**Vulnerability Assessment Standard**

|  |  |
| --- | --- |
| Policy Number | IT-008 |
| Title | Vulnerability Assessment Standard |
| Organization / Authority | eHealth, Inc. |
| Effective Date | October 1, 2013 |
| Review Date | September 1, 2014 |
| Standard Owner – Name | David Rickling |
| Standard Owner - Title | Director, Information Technology and Security |
| Standard Manager - Name | David Rickling |
| Standard Manager - Title | Director, Information Technology and Security |
| For questions about this standard, contact: | Robert Roohparvar, Information Technology and Security Department |
| MARS-E References | AT-3, CA-1, CA-7, RA-5, SI-1, SI-2(3) |
| PCI References |  |
| ISO References |  |
| HIPAA References |  |
| Author This Version: | Robert Roohparvar |

**Table of Contents**

[1. Purpose 3](#_Toc372553854)

[2. Scope 3](#_Toc372553855)

[3. Roles and Responsibilities 3](#_Toc372553856)

[4. Requirements 4](#_Toc372553857)

[5. Performing Vulnerability Scans 5](#_Toc372553858)

[5.1. Types of Scans 5](#_Toc372553859)

[5.2. Regularly Scheduled Scans 5](#_Toc372553860)

[5.2.1. Qualys Vulnerability Management Scans (VM): 5](#_Toc372553861)

[5.2.2. Qualys Web Application Security Scans (WAS): 5](#_Toc372553862)

[5.2.3. PCI Scans: 5](#_Toc372553863)

[5.2.4. Mergers and Acquisitions Scans: 5](#_Toc372553864)

[5.2.5. Incident Response Scans: 6](#_Toc372553865)

[5.2.6. Ad Hoc Scans: 6](#_Toc372553866)

[5.3. New Hosts Scans 6](#_Toc372553867)

[5.4. Scanning Times 6](#_Toc372553868)

[5.5. Freezes and IT Security Oversight 6](#_Toc372553869)

[5.6. Vulnerability Remediation Requirements: 6](#_Toc372553870)

[5.7. Qualys Severity Levels 6](#_Toc372553871)

[5.7.1. Survivability 7](#_Toc372553872)

[5.7.2. Authorization and Access for Scan Requests 7](#_Toc372553873)

[6. Exceptions 7](#_Toc372553874)

[7. Compliance 7](#_Toc372553875)

[8. Related Documents 8](#_Toc372553876)

[9. Contributors/Reviewers 9](#_Toc372553877)

[10. Approvals 9](#_Toc372553878)

[11. Revision History 9](#_Toc372553879)

[Appendix A – Definitions 10](#_Toc372553880)

# Purpose

This standard has been created to document the purpose, process, and procedure for the eHealth Vulnerability Management program with specific guidance for eHealth’s vulnerability management. The intention of this standard is to define the requirements for eHealth to adopt the Vulnerability Management policy and to identify and employ up to date vulnerability identification scanning tools to regularly test web based applications, servers, operating systems, web commerce operating systems, firewalls and routers configurations, etc.

The controls in this standard shall be considered the minimum acceptable requirements for the performance of any vulnerability assessment. This standard sets forth expectations across the entire organization. Additional control measures may apply to certain areas of eHealth. This standard shall not be construed to limit application of more stringent requirements where justified by business needs or assessed risks.

# Scope

This standard applies to all eHealth assets, whether located at an eHealth facility or a third party facility, and whether handled by eHealth employees, or eHealth contractors, vendors, third party service providers, or their staff or agents.

# Roles and Responsibilities

The ***Data/Asset Owner*** is the owner of the data and its associated risk. The Data Owner may transfer the risk to the System Owner or may take an active role to ensure that the System Owner is implementing effective security controls. The Data Owner is also responsible for reporting to IT Security any routine scan that is detected to impact the uptime or bandwidth or availability of any host, network or application.

