**16. Vulnerability Scanning Policy**

Familyfirst is proactive about information security and understands that vulnerabilities need to be monitored on an ongoing basis. Familyfirst utilizes [Nessus Scanner](http://www.tenable.com/products/nessus) from Tenable to consistently scan, identify, and address vulnerabilities on our systems. We also utilize [OSSEC](http://www.ossec.net/) on all systems, including logs, for file integrity checking and intrusion detection.

**16.1 Applicable Standards**

**16.1.1 Applicable Standards from the HITRUST Common Security Framework**

• 10.m - Control of Technical Vulnerabilities

**16.1.2 Applicable Standards from the HIPAA Security Rule**

• 164.308(a)(8) - Evaluation

**16.2 Vulnerability Scanning Policy**

1 Nessus management is performed by the Familyfirst Security Officer with assistance from the VP of Engineering.

2 Nessus is used to monitor all internal IP addresses (servers, VMs, etc) on Familyfirst networks.

3 Frequency of scanning is as follows:

4 on a weekly basis;

5 after every production deployment.

6 Reviewing Nessus reports and findings, as well as any further investigation into discovered vulnerabilities, are the responsibility of the Familyfirst Security Officer. The process for reviewing Nessus reports is outlined below:

7 The Security Officer initiates the review of a Nessus Report by creating an Issue in the JIRA Compliance Review Activity (CRA) Project.

8 The Security Officer, or a Familyfirst Security Engineer assigned by the Security Officer, is assigned to review the Nessus Report.

9 If new vulnerabilities are found during review, the process below is used to test those vulnerabilities is outlined below. Once those steps are completed, the Issue is then reviewed again.

10 Once the review is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further review.

11 If the review is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

12 In the case of new vulnerabilities, the following steps are taken:

• All new vulnerabilities are verified manually to assure they are repeatable. Those not found to be repeatable are manually tested after the next vulnerability scan, regardless of if the specific vulnerability is discovered again.

• Vulnerabilities that are repeatable manually are documented and reviewed by the Security Officer, VP of Engineering, and Privacy Officer to see if they are part of the current risk assessment performed by Familyfirst.

◦ Those that are a part of the current risk assessment are checked for mitigations.

◦ Those that are not part of the current risk assessment trigger a new risk assessment, and this process is outlined in detail in the Familyfirst Risk Assessment Policy.

6 All vulnerability scanning reports are retained for 6 years by Familyfirst. Vulnerability report review is monitored on a quarterly basis using JIRA reporting to assess compliance with above policy.

7 Penetration testing is performed regularly as part of the Familyfirst vulnerability management policy.

• External penetration testing is performed bi-annually by a third party.

• Internal penetration testing is performed quarterly. Below is the process used to conduct internal penetration tests.

i The Security Officer initiates the penetration test by creating an Issue in the JIRA Compliance Review Activity (CRA) Project.

ii The Security Officer, or a Familyfirst Security Engineer assigned by the Security Officer, is assigned to conduct the penetration test.

iii Gaps and vulnerabilities identified during penetration testing are reviewed, with plans for correction and/or mitigation, by the Familyfirst Security Officer before the Issue can move to be approved.

iv Once the testing is completed, the Security Officer approves or rejects the Issue. If the Issue is rejected, it goes back for further testing and review.

v If the Issue is approved, the Security Officer then marks the Issue as Done, adding any pertinent notes required.

• Penetration tests results are retained for 6 years by Familyfirst.

• Internal penetration testing is monitored on an annual basis using JIRA reporting to assess compliance with above policy.

8 This vulnerability policy is reviewed on a quarterly basis by the Security Officer and Privacy Officer.