NIST CYBERSECURITY PRACTICE GUIDE HEALTH IT

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Risk Assessment and Outcomes

Gavin O'Brien

Brett Pleasant

Colin Bowers

Sue Wang

Kangmin Zheng

Kyle Kamke

Nate Lesser

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1e

DRAFT

National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-1e

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

Gavin O'Brien
Nate Lesser
National Cybersecurity Center of Excellence
Information Technology Laboratory

Sallie Edwards
Brett Pleasant
Sue Wang
Kangmin Zheng
The MITRE Corporation
McLean, VA

Colin Bowers
Kyle Kamke
Ramparts, LLC
Clarksville, MD

Leah Kauffman, Editor-in-Chief
National Cybersecurity Center of Excellence
Information Technology Laboratory

July 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

DISCLAIMER

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology Special Publication 1800-1e
Natl. Inst. Stand. Technol. Spec. Publ. 1800-1e, 75 pages (July 2015)
CODEN: NSPUE2

Organizations are encouraged to review all draft publications during public comment periods and provide feedback. All publications from NIST's National Cybersecurity Center of Excellence are available at http://nccoe.nist.gov.

Comments on this publication may be submitted to: HIT_NCCoE@nist.gov

Public comment period: July 22, 2015 through September 25, 2015

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
9600 Gudelsky Drive (Mail Stop 2002) Rockville, MD 20850
Email: nccoe@nist.gov

National Cybersecurity Center of Excellence

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with industry, academic and government experts to build modular, open, end-to-end reference designs that are broadly applicable and repeatable. The center's work results in publically available NIST Cybersecurity Practice Guides, Special Publication Series 1800, that provide users with the materials lists, configuration files, and other information they need to adopt a similar approach.

To learn more about the NCCoE, visit http://nccoe.nist.gov. To learn more about NIST, visit http://www.nist.gov.

NIST Cybersecurity Practice Guides

NIST Cybersecurity Practice Guides (Special Publication series 1800) target specific cybersecurity challenges in the public and private sectors. They are practical, user-friendly guides that facilitate the adoption of standards-based approaches to cybersecurity. They show members of the information security community how to implement example solutions that help them more easily align with relevant standards and best practices.

The documents in this series describe example implementations of cybersecurity practices that may be voluntarily adopted by businesses and other organizations. The documents in this series do not describe regulations or mandatory practices, nor do they carry statutory authority.

Abstract

Health care providers increasingly use mobile devices to receive, store, process, and transmit patient clinical information. According to our own risk analysis, discussed here, and in the experience of many health care providers, mobile devices can present vulnerabilities in a health care organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that mobile devices are being used by many providers for health care delivery before they have implemented safeguards for privacy and security.[*]

This NIST Cybersecurity Practice Guide provides a modular, open, end-to-end reference design that can be tailored and implemented by health care organizations of varying sizes and information technology sophistication. Specifically, the guide shows how health care providers, using open source and commercially available tools and technologies that are consistent with cybersecurity standards, can more securely share patient information among caregivers using mobile devices. The scenario considered is that of a hypothetical primary care physician using

[*] Mobile Devices Roundtable: Safeguarding Health Information Real World Usages and Safeguarding Health Information Real World Usages and Real World Privacy & Security Practices, March 16, 2012, U.S. Department of Health & Human Services

her mobile device to perform reoccurring activities such as sending a referral (e.g., clinical information) to another physician, or sending an electronic prescription to a pharmacy. While the design was demonstrated with a certain suite of products, the guide does not endorse these products in particular. Instead, it presents the characteristics and capabilities that an organization's security experts can use to identify similar standards-based products that can be integrated quickly and cost-effectively with a health care provider's existing tools and infrastructure.

KEYWORDS

implement standards-based cybersecurity technologies; mobile device security standards; HIPAA; electronic health record system; risk management; electronic health record security; breaches of patient health information; stolen medical information; stolen health records

ACKNOWLEDGEMENTS

We gratefully acknowledge the contributions of the following individuals and organizations for their generous contributions of expertise, time, and products.

Name	Organization
Curt Barker	NIST
Doug Bogia	Intel
Robert Bruce	Medtech Enginuity
Lisa Carnahan	NIST
Verbus Counts	Medtech Enginuity
David Low	RSA
Adam Madlin	Symantec
Mita Majethia	RSA
Peter Romness	Cisco
Steve Schmalz	RSA
Ben Smith	RSA
Matthew Taylor	Intel
Steve Taylor	Intel
Jeff Ward	IBM (Fiberlink)
Vicki Zagaria	Intel

Table of Contents

List of Figures

List of Tables

1 Practice Guide Structure

This NIST Cybersecurity Practice Guide describes a standards-based reference design and provides users with the information they need to replicate this approach to securing electronic health records transferred among mobile devices. The reference design is modular and can be deployed in whole or in parts.

This practice guide is made up of five volumes:

- NIST SP 1800-1a: Executive Summary
- NIST SP 1800-1b: Approach, Architecture, and Security Characteristics – what we built and why
- NIST SP 1800-1c: How To Guides – instructions to build the reference design
- NIST SP 1800-1d: Standards and Controls Mapping – listing of standards, best practices, and technologies used in the creation of this practice guide
- **NIST SP 1800-1e: Risk Assessment and Outcomes – risk assessment methodology, results, test and evaluation**

← **YOU ARE HERE**

2 Introduction

NIST SP 1800-1e: Risk Assessment and Outcomes, addresses the methodology used to conduct the reference design system risk assessment, the results of that risk assessment, the intended outcomes of implementing the reference design, and the results of the reference design functional test. This volume is broken into six sections:

- Results – the workflow and summary of the security control implementation (Section 3)
- Security Controls Assessment – scenario based evaluation of the security functionality of the reference design (Section 4)
- Risk Assessment Methodology – the two approaches we took in conducting a system risk assessment of the reference design (Section 5)
- Risk Assessment Results – detailed results of the risk assessments we conducted (Section 6)
- Security Controls Test and Evaluation – security controls and the evidence of their implementation (Section 7)
- Risk Questionnaire for health care organizations selecting a cloud-based EHR provider (Section 8)

3 Results

The features in this reference design and our process of continued risk assessment increase the difficulty for an adversary to gain unauthorized access to patient health information.[1] At the same time, we want to provide authorized users with easy access. The architecture is designed to enhance protection for patient information while minimizing changes to use of systems. As with all components of this reference design, every organization needs to make its own risk-based determinations about which of these capabilities to implement and how.

The security features of the reference design are modeled around the business workflow of a typical user accessing the EHR. This workflow and the relevant security checks are illustrated in Figure 1.

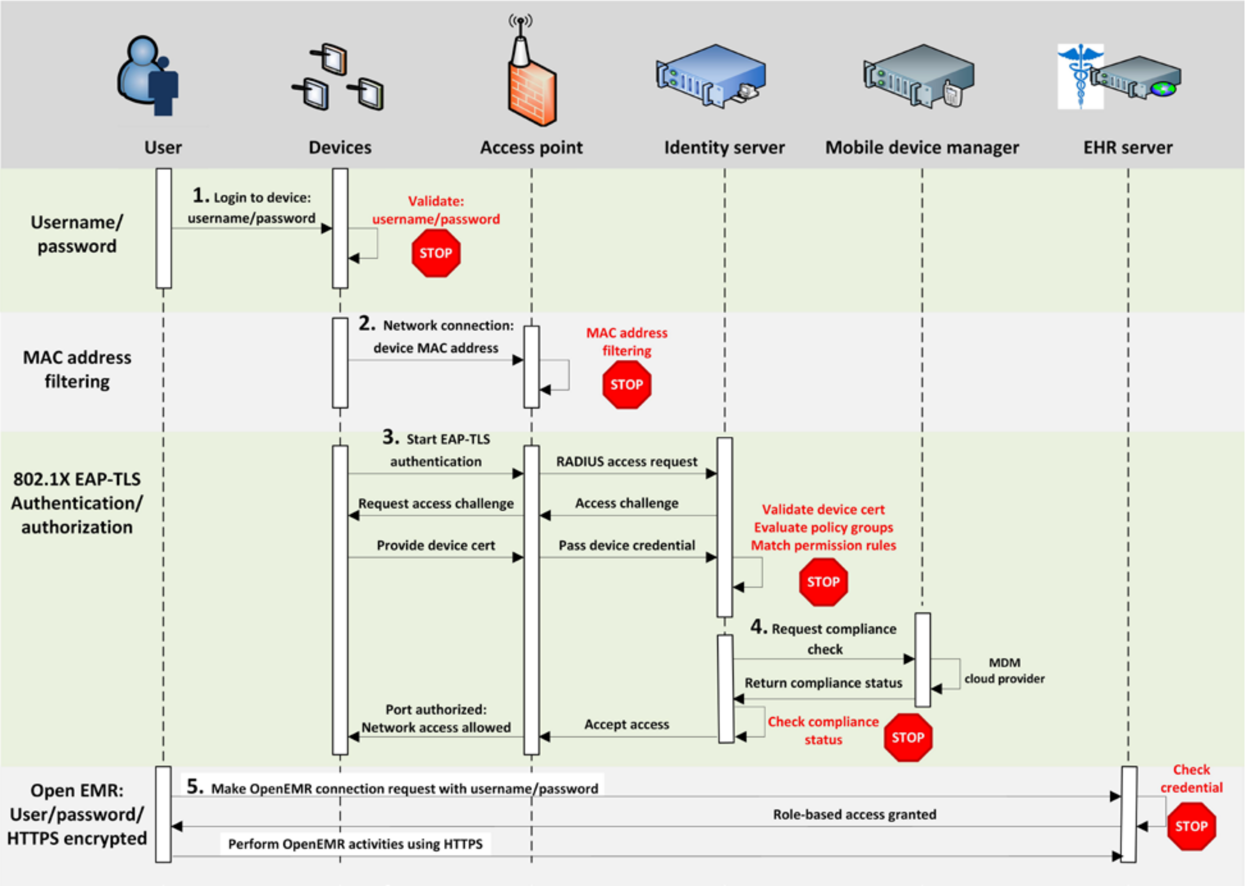


Figure 1: The steps necessary for a user and device to gain access to the electronic health record server.

[1] Here the term "patient health information" refers to any information pertaining to a patient's clinical care. "Protected health information" has a specific definition according to HIPAA that is broader than our scope. We are using "patient health information" so we do not imply that we are further defining protected health information or setting additional rules about how it is handled.

Prior to being granted access to the EHR, the user must follow the following five steps. However, since ease of use is paramount when it comes to the likelihood of adoption in real world environments, all but steps 1 (logging on to the device) and 5 (logging into the EHR) are transparent to the user.

Step 1. The user enters a username and password into the device.

Step 2. Communication starts from the mobile devices located in each organization. Each organization minimally provides APs to facilitate communication to the electronic health record server located in the Data Center. Each connection to an AP must first be challenged and responded to by the device with a proper media access control (MAC) address.

A MAC address cannot be changed on the physical device, but can be changed in the operating system. This makes security bypass trivial for even a low-level attacker. MAC filtering, therefore, is a first layer of defense for identity and access control

Step 3. The device is challenged by the AP for a properly signed and trusted certificate. If a user does not have this certificate on his device, he or she will not be allowed access on the local network to even attempt a connection to the Web-based OpenEMR.

In this simulation, the same certificate authority was used for both the AP and the OpenEMR tool. A hard certification could be a smart card or some other token provided by your IT department. Additional security could be added to this transaction by setting up a separately trusted CA for both and requiring a hard certification for access to either service. This approach would thwart the insider or attacker who has gained access to a lost or stolen device. They may get access to the AP, but not to the OpenEMR.

Step 4. The MDM performs a compliance check on the device based on the policy that was assigned.

Step 5. If a user has bypassed or gained access to a device using the proper MAC and certificate credentials (this assumes that the asset management policy for lost and stolen devices has not been implemented or followed in this case), the device is then challenged by the OpenEMR for additional client authentication using cryptography and a PKI based certificate (mutual authentication). The transaction is logged in the Web application and the MDM used in this build has the ability to track the specific location of a device while the log is open.

The user is then challenged by the OpenEMR for the proper username and password credentials. If an attacker attempts what is known as a brute force attack to gain access to the OpenEMR tool, then the likelihood that there will be a trail for an administrator to follow is higher given that the Web server application logs every attempt. The OpenEMR will also lock out the user after several log in attempts.

In this last step, a user with the right login credentials ultimately logs into the OpenEMR tool.

4 Security Controls Assessment

To demonstrate that our implementation of the security characteristics meets the business challenge, one of our collaborators, Ramparts, conducted an objective assessment of our reference design. The assessment shows that the architecture and implementation provide enhanced security by ensuring that read and write access to electronic health records and patient health information is limited to authorized users.

The assessment was not intended to be a complete test of every aspect of the functionality and security of the architecture or implementation. Such an undertaking would be impractical and difficult. Adapting the principles and implementation details of the reference design to an organization's enterprise infrastructure requires customizations that we cannot fully anticipate. Attempting to do so would potentially invalidate test results for organizations without a similar implementation. We expect that organizations that adopt this reference design will build on the material presented here to update their own system security plans and customize as needed to validate the security of their own implementations.

The assessment is organized in three parts:

1. security scenario assessment – provides evidence that the reference design protects the security of the patient health information in the context of several different attack scenarios
2. functional assessment – provides evidence that key functions described in the NCCoE use case document, "Secure Exchange of Electronic Health Information,"[2] which originally described this challenge, are properly implemented in the build
3. security assessment – provides evidence that the security characteristics specified in the use case are properly implemented in the build

Each assessment is described in further detail below. Section 5 of this volume contains lists of tests relevant to each type of assessment, many of which were run on the build. Some tests, such as those involving policy, procedure, or physical security, have been included in the appendix to provide guidance in the evaluation of real, operational implementations of the architecture. These tests were not performed on this reference design because they are not relevant to a laboratory setting.

4.1 Security Scenario Assessment

The independent evaluator conducted scenario-based security testing of the reference design to provide assurance that the security of health information could be maintained despite four specific attacks, as outlined in the sections below. In the attack-based scenario tests, NCCoE health IT architects and engineers played the roles of system administrators. During the various attack scenarios, the defenders ran the network to mimic the operations of a large health care organization with the resources to monitor and respond to any detected threats.