The ***System Owner*** is responsible for timely application and operating systems patches in order to reduce the overall risk of the systems under their control, and to comply with eHealth Security Policies. Responsibilities include:

* Cooperate with eHealth IT Security to provide information relative to assets under their control.
* Coordinate with eHealth IT Security to determine a scanning schedule.
* Designate a knowledgeable technical resource to assist eHealth IT Security to understand the internal network architecture.
* View the vulnerability scan report provided by eHealth IT Security.
* Develop a Remediation Plan for exposures identified in the vulnerability scan report and submit it to the IT Security.
* Provide status updates on the Remediation Plan(s) to eHealth stakeholders

The ***IT* *Security team*** is responsible for:

* Defining and implementing security measures and controls to ensure the vulnerability assessments are managed and operated in a secure and effective manner.
* Defining, implementing, managing, monitoring and review the adequacy of controls and security measures in place to measure and enforce conformance to this standard.
* Ensuring that scans are performed as required, requested or scheduled.
* Performing/coordinating vulnerability scans/assessments with system owners and reporting to stakeholders.
* Managing and maintaining vulnerability assessment tools.
* Providing access/creating account to vulnerability assessment tools.
* Training systems and security administrators on vulnerability tools.
* Ensuring that any detected high vulnerabilities (severity 3-5 described in section 5.7) are remediated in a manner consistent with this standard, remediation progress is tracked and status is reported to the system owners.

The ***System Administrator*** is responsible for executing tasks identified in the Remediation Plan. In addition to vulnerability scan performed by IT Security, System Administrators must regularly monitor systems under their control for vulnerabilities, remediation and threats using a variety of available resources.

# Requirements

The following processes are required for Vulnerability Assessment:

All eHealth IT assets on the production network, including laptops, workstations, printers, routers, switches, servers, firewalls, and all other network connected devices, must be scanned periodically to detect critical vulnerabilities on the devices that would pose an unacceptable risk to the eHealth network.

eHealth has selected QualysGuard as the only vulnerability scanning appliance and Software as a Service (SaaS) platform. Only Qualys software and hardware is authorized to perform vulnerability assessments. The use of any other software that performs similar function must be justified by legitimate purposes and recorded as exceptions.

The service must be operated by the IT Security Team and scans will be conducted on recurring or ad hoc basis.

Production scans must have all eHealth web applications hosted on the corporate network scanned weekly to detect critical vulnerabilities in the applications as they would pose an unacceptable risk to the eHealth network.

Qualys Web Application Scan (WAS) is the only approved web application vulnerability assessment tool. As such, only Qualys reports are used for reporting vulnerabilities within an application.

For firewalls and routers configuration vulnerability assessment, eHealth has selected Skybox software to perform the tasks.

Criteria and timeline to address vulnerabilities are addressed in the Security Patch Management Standard IT-007 document.

# Performing Vulnerability Scans

eHealth has selected QualysGuard as the only vulnerability scanning appliance and software as a service (SaaS) platform which provides the following functions:

* Identify active hosts on the network
* Identify active and vulnerable services (ports) on the hosts
* Identify operating systems and applications vulnerabilities
* Test compliance with security policies and regulatory standards

## Types of Scans

There are different types of scans that can be conducted. Some scans are governed to prevent possible impact to the applications and network. These scan types are detailed below:

***Non-intrusive Assessment Scans***, which have minimal impact to the target systems.

***Intrusive Assessment Scans***, which are mainly targeting systems that are in the development network or before deployment in to production services. Intrusive scans attempt to exploit some of the critical vulnerabilities that might disrupt running systems or take a system offline.

***Credential Scans***, which utilize a valid login credential of the target systems and verify internal services, installed applications, and patch levels. Credential scans are more comprehensive and accurate. Credential scans are also much less intrusive as the scanning engine is able to acquire information about the system without attempting to exploit potential vulnerabilities and are eHealth IT Security preferred scanning method.

## Regularly Scheduled Scans

### Qualys Vulnerability Management Scans (VM):

* All external hosts (internet facing hosts) are scanned weekly.
* All internal hosts are scanned monthly.
* These scans can be scheduled and automated to recur weekly or monthly with no impact to the network.

### Qualys Web Application Security Scans (WAS):

* All web applications must be scanned on a weekly basis.

### PCI Scans:

* Qualys VM: All internet facing hosts must have a PCI scan performed monthly for compliance with IT Security requirements and quarterly as is required by PCI regulations.
* Qualys WAS: All web applications must be scanned on a weekly basis.

### Mergers and Acquisitions Scans:

* When a company is acquired by eHealth.

### Incident Response Scans:

* These are scans that are conducted on an ad hoc basis in response to an incident detected on a particular host to determine the likely cause of compromise.

### Ad Hoc Scans:

* All asset owners have the right to know the vulnerabilities that exist on their assets. Upon request, asset owners, after obtaining authorization and providing proof of ownership, may request scans against their assets.

## New Hosts Scans

New hosts introduced to the production network must be scanned and any high vulnerability must be remediated prior to beginning operations of the asset.

