption service providers may find themselves hacked and their encryption services corrupted so that data encrypted under their schemes are visible to malicious actions. This has happened to several providers over time.

Thus, for encryption of data as it moves across the network or across the Internet from one node to another, the encryption service must: a) utilize current standards-based encryption technologies and methods, b) be recognized by industry and/or governmental entities as legitimate providers, and finally, c) have a track record of maintaining system cybersecurity protections and best practices for sanitary data management.

3.1.2 User Authentication – Access/Verify Codes

Parts of the following were adopted from the VA Kernel documentation to define industry standard specifications.

Access Code

The Access code is assigned by IT Service. This code is used by the computer to recognize the user. Each user has a unique Access code. The only way this code can be changed is for the IT Service to edit it. When the code is established by IT, it is encrypted (i.e., it is scrambled according to a cipher). The code is stored in the computer only in this encrypted form. Thus, even if the Access code is viewed, the viewer cannot determine what the user actually types to tell the computer this code.

Verify Code

The Verify Code is usually assigned by the IT Service. Like the Access Code, the Verify Code is also encrypted. The Verify Code is the equivalent of a network password. The user can change the Verify Code at any time. This is done through the Edit User Characteristics menu, which is found in the Toolbox menu (the Toolbox menu can be accessed by entering two question marks (“??”) at the menu prompt.) It is important to note that the VistA system requires users to change their Verify Code on a regular basis. The frequency of changing these codes is set in the KERNEL SYSTEM PARAMETERS file (#8989.3). Security policy states that codes should be changed at least every 90 days.

If IT Service assigns only the Access Code, then the first time the new user signs on to the VistA system, Kernel prompts them to establish a Verify Code. The user cannot proceed with the session until this code is entered and validated by Kernel.

Access and Verify codes must adhere to the following criteria:

• Access and Verify Codes cannot be identical.
• Verify Codes (i.e., passwords) must be at least 8 characters in length.
There is one default type of Verify Code in VistA: the VA VistA standard criteria for Verify Code which is 8-20 characters with at least one uppercase, one numeric, and one non-alpha non-number character. These criteria exceed current industry standard requirements, such as CCHIT and ARRA, each of which have a minimum requirement of an all-alpha mixed-case code.

Verify Codes must be changed at least every 90 days. Information systems should not permit re-assignment of the last three passwords used. Accounts that have been inactive for 90 days should be disabled.

To preclude password guessing, an intruder lockout feature should suspend accounts after five invalid attempts to log on. Where round-the-clock system administration service is available, system administrator intervention should be required to clear a locked account. Where round-the-clock system administration service is not available, accounts should remain locked out for at least ten minutes.

These restrictions should be enforced whenever Access or Verify Codes are created or changed. Users should avoid codes that offer no secrecy (e.g., a child's or spouse's name, a phone number or license plate). If desired, the system can automatically generate codes for users. However, these auto-generated codes can be cryptic (e.g., A$BC402) and are often difficult for users to remember.

For both the Access and Verify Codes, it is important to remember that there is no way to see the codes that were entered for any user. If users forget their Access or Verify Codes, replacement codes must be assigned.

Each time users sign on to a VistA terminal, they see a dialogue similar to the following (depending on the unique physical characteristics of your system):

```
Volume set: VAH     UCI: VAH   Device: _LTA9130: (VAH604/LC-1-1)

ACCESS CODE: <enter access code, it will not be displayed on screen>
VERIFY CODE: <enter verify code, it will not be displayed on screen>
GOOD MORNING Five YOU LAST SIGNED ON TODAY AT 8:30
You have 3 new messages.
```

When the system prompts for the Access and Verify Codes, the text that the user types does not appear on the terminal screen. Thus, even if someone is watching a user sign on, the codes are not shown. If the user enters codes that the system recognizes as valid, it greets the user and proceeds according to the privileges that are assigned to that user.

If the user fails to enter a set of codes that the system recognizes, the user sees a different dialogue, as shown below:
Notice that the system told the user that the first pair of codes was not valid. It did not specify whether the problem was with the Access code or the Verify Code. Thus, a potential hacker is not given any useful information.

Take another look at the sign on dialogue. Notice that the computer tells the user when they last signed on to the system. By asking each user to pay attention to this greeting, you can enlist them in the security process. If the computer reports to a user that they were signed on the day before, and the user knows that they were not at work, then they can report that information as a possible security violation.

If the user fails to gain access (i.e., multiple unsuccessful attempts are made in succession), then the device may lock. When the device locks, then no user can log onto the system through that device until either the lockout time expires or IT Service intervenes. The device lockout time is defined in the KERNEL SYSTEM PARAMETERS file (#8989.3) as a system default but may be overridden by a lockout time that IT Service associates with a specific device (e.g., a modem).

The enforcement of the pattern match for Verify Code is not done in the meta-dictionary. Rather the dictionary invokes VistA M programming code to validate the entry. Users do not directly access or modify M programming code.

### 3.1.3 Non-Person Authentication

Data that are sent to VistA for computation or persistence may come from non-VistA systems that do not share VistA’s user authentication requirements. For example, an image acquisition system such as a CT scanner may not be capable of transmitting authenticated user credentials (or any credentials at all) to VistA. Systems, as opposed to person users, that interact with VistA are referred to as non-person entities (NPEs).
The interaction of NPEs with VistA raises two issues. The first is that the **provenance** of VistA data received from such systems, whether the data are authentic or not, may not be precisely discernable. The second is that data may be transmitted to VistA with no **accountability** for its origin or intent.

Even though NPEs may be shielded by the VA enterprise firewall, the potential of harm to patients still exists. Malicious actors inside VA who have access to such non-VistA systems can transmit bogus data for inclusion in patients’ medical records anonymously, without those data being traceable to the originating user. The possibility of incorrect treatment decisions being made on the basis of bogus, untraceable data is a patient safety risk.

VA has undertaken an enterprise-wide approach to enterprise security that is intended to provide the following benefits:

- Ensures compliance with VA’s Personal Identity Verification (PIV)-only authentication and enterprise on-boarding and off-boarding (per Continuous Readiness in Security Program (CRISP)) for NPEs.
- Validates accurate, unambiguous NPEs to enterprise resources (vice generic "application proxy" user accounts) through integration with Single Sign-On Internal and External (SSOi/SSOe).
- Simplifies the technology stack by using Enterprise Shared Services (ESS) and IAM, resulting in improved reliability and maintainability.
- The specific actions to be undertaken in VA systems are the following:
  - Correlate the target NEW PERSON File (#200) to IAM Provisioning with some account management functions provided by the Provisioning engine.
  - Manage direct user login to backend systems (terminal session, Computerized Patient Record System, etc.) with IAM SSOi/SSOe with SSOi/SSOe tokens.

### 3.1.4 Restriction of Access to Patient-Sensitive Information

Access to patient sensitive information is managed at VA by applying processes and procedures based on the NIST SP 800-37 Risk Management Framework (RMF), FIPS 199 categorization, and VA Handbooks 6500, 6500.3, and 6500.6. Support is provided to VA teams for any continuous monitoring as part of VA’s CRISP initiative. Necessary documentation is developed to achieve and maintain system authorization. Any discovered security vulnerabilities are mitigated in a timely and verifiable manner using standards outlined in the RMF. The complete assessment and authorization (A&A) process is compliant with the FISMA High certification level for confidentiality, integrity, and availability.

---

We recommend that all VistA installations use and continue to expand on existing templates, checklists, tools, Standard Operating Procedures, and policies to maintain A&A for VistA. This recommendation ensures support of the Risk Management Framework (RMF) implementation for all categorizations of Information Systems (IS), enclaves, and application systems in accordance with NIST SP 800-37.

Test data and pseudonymized production data must conform to the following privacy standards and practices:

- Social Security Numbers
  - Social Security Numbers must begin with 000 or 666 (e.g. 000-45-6789, 666-45-6789).

- Patient Names
  - The patient name must be constructed from the abbreviated application name concatenated with “patient” for the last name and the use of textual numbers or a numeric for the first name. An alpha character or numeric can be added to the last name to make it more distinctive in recognizing specific test entities. (e.g. CPRSpatient, One; CPRSpatient2, One; CPRSpatientA, One; CPRSpatient, 12)

- Provider Names
  - The provider name must be constructed from the abbreviated application name concatenated with “provider” for the last name, and the use of textual numbers or a numeric for the first name. An alpha character or number can be added to the last name to make it more distinctive in recognizing specific test entities. (E.g. CPRSprovider, One; CPRSprovider1, One; CPRSproviderB, One; CPRSprovider, 12).

- Claim Numbers & Service Numbers
  - Claim numbers and service numbers must begin with 000, 666, or be covered or removed permanently using image editing software.

- Address Information
  - The Street Address, City, County, Precinct information must be de-identified (scrambled) to contain random numbers and/or alpha characters that may not be used to identify an individual. The initial three digits of a zip code must be changed to 000.

- Dates
  - The following format must be followed for referencing all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
  - All elements of dates must be de-identified (scrambled) to contain random numbers that may not be used to identify an individual.

- Telephone Numbers
  - The telephone number must use 555 as the prefix (not area code) for each number (e.g. 561-555-1234).
• Fax Numbers
  o Fax numbers must use 555 as the prefix (not area code) for each number (e.g.
    561-555-1234).

• Email Addresses
  o The electronic mail address must be de-identified (scrambled) to contain random
    numbers and/or alpha characters that may not be used to identify an individual.

• Full face photographic images and any comparable images
  o Full face photographic images and any comparable images shall be removed.