When testing transitioned to a new attacker scenario, the system administrators reset any mitigations (technical and procedural) that were put in place. Mitigations included resetting passwords but did not include blocking VPN access or the attacker's initial foothold. The test procedure assumed the attacker was able to compromise an internal Windows desktop computer.

[2] http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_HIT_MobileDevices_UseCase.pdf

The independent evaluator demonstrated that the use case architecture and implementation provide enhanced security with respect to the goal of ensuring that only authorized users are able to gain read and write access to the electronic health record system and patient health information.

4.1.1 Lost Mobile Device Scenario

In this scenario, an attacker acquired a mobile health device through theft or loss. The device had access to the electronic health record system at some point in time.

The device did not have any patient health information saved. We examined the device for remnants of patient health information provided this doesn't pose a significant risk to the device. In other words, we expected the device to be rooted in order to acquire a forensic image of the device's disk and memory.

Upon discovery of the lost device, the device should be blocked from accessing any resources on the Health ISP network. At a time coordinated with us, the defenders implemented a block.

A file or note containing example sensitive information was created and saved on the device. At a time coordinated with us, the defenders initiated a remote wipe. We verified the sensitive information was removed and the device wiped.

4.1.2 Internal Network Access Scenario

In this scenario, an attacker accessed the internal health ISP network. The attacker obtained access to the network through a phishing campaign and maintained a persistent presence on a Windows desktop computer. This persistent presence is represented by the ability to gain remote access to a desktop using low-level captured Windows domain credentials. In a real-world scenario, this would typically take the form of a backdoor with a network traffic redirector.

Through this foothold, the attacker obtained a network diagram of the health ISP. While the attacker obtained access, he did not obtain system administrator credentials.

Testing validated the defense-in-depth strategy and demonstrated that, for many of the weaknesses found, the architecture’s security characteristics, such as access controls, helped to limit the damage.

4.1.3 OpenEMR Access Scenario

In this scenario, an attacker accessed the OpenEMR Web application with typical user credentials (e.g. receptionist, accountant). The attacker was either a malicious insider with routine access to the system or an outsider who captured the user's credentials.

The attacker gained a foothold within the network and attempted to breach the security of patient health information. As in the internal network access scenario, testing demonstrated that access control helped to reduce the amount of patient health information to which the attacker had access.

4.1.4 Physical Access Scenario

In this scenario, an attacker had physical access to the Data Center. We assumed the attacker had unsupervised access for an extended period of time to the Data Center. The attacker was able to bring in electronics and tools. The attacker connected to our access point and logged and monitored network traffic. The test showed that all traffic was encrypted, thereby rendering it unusable by the attacker.

4.2 Functional Assessment

An independent functional test ensured that the build provides key functions described in the use case: A hypothetical primary care physician using a mobile device can securely send

- a referral from one physician to the electronic health record repository, from which a second physician retrieves the referral
- a prescription to the pharmacy

The subsections below briefly describe the intent of each function and then describe the validation and the results. The procedures used for each functional test are included in Section 5 of this volume.

4.2.1 Send a Referral

This test evaluated the capability of the electronic health record solution to electronically create and transmit a referral to another physician. In this scenario, the receiving physician was able to access the same electronic health record application as the referring physician. The receiving physician got the referral and accessed the patient record via a mobile device. When treatment was provided, the receiving physician updated the patient record in the electronic health record application. The original referring physician was notified of the action and accessed the updated patient record.

4.2.2 Send a Prescription

This test validated the electronic health record solution's prescription-sending capability. The test simulated a physician using a mobile device and electronic health record application to send a prescription

- to a pharmacy directly through the electronic health record application
- outside of the application via email or fax

These actions were successfully completed.

4.3 Security Assessment

A security assessment evaluated the security characteristics that we thought were satisfied by the architecture. To determine what tests to include, we consulted Table 1: *Relevant Standards and Controls* in NIST SP 1800-1d: *Standards and Controls Mapping*. Five security characteristic requirements are listed:

1. access control
2. audit controls/monitoring
3. device integrity
4. person or entity authentication
5. transmission security

In the table, each of these characteristics is further classified by the Cybersecurity Framework categories and subcategories to which they map. The Cybersecurity Framework subcategories were used to determine which tests to include in the security assessment by consulting the specific sections of each standard that were cited in reference to that subcategory. An example of the process is depicted in Figure 2.

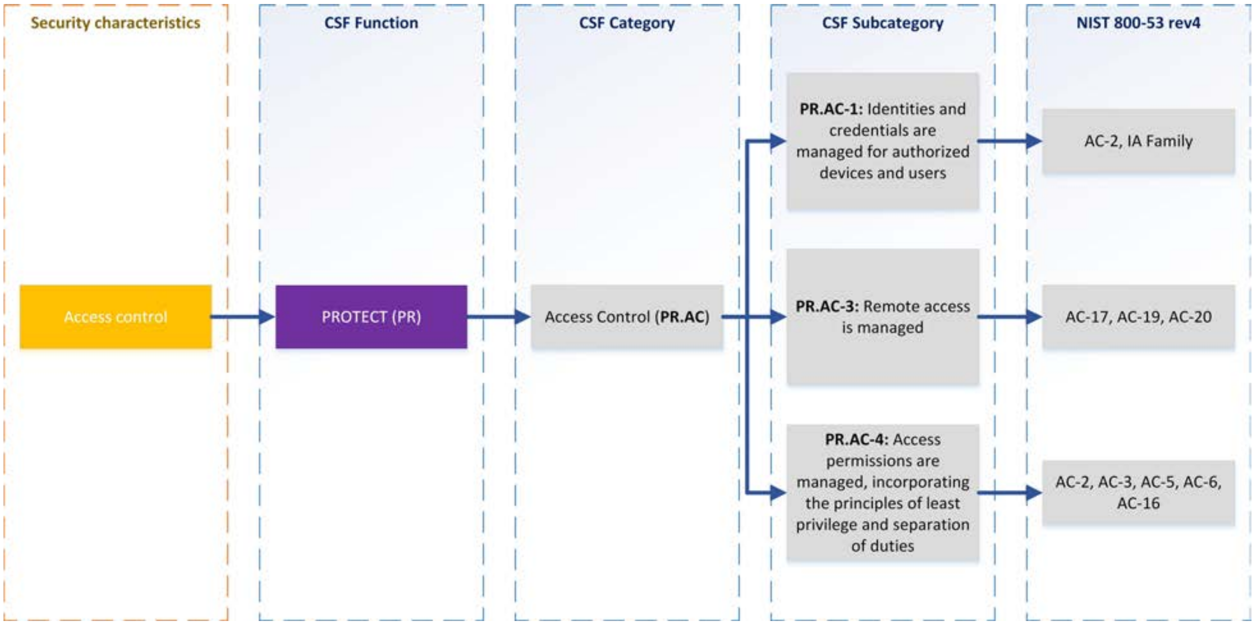

Security characteristics
CSF Function
CSF Category
CSF Subcategory
NIST 800-53 rev4
Access control
PROTECT (PR)
Access Control (PR.AC)
PR.AC-1: Identities and credentials are managed for authorized devices and users
PR.AC-3: Remote access is managed
PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties
AC-2, IA Family
AC-17, AC-19, AC-20
AC-2, AC-3, AC-5, AC-6, AC-16

Figure 2: An example of the process for determining which tests to include in the security assessment.

The security standards that are mapped to the Framework subcategories provided additional validation points. By systematically developing tests based on the Framework subcategories, we generated a set of reasonably comprehensive tests for the security characteristic requirements we identified when we first identified this challenge.[3]

For practical reasons, not all of these tests were run on the example build. All security assessment tests are included in Section 5 of this volume to help users evaluate their own operational implementation of the architecture and provide guidance on testing policy, procedures, and components, and other aspects of security that are relevant in an operational environment. Section 6 of this volume shows which of the tests were run on our example build, and which were not.

5 Risk Assessment Methodology

As outlined by NIST SP 800-30, organizations conduct risk assessment by executing the following tasks:

- identify threat source and events
- identify vulnerabilities and predisposing conditions
- determine likelihood of occurrence
- determine magnitude of impact

[3] http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_HIT_MobileDevices_UseCase.pdf

- determine risk

We offer two methods for conducting a risk assessment.

1) Table-driven method: by following the task list and exemplary tables that outlined the section 3.2, *"Conducting the Risk Assessment"* and the Appendices D – I in NIST SP 800-30. This was the initial risk assessment for this use case, which was conducted prior to the lab architecture design and build.

2) Attack/fault-tree assessment methodology[4]: as referenced in 800-30[5]. The attack/fault tree methodology was customized for this use case. This was conducted by decomposing the architecture of the use case.

Both methods performed a risk assessment and an analysis against this use case for all risk factors, and then determining the risks of:

- **Loss of Confidentiality** – impact of unauthorized disclosure of sensitive information
- **Loss of Integrity** – impact if system or data integrity is lost by unauthorized changes to the data or system
- **Loss of Availability** – impact to system functionality and operational effectiveness

The table-driven method provides a technique for assessing the risks without using any software tools. On the other hand, the fault-tree technique, by using a Decision Programing Language (DPL) tool allows us to do a graph-based analysis and use specific threat events to generate threat scenarios. The modeling and simulation produces a large number of threat scenarios, which provides us a way to restrict the analysis on a focused subset.

The risk assessments determine a list of the risks and their levels of severity. The identified risks are used as the foundation for us to validate the security characteristics. The mapping to the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the Cybersecurity Framework, or CSF) and security controls enable us to provide countermeasures by building the enterprise infrastructure with all necessary components. The organization can take actions to address those risks and protect its health information. This section provides examples on using both assessment methods and the complete assessment results can be found in Section 6 of this volume.

5.1 Table-Driven Risk Assessment Example:

This section provides a walkthrough for assessing and identifying

- an example adversarial risk

[4] Ramparts LLC created and used this methodology (Ramparts Risk Assessment Methodology) on the use case. This methodology uses and maps the use case's security characteristics into the NIST Cyber Security Framework. In addition it combines techniques pioneered in NIST SP 800-30, SP 800-53 rev4, Mission Oriented Risk and Design Analysis (MORDA) of Critical Information Systems, Risk Analysis Model (RAM) – Eight Annual Canadian Computer Security Symposium, and Intelligence-Driven Computer Network Defense informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

[5] NIST SP 800-30, Guide for Conducting Risk Assessments, page 15, section 2.3.3 Analysis Approaches

- an example of non-adversarial risk

During the risk assessment process, we followed the tasks outlined in the Section 3.2 *"Conducting the Risk Assessment"* and use the reference tables, templates, and assessment scale tables that are outlined in the Appendices D – I in NIST SP 800-30.

To recap, we performed the following tasks[6]:

Task 2-1:	Identify and characterize threat sources of concern.
Task 2-2:	Identify potential threat events.
Task 2-3:	Identify vulnerabilities and predisposing conditions.
Task 2-4:	Determine the likelihood.
Task 2-5:	Determine the impact.
Task 2-6:	Determine the risk.

For each task, we produced a number of intermediate tables with the outputs used by the final Task 2-6 for determining the risks. The intermediate tables are omitted from this document as their outputs are being aggregated into the final tables. Our assessment results are captured in the following groups, with the risk level sorted from high to low.

- Adversarial Risk (Loss of Confidentiality)
- Adversarial Risk (Loss of Integrity)
- Adversarial Risk (Loss of Availability)
- Non-Adversarial Risk (Loss of Confidentiality)
- Non-Adversarial Risk (Loss of Integrity)
- Non-Adversarial Risk (Loss of Availability)

Refer to Section 6 *Risk Assessment Results* for the details.

The *Adversarial Risk* template table and *Non-Adversarial Risk* template table below capture the assessment results for each risk factor. Following each template table, the detailed steps and example walkthroughs are presented. For each step, the guide provides the details on how the sample risk assessment was conducted in the column "Example Walkthrough / Explanations."

[6] NIST SP 800-30, Guide for Conducting Risk Assessments, page 29, Section 3.2, Conducting the Risk Assessment

Table 1: Adversarial Risk Template[7]

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	**Threat Sources**	**Threat Source Characteristics**			**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities and Predisposing Conditions**	**Severity and Pervasiveness**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**
		Capability	**Intent**	**Targeting**								
Exploit known vulnerabilities in mobile systems and devices (e.g., laptops, PDAs, smart phones)	Adversarial/hacker	Moderate	High	Low	Possible	Moderate	Malware - TECHNICAL/ Architectural and Functional	Moderate	Moderate	Moderate	Low	Moderate

[7] Based on NIST SP 800-30, Guide for Conducting Risk Assessments, Table I-5: Template – Adversarial Risk.

Table 2: Adversarial Risk Sample Walkthrough[8]

Column	Heading	Content	Example Walkthrough / Explanations
1	Threat Event	Identify threat event.	Based on the use case, one example threat event is selected: "Exploit known vulnerabilities in mobile systems and devices (e.g., laptops, PDAs, smart phones)"
2	Threat Sources	Identify threat sources that could initiate the threat event.	"Adversarial/hacker" could initiate the exploitation
3	Capability	Assess threat source capability.	The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks
4	Intent	Assess threat source intent.	The adversary seeks to disrupt the organization's cyber resources, so the source intent is "Moderate"
5	Targeting	Assess threat source targeting.	The threat source targeting is low, as attackers can only use publicly available information to target
6	Relevance	Determine relevance of threat event. If the relevance of the threat event does not meet the organization's criteria for further consideration, do not complete the remaining columns.	The relevance of this threat event is "possible"
7	Likelihood of Attack Initiation	Determine likelihood that one or more of the threat sources initiates the threat event, taking into consideration capability, intent, and targeting.	With the moderate capability and intent and low threat source targeting, the adversary is somewhat likely to initiate the treat event, so the "Moderate" is used here

[8] Based on NIST SP 800-30, Guide for Conducting Risk Assessments, Table I-4: Column Descriptions for Adversarial Risk Table.