## Scanning Times

Scanning times are defined as follows:

* All automated scanning for internal need to be scheduled to avoid impact of month end and quarter end freezes (as defined in Section 5.5)
* Incident related scans may be executed at any time by request of the Incident Response team.

## Freezes and IT Security Oversight

Some scans may be restricted by the quarter end freezes. Because these scans are so large, there is a risk that continuous scanning may increase systems’ load and prevent them from prforming critical functions. If new scanners are added to the network or a new type of network wide scan is required, IT Security will be engaged to review the risks involved.

## Vulnerability Remediation Requirements:

Criteria and timeline to address vulnerabilities are addressed in the Security Patch Management Standard IT-007 document.

## Qualys Severity Levels

Each type of vulnerability is assigned a severity level, which is determined by the security risk associated with its exploitation. The following tables describe possible consequences related to each vulnerability type.

| **Severity** | **Level** | **Description** |
| --- | --- | --- |
| vuln_level1.gif | **Minimal** Level 1 | Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities. |
| vuln_level2.gif | **Medium** Level 2 | Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions. |
| vuln_level3.gif | **Serious** Level 3 | Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying. |
| vuln_level4.gif | **Critical** Level 4 | Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host. |
| vuln_level5.gif | **Urgent** Level 5 | Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors. |

### Survivability

Should a routine scan be determind to potentially impact the uptime, bandwidth or availability of any host, network or application, this should be reported immediately to IT Security as an incident. Qualys uses only non-destructive testing and does not consume excessive bandwidth during scans. Thus, any impact detected speaks to the survivability of the asset more than the impact of the scanning procedure. The host or application would need to be hardened to survive normal scanning activity.

### Authorization and Access for Scan Requests

The IT Security Team will ensure that asset owners are authorized to request scans and will manage the requestor’s access to the scan results, whether it is by email or through access to the Qualys Portal.

# Exceptions

Exceptions to this standard must be unanimously approved by the Director of Information Technology and Security and the requesting Business Unit Leadership (VP).

The [Risk Exception Request Form](http://sjmsp01/dept/it/iss/Audit%20Support%20Documentation/Forms/AllItems.aspx?RootFolder=%2fdept%2fit%2fiss%2fAudit%20Support%20Documentation%2fRisk%20Exception%20Requests&FolderCTID=&View=%7b0C73D1DD%2d34F7%2d4A5A%2dA399%2d50D8444E8CC5%7d) can be obtained from the Corporate Policy area on eHealth’s Intranet.

Before submitting your Risk Registration Request forms to [security@eHealth.com](mailto:security@eHealth.com), please ensure you have obtained all the relevant Business and IT Acceptance’s for the risk.

# Compliance

This standard will be enforced by Information Technology and Security Team. The Information Technology and Security Team will use a variety of tools to monitor and assess whether security controls and measures have been implemented and are being followed.

Non-compliance with this standard will result in notifications to the employee and management. Further consequences may include disciplinary action (up to and including termination of employment). eHealth may also pursue any other available legal remedies.

# Related Documents

This document is part of the eHealth cohesive set of security policies and support documents. The following list may apply to the topics covered in this document and, as such, the applicable policies and supporting documents should be reviewed as necessary.

* Security Patch Management Standard IT-007
* [MARS-e Support Documents](http://sjmsp01/dept/it/iss/Lists/Assets/AllItems.aspx)

# Contributors/Reviewers

| **Date** | **Reviewer** | **Title** | **Functional Area** |
| --- | --- | --- | --- |
| 09/30/13 | Jiang Wu (for David Rickling) | Director, Information Technology and Security | Information Technology and Security |
| 09/03/13 | Suko Nishimura | Director, Corporate Technology | Corporate Technology |
| 09/05/13 | Rachel Jaris | Director, Internal Audit | Internal Audit |
| 11/18/13 | Bryan Chin | Program Manager | Information Technology |

# Approvals

| **Date** | **Approver** | **Title** | **Functional Area** |
| --- | --- | --- | --- |
| 11/25/13 | Jiang Wu | SVP, Engineering | Engineering |

# Revision History

| Date | Version | Content Contributors | Description of Change |
| --- | --- | --- | --- |
| 11/18/13 | 1.00 | Robert Roohparvar | Initial version. |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Appendix A – Definitions

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Term 1** | Definition Content |
| **Term 2** | Definition Content |
| **Term 3** | Definition Content |
| **Term 4** | Definition Content |