• Other
  o Certificate, License, Serial, Plate, Device, Biometric, Health Plan, Vehicle
    Identification Numbers or any other unique identifying information, characteristic,
    or code shall be de-identified (scrambled) to contain random numbers and/or alpha
    characters that may not be used to identify an individual.

Furthermore, documents may not use examples that may infringe on copyrights or be considered offensive.

### 3.1.5 Media/PHI Management and the Final Disposition of Data

In accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
guidance is provided on how to securely manage media and PHI. It includes guidance for the final
disposition of such data and applies to all employees, agents and contractors that perform duties
in conjunction with the access, distribution, dissemination, modification, and management of
Protected Health Information (PHI) and media containing PHI. Adequate controls including
encryption must be in place to protect physical media containing PHI while in transport to help
prevent unauthorized acquisition of or access to this data in the event the physical media on which
PHI is stored is lost or stolen. It is recommended that employees, agents and contractors follow
the procedures found in Appendix A when shipping and receiving PHI and that they file a policy
exception request at anytime the procedures outlined in Appendix A cannot be followed.

This will give guidance on how to manage media and PHI in both electronic and paper forms,
throughout its lifecycle, including the final disposition of such data. The policy located in Appendix
A was originally developed by MedForeSight and has been modified to address a VistA
installation in accordance with 45 C.F.R. (Combined Federal Regulation) § 164.310, “Security
Standards for the Protection of Electronic Protected Health Information”, commonly known as the
Security Rule. The original policy was drafted for an organization looking to acquire EHNAC
Accreditation in which the organization was successful.

### 3.1.6 Access Tracking

VistA provides means at two major levels to track access to the system and its features. Kernel’s
Establish System Audit Parameters option (XUAUDIT) allows audit parameters to be set up
alongside the other site parameters available through the Enter/Edit Site Parameters option
(XUSITE Parm). Audits may be set up on menu options, devices, software namespaces, all activity
of individual users, and/or failed access attempts. A beginning date and ending date must be
defined in order for these audits to be activated. Refer to Chapter 2, “Implementation and Maintenance,” in the *Kernel Technical Manual*, as well as to the *Kernel Security Tools Manual*.

Using the Auditing API within VA File Manager, audits may be set up on individual fields, entire files, and data dictionaries to track changes to both data and metadata. The scope and duration of audits are tracked automatically, as well as the distinct changes to metadata/data elements. Refer to Chapter 7, “Auditing API,” in the *VA FileMan Programmer Manual*.

### 3.2 Integrity Issues

Integrity issues in VistA implementations fall under the areas of *version management*, *modifications to data in transit*, *continuous regression testing*, *logging and auditing* and *external threat analysis*. More detail will be provided in each of these areas within its own subsection of this document; however, a brief overview of the impact on integrity related to each area will be discussed here.

- **Version Management** - Version management integrity validates not only the code base of product releases, but is also used to manage the versions of updates to third party software and operating systems. It is integral in the coordination of implementations to ensure that past issues have been eradicated and not re-introduced into the production environment. See Section 3.2.1.

- **Data in Transit** – Data in transit is most vulnerable when transmitted over the open internet. Encrypting files alone is not enough to verify the integrity of the contents of files. Having the encryption process also perform some form of checksum validation will ensure that the file transmitted is the exact file that was received. See Section 3.2.2.

- **Continuous Regression Testing** – Regression testing ensures the integrity of the development and testing process. Ensuring the coding taking place does not break functionality that worked prior to the “fix” is the primary function of regression testing. See Section 3.2.3.

- **Logging and Auditing** – Logging user activity provides the security in knowing that user actions are fully documented so if the time comes, where it needs to be determined what the user did at any point, the log file will provide the information necessary to validate such activity. See Section 3.2.4.

- **External Threat Analysis** – Hiring a third party to perform a threat analysis provides the integrity necessary to avoid the perception that the analysis was performed by workforce members who have a stake in a positive outcome. It is important to avoid the “fox in the henhouse” perception when it comes to evaluating threats and vulnerabilities. See Section 3.2.5.
3.2.1 Version Management

Sites not running current, or currently patched, versions of VistA software may be exposed to risks that have been mitigated in more recent versions. The intrinsic threat level is low, since VistA distributions from VA, OSEHRA, and well-known public and private sources are engineered to isolate and control risks to patient data confidentiality, integrity, or availability.

Even so, measures should be taken to validate frequently, even continuously, that VistA code bases have not been compromised by malicious activity subsequent to installation of the officially released code. These validations might include checksum revalidations, standards and conventions validations, re-baselining, functionality audits, and continuous regression testing.

- **Checksum revalidations** - All VistA MUMPS source files are released with checksums. These checksums should be kept in a secure location and revalidated periodically to ensure that MUMPS routines have not been tampered with.

- **Re-baselining** - VistA code and data dictionaries can periodically be refreshed from the distribution directory from which they were installed. To prevent local modifications from being overwritten, such modifications should be reviewed and committed to the same distribution directory.

- **Functionality audits** - When integration and end-to-end workflow testing scripts are available, such scripts should periodically be executed to ensure that code still works as intended. Anomalies raised by such tests can expose both code tampering instances as well as possible vulnerabilities, not previously identified, to availability of data or functionality.

3.2.2 Data in Transit

Malicious viewing and modification of patient data being interoperated to and from VistA instances are risks with two kinds of consequences.

- Any malicious activity of this nature compromises the **confidentiality** of data. Secure data channels should be chosen for transmission of VistA data, encrypting packets and payloads wherever feasible.

- Additionally, malicious modifications compromise data **integrity**. Thus, data hashing algorithms or digital signatures should be chosen that allow receivers to validate that the data transmitted to them has not been tampered with.

3.2.3 Continuous Regression Testing

VistA’s MUMPS code base can be tested with various tools such as M-Unit, RaSR, Selenium, and Sikuli, using a test harness such as CDash. OSEHRA uses these tools for nightly tests of the OSEHRA VistA code base. Analysis of testing failures can reveal vulnerabilities to be mitigated.
3.2.4 Logging and Auditing

3.2.4.1 Logging

The accumulation and storage of log files is extremely important for both network and infrastructure security. The events logged in both of these settings reflect upon each other, i.e. logging entry and exit, including what is accessed between those major events. Usually logs must be managed by Security Information and Event Management (SIEM) software or another type of log management software regardless of what generates the log data.

NIST Special Publication 800-92 defines log sources, which fall into the categories of security software, operating systems, and applications. Logging can be based on a set of events which can vary by the scope of the parameters.

VistA’s Kernel has the capability to log several events. Kernel keeps a constant Sign-On Log and Programmer Mode Log, both of which record all instances of when a sign-on occurs in VistA, whether it is in programmer mode or not. For these records, the user, date and time is recorded. Another capability which can be initiated by audit is the Failed Access Attempts Log which “can be used to record information about sign-ons that were attempted but failed.” Any logs that must be initiated should always have set parameters such as the domain name, audit date of initiation, date of termination, and others be monitored continuously, per the Information System Owner’s specifications.

3.2.4.2 Auditing

In order to mitigate risk of breach and track suspicious activity, proper auditing policy and procedures must be followed. In compliance with NIST SP 800-53, VA Handbook 6500 recommends control value minimums for audit events. The auditable events may include:

- actions of system administrators and operators;
- production of printed output;
- new objects and deletion of objects in user address space;
- security-relevant events;
- system configuration activities and events;
- events relating to use of privileges;
- all events relating to user identification and authentication; and/or
- the setting of user identifiers.

Such auditable events should be subject to audit generation based on components determined by the IS Owner, which are also described in more detail by VA Handbook 6500. Extending on

---

the recommendations for audit events, the publications deem that records should be reviewed, analyzed and reported by the information technology office, such as OI&T for VA. Audit records should also be kept effectively and securely. The IS Owner should determine frequency of back up and which users have access, per VA 6500.

The Kernel Security Tools Manual covers security features in user security, menu management, audit features, and software integrity. The section covering Kernel audit features discusses both System Access Audits and Option and Server Usage Audits. In addition to reviewing the Kernel Security Tools Manual for audit capability information, it is advised that the technical manual for each clinical application be reviewed; for more information view the VA Software Document Library (https://www.va.gov/vdl/section.asp?secid=1).

VistA’s Fileman contains options for audit procedures. For auditing a Data Field and a Data Dictionary there are abilities to set the audit, review the audit trail, and purge the audit trail. Files in the VA FileMan List associated with audits are the Audit and DD AUDIT files. The DD AUDIT file "stores the changes made to data dictionaries," and the AUDIT file stores the date and time, user’s name, and old and new data values of changes made to audited fields. For each application, security guidelines should be reviewed per the appropriate manual such as NIST SP 800-52 or VA Handbook 6500, and conversely application developers should include security information in their technical documentations including role based access keys, sign-on security, electronic signature functionality, file protections, and audits.

### 3.2.5 External Threat Analysis

VistA code strictly limits the use of *socket communications*. The modules that facilitate communication using Internet pipes are few in number and easily isolated. All socket communications should be performed through approved Kernel utilities for MUMPS code, or similar approved utilities for other implementation technologies such as Delphi and node.js. Code bases should be examined using tools such as XINDEX (for MUMPS) and Fortify (for other technologies) to identify vulnerabilities that may have been introduced through non-approved code or coding techniques.