8	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event and the predisposing conditions which could increase the likelihood of adverse impacts.	Based on the vulnerabilities related to IT system and vulnerability assessments, the vulnerabilities (Malware) can be exploited by hackers by using specific products or product lines, which could increase the likelihood of adverse impacts
9	Severity Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions.	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective
10	Likelihood Initiated Attack Succeeds	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration threat source capability, vulnerabilities, and predisposing conditions.	Based on the moderate treat source capability and severity pervasiveness, if the threat event is initiated or occurs, it is somewhat likely to have adverse impacts, which should be rated as “Moderate”
11	Overall Likelihood	Determine the likelihood that the threat event will be initiated and result in adverse impact (i.e., combination of likelihood of attack initiation and likelihood that initiated attack succeeds).	The overall likelihood is the combination of likelihood of attack initiation (Column 7, Moderate) and likelihood that initiated attack succeeds (Column 10, Moderate). By checking **Table 5: Assessment Scale – Overall Likelihood**, the Overall Likelihood is Moderate.
12	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event.	With this threat event, it is potentially harm to organizational operations. This threat event could be expected to have a serious adverse effect on organization operations, as the mobile system and / or mobile devices might loss the availability. The level of impact is Moderate.
13	Risk	Determine the level of risk as a combination of likelihood and impact.	The level of risk is a combination of likelihood (Column 11, Moderate) and impact (Column12, Moderate). By checking **Table 6: Assessment Scale – Level of Risk (combination of likelihood and impact)**, the Level of Risk is Moderate.

285 *Table 3: Non-Adversarial Risk Template*[9]

1	2	3	4	5	6	7	8	9	10	11
Threat Event	**Threat Sources**	**Range of Effects**	**Relevance**	**Likelihood of Event Occurring**	**Vulnerabilities and Predisposing Conditions**	**Severity and Pervasiveness**	**Likelihood Event Results in Adverse Impact**	**Overall Likelihood**	**Level of Impact**	**Risk**
Incorrect privilege settings	Accidental (users, admin users)	Moderate	Predicted	Moderate	INFORMATION-RELATED/Special Access Programs	Moderate	High	Moderate	Moderate	Low

286

287 *Table 4: Non-Adversarial Risk Sample Walkthrough*[10]

Column	Heading	Content	Example Walkthrough / Explanations
1	Threat Event	Identify threat event.	Based on the use case, one example threat event is selected: “Incorrect privilege settings”
2	Threat Sources	Identify threat sources that could initiate the threat event.	“Accidental (users, admin users)” could initiate the exploitation

[9] Based on NIST SP 800-30, Guide for Conducting Risk Assessments, Table I-7: Template – Non-Adversarial Risk.

[10] Based on NIST SP 800-30, Guide for Conducting Risk Assessments, Table I-6: Column Descriptions for Non-Adversarial Risk Table.

3	Range of Effects	Identify the range of effects from the threat source.	The effects of the accident are wide-ranging, involving a significant portion of the cyber resources of the information systems including some critical resources. So the “Moderate” is used here
4	Relevance	Determine relevance of threat event. If the relevance of the threat event does not meet the organization’s criteria for further consideration, do not complete the remaining columns.	The relevance of this threat event is “Predicted”
5	Likelihood of Threat Event Occurring	Determine the likelihood that the threat event will occur.	Accident is somewhat likely to occur; so the “Moderate” is used here
6	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities which could be exploited by threat sources initiating the threat event and the predisposing conditions which could increase the likelihood of adverse impacts.	Based on the vulnerabilities related to IT system and vulnerability assessments, the vulnerabilities (related to incorrect privilege settings) can be exploited by accidentally by users, which could increase the likelihood of adverse impacts
7	Severity Pervasiveness	Assess severity of vulnerabilities and pervasiveness of predisposing conditions.	The vulnerability is of moderate concern, based on the exposure of the vulnerability and ease of exploitation and/or on the severity of impacts that could result from its exploitation. Relevant security control or other remediation is partially implemented and somewhat effective.
8	Likelihood Threat Event Results in Adverse Impact	Determine the likelihood that the threat event, once initiated, will result in adverse impact, taking into consideration vulnerabilities and predisposing conditions.	Based on the moderate treat source capability and severity pervasiveness, if the threat event is initiated or occurs, it is highly likely to have adverse impacts, which should be rated as “High”
9	Overall Likelihood	Determine the likelihood that the threat event will occur and result in adverse impacts (i.e., combination of likelihood of threat occurring and likelihood that the threat event results in adverse impact).	The likelihood that the threat event will occur and result in adverse impacts is the combination of likelihood of threat occurring (Column 5, Moderate) and likelihood that the threat event results in adverse impact (Column 8, High). By checking **Table 5: Assessment Scale – Overall Likelihood**, the Overall Likelihood is Moderate.

10	Level of Impact	Determine the adverse impact (i.e., potential harm to organizational operations, organizational assets, individuals, other organizations, or the Nation) from the threat event.	With this threat event, it is potentially harm to organizational operations and information related special access program. This threat event could be expected to have a serious adverse effect on organization operations, as the mobile system and / or mobile devices might loss the availability. The level of impact is Moderate.
13	Risk	Determine the level of risk as a combination of likelihood and impact.	The level of risk is a combination of likelihood (Column 9, Moderate) and impact (Column 10, Moderate). By checking **Table 6: Assessment Scale – Level of Risk (combination of likelihood and impact)**, the Level of Risk is Moderate.

Table 5: Assessment Scale – Overall Likelihood[11]

Likelihood of Threat Event Initiation or Occurrence	**Likelihood Threat Events Result in Adverse Impacts**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

[11] Based on NIST 800-30, Guide for Conducting Risk Assessments, Table G-5: Assessment Scale – Overall Likelihood.

Table 6: Assessment Scale – Level of Risk (combination of likelihood and impact)[12]

Likelihood **(Threat Event Occurs and Results in Adverse Impact)**	**Level of Impact**				
	Very Low	**Low**	**Moderate**	**High**	**Very High**
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

[12] Based on NIST 800-30, Guide for Conducting Risk Assessments, Table I-2: Assessment Scale – Level of Risk (Combination of Likelihood and Impact).

5.2 Ramparts' Attack/Fault-Tree-Driven Risk Assessment Example

NIST worked with Ramparts, LLC to perform a risk assessment using attack/fault trees. The methodology allowed us to identify and prioritize the impacts of the attack events. Prioritizing the impacts of the attack event focused our attack-based scenario testing, countermeasure implementation and countermeasure development.

When selecting the analysis approach, graph-based analysis provides an effective way to account for the many-to-many relationships between:

(i) threat sources and threat events,

(ii) threat events and vulnerabilities, and

(iii) threat events and impacts/assets.

Steps:

The steps involved in Ramparts' attack/fault tree risk assessment methodology are the following:

1. Scope the Risk Assessment (Define the Potential Harm, Security Characteristics, Critical Data Assets, and map to NIST Cyber Security Framework.)
2. Create Attack Event Trees (Threat Scenarios) that target the Security Characteristics and Critical Data Assets
3. Assign Countermeasures/Safeguards
4. Assign Likelihood of Occurrence of the Security Characteristics being compromised based on the Industry's Primary Adversaries
5. Analysis and Present Results (Identify where the greatest relative risk to the system resides and where future efforts to minimize the risk should be placed.)

Step-1: Scoping the Risk Assessment

The CSF is being used to communicate the scope of this risk assessment. The Potential Harm at its highest level has been defined as risk to the confidentiality, integrity, and availability of patient health information. The security characteristics as defined in Table 2 are mapped into the CSF and other standards.

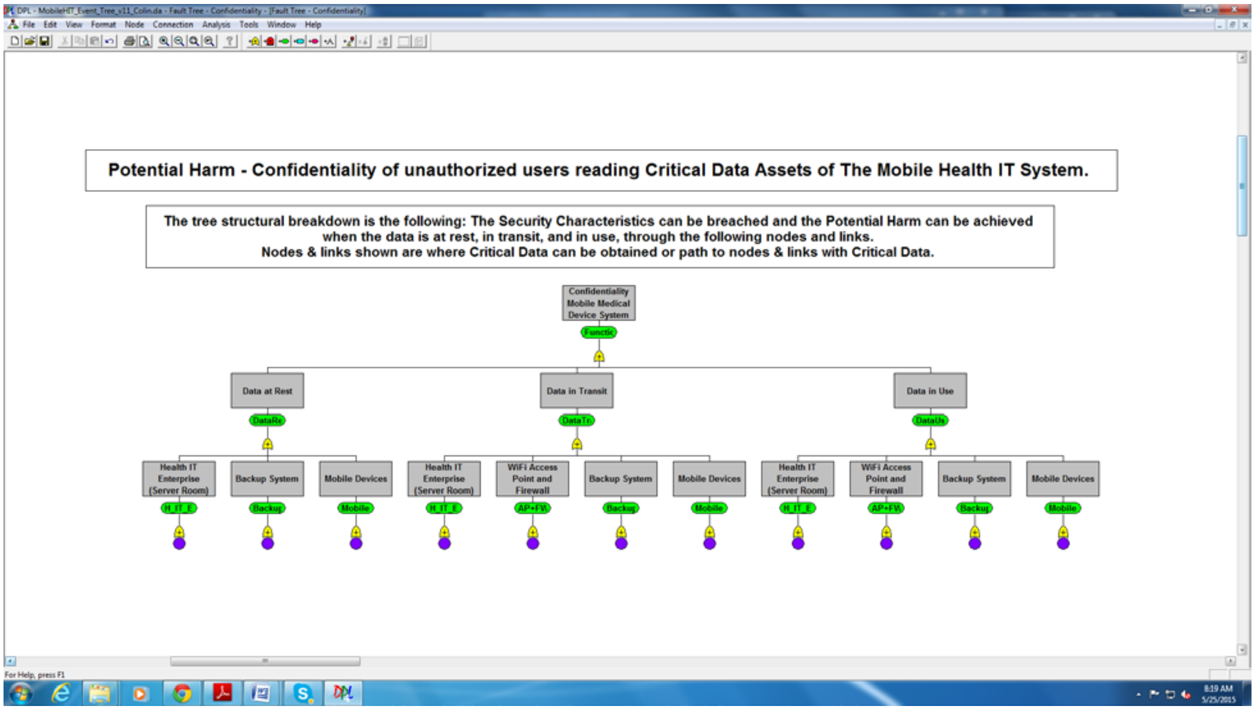
Step-2: Create Attack Event Trees (Attack Scenarios) with Countermeasures and Safeguards

The potential attack events are developed using event trees. We define a logical structure where the lower level events can be given a likelihood of occurrence. A logical structure will also allow security experts with different specialties to more easily review and contribute to the assessment. The event nodes were decomposed to a level where a likelihood of occurrence could be assigned. The events in an attack scenario that need to occur in parallel to be successful are AND'ed together. The events that can happen in parallel are OR'ed together.

The logical structure for of the attack event trees chosen for this use case was the following:

1. A separate attack tree was created for three potential harms to confidentiality, integrity and availability
2. At the top of each tree the potential harm was defined, as the risk being modeled and measured
3. The second layer of the tree was modeled as data at rest, data in transit, and data in use

4. At the third layer modeled the devices and data nodes of the system. Reference the confidentiality attack tree below



Potential Harm - Confidentiality of unauthorized users reading Critical Data Assets of The Mobile Health IT System.

The tree structural breakdown is the following: The Security Characteristics can be breached and the Potential Harm can be achieved when the data is at rest, in transit, and in use, through the following nodes and links.
Nodes & links shown are where Critical Data can be obtained or path to nodes & links with Critical Data.

DPL - MobileHIT_Event_Tree_v11_Colin.da - Fault Tree - Confidentiality - [Fault Tree - Confidentiality]
File Edit View Format Node Connection Analysis Tools Window Help
Confidentiality Mobile Medical Device System
Functic
Data at Rest
DataRe
Data in Transit
DataTr
Data in Use
DataUs
Health IT Enterprise (Server Room)
H_IT_E
Backup System
Backup
Mobile Devices
Mobile
Health IT Enterprise (Server Room)
H_IT_E
WiFi Access Point and Firewall
AP+FW
Backup System
Backup
Mobile Devices
Mobile
Health IT Enterprise (Server Room)
H_IT_E
WiFi Access Point and Firewall
AP+FW
Backup System
Backup
Mobile Devices
Mobile
For Help, press F1
8:19 AM
5/25/2015

Step-3: Assign Countermeasures/Safeguards

The countermeasures/safeguards detailed in *NIST SP 1800-1b: Approach, Architecture, and Security Characteristics*, sections 4 and 5, as appropriate, were assigned to the low level attack events.

As an example, up to date antivirus software running on the mobile device was assigned when modeling the “Install File Copying Malware” event. Then this countermeasure was part of the consideration in assigning the Likelihood of Occurrence (step 4).

Step-4: Assign Likelihood of Occurrence at the lowest level attack event that will cause the Security Characteristics being compromised) based on the Industry’s Primary Adversaries

The likelihood of occurrence is assigned as Very High, High, Medium-High, Medium, Low-Medium, Low, and Very Low. When getting expert opinions as input, this level of granularity might be too detailed, so a High, Medium, and Low relative qualitative scale could have been used instead.

The following scale of likelihoods was used:

Value	Qualitative Numeric Value
Low	.01
Medium Low	.1
Medium	.5
Medium High	.75

High	.9

The qualitative numeric values are used within the event trees to calculate probabilities at the higher levels of the trees. This was used to assess whether particular attack scenarios are more likely to occur.

The following criteria are being used when assigning a likelihood of occurrence values to the low level event (leaf) of the attack tree:

1. The adversary's likelihood of success. This success criterion considers the protection countermeasures deployed in the system, the complexity of the event and the availability of known exploits.

2. The adversary's likelihood of not being detected. Not all detections are created equal. Where appropriate, the seven stages in the Kill Chain model are considered. Detection during the reconnaissance stage (early in the attack) may be much more advantageous than detection during the Actions on Objectives stage (late in the attack). Obviously when the adversary has been able to egress critical data for months or years, and may have established other accesses into the system, the damage could be much greater. The detection countermeasures deployed in the system are considered for the detection criteria.