Connections to filesystems that are used for *semaphore communications* or other file transfers should be configured to disable the ability to use such connections for access to VistA user or administrative functions. Directories used for file exchanges with entities outside the enterprise should be staged on servers that do not permit breach of the enterprise firewall. Connections

---

should be made using Secure Shell protocol (SSH),\textsuperscript{12} and files to be exchanged should be encrypted and digitally signed. Ports used for file exchange should be continuously monitored for suspicious activity.

### 3.3 Availability Issues

#### 3.3.1 Data Availability

It is important to have a documented record of all servers, applications and datasets that are critical for business continuity. There should be contingency plans in place to ensure that critical data will be available to those who need it, especially during times of crisis. The current security landscape makes this a significant challenge, given the ease with which attackers can hinder data availability. Attackers may employ any of a number of techniques, including ransomware and denials of service at both the network and application level.

If critical files or databases become corrupt, erased, or encrypted by a hostile actor, the most expeditious method of recovery will be through the restoration of backup files (see Failover and Disaster Recovery below). The backup interval may (and should) differ across the organization, depending upon the importance of the data being protected. When possible, current backups of the most sensitive data should also be kept in an offline format (tapes, etc.) to protect against the backup files and servers themselves being attacked. \textit{All backups should be tested on a regular basis as part of an enterprise disaster recovery plan.} Backup testing is often overlooked (or subject to procrastination due to the inconvenience), and problems are not discovered until a genuine crisis - often with severe consequences.

Denials of service are a serious threat that requires advance planning. If countermeasures are planned, simple resource starvation or memory depletion attacks against a critical host or application can often be quickly dealt with using a combination of protocol filters and redundant servers. Network-based bandwidth depletion attacks can be more complicated, and often require multiple diverse network routes or external services. For Internet-facing applications, anti-DDoS services from companies such as CloudFlare or Akamai can provide adequate protection from both types of attacks. Again, tests must be conducted regularly to determine that any denial-of-service protections work as planned.

#### 3.3.2 Capacity

Capacity monitoring is an important part of any organization’s infrastructure because the active monitoring of systems allows network administrators to be the first responders when systems are not behaving as expected. Capacity monitors allow for the monitoring of CPU utilization, bandwidth utilization, disk space, and process run times. Capacity monitoring should be a daily

\textsuperscript{12} Although Secure Shell (SSH) is intended to preserve data confidentiality and integrity, a document leaked by Edward Snowden in 2014 (\url{http://www.spiegel.de/media/media-35515.pdf}) seems to indicate that the National Security Agency has on some occasions successfully hacked SSH.
activity and, in some cases, an all-day activity. Aside from the monitoring of capacity, it is equally important to have a formal capacity plan in place.

A capacity plan documents the capacity requirements of all critical production systems, analyzes current utilization of those systems, and provides plans based on the expected utilization of those systems. This plan must be well-maintained and must include items such as:

1. Charts or graphs showing the current capacity and utilization of CPU, disk storage, networks, and communication lines.
2. Established thresholds ("high water marks") for each of the monitors at which point, specific documented action will be taken.
3. An assessment of datacenter power, HVAC, footprint, and fire suppressant requirements.
4. A description of how capacity is assured as new clients and new applications are implemented, and as client behaviors change.
5. A description of how the procurement process is managed to ensure additional capacity arrives in time.

By establishing thresholds for each of the capacity areas noted, an organization can then program alerts to notify administrators when the threshold is breached for a predetermined period of time. When notified of a capacity issue, the administrators are allowed the ability to address the issue before performance becomes a problem.

### 3.3.3 Timely Accessibility

While noticeable wait times for display and persistence of data can be annoying, they also can present security risks on several levels. When data, particularly real-time patient observations, are not updated in persistence or displayed within a few seconds of being collected or requested, there is a risk in emergent situations that a clinical decision will be made on the basis of incorrect data, impacting patient safety. The same is true in non-emergent situations when clinical reports such as medication administration, laboratory collection, and pick lists are not available promptly to responsible clinicians and technicians responsible for bedside patient interactions and interventions.

Data latency or delays can have a cascading effect. When a data update at a receiving system times out because of processor delays, one or more duplicate updates may be transmitted by a sending system, further impeding data persistence, throughput, and accurate patient care. In certain situations, backlogs of timed-out data update transmissions can "catch up" with receiving systems and be incorrectly persisted, instead of being rejected because of supersession by subsequent transmissions. This can result in duplications of such interventions as medication and radiation administrations and specimen collections, with possible significant adverse effect to the patient.

Finally, overall system slowdowns can impact the issuance or validation of security certificate assertions. In certain cases, this could result in either blockage of clinician access to systems or in the inappropriate use of ‘break-the-glass’ security workarounds.
All integration and acceptance testing of systems and subsystems should evaluate system performance, reporting, and recovery in situations where latency, persistence timeouts, and similar conditions occur.

### 3.3.4 Failover & Disaster Recovery

It is essential to have written policies and procedures in place for responding to an emergency or other occurrence such as fire, vandalism, system failure, or natural disasters that impacts systems that contain Electronic PHI. The plan should document the policies and procedures for various levels of emergency including but not limited to fire, vandalism, system failure, or natural disasters.

There should also be established procedures to create, archive, index and maintain retrievable exact copies of Electronic PHI in support of restoration of such data during an emergency. Disaster recovery procedures should ensure that any loss of data can be restored, with the Recovery Point Objective not to exceed 48 hours and the Recovery Time Objective not to exceed 48 hours for critical transaction processing. Recovery Point Objective is the maximum targeted period in which data might be lost from an IT service due to a major incident. It directly pertains to the amount of time between backups of systems and data. Recovery Time Objective is the amount of time it will take, during a crisis, to restore an application or data required to resume business continuity.

The Disaster Recovery Plan should contain the following components:

- Procedures for notifying trading partners of disaster and plan for recovery.
- Procedures for protecting safety of employees and safeguarding of facilities with resumption of work.
- Procedures for contacting any third-party vendors or suppliers for equipment, applications, and/or data retrieval and restoration.
- Key personnel contact listing including office phone, home phone, and cell phone of each individual where appropriate.
- Identification of tasks for the restoration of any and all systems, applications, and data.
- Assignment of tasks to a job classification (i.e. Unix administrator) and assign a time frame for completion of the task.

To ensure integrity in the system, there must be implemented and documented procedures for periodic testing, assessment, review and revision of disaster recovery and emergency mode operation plans. Testing and all appropriate revisions should occur no less than annually.
4 Strategies for the Next Generation EHR

This section provides additional recommendations based upon current topics of discussion for future VistA implementations such as VistA in the Cloud.

4.1 Cloud Service Provider Requirements

This will give guidance on how to set forth the proper procedures for securely managing protected health information (PHI) in a federally FedRAMP certified Cloud Service Provider (CSP) environment. Grouped into three broad categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), cloud services can be deployed as Public, Private or Hybrid models. These terms, along with FedRAMP, a federal certification which enables cloud services Authority to Operate (ATO) in federal networks, are defined Appendix B. It is recommended that employees follow the procedures found in Appendix B when managing FedRAMP certified CSPs which are authorized to access, store or transmit PHI related to the designated organization and should file a policy exception request at any time the procedures in Appendix B cannot be followed.

The policy located in Appendix B is based on the EHNAC Cloud Enabled Accreditation Program (CEAP) which in turn has been developed in accordance with standards promulgated by the Cloud Security Alliance, PCI (Payment Card Industry Data Security Standard), NIST (National Institutes of Standards & Technology), ISO (International Organization for Standardization), FedRAMP (Federal Risk and Authorization Management Program) and ISACA (Information Systems Audit and Control Association).

4.2 Building Security Requirements into Open Architecture

The secure implementation of systems within open architecture requires attention both to the modular and integrative aspects of enterprise security. Individual systems (modules) must adhere to the enterprise requirements developed in conformance with the recommendations presented elsewhere in this document. At the same time, the ability to pass and validate credentials, enforce constraints, test assertions, and report vulnerabilities and breaches must be consistently implemented and enforced across systems within the architecture.

Open-architecture interoperability initiatives face the challenge of developing, presenting, and certifying such recommendations. The Services Oriented Architecture (SOA) Work Group of Health Level Seven International (HL7) is at this writing (January 2017) working on a Privacy, Access, and Security Services (PASS) Alpha Project to develop

...specifications [that] define a set of encapsulated, loosely-coupled and composable service components that can contribute to ensuring the confidentiality and integrity of healthcare information. These specifications are intended to align with the SAEAF [Services Aware Enterprise Architecture Framework, now Service-Aware Interoperability Framework (SAIF)] and may include domain analysis/information models, service
functional models, collaboration analysis models, platform independent models and platform specific models.\textsuperscript{13}

The Healthcare Services Specification Project (HSSP), jointly sponsored by HL7 and the Object Management Group (OMG), envisions that PASS “will provide a simple interface for all privacy, access control, consent, identity management and other security services that are needed in a service-oriented health information architecture.”\textsuperscript{14} At least within U.S. Federal settings, these evolving standards should be developed and implemented in conjunction with the “Identify-Protec t-Detect-Respond-Recover” approach outlined in Appendix A of the NIST \textit{Framework for Improving Critical Infrastructure Cybersecurity}. It is anticipated that the evolving standards and recommendations of the Healthcare Services Platform Consortium (HSPC) will incorporate PASS and other HSSP cybersecurity work products.

\section*{4.3 COTS Acquisition Considerations}

There are two frames of reference within which information security of acquired commercial “off-the-shelf” systems (COTS) should be taken into account. Departmental subsystems such as EKG carts, robotic microscopes and scalpels, and laboratory analyzers should meet all the requirements of this document with respect to security, privacy, and accessibility. The last is particularly true if it is decided, for example, to forgo the integrated storage capabilities of VistA Imaging for those of a commercial image storage subsystem such as a Picture Archiving and Communication System (PACS). Such subsystems should be thoroughly stress-tested to mitigate risks of data unavailability. The costs and risks of surrendering custody of enterprise patient data to third-party systems must also be taken into account, particularly if is decided later to replace one third-party system with another.

The decision to replace an entire enterprise VistA EHR with a COTS must not be taken without considering the information security issues that must be mitigated within each subsystem and module of the COTS as well as by the COTS as a whole. Where the COTS, as is increasingly the case, encapsulates loosely-coupled functionalities and / or functionalities from multiple vendors, the COTS' internal interoperability security risks must be evaluated and mitigated, either by implementing an open architecture such as that modeled by HSSP or a validatable proprietary architecture.

Either subsystem or full-system replacements must be thoroughly tested to ensure that their database and storage technologies maintain availability during times of high usage and provide sufficient redundancy and failover capability to allow fast, smooth disaster recovery. Person and non-person authentication must meet enterprise security and accountability requirements with the same strictness and consistency as is recommended within this document for an enterprise VistA installation.

\textsuperscript{13} Health Level Seven International, “\textit{Project Summary for Privacy, Access and Security Services (PASS) Alpha Project},” July 2015.

\textsuperscript{14} Healthcare Services Specification Project, “\textit{Active Projects},” November 2016.
5 Leveraging Others’ Experience

This final section offers sources for additional information, both from other major healthcare IT implementers and standards organizations.

5.1 Large Providers

In a report published 16 September 2016, the Government Accountability Office (GAO) documented that cyber incidents aimed at federal agencies had spiked nearly 1,300% in the decade from Fiscal Year 2006 to 2015 (GAO-16-885T). In the most prominent of these federal incidents, the Office of Personnel Management (OPM) was breached exposing the personally identifiable information of more than 22 million citizens including 5.6 million fingerprint records.

Beyond federal government vulnerabilities, the healthcare industry has become a high value target and has accounted for a number of large U.S. data breaches. For example, in 2015 the Excellus BlueCross BlueShield breach exposed the personal data of over 10 million members; the Premera Blue Cross breach affected the data of more than 11 million members; and the Anthem Blue Cross breach made history as the largest healthcare data breach ever recorded with approximately 78.8 million highly-sensitive patient records exposed. The Anthem attack then followed by breaches at CareFirst BlueCross BlueShield and the UCLA Health Systems. In 2016, Phoenix, Arizona based Banner Health was breached in an attack that affected 3.62 million individuals; Newkirk Products, a “Business associate” vendor that produces identification cards for payers, was breached in an attack that compromised 3.47 million individuals; and, Premier Healthcare was put at risk when over 200,000 individuals were impacted by a stolen laptop containing PHI (Protected Health Information).

Typically, the healthcare data thieves are after medical records because of the wealth of valuable data contained within them. These include data elements such as: clinical medical information and prescriptions; name, address, telephone and fax numbers; E-mail addresses; medical insurance and/or Social Security numbers; important dates; information about beneficiary families; financial information, i.e., account numbers, insurance policies, certificate numbers; medical device information; Internet Protocol (IP) addresses and/or URLs; biometric data, i.e., finger, retinal or voice prints and/or DNA; and facial photographic images or images that have unique identifying characteristics.

Since the enactment of HIPAA, the Department of Health and Human Services (HHS), Office of Civil Rights (OCR) has been responsible for enforcing the laws protecting health information. Since 2003 they have received over 140,000 HIPAA complaints. Over that period they have resolved over 90% of the complaints resulting in fine levies of over $48,000,000 (OCR Enforcement Results). But, fines are only one of the costs stemming from these health-related data breaches. In its 2015 Cost of Data Breach Study: Global Analysis, the Ponemon Institute put the average cost of a healthcare data breach in the United States at $398 per exposed personally identifiable medical record. This includes the costs of investigation, remediation, notification, credit monitoring and other possible costs, such as fines and legal bills. In addition,
health systems are becoming increasingly subjected to ransomware attacks in which hackers technically deny access to the organization’s healthcare data system until a ransom, usually in bitcoin, is paid to regain access.

As “Covered Entities” under the HIPAA law, senior leadership of large healthcare organizations are becoming increasingly cognizant of their need to create strong, comprehensive, sustainable cybersecurity policies, procedures and infrastructures that can effectively operate in a rapidly changing and hostile IT environment. This begins by addressing three threshold questions. These are: What encompasses my organization's network (including mobile, remote and cloud assets)?; Who has access to my organizational network (to include Business Associates, Cloud Service Providers and Vendors)?; and, What are the risks inherent in the network for which I am responsible (as documented in periodic Independent Vulnerability Assessments)?

After these threshold questions are addressed, effective large healthcare organizations are then focusing on questions of greater detail. By answering these questions they can craft policies, processes and procedures specific to their needs and operational requirements. These questions include:

- Does the organization conduct and follow-up on periodic 3rd party Risk Assessments?
- How do users obtain authorized access to PHI applications and data managed?
- Who determines who has access to our network?
- How do we authenticate access to our network?
- Do we track and document access to PHI?
- Is network security consistent across all company locations and access points?
- Are employees blocked from accessing potentially dangerous websites?
- Do we protect and document changes to the network configuration?
- How is our network equipment kept up to date?
- Are mobile employees protected when they access internal applications or SaaS products from their homes, airports, coffee shops, shared work spaces, etc.?
- Is employee health data security training conducted and fully documented?
- Are employees organized for and practice incident response and disaster recovery procedures?
- Do we audit the adequacy of the health data security agreements and policies of our Business Associates, Vendors, Sub-contractors and partners?
- How many attacks does the organization experience each day/week/month and how many are successfully blocked?

Over the last twelve months, some of the most complex, large Healthcare Organizations (HCOs) are beginning to exhibit a pattern of data security risk mitigation that are resulting in best practices. For example, in 2015 millions of individuals were affected by the exposure of their PHI. These exposures were primarily due to breaches at large healthcare payer organizations and insurance operators. In 2016, there has been a significant decline in breaches emanating from these large health insurer/payer organizations.
The Health IT data security best practices we observe emerging among large, complex HCOs include:

- The introduction of periodic, comprehensive and objective third-party evaluations of business operations and risk assessment vulnerability based on adherence to HIPAA, HITECH and other federal/state regulations for data privacy, security and confidentiality.
- Ensuring that Health IT technical management is conducted in accordance with industry standards for HL7, SNOMED, CCR, CCD, CDA, C32, DICOM, NCPDP, X12 and other formats.
- The implementation of continuous monitoring and testing systems, policies, and quality improvement processes for healthcare delivery workflows, incident response, business continuity and disaster recovery.
- The institution of well documented employee training programs on the methods and procedures to mitigate health data security risks while improving Health IT management efficiency and service levels.
- The rigorous management of partnership relationships to ensure business associates, sub-contractors, trading partners and vendors conduct ongoing assessments of their privacy and security operations, and have policies and procedures in place to safeguard PHI.
- Employment of comprehensive technical assessment systems to measure, document and audit health data transmissions, security, timeliness, accuracy, systems availability, capacity monitoring, Internet usage, storage and retrieval.

Ultimately, best practice large organizations are concluding that a multi-pronged approach to cyberhealth security is the most beneficial. A comprehensive defense in depth strategy assures that there is no single point of failure in the protection of PHI and best positions an organization to develop a culture of security that enables the enterprise to sense and effectively respond as the threat to sensitive health data exposure inevitably evolves going forward.

5.2 NIST

NIST Cybersecurity Framework

NIST, in mid-2016 published a spreadsheet cross-referencing several security frameworks against a framework core set of controls. Among the security frameworks in the comparison are COBIT® 5, ISO 27000, and NIST SP 800-53 R4. The spreadsheet comparison may be found at: [http://www.nist.gov/cyberframework/]

NIST SP 800-53 Revision 4

NIST SP 800-53R4 outlines security and privacy controls for Federal information systems and organizations. The introduction to the document notes the special publication revision 4: “has been updated to reflect the evolving technology and threat space. Example areas include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems.” [http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800-53r4_summary.pdf]
5.3 Other Security Frameworks

Evaluation of other security frameworks was conducted and determined that further investigation may result in additional best practices that may be utilized to enhance the security of VistA.

**COBIT® 5**

COBIT 5 is a business framework created to manage enterprise level IT. The framework is created and managed by ISACA and includes controls related to risk and information security. [http://www.isaca.org/cobit/pages/cobit-5-framework-product-page.aspx]

**ISO 27000**

Managed by the International Organization for Standardization, the ISO 27000 series of standards provides best practices for information security management systems related to risk and controls. The standards are meant to serve organizations of any size. [http://www.iso.org/iso/iso27001]

**FedRAMP**

“FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud-based services.” [https://www.fedramp.gov/resources/documents-2016/]

**ONC Health IT Certification Program**

The ONC Health IT Certification Program was designed to validate EHR functionality and interoperability between certified EHRs. Among the standards are areas such as the privacy and security embedded within the EHR. The standards require compliance with HL7 messaging standards as well as transport standards to secure and provide integrity controls surrounding data exchanges. The standards and certification regulations may be found here: [https://www.healthit.gov/policy-researchers-implementers/standards-and-certification-regulations]
Appendix A – PHI Policy Template

In accordance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), this Appendix provides a policy template for securely managing media and PHI. It includes guidance for the final disposition of such data and applies to all employees, agents and contractors that perform duties in conjunction with the access, distribution, dissemination, modification, and management of Protected Health Information (PHI) and media containing PHI. Adequate controls including encryption must be in place to protect physical media containing PHI while in transport to help prevent unauthorized acquisition of or access to this data in the event the physical media on which PHI is stored is lost or stolen. It is recommended that employees, agents and contractors follow the procedures found in Appendix A when shipping and receiving PHI and that they file a policy exception request at anytime the procedures outlined in Appendix A cannot be followed.