3. The adversary's resources required. The costs to the adversary in time and money is given a qualitative value for the event. Borrowing from MORDA (Mission Oriented Risk and Design Analysis) the following scale was used:

• Value	• Range
• Free	• 0-$1,000
• Very Low	• $1,000 -$10,000
• Low	• $10,000 - $100,000
• Medium	• $100,000 - $1 Million
• High	• $1 Million - $10 Million
• Very High	• >$10 Million

The assumption we used for this assessment was that the attacks that the potential adversaries would use are in the Very Low to Free resource levels.

4. When coming up with a single qualitative value to assign to the attack tree event, start with the likelihood of success, followed by the likelihood of detection, then the adversary's resources required.

   Understand that if an event is scored with a Low adversary's likelihood of success, it is still important to consider the adversary's likelihood of not being detected. A detection countermeasure(s) can help to protect the critical data from zero day attacks (unknown/unreported/unpatched attacks) and minimize the potential damage from all successful attacks on the critical data.

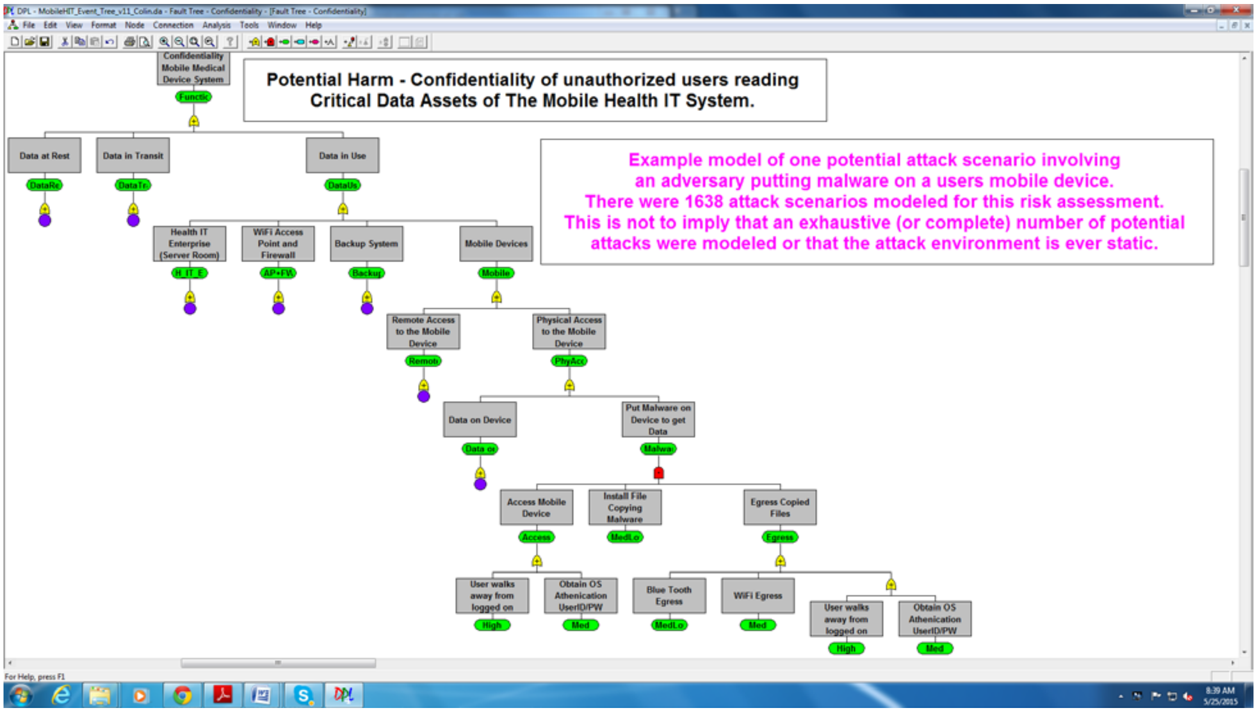
   This assessment is giving equal weight to the adversary's likelihood of success and not being detected. One goal of any organization providing good security is to make the resources an adversary would need to accomplish their cost prohibitive objective. For this assessment we have assumed those same low level resources for all attack scenarios.

   The table below shows how the three types of "Adversary Likelihoods" can be combined to come up with a single value for the Assigned Likelihood of Occurrence.

Event	Adversary's Likelihood of Success	Adversary's Likelihood of Not being Detected	Adversary's Resources Required	Assigned Likelihood of Occurrence Value
A	Very Low	Very Low	Free/Very Low	Very Low
B	Very Low	Low	Free/Very Low	Low
C	Very Low	Medium	Free/Very Low	Low-Medium
D	Very Low	High	Free/Very Low	Medium
E	Very Low	Very High	Free/Very Low	Medium-High
F	Low	Very Low	Free/Very Low	Low
G	Low	Low	Free/Very Low	Low
H	Low	Medium	Free/Very Low	Low-Medium
I	Low	High	Free/Very Low	Medium
J	Low	Very High	Free/Very Low	Medium-High
K	Medium	Very Low	Free/Very Low	Low-Medium
L	Medium	Low	Free/Very Low	Low-Medium
M	Medium	Medium	Free/Very Low	Medium
N	Medium	High	Free/Very Low	Medium-High
O	Medium	Very High	Free/Very Low	Medium-High
P	High	Very Low	Free/Very Low	Medium
Q	High	Low	Free/Very Low	Medium

R	High	Medium	Free/Very Low	Medium-High
S	High	High	Free/Very Low	High
T	High	Very High	Free/Very Low	Very High
U	Very High	Very Low	Free/Very Low	Medium
V	Very High	Low	Free/Very Low	Medium
W	Very High	Medium	Free/Very Low	Medium-High
X	Very High	High	Free/Very Low	High
Y	Very High	Very High	Free/Very Low	Very High

See below for one complete attack branch (scenario). This branch shows the attack for Data in Use, Physical Access to the mobile Device and Putting Malware on Device to get Data.


DPL - MobileHIT_Event_Tree_v11_Colin.da - Fault Tree - Confidentiality - [Fault Tree - Confidentiality]
File
Edit
View
Format
Node
Connection
Analysis
Tools
Window
Help
Confidentiality Mobile Medical Device System
Functic
Data at Rest
DataRe
Data in Transit
DataTr
Data in Use
DataUs
Health IT Enterprise (Server Room)
H_IT_E
WiFi Access Point and Firewall
AP+FW
Backup System
Backup
Mobile Devices
Mobile
Remote Access to the Mobile Device
Remot
Physical Access to the Mobile Device
PhyAcc
Data on Device
Data or
Put Malware on Device to get Data
Malwa
Access Mobile Device
Access
Install File Copying Malware
MedLo
Egress Copied Files
Egress
User walks away from logged on
High
Obtain OS Athenication UserID/PW
Med
Blue Tooth Egress
MedLo
WiFi Egress
Med
User walks away from logged on
High
Obtain OS Athenication UserID/PW
Med
For Help, press F1
8:39 AM
5/25/2015

Potential Harm - Confidentiality of unauthorized users reading Critical Data Assets of The Mobile Health IT System.

Example model of one potential attack scenario involving an adversary putting malware on a users mobile device. There were 1638 attack scenarios modeled for this risk assessment. This is not to imply that an exhaustive (or complete) number of potential attacks were modeled or that the attack environment is ever static.

Step 5: Analysis and Present Results

Using established reliability probability theory, where the events in the tree structure that are OR'ed together (those that can happen in parallel) can have their probabilities represented as P = 1-(1-p2)(1-p3), which is 1 minus the probability that both event2 and event3 have been accomplished by an adversary. Events AND'ed together (those that are sequential) can be represented as P = p4*p5 which is the probably that neither event4 nor event5 had been accomplished.

In the complex attack tree structure that was modeled the following analytics were run and results used:

1) Partial derivatives were used to show where changes to the low level attack events would have the greatest impact.

2) Calculated minimal cut sets gave the total number of attacks that were modeled.

An in-depth discussion of analytics used can be found in “Risk Analysis Model (RAM) – Eight Annual Canadian Computer Security Symposium”.

The risk assessment methodology used here will typically be used to effectively and efficiently focus the evidence-based vulnerability testing used by system implementers & countermeasure developers, and as shown below input into a risk management system/framework.

6 Risk Assessment Results

6.1 Table-Driven Risk Assessment Results

Table 7: Table-Driven Results – Adversarial Risk based on Confidentiality

1	2	3	4	5	6	7	8	9	10	11	12	13	
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk	Risk Score
		Capability	Intent	Targeting									
System intrusion and unauthorized system access	Adversarial/hacker	Moderate	High	High	Possible	Moderate	Possible weak passwords due to lack of password complexity control	High	High	High	Very High	Very High	10
Obtain sensitive information through network sniffing of external networks.	Adversarial/hacker	Low	Moderate	Moderate	Predicted	Moderate	Inadequate incorporation of security into architecture and design	Moderate	High	High	Very High	Very High	10
Stolen mobile devices	Adversarial/hacker	High	High	High	Confirmed	High	Lack of user training and physical security	High	High	High	High	High	8

Conduct communications interception attacks.	Adversarial/hacker	Low	High	Moderate	Possible	Moderate	Lack of transmission encryption leading to interception of unencrypted data	High	High	High	High	High	8
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., Web defacement).	Adversarial/hacker	Moderate	Moderate	Moderate	Predicted	Moderate	Inadequate access control and / or enforcement Inadequate data retention, backup and recovery	Moderate	Moderate	High	High	High	8
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones)	Adversarial/hacker	Moderate	High	High	Possible	High	Malware - TECHNICAL/Architectural and Functional	Moderate	Moderate	Moderate	High	Moderate	5
Deliver/insert/install malicious capabilities.	Adversarial/hacker	Moderate	High	Moderate	Anticipated	Moderate	Inadequate incorporation of security into architecture and design	Moderate	Moderate	Moderate	High	Moderate	5
Conduct an attack (i.e., direct/coordinate attack tools or activities).	Adversarial/hacker	Moderate	Moderate	Moderate	Anticipated	Moderate	Inadequate incorporation of security into architecture and design	Moderate	Moderate	Moderate	Moderate	Moderate	5

Table 8: Table-Driven Results – Adversarial Risk based on Integrity

1	2	3	4	5	6	7	8	9	10	11	12	13	
Threat Event	**Threat Sources**	**Threat Source Characteristics**			**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities and Predisposing Conditions**	**Severity and Pervasiveness**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk Score**
		Capability	**Intent**	**Targeting**									
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., Web defacement).	Adversarial/hacker	Moderate	Moderate	Moderate	Predicted	Moderate	Inadequate access control and / or enforcement Inadequate data retention, backup and recovery	Moderate	Moderate	High	Very High	Very High	10
Stolen mobile devices	Adversarial/hacker	High	High	High	Confirmed	High	Lack of user training and physical security	High	High	High	High	High	8
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones)	Adversarial/hacker	Moderate	High	High	Possible	High	Malware - TECHNICAL/Architectural and Functional	Moderate	Moderate	Moderate	High	High	8

System intrusion and unauthorized system access	Adversarial/hacker	Moderate	High	High	Possible	Moderate	Possible weak passwords due to lack of password complexity control	High	High	High	Moderate	Moderate	8
Conduct communications interception attacks.	Adversarial/hacker	Low	High	Moderate	Possible	Moderate	Lack of transmission encryption leading to interception of unencrypted data	High	High	High	High	High	8
Conduct an attack (i.e., direct/coordinate attack tools or activities).	Adversarial/hacker	Moderate	Moderate	Moderate	Anticipated	Moderate	Inadequate incorporation of security into architecture and design	Moderate	Moderate	Moderate	High	High	8
Obtain sensitive information through network sniffing of external networks.	Adversarial/hacker	Low	Moderate	Moderate	Predicted	Moderate	Inadequate incorporation of security into architecture and design	Moderate	High	High	High	High	8
Deliver/insert/install malicious capabilities.	Adversarial/hacker	Moderate	High	Moderate	Anticipated	Moderate	Inadequate incorporation of security into architecture and design	Moderate	Moderate	Moderate	High	Moderate	5

Table 9: Table-Driven Results – Adversarial Risk based on Availability

1	2	3	4	5	6	7	8	9	10	11	12	13	
Threat Event	**Threat Sources**	**Threat Source Characteristics**			**Relevance**	**Likelihood of Attack Initiation**	**Vulnerabilities and Predisposing Conditions**	**Severity and Pervasiveness**	**Likelihood Initiated Attack Succeeds**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk Score**
		Capability	**Intent**	**Targeting**									
Stolen mobile devices	Adversarial/hacker	High	High	High	Confirmed	High	Lack of user training and physical security	Moderate	Moderate	High	High	High	8
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones)	Adversarial/hacker	Moderate	High	High	Possible	High	Malware - TECHNICAL/Architectural and Functional	Moderate	Moderate	Moderate	High	High	8
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., Web defacement).	Adversarial/hacker	Moderate	Moderate	Moderate	Predicted	Moderate	Inadequate access control and /or enforcement Inadequate data retention, backup and recovery	Moderate	Moderate	High	High	High	8

System intrusion and unauthorized system access	Adversarial/hacker	Moderate	High	High	Possible	Moderate	Possible weak passwords due to lack of password complexity control	Moderate	Moderate	Moderate	High	Moderate	5
Conduct communications interception attacks.	Adversarial/hacker	Low	High	Moderate	Possible	Moderate	Lack of transmission encryption leading to interception of unencrypted data	Moderate	Moderate	Moderate	High	Moderate	5
Deliver/insert/install malicious capabilities.	Adversarial/hacker	Moderate	High	Moderate	Anticipated	Moderate	Inadequate incorporation of security into architecture and design	Moderate	Moderate	Moderate	High	Moderate	5
Obtain sensitive information through network sniffing of external networks.	Adversarial/hacker	Low	Moderate	Moderate	Predicted	Moderate	Inadequate incorporation of security into architecture and design	Moderate	Low	Moderate	Moderate	Moderate	5
Conduct an attack (i.e., direct/coordinate attack tools or activities).	Adversarial/hacker	Moderate	Moderate	Moderate	Anticipated	Moderate	Inadequate incorporation of security into architecture and design	Moderate	Low	Low	Moderate	Low	2