This policy template includes guidance on how to manage media and PHI in both electronic and paper forms, throughout its lifecycle, including the final disposition of such data. It was originally developed by MedForeSight and has been modified to address a VistA installation in accordance with 45 C.F.R. (Combined Federal Regulation) § 164.310, “Security Standards for the Protection of Electronic Protected Health Information”, commonly known as the Security Rule. The original policy was drafted for an organization looking to acquire EHNAC Accreditation in which the organization was successful.

POLICY:

This policy sets forth the proper procedures for securely shipping physical media that contains PHI outside of the organization, as well as the procedures for receiving such physical media. Adequate controls including 256-bit encryption must be in place to protect physical media containing PHI while in transport to help prevent unauthorized acquisition of or access to this data in the event the physical media on which PHI is stored is lost or stolen. Employees should follow these procedures when shipping and receiving PHI and must file a policy exception request at any time the procedures outlined herein cannot be followed.

DEFINITIONS:

“Electronic media” means (1) Electronic storage media including memory devices in computers (hard drives) and any removable / transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or (2) Transmission media used to exchange information already in electronic storage media. Certain transmissions, including of paper via facsimile, and voice via telephone, are not considered to be transmissions via electronic media because the information being exchanged did not exist in electronic form before the transmission.

“Electronic protected health information” or “E-PHI” means protected health information that is transmitted by electronic media or maintained in electronic media.

“Individually identifiable health information” means information, including demographic information collected from an individual, that:

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

a. That identifies the individual; or
b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

“Physical Media” means electronic storage media and tangible material used to store data, including but not limited to tapes, cassette cartridges, disks, CDs, DVDs, paper, SD cards and flash drives.

“Protected health information” or “PHI” means individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

“Transport” means physical movement of physical media from its current location to any other location.

PROCEDURES:

A. Maintaining an Inventory of Data on Physical Media
Where appropriate, Division heads will designate a point of contact responsible for maintaining physical media inventory. The physical media inventory must be updated upon the receipt, transport, or disposal of physical media containing PHI. Additionally, the designated point of contact shall be responsible for periodically verifying the accuracy of the inventory records.

B. Procedures for Securely Sending Physical Media
Prior to routing physical media containing PHI, the designated point of contact will: (1) identify the individual responsible for receipt of the physical media, (2) contact the intended recipient to confirm date/time of transport (e-mail is sufficient), and (3) request written (e-mail is sufficient) confirmation of receipt from recipient. Where obtaining this information is not possible, employees should document their efforts and the results in the physical media inventory. See Attachment A. Additionally the inventory should include tracking or other identification numbers associated with shipment and indicate whether the data media received are placed into storage or returned, destroyed, or data properly erased.

Points of contact should use packaging effectively to help enhance security in transporting physical media containing PHI. See Attachment B.

C. Procedures for Securely Receiving Physical Media

Prior to receiving PHI data, the appropriate business unit should work with the all involved parties to implement secure, electronic methods for transporting data. If the data cannot be sent securely electronically and the data must be shipped using physical media, the sender must encrypt the PHI on the physical media using at least 256-bit encryption prior to transport, in addition to other reasonable measures to meet all parties business practices.
Inspection
Packages containing physical media that may contain PHI must be inspected for damage prior to accepting delivery. Delivery must be immediately refused for any packages that are discovered to be damaged. The damage must be documented by the inspecting employee. All instances of damage or missing physical media, regardless of when the damage or loss is discovered, must be immediately reported. If damaged packages are accidentally accepted, onward delivery must not be performed.

Tracking
Upon receipt of physical media containing PHI, employees should promptly confirm receipt with sender. Employees must log receipt into the appropriate physical media inventory. In order to ensure the security of the physical media containing PHI the following shall be required:

- Physical media shall not be transported through a major distribution hub (no mass handling or automated sorting)
- Point to point monitoring shall be required (e.g., signatures designating any change of custody – sender, courier or receiver, bar code scanning, delivery control numbers, logging)
- Materials or items must not be left unattended or in an unsecured vehicle
- Manifests are required and must include shipper, receiver, and driver signatures with delivery time and pick-up
- GPS tracking of physical media with PHI, where possible

Access
Designated points of contact within each unit should ensure that:

- Physical media is stored in a locked room or cabinet
- Access to storage areas is limited and restricted to those with a need to carry out their job responsibilities
- Removal of media is recorded, including identification of the handler, purpose, date, time, intended disposition, and expected return date if applicable

D. Recycling:
For purposes of this Policy, Recycling is any reuse of intact media or devices, this includes:

- Reuse in a different location than its current location.
- Reuse by staff members who are not authorized to see the data the media or device contained in its original use.
- Reuse by transfer to another entity outside of the organization.
- Donation to charitable, educational or other organizations.
- Sale or transfer to the general public.

Data Media are rendered unreadable either by thorough erasure or by physical destruction. Thorough erasure includes; repeated complete reformatting and over-writing of the media after data erasure, and/or complete degaussing using a device specifically designed for magnetic media disposal.
Magnetic storage (e.g., disk drives) must be either multiply-reformatted, overwritten, degauss or removed from devices that have been declared surplus, defective or obsolete and are to scheduled to be disposed of or recycled.

Devices (e.g., workstations and desktop personal computers) that are to be reused or recycled must have their hard disk drives reformatted and then overwritten (the installation of a new standard operating system and suite of standard business software after the reformatting can serve as the final overwrite).

E. Dissemination and Training
This policy will be disseminated to employees and the business units handling PHI. All vendors who conduct business and transport physical media to and from the organization shall agree to the terms and conditions of this policy.

The designated point of contact will provide information to management for training employees on this policy for transporting physical media containing PHI and compliance with relevant privacy and information security laws, regulations, and requirements.

F. Review, Updates, and Monitoring Compliance
This policy will be reviewed at least annually and updated as appropriate. The Chief Security Officer shall be responsible for auditing business functions to ensure compliance with this policy.

G. Vendor Relationships
Each contract with vendors shall outline requirements for the safe handling of information as they apply to storage and transport, including access controls, copying, authentication systems, or encryption. Vendors will agree and acknowledge that they have the following:

- Media Storage: Procedures for safe storage of both electronic and print media including requirements for the copying of archived data should that media deteriorate.
- Media Destruction: Procedures for securely erasing data from media or physically destroying media, as well as any requirements for securing transport to facilities for erasure or destruction.
- Media Transport: Information-handling procedures for storage, packaging for internal messenger, packaging for external mail or courier services, shipping tracking, and destruction.
- Audit: Requirements for validating transport and storage controls, data erasure and media destruction methods, and requirements for timing for destruction.
- Incident Management and Escalation: Clear definition around what constitutes “lost media” and the timeline for notifying the Department when an incident has occurred.

H. Destruction/disposal of PHI Media
The purpose of this procedure is to assure that PHI is destroyed in accordance with HIPAA. Destruction/disposal of protected health information will be carried out in accordance with federal and state law. The schedule for destruction/disposal shall be suspended for records involved in any open investigation, audit, or litigation. Physical destruction may be accomplished by: shredding, pulverizing, crushing, melting, incineration or a combination of these.

Procedures
● Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
● Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a qualified protective order will be obtained to ensure that the records are returned to the organization or properly destroyed/disposed of by the requesting party.
● Records or other documents containing PHI scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal is complete. This means that this material should be stored in secure containers (not in wastebaskets, boxes, recycle bins, etc.) until the time of destruction/disposal.
● Contracts between the organization and its business associates will provide that, upon termination of the contract, the business associate will return or destroy/dispose of all Protected Health Information. The destruction of PHI by the Business Associate will be documented in writing and sent to the organization.
   ○ Date of destruction/disposal.
   ○ Method of destruction/disposal.
   ○ Description of the destroyed/disposed record series or medium.
   ○ Inclusive dates covered.
   ○ A statement that the PHI was destroyed/disposed of in the normal course of business.
   ○ The signatures of the individuals supervising and witnessing the destruction/disposal.
● If such return or destruction/disposal is not feasible, the contract will limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
   A record of all case files containing protected health information that are destroyed or disposed will be made and retained permanently. Permanent retention is required because the records of destruction/disposal may become necessary to demonstrate that the PHI were destroyed/disposed of in the regular course of business. Records of destruction/disposal should include:
   ○ Date of destruction/disposal.
   ○ Method of destruction/disposal.
   ○ Description of the destroyed/disposed record series or medium.
   ○ Inclusive dates covered.
   ○ A statement that the PHI records were destroyed/disposed of in the normal course of business.
   ○ The signatures of the individuals supervising and witnessing the destruction/disposal.
● If destruction/disposal services are contracted or performed by another entity, the contract or agreement will provide that the business associate will establish the permitted and required uses and disclosures of information by the business associate as set forth in the federal and state law and include the following elements:
○ Specify the method of destruction/disposal.
○ Specify the time that will elapse between acquisition and destruction/disposal of data/media.
○ Establish safeguards against breaches in confidentiality.
○ Indemnify the organization from loss due to unauthorized disclosure.
○ Require that a business associate maintain liability insurance in specified amounts at all times the contract is in effect.
○ Provide proof of destruction/disposal.