Table 10: Table-Driven Results – Non-Adversarial Risk based on Confidentiality

1	2	3	4	5	6	7	8	9	10	11	
Threat Event	**Threat Sources**	**Range of Effects**	**Relevance**	**Likelihood of Event Occurring**	**Vulnerabilities and Predisposing Conditions**	**Severity and Pervasiveness**	**Likelihood Event Results in Adverse Impact**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk Score**
Spill sensitive information	Accidental (users, admin users)	Moderate	Predicted	Low	Inadequate user training Untraceable user actions	Moderate	Very High	Very High	Very High	Very High	10
Lost mobile device	Accidental (users)	Very Low	Confirmed	Moderate	INFORMATION-RELATED/Special Access Programs	Moderate	High	High	High	High	8
Incorrect privilege settings	Accidental (users, admin users)	High	Predicted	Moderate	INFORMATION-RELATED/Special Access Programs	Moderate	High	Moderate	High	High	8
Mishandling of critical and/or sensitive information by authorized users	Accidental (users, admin users)	High	Predicted	Low	Inadequate user training Untraceable user actions	Moderate	Very High	Moderate	High	High	8
Walks away from logged-on devices	Accidental (users)	Low	Confirmed	Moderate	Inadequate user training	Moderate	High	Moderate	Moderate	Moderate	5

Downloads viruses or other malware	Accidental (users)	Low	Confirmed	Moderate	Inadequate user training Lack of policy enforcement In adequate configuration management	Moderate	Moderate	Moderate	Moderate	Moderate	5
Uses an unsecure Wi-Fi network	Accidental (users)	Very Low	Confirmed	High	Inadequate user training	Low	Moderate	Moderate	Moderate	Moderate	5
Introduction of vulnerabilities into software products	STRUCTURAL (Software)	High	Expected	Moderate	Inadequate change management and/or configuration management	High	Moderate	Moderate	Moderate	Moderate	5
Weak Access Control	Accidental (users, admin users)	High	Predicted	Moderate	Inadequate access control and/or enforcement	High	Moderate	Moderate	Moderate	Moderate	5
Disk error	STRUCTURAL (IT Equipment)	High	Expected	Moderate	Lack of environmental controls	Moderate	Low	Low	Moderate	Low	2

421 *Table 11: Table-Driven Results – Non-Adversarial Risk based on Integrity*

1	2	3	4	5	6	7	8	9	10	11	
Threat Event	**Threat Sources**	**Range of Effects**	**Relevance**	**Likelihood of Event Occurring**	**Vulnerabilities and Predisposing Conditions**	**Severity and Pervasiveness**	**Likelihood Event Results in Adverse Impact**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk Score**
Mishandling of critical and/or sensitive information by authorized users	Accidental (users, admin users)	High	Predicted	Low	Inadequate user training Untraceable user actions	Moderate	Very High	Very High	Very High	Very High	10
Spill sensitive information	Accidental (users, admin users)	Moderate	Predicted	Low	Inadequate user training Untraceable user actions	Moderate	Very High	High	High	High	8
Lost mobile device	Accidental (users)	Very Low	Confirmed	Moderate	INFORMATION-RELATED/Special Access Programs	Moderate	High	High	High	High	8
Incorrect privilege settings	Accidental (users, admin users)	High	Predicted	Moderate	INFORMATION-RELATED/Special Access Programs	Moderate	High	Moderate	High	High	8
Walks away from logged-on devices	Accidental (users)	Low	Confirmed	Moderate	Inadequate user training	Moderate	High	Moderate	Moderate	Moderate	5

Downloads viruses or other malware	Accidental (users)	Low	Confirmed	Moderate	Inadequate user training Lack of policy enforcement Inadequate configuration management	Moderate	Moderate	Moderate	Moderate	Moderate	5
Uses an unsecure Wi-Fi network	Accidental (users)	Very Low	Confirmed	High	Inadequate user training	Low	Moderate	Moderate	Moderate	Moderate	5
Introduction of vulnerabilities into software products	STRUCTURAL (Software)	High	Expected	Moderate	Inadequate change management and/or configuration management	High	Moderate	Moderate	Moderate	Moderate	5
Weak Access Control	Accidental (users, admin users)	High	Predicted	Moderate	Inadequate access control and/or enforcement	High	Moderate	Moderate	Moderate	Moderate	5
Disk error	STRUCTURAL (IT Equipment)	High	Expected	Moderate	Lack of environmental controls	Moderate	Low	Low	Moderate	Low	2

Table 12: Table-Driven Results – Non-Adversarial Risk based on Availability

1	2	3	4	5	6	7	8	9	10	11	
Threat Event	**Threat Sources**	**Range of Effects**	**Relevance**	**Likelihood of Event Occurring**	**Vulnerabilities and Predisposing Conditions**	**Severity and Pervasiveness**	**Likelihood Event Results in Adverse Impact**	**Overall Likelihood**	**Level of Impact**	**Risk**	**Risk Score**
Lost mobile device	Accidental (users)	Very Low	Confirmed	Moderate	INFORMATION-RELATED/Special Access Programs	Moderate	Very High	Very High	Very High	Very High	10
Mishandling of critical and/or sensitive information by authorized users	Accidental (users, admin users)	High	Predicted	Low	Inadequate user training Untraceable user actions	Moderate	High	High	High	High	8
Spill sensitive information	Accidental (users, admin users)	Moderate	Predicted	Low	Inadequate user training Untraceable user actions	Moderate	Very High	High	High	High	8
Downloads viruses or other malware	Accidental (users)	Low	Confirmed	Moderate	Inadequate user training Lack of policy enforcement Inadequate configuration management	Moderate	Moderate	High	High	High	8
Introduction of vulnerabilities into software products	STRUCTURAL (Software)	High	Expected	Moderate	Inadequate change management and/or configuration management	High	Moderate	High	High	High	8

Disk error	STRUCTURAL (IT Equipment)	High	Expected	Moderate	Lack of environmental controls	Moderate	Low	High	High	High	8
Incorrect privilege settings	Accidental (users, admin users)	High	Predicted	Moderate	INFORMATION-RELATED/Special Access Programs	Moderate	High	Moderate	Moderate	Moderate	5
Walks away from logged-on devices	Accidental (users)	Low	Confirmed	Moderate	Inadequate user training	Moderate	High	Moderate	Moderate	Moderate	5
Uses an unsecure Wi-Fi network	Accidental (users)	Very Low	Confirmed	High	Inadequate user training	Low	Moderate	Moderate	Moderate	Moderate	5
Weak Access Control	Accidental (users, admin users)	High	Predicted	Moderate	Inadequate access control and/or enforcement	High	Moderate	Moderate	Moderate	Moderate	5

6.2 Fault-Tree Risk Assessment Results

Table 13: Fault-Tree Results Based on Confidentiality

Partial Derivative	Probability	Maximum Impact	Event
0.0715	0.9	0.0644	User_walks_away_from_logged_on_Mobile_Device1
0.0715	0.9	0.0644	User_walks_away_from_logged_on_Mobile_Device54
0.00732	0.1	0.000732	Install_File_Copying_Malware
0.00732	0.1	0.000732	Install_File_Copying_Malware551
0.000385	0.9	0.000347	User_walks_away_from_logged_on_Mobile_Device443
0.000385	0.9	0.000347	User_walks_away_from_logged_on_Mobile_Device554
0.000604	0.5	0.000302	Mobile_Device_User_Does_Not_Notice
0.00302	0.1	0.000302	Connect_as_OpenEMR2
0.000335	0.9	0.000302	Ask_Receives_Critical_Data_from_the_User1
0.000335	0.9	0.000302	Disconnect_OpenEMR
0.000169	0.9	0.000152	User_walks_away_from_logged_on_Mobile_Device442
0.000169	0.9	0.000152	User_walks_away_from_logged_on_Mobile_Device555
7.22E-05	0.9	6.50E-05	Steal_Media2
0.0065	0.01	6.50E-05	Decrypt_Critical_Data11
7.22E-05	0.9	6.50E-05	Steal_Media40
0.0065	0.01	6.50E-05	Decrypt_Critical_Data440
0.0065	0.01	6.50E-05	Decrypt_Critical_Data554
7.22E-05	0.9	6.50E-05	Steal_Media54
6.51E-05	0.9	5.86E-05	PluginHub
0.00586	0.01	5.86E-05	Decrypt_Critical_Data443
6.51E-05	0.9	5.86E-05	PluginHub54
0.00586	0.01	5.86E-05	Decrypt_Critical_Data534
6.33E-05	0.9	5.70E-05	Laptop_Wireshark2
6.33E-05	0.9	5.70E-05	Laptop_Wireshark54
0.00396	0.01	3.96E-05	Decrypt_Backup_Data_at_Rest25
0.00396	0.01	3.96E-05	Decrypt_Backup_Data_at_Rest544
7.71E-05	0.5	3.85E-05	Obtain_OS_Athenication443
7.71E-05	0.5	3.85E-05	Obtain_OS_Athenication555

0.00359	0.01	3.59E-05	Decrypt_the_Back_up4
0.00359	0.01	3.59E-05	Decrypt_the_Back_up54
7.19E-05	0.5	3.59E-05	During_Phyiscal_Transfer_Obtain_Copy54
7.19E-05	0.5	3.59E-05	During_Phyiscal_Transfer_Obtain_Copy1
6.47E-05	0.5	3.24E-05	Obtain_a_copy_of_the_backup
6.47E-05	0.5	3.24E-05	Obtain_a_copy_of_the_backup54
3.37E-05	0.5	1.69E-05	WiFi_Egress442
3.37E-05	0.5	1.69E-05	WiFi_Egress54
3.37E-05	0.5	1.69E-05	Obtain_OS_Athenication442
3.37E-05	0.5	1.69E-05	Obtain_OS_Athenication55
3.23E-05	0.5	1.61E-05	Send_Data_to_New_GW
3.23E-05	0.5	1.61E-05	Acquire_Password2
0.00161	0.01	1.61E-05	Decrypt_Critical_Data16
3.23E-05	0.5	1.61E-05	Acquire_Password54
1.79E-05	0.9	1.61E-05	Capture_Critical_Data2
3.23E-05	0.5	1.61E-05	Send_Data_to_New_GW54
0.00161	0.01	1.61E-05	Decrypt_Critical_Data1554
1.79E-05	0.9	1.61E-05	Capture_Critical_Data554
0.000135	0.1	1.35E-05	Critical_Data_is_Resident_on_the_Mobile_Device
0.000135	0.1	1.35E-05	Critical_Data_is_Resident_on_the_Mobile_Device54
0.00114	0.01	1.14E-05	Decrypt_Critical_Data338
0.00114	0.01	1.14E-05	Decrypt_Critical_Data339
0.00114	0.01	1.14E-05	Decrypt_Critical_Data7
0.00114	0.01	1.14E-05	Decrypt_Critical_Data5
0.00114	0.01	1.14E-05	Decrypt_Critical_Data552
0.00114	0.01	1.14E-05	Decrypt_Critical_Data53
0.00088	0.01	8.80E-06	Decrypt_Critical_Data35
0.00088	0.01	8.80E-06	Decrypt_Critical_Data40
0.00088	0.01	8.80E-06	Decrypt_Critical_Data54
1.02E-05	0.75	7.67E-06	Thumb_Drive40
1.02E-05	0.75	7.67E-06	Thumb_Drive
1.02E-05	0.75	7.67E-06	Thumb_Drive54

0.000716	0.01	7.16E-06	Blue_Tooth_Access
7.16E-05	0.1	7.16E-06	Critical_Data_residue_on_Mobile_device2
7.16E-05	0.1	7.16E-06	Gain_Access_to_the_Backup_System1
0.000716	0.01	7.16E-06	Decrypt_Backup_Data_at_Rest21
0.000716	0.01	7.16E-06	Blue_Tooth_Access454
7.16E-05	0.1	7.16E-06	Backup_data_Captured1
7.16E-05	0.1	7.16E-06	Critical_Data_residue_on_Mobile_device454
7.16E-05	0.1	7.16E-06	Gain_Access_to_the_Backup_System54
0.000716	0.01	7.16E-06	Decrypt_Data20
7.16E-05	0.1	7.16E-06	Backup_data_Captured54
0.000716	0.01	7.16E-06	Decrypt_Data54
0.000716	0.01	7.16E-06	Decrypt_Backup_Data_at_Rest54
0.000674	0.01	6.74E-06	Remote_Access_to_the_MDM1
0.000674	0.01	6.74E-06	Phyisical_Access_to_the_MDM1
0.000674	0.01	6.74E-06	Remote_Access_to_the_MDM54
0.000674	0.01	6.74E-06	Phyisical_Access_to_the_MDM54
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR339
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR38
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR53
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR52
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR5
6.70E-05	0.1	6.70E-06	Access_to_Health_IT_OpenEMR9
7.16E-06	0.9	6.44E-06	WiFi_Data_Capture2
6.44E-05	0.1	6.44E-06	Decrypt_WiFi_Data_Transfer3
0.000644	0.01	6.44E-06	Decrypt_Critical_Data14
0.000644	0.01	6.44E-06	Decrypt_Critical_Data544
6.44E-05	0.1	6.44E-06	Decrypt_WiFi_Data_Transfer54
7.16E-06	0.9	6.44E-06	WiFi_Data_Capture54
7.13E-06	0.9	6.42E-06	Image_Disk_with_Forensic_Tool1
7.13E-06	0.9	6.42E-06	Image_Disk_with_Forensic_Tool54
0.000625	0.01	6.25E-06	Decrypt_Critical_Data31
0.000625	0.01	6.25E-06	Decrypt_Critical_Data51

0.000625	0.01	6.25E-06	Decrypt_Critical_Data37
5.19E-05	0.1	5.19E-06	Access_to_Health_IT_OpenEMR40
5.19E-05	0.1	5.19E-06	Access_to_Health_IT_OpenEMR45
5.19E-05	0.1	5.19E-06	Access_to_Health_IT_OpenEMR54
1.02E-05	0.5	5.11E-06	Buying_Malware
1.02E-05	0.5	5.11E-06	Buying_Malware37
1.02E-05	0.5	5.11E-06	Buying_Malware51
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR7
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR11
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR39
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR338
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR552
4.20E-05	0.1	4.20E-06	Access_to_Health_IT_OpenEMR553
3.68E-05	0.1	3.68E-06	Access_to_Health_IT_OpenEMR2
3.68E-05	0.1	3.68E-06	Access_to_Health_IT_OpenEMR337
3.68E-05	0.1	3.68E-06	Access_to_Health_IT_OpenEMR51
3.60E-05	0.1	3.60E-06	Access_the_Backup_system_on_site1
3.60E-05	0.1	3.60E-06	Access_the_Backup_system_on_site54
3.25E-05	0.1	3.25E-06	Access_to_Health_IT_OpenEMR35
3.25E-05	0.1	3.25E-06	Access_to_Health_IT_OpenEMR440
3.25E-05	0.1	3.25E-06	Access_to_Health_IT_OpenEMR554
5.80E-06	0.5	2.90E-06	Mobile_Device_User_Does_Not_Notice38
0.00029	0.01	2.90E-06	Decrypt_Critical_Data52
0.00029	0.01	2.90E-06	Decrypt_Critical_Data38
2.90E-05	0.1	2.90E-06	Connect_as_OpenEMR38
5.80E-06	0.5	2.90E-06	Mobile_Device_User_Does_Not_Notice52
3.22E-06	0.9	2.90E-06	Ask_Receives_Critical_Data_from_the_User38
3.22E-06	0.9	2.90E-06	Disconnect_OpenEMR38
3.22E-06	0.9	2.90E-06	Disconnect_OpenEMR52
2.90E-05	0.1	2.90E-06	Connect_as_OpenEMR52
3.22E-06	0.9	2.90E-06	Ask_Receives_Critical_Data_from_the_User52
3.58E-06	0.75	2.68E-06	Malicious_Access_Point1

2.68E-05	0.1	2.68E-06	Critical_data_is_resident_on_Mobile_device1
0.000268	0.01	2.68E-06	Access_from_AP_to_Mobile_Device1
5.37E-06	0.5	2.68E-06	Mobile_Device_Attaches_to_Malicious_Access_Point1
0.000268	0.01	2.68E-06	Access_from_AP_to_Mobile_Device54
3.58E-06	0.75	2.68E-06	Malicious_Access_Point54
2.68E-05	0.1	2.68E-06	Critical_data_is_resident_on_Mobile_device54
5.37E-06	0.5	2.68E-06	Mobile_Device_Attaches_to_Malicious_Access_Point54
2.31E-05	0.1	2.31E-06	Access_to_Health_IT_OpenEMR4
2.31E-05	0.1	2.31E-06	Access_to_Health_IT_OpenEMR37
2.31E-05	0.1	2.31E-06	Access_to_Health_IT_OpenEMR551
1.87E-05	0.1	1.87E-06	Blue_Tooth_Egress442
1.87E-05	0.1	1.87E-06	Blue_Tooth_Egress54
0.000148	0.01	1.48E-06	Access_from_AP_to_Mobile_Device443
1.97E-06	0.75	1.48E-06	Malicious_Access_Point443
2.95E-06	0.5	1.48E-06	Mobile_Device_Attaches_to_Malicious_Access_Point443
1.48E-05	0.1	1.48E-06	Install_File_Copying_Malware443
2.41E-06	0.5	1.21E-06	WiFi_Egress443
1.13E-05	0.1	1.13E-06	Access_thru_HIT_Server_Room_Firewall
0.000113	0.01	1.13E-06	Decrypt_Critical_Data
1.13E-05	0.1	1.13E-06	Access_thru_HIT_Server_Room_Firewall50
0.000113	0.01	1.13E-06	Decrypt_Critical_Data36
1.13E-05	0.1	1.13E-06	Access_thru_HIT_Server_Room_Firewall36
0.000113	0.01	1.13E-06	Decrypt_Critical_Data50
1.43E-06	0.5	7.13E-07	Obtain_OS_Athenication1
1.43E-06	0.5	7.13E-07	Obtain_OS_Athenication54
6.69E-06	0.1	6.69E-07	Access_to_Health_IT_OpenEMR
6.69E-06	0.1	6.69E-07	Access_to_Health_IT_OpenEMR36
6.69E-06	0.1	6.69E-07	Access_to_Health_IT_OpenEMR50
7.15E-07	0.9	6.44E-07	Capture_Critical_Data54
6.44E-05	0.01	6.44E-07	Breach_Firewall54
6.44E-05	0.01	6.44E-07	Decrypt_Critical_Data154

5.68E-06	0.1	5.68E-07	Coding_Malware
5.68E-06	0.1	5.68E-07	Coding_Malware37
5.68E-06	0.1	5.68E-07	Coding_Malware51
4.19E-06	0.1	4.19E-07	Access_to_Health_IT_OpenEMR30
4.19E-06	0.1	4.19E-07	Access_to_Health_IT_OpenEMR366
4.19E-06	0.1	4.19E-07	Access_to_Health_IT_OpenEMR550
7.15E-07	0.5	3.58E-07	Capture_Critical_Data3
3.58E-05	0.01	3.58E-07	Breach_Firewall
3.58E-05	0.01	3.58E-07	Decrypt_Critical_Data15
2.84E-06	0.1	2.84E-07	Egress_Data_Thru_Firewall40
2.84E-06	0.1	2.84E-07	Egress_Data_Thru_Firewall2
2.84E-06	0.1	2.84E-07	Egress_Data_Thru_Firewall54
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management34
2.50E-06	0.1	2.50E-07	VPN_Server32
2.50E-06	0.1	2.50E-07	Risk_Manager32
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners32
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root2
2.50E-06	0.1	2.50E-07	DNS_Server_Ext34
2.50E-06	0.1	2.50E-07	Health_IT_DNS34
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_34
2.50E-06	0.1	2.50E-07	Health_IT_DNS32
2.50E-06	0.1	2.50E-07	DNS_Server_Ext32
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root32
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_32
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management32
2.50E-06	0.1	2.50E-07	Virus_Malware32
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_32
2.50E-06	0.1	2.50E-07	Risk_Manager34
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners34
2.50E-06	0.1	2.50E-07	Virus_Malware34
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_34
2.50E-06	0.1	2.50E-07	VPN_Server34

2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_38
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_38
2.50E-06	0.1	2.50E-07	Virus_Malware38
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management38
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners38
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root38
2.50E-06	0.1	2.50E-07	DNS_Server_Ext38
2.50E-06	0.1	2.50E-07	Health_IT_DNS38
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_39
2.50E-06	0.1	2.50E-07	VPN_Server38
2.50E-06	0.1	2.50E-07	VPN_Server39
2.50E-06	0.1	2.50E-07	Risk_Manager39
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners39
2.50E-06	0.1	2.50E-07	Virus_Malware39
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_39
2.50E-06	0.1	2.50E-07	Risk_Manager38
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management39
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root39
2.50E-06	0.1	2.50E-07	Health_IT_DNS39
2.50E-06	0.1	2.50E-07	DNS_Server_Ext39
2.50E-06	0.1	2.50E-07	VPN_Server53
2.50E-06	0.1	2.50E-07	Risk_Manager53
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners53
2.50E-06	0.1	2.50E-07	Virus_Malware53
2.50E-06	0.1	2.50E-07	Health_IT_DNS53
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_53
2.50E-06	0.1	2.50E-07	VPN_Server52
2.50E-06	0.1	2.50E-07	DNS_Server_Ext53
2.50E-06	0.1	2.50E-07	Vulnerability_Scanners52
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management53
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root53
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_53

2.50E-06	0.1	2.50E-07	Risk_Manager52
2.50E-06	0.1	2.50E-07	Health_IT_CA_Root52
2.50E-06	0.1	2.50E-07	Mobile_Network_Access_Control__NAC_52
2.50E-06	0.1	2.50E-07	DNS_Server_Ext52
2.50E-06	0.1	2.50E-07	Health_IT_Configuration_Management52
2.50E-06	0.1	2.50E-07	Virus_Malware52
2.50E-06	0.1	2.50E-07	Health_IT_DNS52
2.50E-06	0.1	2.50E-07	Intrusion_Detection_System__IDS_52
1.94E-06	0.1	1.94E-07	Health_IT_CA_Root40
1.94E-06	0.1	1.94E-07	Intrusion_Detection_System__IDS_40
1.94E-06	0.1	1.94E-07	DNS_Server_Ext40
1.94E-06	0.1	1.94E-07	Mobile_Network_Access_Control__NAC_40
1.94E-06	0.1	1.94E-07	Vulnerability_Scanners40
1.94E-06	0.1	1.94E-07	Health_IT_Configuration_Management40
1.94E-06	0.1	1.94E-07	Health_IT_DNS40
1.94E-06	0.1	1.94E-07	VPN_Server40
1.94E-06	0.1	1.94E-07	Virus_Malware40
1.94E-06	0.1	1.94E-07	Risk_Manager40
1.94E-06	0.1	1.94E-07	Health_IT_Configuration_Management54
1.94E-06	0.1	1.94E-07	Health_IT_CA_Root54
1.94E-06	0.1	1.94E-07	Vulnerability_Scanners54
1.94E-06	0.1	1.94E-07	Intrusion_Detection_System__IDS_54
1.94E-06	0.1	1.94E-07	Health_IT_DNS54
1.94E-06	0.1	1.94E-07	DNS_Server_Ext54
1.94E-06	0.1	1.94E-07	Health_IT_CA_Root35
1.94E-06	0.1	1.94E-07	Mobile_Network_Access_Control__NAC_54
1.94E-06	0.1	1.94E-07	DNS_Server_Ext35
1.94E-06	0.1	1.94E-07	Health_IT_Configuration_Management35
1.94E-06	0.1	1.94E-07	Health_IT_DNS35
1.94E-06	0.1	1.94E-07	Intrusion_Detection_System__IDS_35
1.94E-06	0.1	1.94E-07	Risk_Manager54
1.94E-06	0.1	1.94E-07	Virus_Malware54

1.94E-06	0.1	1.94E-07	Vulnerability_Scanners35
1.94E-06	0.1	1.94E-07	Risk_Manager35
1.94E-06	0.1	1.94E-07	VPN_Server35
1.94E-06	0.1	1.94E-07	VPN_Server54
1.94E-06	0.1	1.94E-07	Mobile_Network_Access_Control__NAC_35
1.94E-06	0.1	1.94E-07	Virus_Malware35
3.25E-07	0.5	1.62E-07	Mobile_Device_User_Does_Not_Notice443
3.25E-07	0.5	1.62E-07	Ask_Receives_Critical_Data_from_the_User443
1.62E-06	0.1	1.62E-07	Connect_as_OpenEMR443
1.62E-06	0.1	1.62E-07	Connect_as_OpenEMR54
3.25E-07	0.5	1.62E-07	Ask_Receives_Critical_Data_from_the_User54
3.25E-07	0.5	1.62E-07	Mobile_Device_User_Does_Not_Notice54
1.37E-06	0.1	1.37E-07	Virus_Malware37
1.37E-06	0.1	1.37E-07	Health_IT_CA_Root37
1.37E-06	0.1	1.37E-07	Mobile_Network_Access_Control__NAC_37
1.37E-06	0.1	1.37E-07	Health_IT_Configuration_Management37
1.37E-06	0.1	1.37E-07	Vulnerability_Scanners37
1.37E-06	0.1	1.37E-07	Risk_Manager37
1.37E-06	0.1	1.37E-07	VPN_Server37
1.37E-06	0.1	1.37E-07	Health_IT_DNS37
1.37E-06	0.1	1.37E-07	Intrusion_Detection_System__IDS_37
1.37E-06	0.1	1.37E-07	Risk_Manager12
1.37E-06	0.1	1.37E-07	Health_IT_CA_Root3
1.37E-06	0.1	1.37E-07	DNS_Server_Ext11
1.37E-06	0.1	1.37E-07	DNS_Server_Ext37
1.37E-06	0.1	1.37E-07	Health_IT_DNS5
1.37E-06	0.1	1.37E-07	Intrusion_Detection_System__IDS_6
1.37E-06	0.1	1.37E-07	VPN_Server13
1.37E-06	0.1	1.37E-07	Virus_Malware9
1.37E-06	0.1	1.37E-07	Vulnerability_Scanners8
1.37E-06	0.1	1.37E-07	Health_IT_Configuration_Management4
1.37E-06	0.1	1.37E-07	Mobile_Network_Access_Control__NAC_7

1.37E-06	0.1	1.37E-07	Health_IT_Configuration_Management51
1.37E-06	0.1	1.37E-07	Health_IT_DNS51
1.37E-06	0.1	1.37E-07	Intrusion_Detection_System__IDS_51
1.37E-06	0.1	1.37E-07	DNS_Server_Ext51
1.37E-06	0.1	1.37E-07	Vulnerability_Scanners51
1.37E-06	0.1	1.37E-07	Risk_Manager51
1.37E-06	0.1	1.37E-07	VPN_Server51
1.37E-06	0.1	1.37E-07	Health_IT_CA_Root51
1.37E-06	0.1	1.37E-07	Mobile_Network_Access_Control__NAC_51
1.37E-06	0.1	1.37E-07	Virus_Malware51
1.34E-06	0.1	1.34E-07	Blue_Tooth_Egress443
2.49E-07	0.1	2.49E-08	Health_IT_Configuration_Management
2.49E-07	0.1	2.49E-08	Health_IT_CA_Root
2.49E-07	0.1	2.49E-08	VPN_Server
2.49E-07	0.1	2.49E-08	Vulnerability_Scanners
2.49E-07	0.1	2.49E-08	Virus_Malware
2.49E-07	0.1	2.49E-08	Risk_Manager
2.49E-07	0.1	2.49E-08	DNS_Server_Ext
2.49E-07	0.1	2.49E-08	Health_IT_DNS
2.49E-07	0.1	2.49E-08	Intrusion_Detection_System__IDS_
2.49E-07	0.1	2.49E-08	Mobile_Network_Access_Control__NAC_
2.49E-07	0.1	2.49E-08	Health_IT_DNS36
2.49E-07	0.1	2.49E-08	DNS_Server_Ext36
2.49E-07	0.1	2.49E-08	Health_IT_CA_Root36
2.49E-07	0.1	2.49E-08	Health_IT_Configuration_Management36
2.49E-07	0.1	2.49E-08	Intrusion_Detection_System__IDS_36
2.49E-07	0.1	2.49E-08	Vulnerability_Scanners36
2.49E-07	0.1	2.49E-08	Virus_Malware36
2.49E-07	0.1	2.49E-08	Risk_Manager36
2.49E-07	0.1	2.49E-08	VPN_Server36
2.49E-07	0.1	2.49E-08	Mobile_Network_Access_Control__NAC_36
2.49E-07	0.1	2.49E-08	Vulnerability_Scanners50