PHI media will be destroyed/disposed of using a method that ensures the information cannot be recovered or reconstructed. Methods of destruction/disposal may be reassessed annually by the Security Officer, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

Form A - Physical Media Inventory for PHI

Each record listed in the physical media inventory must include:

- Origin of data
  - designated owner of the physical media
  - technical contact of data creation
- Destination (location to which the physical media will be transported or received)
- Frequency of transport (e.g., daily, weekly, monthly, periodic)
- Physical media type
- Approximate number of records contained in the physical media
- Data type (e.g., “public information”; “PHI”)
- Encryption, if not public information (e.g., give password or specify other means)
- Number of items typically included in the shipment
- Size of data on media (e.g., 100 MB, 3 GB)
- Data protections in place to help protect the physical media from loss, theft, or unauthorized disclosure
- Description of shipping method and level of service
- Risk (e.g., no impact, minor, significant, tangible, serious, grave)

The physical media inventory must be updated upon the receipt, transport, or disposal of physical media.

Form B - Packaging Physical Media

Employees and vendors should enhance the security in transporting physical media, especially when the media contains PHI.

Envelopes shall not be utilized to ship physical media containing PHI. Metal containers with a locking mechanism should be used. If metal containers are not available or are not practical for shipments, employees and vendors may use hard cardboard boxes that comply with the following parameters:
1606 • Prior to packaging, duplicate the media and securely store the duplicate so that it may be promptly identified, located and used as needed, in the event of a loss
1607 • Secure the data on the media through encryption, such as a strong password, or other technological means
1608 • Double box the package, i.e., place the inner container in a new, outer corrugated cardboard box
1609 • Tape with 2” pressure sensitive shipping tape
1610 • Reinforce the box at four corner points and place tape across box
1611 • Lock or seal containers before leaving secure premises
1612 • Enclose the physical media in tamper-resistant / tamper-evident wrap
1613 • Do not mark the outside of the box with information pertaining to its contents or classification
1614 • Shipments should be addressed clearly to a specific recipient by name, using business address.

Form C

CERTIFICATE OF DESTRUCTION

The information described below was destroyed in the normal course of business pursuant to the organizational retention schedule and destruction policies and procedures.

<table>
<thead>
<tr>
<th>Date of Destruction:</th>
<th>Authorized By:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Description of Information Disposed Of/Destroyed:

<table>
<thead>
<tr>
<th>Inclusive Dates Covered:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
</tbody>
</table>

METHOD OF DESTRUCTION:

• Burning
• Overwriting
• Pulping
• Pulverizing
• Reformatting
• Shredding
<table>
<thead>
<tr>
<th>Records Destroyed By*</th>
</tr>
</thead>
<tbody>
<tr>
<td>If On Site, Witnessed By:</td>
</tr>
<tr>
<td>Department Manager:</td>
</tr>
</tbody>
</table>

*If records destroyed by outside firm, must confirm a contract exists
Appendix B – CSP Policy Template

This policy template will give guidance on how to set forth the proper procedures for securely managing protected health information (PHI) in a federally FedRAMP certified Cloud Service Provider (CSP) environment. Grouped into three broad categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), cloud services can be deployed as Public, Private or Hybrid models. These terms, along with FedRAMP, a federal certification which enables cloud services Authority to Operate (ATO) in federal networks, are defined Appendix B. It is recommended that employees follow the procedures found in Appendix B when managing FedRAMP certified CSPs which are authorized to access, store or transmit PHI related to the designated organization and should file a policy exception request at anytime the procedures in Appendix B cannot be followed.

The preceding is based on the EHNAC Cloud Enabled Accreditation Program (CEAP) which in turn has been developed in accordance with standards promulgated by the Cloud Security Alliance, PCI (Payment Card Industry Data Security Standard), NIST (National Institutes of Standards & Technology), ISO (International Organization for Standardization), FedRAMP (Federal Risk and Authorization Management Program) and ISACA (Information Systems Audit and Control Association).

POLICY:

This policy sets forth the proper procedures for securely managing protected health information (PHI) in a federally FedRAMP certified Cloud Service Provider (CSP) environment. Adequate controls should be in place to protect PHI to prevent unauthorized acquisition of or access to this data. Employees should follow these procedures when managing FedRAMP certified CSPs which are authorized to access, store or transmit PHI related to the designated organization and should file a policy exception request at anytime the procedures outlined herein cannot be followed. Cloud services are grouped into three broad categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), and can be deployed as Public, Private or Hybrid models. These terms, along with FedRAMP, a federal certification which enables cloud services Authority To Operate (ATO) in federal networks, are defined below.

DEFINITIONS:

A. FedRAMP. The Federal Risk and Authorization Management Program, or FedRAMP, is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. FedRAMP is the result of close collaboration with cybersecurity and cloud experts from the General Services Administration (GSA), National Institute of Standards and Technology (NIST), Department of Homeland Security (DHS), Department of Defense (DOD), National Security Agency (NSA), Office of Management and Budget (OMB), the Federal Chief Information Officer (CIO) Council and its working groups, as well as private industry.
B. Software as a Service (SaaS). Provides users with the ability to access applications over a network. Organizations and users that use SaaS interact with an application and offload the supporting operating systems and infrastructure to the cloud provider. Examples of SaaS software include email, virtual desktop, and office productivity applications over the Internet.

C. Platform as a Service (PaaS). Provides developers with an environment for creating custom applications without the need to be concerned with managing the underlying operating systems and infrastructure. Developers are given environments such as .NET, Java, Python, and many other languages through a PaaS provider’s website. They are able to write code by using the website interface or upload code they have created using version control software like Git. Developers can then publish their code on the PaaS provided website. PaaS providers are able to automatically scale the power of a developed web application according to its use or other metrics.

D. Infrastructure as a Service (IaaS). Provides the most control over resources of all the service options. IaaS gives system administrators access to storage, networking, virtual machines, and other low level infrastructure. Administrators are able to rapidly provision virtual machines, deploy operating systems, and manage them via their web browsers. The virtual machines can then be used to host different development platforms for developers and software that end users can access. One major difference between IaaS and the other two cloud service types is that the responsibility of the configuration and security of the operating systems do fall on the system administrators.

E. Private Cloud. When an organization’s cloud sharing requirement is to keep the cloud resources available only internally. This is useful when the need is to keep information private. Thus, the deployment model is referred to as a Private Cloud.

F. Public Cloud. When an organization chooses to share or use cloud services within a community of interest and/or with external partners. This form of deployment is referred to as a Public Cloud model.

G. Hybrid Cloud. This model combines the Private and Public deployment models for a customized implementation.

H. Network Security. Refers to physical and software preventive measures an organization takes to protect its network from unauthorized access, misuse, malfunction, modification, destruction and improper disclosure.

I. Application Security. Refers to any methodology designed to ensure that applications adhere to and enforce the security requirements of the environment in which they are located. It encompasses the prevention of unwanted events, such as flaws that may be ingrained in a code that a hacker can exploit and ensuring desired events occur, such as encryption of confidential patient data.

PROCEDURES:

A. Security Layers

To ensure that CSPs providing health related services to the organization in managing PHI, the following procedures will be adhered to create an acceptable cloud based defense in depth that hardens security at seven distinct layers:
• **Physical** – data storage in top tier data centers (Tier IV and Tier III, as defined in subsection B below), i.e., secure location, 24/7 security, hardened facility, redundant power and bandwidth, perimeter sensor-monitoring and badged or biometric entry into secure areas.

• **Network** – enterprise-grade hardware, advanced firewall configuration, SSL VPN security, intrusion detection and prevention, and threat management response processes and procedures.

• **Application** – data encryption (at rest and in transit), anti-virus protection, patching, two-factor authentication, malware protection and log management.

• **Server** – file integrity monitoring, patching, role-based access controls and Security Information and Event Management (SIEM).

• **Data** – backup, at-rest and in-transit encryption, retention, destruction, archiving, SIEM and lifecycle management.

• **Devices** – mobile, traditional medical devices, home telehealth, as well as BYOD concerns.

• **User** – two-factor authentication, social engineering and hacking, policies related to passwords and BYOD, corporate policy, continuous education and ethical hacking.

**B. Physical Security**

If the physical security of a center is compromised, it could render an entire system unavailable – a scenario that could cause damage to any organization, but is particularly serious to a healthcare provider that relies on systems not only for business management, but for delivering patient care.

There are four certification levels of cloud environment data centers:

• Tier IV: Fault-tolerant site infrastructure

• Tier III: Concurrently maintainable site infrastructure

• Tier II: Redundant capacity components site infrastructure (redundant)

• Tier I: Basic site infrastructure (non-redundant)

Tiers IV and III are considered top-tier data centers. Tier IV is generally reserved for the U.S. government’s highest level (top-secret) security data. Tier III data centers meet stringent HIPAA requirements. Tier II, Tier I and uncertified centers are not HIPAA-compliant. Tier IV and III data centers should have in place the following physical security:

• **Safe locations**: Centers are purposely built in safe locations with few natural hazards, like severe weather or seismic issues.

• **Multiple feeds from power substations**: By balancing the power load across two or more feeds, the operator has the flexibility to adjust in case of power surges, brown
outs or complete failure of a single source. It also allows for instant redundancy as there is a lower percentage of power to transfer if a source completely fails.

- **Multiple and disparate conduits for power and bandwidth:** If one conduit is severed, either due to an accident or to vandalism, having multiple feeds into the building for power and Internet is crucial to system availability.