2.49E-07	0.1	2.49E-08	Virus_Malware50
2.49E-07	0.1	2.49E-08	DNS_Server_Ext50
2.49E-07	0.1	2.49E-08	Risk_Manager50
2.49E-07	0.1	2.49E-08	Health_IT_Configuration_Management50
2.49E-07	0.1	2.49E-08	Health_IT_DNS50
2.49E-07	0.1	2.49E-08	Intrusion_Detection_System__IDS_50
2.49E-07	0.1	2.49E-08	VPN_Server50
2.49E-07	0.1	2.49E-08	Mobile_Network_Access_Control__NAC_50
2.49E-07	0.1	2.49E-08	Health_IT_CA_Root50
1.97E-08	0.75	1.48E-08	Malicious_Access_Point554
2.95E-08	0.5	1.48E-08	Mobile_Device_Attaches_to_Malicious_Access_Point554
1.48E-06	0.01	1.48E-08	Access_from_AP_to_Mobile_Device554
1.48E-06	0.01	1.48E-08	Blue_Tooth_Access554
1.48E-07	0.1	1.48E-08	Install_File_Copying_Malware554
2.41E-08	0.5	1.21E-08	WiFi_Egress554
1.34E-08	0.1	1.34E-09	Blue_Tooth_Egress554

Table 14: Fault-Tree Results Based on Integrity

Partial Derivative	Probability	Maximum Impact	Event
0.815	0.9	0.733	Physical_Access___User_walks_away_from_logged_on_Mobile_Device1
0.0855	0.1	0.00855	Install_File_Modifying_Malware
0.0855	0.1	0.00855	Install_File_Modifying_Malware123
0.0045	0.9	0.00405	User_walks_away_from_logged_on_Mobile_Device4433
0.0045	0.9	0.00405	User_walks_away_from_logged_on_Mobile_Device443
0.0009	0.5	0.00045	Obtain_OS_Athenication4433
0.0009	0.5	0.00045	Obtain_OS_Athenication443
0.0307	0.01	0.000307	Access_from_AP_to_Mobile_Device1
0.000613	0.5	0.000307	Mobile_Device_Attaches_to_Malicious_Access_Point1

0.000409	0.75	0.000307	Malicious_Access_Point1
0.0033	0.01	3.30E-05	Changing_Crtical_Data4122
0.0033	0.01	3.30E-05	Changing_Crtical_Data4
6.60E-05	0.5	3.30E-05	Mobile_Device_User_Does_Not_Notice
3.67E-05	0.9	3.30E-05	Ask_Receives_Critical_Data_from_the_User1
0.00033	0.1	3.30E-05	Connect_as_OpenEMR2
6.60E-05	0.5	3.30E-05	Mobile_Device_User_Does_Not_Notice1221
3.67E-05	0.9	3.30E-05	Ask_Receives_Critical_Data_from_the_User1211
3.67E-05	0.9	3.30E-05	Disconnect_OpenEMR1222
3.67E-05	0.9	3.30E-05	Disconnect_OpenEMR
0.00033	0.1	3.30E-05	Connect_as_OpenEMR2122
0.00306	0.01	3.06E-05	Access_from_AP_to_Mobile_Device554
0.00306	0.01	3.06E-05	Access_from_AP_to_Mobile_Device443
4.07E-05	0.75	3.06E-05	Malicious_Access_Point554
4.07E-05	0.75	3.06E-05	Malicious_Access_Point443
0.000306	0.1	3.06E-05	Install_File_Modifyying_Malware554
6.11E-05	0.5	3.06E-05	Mobile_Device_Attaches_to_Malicious_Access_Point554
6.11E-05	0.5	3.06E-05	Mobile_Device_Attaches_to_Malicious_Access_Point443
0.000306	0.1	3.06E-05	Install_File_Modifying_Malware443
0.000204	0.01	2.04E-06	Force_Backup_Online__Critical_System_Failure274
0.000204	0.01	2.04E-06	Decrypt_the_Back_up54
0.000204	0.01	2.04E-06	Force_Backup_Online__Critical_System_Failure27
4.07E-06	0.5	2.04E-06	Replace_with_Modified_Backup1
0.000204	0.01	2.04E-06	Decrypt_the_Back_up4
4.07E-06	0.5	2.04E-06	During_Phyiscal_Transfer_Obtain_Copy1
4.07E-06	0.5	2.04E-06	During_Phyiscal_Transfer_Obtain_Copy54
4.07E-06	0.5	2.04E-06	Replace_with_Modified_Backup14
6.60E-07	0.5	3.30E-07	Mobile_Device_User_Does_Not_Notice32
3.30E-05	0.01	3.30E-07	Changing_Crtical_Data3212
3.30E-05	0.01	3.30E-07	Decrypt_Critical_Data52

3.30E-06	0.1	3.30E-07	Connect_as_OpenEMR52
3.67E-07	0.9	3.30E-07	Disconnect_OpenEMR52
3.67E-07	0.9	3.30E-07	Ask_Receives_Critical_Data_from_the_User52
6.62E-06	0.01	6.62E-08	Re_Encrypt_Modified_Critical_Data2644
6.62E-06	0.01	6.62E-08	Decrypt_Critical_Data534
6.62E-06	0.01	6.62E-08	Changing_Crtical_Data2644
7.35E-08	0.9	6.62E-08	PluginHub
7.35E-08	0.9	6.62E-08	PluginHub54
6.62E-06	0.01	6.62E-08	Decrypt_Critical_Data443
6.62E-06	0.01	6.62E-08	Changing_Crtical_Data264
6.62E-06	0.01	6.62E-08	Re_Encrypt_Modified_Critical_Data264
7.15E-08	0.9	6.43E-08	Laptop_Wireshark54
7.15E-08	0.9	6.43E-08	Laptop_Wireshark2
2.04E-08	0.9	1.83E-08	Capture_Critical_Data554
3.67E-08	0.5	1.83E-08	Acquire_Password54
3.67E-08	0.5	1.83E-08	Send_Data_to_New_GW54
1.83E-06	0.01	1.83E-08	Re_Encrypt_Modified_Critical_Data2654
2.04E-08	0.9	1.83E-08	Capture_Critical_Data2
1.83E-06	0.01	1.83E-08	Changing_Crtical_Data2654
1.83E-06	0.01	1.83E-08	Decrypt_Critical_Data1554
3.67E-08	0.5	1.83E-08	Acquire_Password2
3.67E-08	0.5	1.83E-08	Send_Data_to_New_GW
1.83E-06	0.01	1.83E-08	Changing_Crtical_Data265
1.83E-06	0.01	1.83E-08	Decrypt_Critical_Data16
1.83E-06	0.01	1.83E-08	Re_Encrypt_Modified_Critical_Data265
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data6
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data35
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data6
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data53
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data552
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data233
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data323

1.29E-06	0.01	1.29E-08	Changing_Crtical_Data323
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data233
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data333
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data7
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data3
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data31
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data333
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data5
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data338
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data23
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data339
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data32
1.29E-06	0.01	1.29E-08	Changing_Crtical_Data23
1.29E-06	0.01	1.29E-08	Re_Encrypt_Modified_Critical_Data32
1.00E-06	0.01	1.00E-08	Re_Encrypt_Modified_Critical_Data2633
1.00E-06	0.01	1.00E-08	Changing_Crtical_Data26
1.00E-06	0.01	1.00E-08	Re_Encrypt_Modified_Critical_Data26
1.00E-06	0.01	1.00E-08	Decrypt_Critical_Data54
1.00E-06	0.01	1.00E-08	Changing_Crtical_Data2633
1.00E-06	0.01	1.00E-08	Decrypt_Critical_Data40
1.16E-08	0.75	8.72E-09	Thumb_Drive40
1.16E-08	0.75	8.72E-09	Thumb_Drive54
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR339
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR53
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR52
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR45
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR38
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR9
7.62E-08	0.1	7.62E-09	Access_to_Health_IT_OpenEMR5
7.33E-07	0.01	7.33E-09	Re_Encrypt_Modified_Critical_Data2623
7.33E-07	0.01	7.33E-09	Changing_Crtical_Data2623
7.33E-07	0.01	7.33E-09	Decrypt_Critical_Data544

7.33E-08	0.1	7.33E-09	Decrypt_WiFi_Data_Transfer3
8.15E-09	0.9	7.33E-09	WiFi_Data_Capture54
7.33E-08	0.1	7.33E-09	Decrypt_WiFi_Data_Transfer54
8.15E-09	0.9	7.33E-09	WiFi_Data_Capture2
7.33E-07	0.01	7.33E-09	Decrypt_Critical_Data14
7.33E-07	0.01	7.33E-09	Re_Encrypt_Modified_Critical_Data262
7.33E-07	0.01	7.33E-09	Changing_Crtical_Data262
7.11E-07	0.01	7.11E-09	Decrypt_Critical_Data31
7.11E-07	0.01	7.11E-09	Decrypt_Critical_Data51
7.11E-07	0.01	7.11E-09	Re_Encrypt_Modified_Critical_Data223
7.11E-07	0.01	7.11E-09	Re_Encrypt_Modified_Critical_Data2
7.11E-07	0.01	7.11E-09	Changing_Crtical_Data223
7.11E-07	0.01	7.11E-09	Changing_Crtical_Data2
7.11E-07	0.01	7.11E-09	Decrypt_Critical_Data37
7.11E-07	0.01	7.11E-09	Re_Encrypt_Modified_Critical_Data22
7.11E-07	0.01	7.11E-09	Changing_Crtical_Data22
5.90E-08	0.1	5.90E-09	Access_to_Health_IT_OpenEMR40
5.90E-08	0.1	5.90E-09	Access_to_Health_IT_OpenEMR54
1.16E-08	0.5	5.81E-09	Buying_Malware
1.16E-08	0.5	5.81E-09	Buying_Malware51
1.16E-08	0.5	5.81E-09	Buying_Malware37
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR35
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR7
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR11
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR338
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR39
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR552
4.78E-08	0.1	4.78E-09	Access_to_Health_IT_OpenEMR553
4.19E-08	0.1	4.19E-09	Access_to_Health_IT_OpenEMR337
4.19E-08	0.1	4.19E-09	Access_to_Health_IT_OpenEMR2
4.19E-08	0.1	4.19E-09	Access_to_Health_IT_OpenEMR51
3.70E-08	0.1	3.70E-09	Access_to_Health_IT_OpenEMR554

3.70E-08	0.1	3.70E-09	Access_to_Health_IT_OpenEMR440
2.63E-08	0.1	2.63E-09	Access_to_Health_IT_OpenEMR37
2.63E-08	0.1	2.63E-09	Access_to_Health_IT_OpenEMR551
2.63E-08	0.1	2.63E-09	Access_to_Health_IT_OpenEMR4
1.29E-08	0.1	1.29E-09	Access_thru_HIT_Server_Room_Firewall
1.29E-08	0.1	1.29E-09	Access_thru_HIT_Server_Room_Firewall36
1.29E-08	0.1	1.29E-09	Access_thru_HIT_Server_Room_Firewall50
1.29E-07	0.01	1.29E-09	Decrypt_Critical_Data50
1.29E-07	0.01	1.29E-09	Re_Encrypt_Modified_Critical_Data3
1.29E-07	0.01	1.29E-09	Changing_Crtical_Data1
1.29E-07	0.01	1.29E-09	Changing_Crtical_Data2211
1.29E-07	0.01	1.29E-09	Re_Encrypt_Modified_Critical_Data2211
1.29E-07	0.01	1.29E-09	Decrypt_Critical_Data36
1.29E-07	0.01	1.29E-09	Changing_Crtical_Data221
1.29E-07	0.01	1.29E-09	Re_Encrypt_Modified_Critical_Data221
1.29E-07	0.01	1.29E-09	Decrypt_Critical_Data
7.62E-09	0.1	7.62E-10	Access_to_Health_IT_OpenEMR
7.62E-09	0.1	7.62E-10	Access_to_Health_IT_OpenEMR50
7.62E-09	0.1	7.62E-10	Access_to_Health_IT_OpenEMR36
8.15E-10	0.9	7.33E-10	Capture_Critical_Data54
7.33E-08	0.01	7.33E-10	Changing_Crtical_Data2634
7.33E-08	0.01	7.33E-10	Re_Encrypt_Modified_Critical_Data2634
7.33E-08	0.01	7.33E-10	Breach_Firewall54
7.33E-08	0.01	7.33E-10	Decrypt_Critical_Data154
6.46E-09	0.1	6.46E-10	Coding_Malware
6.46E-09	0.1	6.46E-10	Coding_Malware51
6.46E-09	0.1	6.46E-10	Coding_Malware37
4.78E-09	0.1	4.78E-10	Access_to_Health_IT_OpenEMR30
4.78E-09	0.1	4.78E-10	Access_to_Health_IT_OpenEMR550
4.78E-09	0.1	4.78E-10	Access_to_Health_IT_OpenEMR366
4.07E-08	0.01	4.07E-10	Changing_Crtical_Data263
4.07E-08	0.01	4.07E-10	Re_Encrypt_Modified_Critical_Data263

4.07E-08	0.01	4.07E-10	Breach_Firewall
4.07E-08	0.01	4.07E-10	Decrypt_Critical_Data15
8.15E-10	0.5	4.07E-10	Capture_Critical_Data3
3.23E-09	0.1	3.23E-10	Egress_Data_Thru_Firewall54
3.23E-09	0.1	3.23E-10	Egress_Data_Thru_Firewall40
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management35
2.84E-09	0.1	2.84E-10	DNS_Server_Ext35
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_52
2.84E-09	0.1	2.84E-10	Health_IT_DNS52
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root38
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management53
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_52
2.84E-09	0.1	2.84E-10	VPN_Server34
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners52
2.84E-09	0.1	2.84E-10	DNS_Server_Ext53
2.84E-09	0.1	2.84E-10	Risk_Manager52
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root35
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root53
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_32
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management52
2.84E-09	0.1	2.84E-10	VPN_Server52
2.84E-09	0.1	2.84E-10	Virus_Malware52
2.84E-09	0.1	2.84E-10	Health_IT_DNS53
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management38
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_35
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root32
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners53
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management32
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_32
2.84E-09	0.1	2.84E-10	Risk_Manager53
2.84E-09	0.1	2.84E-10	DNS_Server_Ext32
2.84E-09	0.1	2.84E-10	Health_IT_DNS32