- **Single use, single design:** Buildings designed specifically for secure data storage should have reinforced physical structures such as concrete bollards, steel-lined walls, bulletproof glass and perimeter fencing.

- **Non multi-tenant:** Threats increase as the number of individuals with access to a building increases. Therefore, a data center should not be located in a multi-tenant facility.

- **24/7 monitoring:** Physical access is controlled around the clock. On-site technical personnel are also available 24/7.

- **Perimeter security:** Video- and/or electronic-surveillance devices are used and security guards are often employed.

- **Two-factor authentication:** To enter, personnel should pass through electronic and identity authentication systems, such as badge and biometric systems.

- **Biometric access:** Involves establishing someone’s identity based on chemical, behavioral or physical attributes of that individual.

- **Man traps:** A small room designed to “trap” individuals trying to enter the facility.

- **Backup power security:** Emergency or backup power is used to keep critical data center security equipment operational at all times. Generators and UPS are generally combined into a single backup power solution.

- **Discreet room access and cage or cabinet access:** Access to room is limited; cabinets and cages that house hardware are locked and secure.

- **HVAC systems:** In tier IV centers, the heating, ventilating and air-conditioning (HVAC) systems are not drawing air from outdoors, but are set to recirculate. If there ever were a biological or chemical attack, or heavy smoke, this will protect data center staff and components.

- **Authorized personnel-only access:** Only a few employees are allowed to access the data center. Security-escorted entry is recorded by time-stamped logs.

- **Background checks:** Employees are required to pass stringent background checks as well as drug testing. They also should sign confidentiality agreements.

- **Restricted vendor access:** Vendors should carry a photo ID badge and be accompanied by authorized data center personnel at all times.

**C. Network Security**

In order to secure the network, the organization should build in multiple layers of protection. Network security issues that threaten the healthcare organization, include:

- Viruses, Trojan horses and “worms” using known signatures
• Attacks by hackers with a specific target in mind
• Spyware or adware driving unmonitored processes (some are relatively harmless, but others are used to steal passwords and gain unauthorized access to the network)
• “Denial of service” attacks designed to interrupt the ability to access information
• Data interception and monetary or identity theft as a result of finding a hole in network security
• Advanced persistent threats that sit silently in the background learning about network weaknesses that can be exploited later
• New viruses for which there is no known signature (called “zero-day” or “zero-hour” attacks) put networks at risk until a patch or defense is developed.

A layered series of network safeguards and protections should include but are not limited to:

**Advanced firewall configurations:** Robust filters are configured to security requirements, stopping known threats from attacking the network while allowing legitimate traffic to pass through. The firewalls should be constantly maintained and updated with the latest security vulnerability patches or firmware upgrades.

**Enterprise-grade hardware:** This hardware should be designed and certified for enterprise use, and include the latest security features to reduce vulnerability. They should have required feature sets such as web application filtering or intrusion detection system capability.

**Intrusion detection and prevention systems (IDPS):** These appliances monitor network activities and alert the organization to suspicious activity, allowing time to shut down areas under attack before security can be penetrated.

**Network design:** The network design should avoid known security vulnerabilities, adhere to well-established, third party best practices. For healthcare, that includes requirements for HIPAA compliance. It should also incorporate means of isolating detected threats to prevent damage to the organization while maintaining its ability to function normally. Detection should always include network monitoring to alert the organization when there is a security threat stemming from a vulnerability, access control or other means.

**Log management:** This tool detects and traces failed login attempts from known and unknown actors, registry changes, services installed and uninstalled, web server attacks and other suspicious behavior throughout a network. It can trigger advanced firewall changes to lock out unwanted attempts from IP addresses.

**Penetration testing:** The IT department should launch periodic planned attacks on its own network (or hire a “white hat” hacking firm) in order to test its defenses and discover security gaps.
Security information and event management (SIEM): Including appliances, software and managed services, SIEM analyzes security alerts provided by network hardware and applications in real time. It also logs security data and can produce compliance reports. SIEM is particularly helpful in allowing healthcare organizations to correlate data coming in from multiple security sources and recognize unusual activities that don’t tie in to a known threat.

Secure Sockets Layer virtual private network (SSL VPN): It allows data transmission through an encrypted tunnel to a VPN concentrator. Many SSL VPN appliances are also capable of integrating two-factor authentication technologies to enable another layer of security.

Threat management response: Signature-based detection combined with anomaly detection allows security teams to react quickly to known threats, isolating infected computers or devices before the threat becomes pervasive.

Vulnerability testing: This tool proactively identifies vulnerabilities within the IT environment to minimize risk.

Vulnerability monitoring: This involves continuous scanning of the IT infrastructure to identify known weaknesses so they can be remediated quickly.

D. Application Security

In large healthcare organizations, the number of applications and the interactions among them can be highly complex. In fact, each application can potentially interact with dozens of others. In most healthcare settings, there is a web of application interfaces and data, along with legacy components that have been developed or integrated by multiple divisions within the healthcare organization. This environment is highly challenging and includes a number of risks, for example:

- Hackers may locate software bugs in the server or its OS and gain access to the server.
- Denial of service (DoS) attacks may be directed to the server.
- Unauthorized parties may read confidential server information.
- Unencrypted or poorly encrypted information being transmitted between the server and the client may be intercepted.
- Hackers can gain access to the network by attacking the server.
- Rogue processes that are not healthcare-specific may be active on the server, causing vulnerabilities that organizations are not aware of.
- Network access ports may be left open by default, allowing for future vulnerabilities.
In addition to preventive measures, such as the implementation of anti-virus and anti-malware software and installing patches as they are made available by the application developers, key best practice elements of application security also include:

**Data encryption (at rest and in transit)** is the conversion of data into a form that cannot be read without the proper encryption key.

**Two-factor authentication** requires a user present not only a username and password but also another form of identification. The second form is generally something the user knows, such as a personal identification number; something the user has, such as an electronic security badge; or something that is inherent to the user, such as a fingerprint or voice print.

**Log management** detects any failed login attempts from known and unknown actors, any registry changes, any services installed and uninstalled, any web server attacks and other suspicious behavior throughout a network. It is a tool to detect occurrence of these actions but also in helping to trace the possible source.

**Web application firewalls** block dangerous web application attacks such as SQL injection, cross-site scripting and cross-site request forgeries, an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.

**Application design** to ensure the methods used follow the best practices for ensuring security. Thorough testing for known application security risks should be incorporated into the overall development plan.

**Vulnerability testing** involves using tools to proactively identify weaknesses and vulnerabilities within the IT environment so controls can be implemented to minimize those risks.

**Code reviews** of internally developed applications are necessary in order to locate and repair mistakes overlooked in the initial development phase.

**Threat management response** is signature-based detection combined with anomaly detection to rapidly recognize that something unusual is taking place. It allows security teams to react quickly to known threats, isolating infected computers or devices before the threat becomes pervasive while minimizing false alarms.

## E. Server Security

Servers require oversight in a variety of areas in order to stay secure. Like application security, they rely on patching as well as security information and event management. All servers should go through a hardening process prior to being implemented to production. Best practices for server security include:

- **File integrity monitoring (FIM):** An internal process or control for validating the integrity of the operating system and application software files. As files change, notifications go out to ensure that file changes were intended.
• Role-based access controls (RBAC): An approach that restricts system access to authorized users.

F. Data Security
One of the most important security best practices a healthcare organization can follow is to ensure its data is encrypted at rest as well as in transit. Encryption methods for data in transit may include technologies that help organizations avoid having to control their data over the public Internet, such as secure MPLS connectivity or SSL VPN-only access to the application. The cloud data security plan will include:

• **Policies for data retention, archiving and destruction.** Any PHI or other confidential data that is legally required to be retained or archived should be stored in compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations, and should be encrypted. This includes archived email, which often contains PHI and other confidential information. Electronic PHI designated for destruction should be removed according to HIPAA requirements, which include using software or hardware products to overwrite media with non-sensitive data (clearing), degaussing or exposing the media to a strong magnetic field in order to disrupt the recorded magnetic domains (purging) or destroying the media containing the PHI completely.

• **Data lifecycle management.** These policies relate to where and how data is stored. It is important to ensure that PHI is fully encrypted regardless of where it is in the lifecycle.

• **Data inventory and safeguards.** Data should be inventoried so the organization understands all the types of data it has, where it is stored, which systems are accessing it and how it is being used. Some of the technologies used to protect this data may include firewalls, log management, threat management, file integrity monitoring and vulnerability scans.

G. Mobile, Medical Devices, Home Telehealth and BYOD
Mobile devices, traditional medical devices (imaging, diagnostic and therapeutics devices), “bring your own device,” or BYOD, and home telehealth (HT) are becoming increasingly important care coordination factors across the enterprise. However, these end point devices involve security risks. Patient information can be accessed if a device is lost or stolen and many healthcare organizations have been cited for violating HIPAA security rules when a user’s device containing patient health information has been lost or is otherwise accessed by unauthorized users. Cloud-based virtual desktop infrastructure (VDI) is one way to mitigate this risk. This approach enables authorized users to medical devices or other types of thin clients to access files, data and applications that are hosted on remote servers. VDI removes some level of risk by eliminating the need to manage patches, upgrades and security for endpoint devices. By placing VDI in the cloud, a service provider takes on the responsibility for all operational requirements, including
management and maintenance of the VDI infrastructure. Thin clients are used to connect end-users to cloud-based services. Moving the client/desktop infrastructure to the cloud places all patient information behind a password-protected firewall. Healthcare data, however, should have additional security in order to meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA). Additional security considerations include:

- **Encryption** – Encrypting hospital-managed data while in motion over the network or at rest in the data center protects the information from all unauthorized personnel.

- **Multi-factor authentication** – Rather than require a simple username and password, multi-factor authentication requires the presentation of two or more of the three authentication factors: a knowledge factor (something the user “knows”), a possession factor (something the user “has”), and an inherence factor (something the user “is”). After presentation, each factor should be validated by the other party for authentication.

- **Role-based delivery of information** – Depending on a person’s role within the healthcare environment, only certain patient information is accessible.

When applied correctly, cloud-based VDI allows users access to end point devices where PHI is maintained behind the data center firewall and thereby reduces the risk of violating HIPAA and other regulatory compliance requirements.

### H. Users

The organization will ensure that the CSP has established and enforces formal, documented policies around every aspect of PHI data access. These include policies for:

- **Business Associate Agreements (BAA)**
- Identifying the security executive responsible for developing, implementing, monitoring and communicating HIPAA-compliant security

- **Authorization and documentation of who is allowed to access and work with PHI**
- **Permissions for their level of access**
- **Where access to PHI is and is not allowed**
- **Devices on which access to different types of data is allowed**
- **Detection of security incidents**
- **Sanctions for employees who do not follow policies**
- **Constant re-education on policies and procedures with annual refresher courses on user security**
- **Incident Response, Business Continuity and Disaster Recovery**

The organization will work with CSPs, especially their Human Resources departments, to ensure that people responsible for security are aware of changes that could constitute threats, particularly resignation or termination of network administrators or other trusted IT personnel with high-level PHI access. The designated group will audit on a periodic basis CSP enforcement of:
- **Passwords and user authentication** – The use of strong (random letter, number and symbol combination) passwords.

- **Two-factor authentication** - Not only something the user knows (password), but also something the user has (such as a proximity badge) and something inherent to the user (fingerprint, voice print).

- **Mobile Device, Medical Device, Home Telehealth and BYOD End Point Device Policies** – Specific policies, procedures and requirements – such as the use of passwords and biometric data (where available) to access the device – should be enacted and vigorously enforced to prevent data loss.

- **User training** – Document that policies and procedures are established and users are regularly trained on them. The CSP should have records that personnel are periodically tested on user knowledge and adherence to security protocols, close gaps in performance, educate users on the importance of following corporate policy, and that sanctions can be levied when policies are violated.

- **Third Party Vulnerability Testing and Accreditation** – User security policies and procedures should be tested through periodic vulnerability and, where appropriate, accreditation, such as DIRECT protocol utilization.

---

**I. Dissemination and Training**

This policy will be disseminated to employees and business units within the organization that procure and manage cloud services for the management of PHI. All vendors who conduct business and manage cloud based PHI services shall agree to the terms and conditions of this policy. The designated contact will provide information to management for training employees on this policy for contracting and managing CSP services related to PHI and the compliance with relevant privacy and information security laws, regulations, and requirements.

**J. Review, Updates, and Monitoring Compliance**

This policy will be reviewed at least annually and updated as appropriate. The designated contact shall be responsible for auditing business functions to ensure compliance with this policy. Third Party independent reviews of CSP policies, procedure and evidence based compliance should be conducted on a periodic basis.

**K. Vendor Relationships**

Each contract with vendors shall outline requirements for the safe cloud handling of PHI information as they apply to PHI storage and transport, including access controls, copying, authentication systems, or encryption. Vendors will agree and acknowledge that they have the following:

- Procedures for safe storage and handling of PHI including requirements for back-up of data.
- Procedures for securely destroying data, as well as any requirements for securing transport to facilities for erasure or destruction.
Incident Management and Escalation: Clear definition around what constitutes “lost media” and the timeline for notifying the Department when an incident has occurred.

Audit: Third Party periodic reviews validating PHI transport, storage, back-up, incident response, business continuity and disaster recovery controls, data erasure and media destruction methods, and requirements for timing for destruction.
## Appendix C – Acronyms

<table>
<thead>
<tr>
<th>Acronym or Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARRA</td>
<td>American Recovery and Reinvestment Act of 2009</td>
</tr>
<tr>
<td>ATO</td>
<td>Authority to Operate</td>
</tr>
<tr>
<td>BAA</td>
<td>Business Associate Agreements</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring Your Own Device</td>
</tr>
<tr>
<td>CAT</td>
<td>Computerized Axial Tomography</td>
</tr>
<tr>
<td>CCD</td>
<td>Continuity of Care Document</td>
</tr>
<tr>
<td>CCHIT</td>
<td>Certification Commission for Healthcare Information Technology</td>
</tr>
<tr>
<td>CCR</td>
<td>Continuity of Care Record</td>
</tr>
<tr>
<td>CCTV</td>
<td>Closed-Circuit Television</td>
</tr>
<tr>
<td>CDA</td>
<td>Clinical Document Architecture</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial “off-the-shelf” Systems</td>
</tr>
<tr>
<td>CPRS</td>
<td>Computerized Patient Record System</td>
</tr>
<tr>
<td>CRISP</td>
<td>Continuous Readiness in Security Program</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>CT</td>
<td>Computerized Tomography</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DICOM</td>
<td>Digital Imaging and Communications in Medicine</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DNA</td>
<td>Deoxyribonucleic Acid</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>EKG</td>
<td>Electrocardiogram</td>
</tr>
<tr>
<td>ESS</td>
<td>Enterprise Shared Services</td>
</tr>
<tr>
<td>EV-SSL</td>
<td>Extended Validation – Secure Socket Layer</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>Federal Risk and Authorization Management Program</td>
</tr>
<tr>
<td>FIM</td>
<td>File Integrity Monitoring</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standard</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information Security Management Act</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GSA</td>
<td>General Services Administration</td>
</tr>
<tr>
<td>HCOs</td>
<td>Healthcare Organizations</td>
</tr>
<tr>
<td>HHS</td>
<td>Health and Human Services</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act</td>
</tr>
<tr>
<td>HL7</td>
<td>Health Level 7</td>
</tr>
<tr>
<td>HSPC</td>
<td>Healthcare Services Platform Consortium</td>
</tr>
<tr>
<td>HSPD-12</td>
<td>Homeland Security Presidential Directive 12</td>
</tr>
<tr>
<td>HSSP</td>
<td>Health Services Specification Project</td>
</tr>
<tr>
<td>HT</td>
<td>Home Telehealth</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating, ventilating and air conditioning</td>
</tr>
<tr>
<td>Acronym</td>
<td>Full Form</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>IaaS</td>
<td>Infrastructure as a service</td>
</tr>
<tr>
<td>ID</td>
<td>Identification</td>
</tr>
<tr>
<td>IAM</td>
<td>Identity and Access Management</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IS</td>
<td>Information Systems</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>MAC</td>
<td>Media Access Control</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>MRI</td>
<td>Magnetic Resonance Imaging</td>
</tr>
<tr>
<td>MUMPS</td>
<td>Massachusetts General Hospital Utility Multi-Programming System</td>
</tr>
<tr>
<td>NCPDP</td>
<td>National Council for Prescription Drug Programs</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NPE</td>
<td>Non-Person Entity</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>OCR</td>
<td>Office of Civil Rights</td>
</tr>
<tr>
<td>OI&amp;T</td>
<td>Office of Information and Technology</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>OMG</td>
<td>Object Management Group</td>
</tr>
<tr>
<td>OPM</td>
<td>Office of Personnel Management</td>
</tr>
<tr>
<td>OS</td>
<td>Open Source</td>
</tr>
<tr>
<td>OSEHRA</td>
<td>Open Source Electronic Health Record Alliance</td>
</tr>
<tr>
<td>PaaS</td>
<td>Platform as a Service</td>
</tr>
<tr>
<td>PACS</td>
<td>Physical Access Control Systems</td>
</tr>
<tr>
<td>PASS</td>
<td>Project Summary for Privacy, Access and Security Services</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PIV</td>
<td>Personal Identification Verification</td>
</tr>
<tr>
<td>PHI</td>
<td>Protected Health Information</td>
</tr>
<tr>
<td>RBAC</td>
<td>Role-based Access Controls</td>
</tr>
<tr>
<td>RMF</td>
<td>Risk Management Framework</td>
</tr>
<tr>
<td>Saas</td>
<td>Software as a Service</td>
</tr>
<tr>
<td>SIEM</td>
<td>Security Information and Event Management</td>
</tr>
<tr>
<td>sMIME</td>
<td>Secure/Multipurpose Internet Mail Extensions</td>
</tr>
<tr>
<td>SNOMED</td>
<td>System Nomenclature of Medicine</td>
</tr>
<tr>
<td>SOA</td>
<td>Services Oriented Architecture</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure Shell</td>
</tr>
<tr>
<td>SSID</td>
<td>Service Set Identifier</td>
</tr>
<tr>
<td>SSL/TLS</td>
<td>Secure Sockets Later / Transport Layer Security</td>
</tr>
<tr>
<td>SSOi/SSOe</td>
<td>Single Sign-On Internal and External</td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TWG</td>
<td>Technical Working Group</td>
</tr>
<tr>
<td>VA</td>
<td>Veterans Affairs</td>
</tr>
<tr>
<td>VDI</td>
<td>Virtual Desktop Infrastructure</td>
</tr>
<tr>
<td>VistA</td>
<td>Veterans Information System and Technology Architecture</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WPA2</td>
<td>Wi-Fi Protected Access II</td>
</tr>
<tr>
<td>XSS</td>
<td>Cross-Site Scripting</td>
</tr>
</tbody>
</table>