2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_53
2.84E-09	0.1	2.84E-10	Health_IT_DNS35
2.84E-09	0.1	2.84E-10	DNS_Server_Ext38
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_35
2.84E-09	0.1	2.84E-10	Virus_Malware53
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners35
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_53
2.84E-09	0.1	2.84E-10	VPN_Server35
2.84E-09	0.1	2.84E-10	Virus_Malware35
2.84E-09	0.1	2.84E-10	Risk_Manager35
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners38
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_38
2.84E-09	0.1	2.84E-10	VPN_Server39
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_34
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners39
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_39
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_39
2.84E-09	0.1	2.84E-10	Risk_Manager39
2.84E-09	0.1	2.84E-10	Virus_Malware39
2.84E-09	0.1	2.84E-10	Health_IT_DNS39
2.84E-09	0.1	2.84E-10	DNS_Server_Ext34
2.84E-09	0.1	2.84E-10	Virus_Malware32
2.84E-09	0.1	2.84E-10	Intrusion_Detection_System__IDS_34
2.84E-09	0.1	2.84E-10	Risk_Manager32
2.84E-09	0.1	2.84E-10	Health_IT_DNS34
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root2
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners32
2.84E-09	0.1	2.84E-10	VPN_Server32
2.84E-09	0.1	2.84E-10	Health_IT_DNS38
2.84E-09	0.1	2.84E-10	Risk_Manager34
2.84E-09	0.1	2.84E-10	DNS_Server_Ext52
2.84E-09	0.1	2.84E-10	Risk_Manager38

2.84E-09	0.1	2.84E-10	Health_IT_CA_Root52
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management34
2.84E-09	0.1	2.84E-10	Vulnerability_Scanners34
2.84E-09	0.1	2.84E-10	VPN_Server38
2.84E-09	0.1	2.84E-10	Virus_Malware34
2.84E-09	0.1	2.84E-10	DNS_Server_Ext39
2.84E-09	0.1	2.84E-10	Health_IT_Configuration_Management39
2.84E-09	0.1	2.84E-10	VPN_Server53
2.84E-09	0.1	2.84E-10	Virus_Malware38
2.84E-09	0.1	2.84E-10	Mobile_Network_Access_Control__NAC_38
2.84E-09	0.1	2.84E-10	Health_IT_CA_Root39
2.20E-09	0.1	2.20E-10	Vulnerability_Scanners54
2.20E-09	0.1	2.20E-10	DNS_Server_Ext54
2.20E-09	0.1	2.20E-10	VPN_Server54
2.20E-09	0.1	2.20E-10	Health_IT_Configuration_Management54
2.20E-09	0.1	2.20E-10	Risk_Manager54
2.20E-09	0.1	2.20E-10	Health_IT_DNS54
2.20E-09	0.1	2.20E-10	Intrusion_Detection_System__IDS_54
2.20E-09	0.1	2.20E-10	Mobile_Network_Access_Control__NAC_54
2.20E-09	0.1	2.20E-10	Virus_Malware54
2.20E-09	0.1	2.20E-10	Health_IT_CA_Root54
2.20E-09	0.1	2.20E-10	Health_IT_DNS40
2.20E-09	0.1	2.20E-10	DNS_Server_Ext40
2.20E-09	0.1	2.20E-10	Health_IT_Configuration_Management40
2.20E-09	0.1	2.20E-10	Intrusion_Detection_System__IDS_40
2.20E-09	0.1	2.20E-10	Vulnerability_Scanners40
2.20E-09	0.1	2.20E-10	Mobile_Network_Access_Control__NAC_40
2.20E-09	0.1	2.20E-10	VPN_Server40
2.20E-09	0.1	2.20E-10	Virus_Malware40
2.20E-09	0.1	2.20E-10	Risk_Manager40
2.20E-09	0.1	2.20E-10	Health_IT_CA_Root40
1.83E-09	0.1	1.83E-10	Connect_as_OpenEMR54

3.67E-10	0.5	1.83E-10	Ask_Receives_Critical_Data_from_the_User54
1.83E-09	0.1	1.83E-10	Connect_as_OpenEMR443
3.67E-10	0.5	1.83E-10	Mobile_Device_User_Does_Not_Notice54
3.67E-10	0.5	1.83E-10	Mobile_Device_User_Does_Not_Notice443
3.67E-10	0.5	1.83E-10	Ask_Receives_Critical_Data_from_the_User443
1.56E-09	0.1	1.56E-10	VPN_Server37
1.56E-09	0.1	1.56E-10	Risk_Manager37
1.56E-09	0.1	1.56E-10	Mobile_Network_Access_Control__NAC_37
1.56E-09	0.1	1.56E-10	Virus_Malware37
1.56E-09	0.1	1.56E-10	Intrusion_Detection_System__IDS_37
1.56E-09	0.1	1.56E-10	DNS_Server_Ext11
1.56E-09	0.1	1.56E-10	Health_IT_DNS37
1.56E-09	0.1	1.56E-10	Health_IT_DNS5
1.56E-09	0.1	1.56E-10	Health_IT_Configuration_Management4
1.56E-09	0.1	1.56E-10	Vulnerability_Scanners37
1.56E-09	0.1	1.56E-10	Intrusion_Detection_System__IDS_6
1.56E-09	0.1	1.56E-10	Health_IT_CA_Root3
1.56E-09	0.1	1.56E-10	DNS_Server_Ext37
1.56E-09	0.1	1.56E-10	VPN_Server13
1.56E-09	0.1	1.56E-10	Risk_Manager12
1.56E-09	0.1	1.56E-10	Vulnerability_Scanners8
1.56E-09	0.1	1.56E-10	Health_IT_Configuration_Management37
1.56E-09	0.1	1.56E-10	Virus_Malware9
1.56E-09	0.1	1.56E-10	Health_IT_CA_Root37
1.56E-09	0.1	1.56E-10	Mobile_Network_Access_Control__NAC_7
1.56E-09	0.1	1.56E-10	Health_IT_CA_Root51
1.56E-09	0.1	1.56E-10	DNS_Server_Ext51
1.56E-09	0.1	1.56E-10	Intrusion_Detection_System__IDS_51
1.56E-09	0.1	1.56E-10	Health_IT_DNS51
1.56E-09	0.1	1.56E-10	VPN_Server51
1.56E-09	0.1	1.56E-10	Mobile_Network_Access_Control__NAC_51
1.56E-09	0.1	1.56E-10	Virus_Malware51

1.56E-09	0.1	1.56E-10	Risk_Manager51
1.56E-09	0.1	1.56E-10	Health_IT_Configuration_Management51
1.56E-09	0.1	1.56E-10	Vulnerability_Scanners51
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure264
8.15E-10	0.1	8.15E-11	Backup_data_Captured1
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data284
8.15E-09	0.01	8.15E-11	Decrypt_Data54
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data284
8.15E-10	0.1	8.15E-11	Backup_data_Captured54
8.15E-09	0.01	8.15E-11	Decrypt_Data20
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data28
8.15E-10	0.1	8.15E-11	Gain_Access_to_the_Backup_System1
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data28
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure26
8.15E-10	0.1	8.15E-11	Access_the_Backup_system_on_site1
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure25
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data25
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data25
8.15E-09	0.01	8.15E-11	Decrypt_Backup_Data_at_Rest21
8.15E-09	0.01	8.15E-11	Force_Backup_Online__Critical_System_Failure1
8.15E-09	0.01	8.15E-11	Changing_Crtical_Data8
8.15E-09	0.01	8.15E-11	Re_Encrypt_Modified_Critical_Data8
8.15E-09	0.01	8.15E-11	Decrypt_Backup_Data_at_Rest25
2.84E-10	0.1	2.84E-11	Health_IT_DNS36
2.84E-10	0.1	2.84E-11	VPN_Server
2.84E-10	0.1	2.84E-11	Risk_Manager
2.84E-10	0.1	2.84E-11	Vulnerability_Scanners
2.84E-10	0.1	2.84E-11	Virus_Malware
2.84E-10	0.1	2.84E-11	Health_IT_CA_Root36
2.84E-10	0.1	2.84E-11	DNS_Server_Ext36
2.84E-10	0.1	2.84E-11	Health_IT_DNS

2.84E-10	0.1	2.84E-11	Health_IT_Configuration_Management
2.84E-10	0.1	2.84E-11	DNS_Server_Ext
2.84E-10	0.1	2.84E-11	Health_IT_CA_Root
2.84E-10	0.1	2.84E-11	Mobile_Network_Access_Control__NAC_
2.84E-10	0.1	2.84E-11	Intrusion_Detection_System__IDS_
2.84E-10	0.1	2.84E-11	Health_IT_Configuration_Management36
2.84E-10	0.1	2.84E-11	Risk_Manager36
2.84E-10	0.1	2.84E-11	Mobile_Network_Access_Control__NAC_36
2.84E-10	0.1	2.84E-11	Virus_Malware36
2.84E-10	0.1	2.84E-11	Vulnerability_Scanners36
2.84E-10	0.1	2.84E-11	VPN_Server36
2.84E-10	0.1	2.84E-11	Intrusion_Detection_System__IDS_36
2.84E-10	0.1	2.84E-11	Health_IT_CA_Root50
2.84E-10	0.1	2.84E-11	DNS_Server_Ext50
2.84E-10	0.1	2.84E-11	Virus_Malware50
2.84E-10	0.1	2.84E-11	Vulnerability_Scanners50
2.84E-10	0.1	2.84E-11	Mobile_Network_Access_Control__NAC_50
2.84E-10	0.1	2.84E-11	Intrusion_Detection_System__IDS_50
2.84E-10	0.1	2.84E-11	Health_IT_DNS50
2.84E-10	0.1	2.84E-11	Health_IT_Configuration_Management50
2.84E-10	0.1	2.84E-11	VPN_Server50
2.84E-10	0.1	2.84E-11	Risk_Manager50

Table 15: Fault-Tree Results Based on Availability

Partial Derivative	Probability	Maximum Impact	Event
0.377	0.9	0.339	Degrade_the_Back_up4
0.678	0.5	0.339	During_Phyiscal_Transfer_Obtain_Copy1
0.0455	0.9	0.041	Degrade_the_Back_Up_Media
0.0455	0.9	0.041	Degrade_Back_Up2
0.41	0.1	0.041	Gain_Access_to_the_Backup_System1
0.41	0.1	0.041	Backup_data_Accessed1

0.41	0.1	0.041	Access_the_Backup_system_on_site1
0.0455	0.9	0.041	Degrade_Back_Up
1.56E-12	0.9	1.40E-12	Unplug_Ethernet_Cables_from_Access_Points3
1.56E-12	0.9	1.40E-12	Unplug_Ethernet_Cables_from_Access_Points1
1.56E-12	0.9	1.40E-12	Traffic___High_Volumes_Sent177
1.56E-12	0.9	1.40E-12	Traffic___High_Volumes_Sent111
1.56E-12	0.9	1.40E-12	Physically_Destroy_Any_Critically_Functional_Devices3
1.56E-12	0.9	1.40E-12	Physically_Destroy_Any_Critically_Functional_Devices1
1.56E-12	0.9	1.40E-12	Traffic___High_Volumes_Sent1
1.56E-12	0.9	1.40E-12	Physically_Destroy_Any_Critically_Functional_Devices66
1.02E-12	0.9	9.17E-13	Install_Device_Degrading_Malware411
1.02E-12	0.9	9.17E-13	Install_Device_Degrading_Malware413
4.83E-13	0.9	4.34E-13	User_walks_away_from_logged_on_Mobile_Device4431
4.83E-13	0.9	4.34E-13	User_walks_away_from_logged_on_Mobile_Device4433
3.11E-13	0.5	1.56E-13	WiFI_RF_Jamming_Device_Data_Transfer1
3.11E-13	0.5	1.56E-13	WiFI_RF_Jamming_Device_Data_Transfer3
2.12E-13	0.5	1.06E-13	Acquire_Password21
1.18E-13	0.9	1.06E-13	PluginHub1
1.18E-13	0.9	1.06E-13	Send_Data_to_New_GW_or_Reconfigure1
1.18E-13	0.9	1.06E-13	PluginHub3
2.12E-13	0.5	1.06E-13	Acquire_Password23
1.18E-13	0.9	1.06E-13	Send_Data_to_New_GW_or_Reconfigure3
9.66E-14	0.5	4.83E-14	Obtain_OS_Athenication4433
9.66E-14	0.5	4.83E-14	Obtain_OS_Athenication4431
8.03E-14	0.5	4.01E-14	Buying_Malware22
8.03E-14	0.5	4.01E-14	Buying_Malware9
8.03E-14	0.5	4.01E-14	Buying_Malware
1.73E-13	0.1	1.73E-14	Access_to_HIT_Server_Room_Firewall77
1.73E-13	0.1	1.73E-14	Access_to_HIT_Server_Room_Firewall11

1.73E-13	0.1	1.73E-14	Access_to_HIT_Server_Room_Firewall
1.73E-13	0.1	1.73E-14	Login_3
1.73E-13	0.1	1.73E-14	Connect_as_New_Device0
1.73E-13	0.1	1.73E-14	Login11
1.73E-13	0.1	1.73E-14	Connect_as_New_Device3
1.73E-13	0.1	1.73E-14	Login_66
1.73E-13	0.1	1.73E-14	Connect_as_New_Device55
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall777
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall677
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall277
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall477
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall377
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall311
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall411
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall611
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall711
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall811
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall877
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall211
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall8
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall7
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall2
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall3
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall6
1.56E-13	0.1	1.56E-14	Access_thru_HIT_Server_Room_Firewall4
1.71E-14	0.9	1.54E-14	Degrade_Access_Point11
1.71E-14	0.9	1.54E-14	Degrade_Access_Point3
1.54E-13	0.1	1.54E-14	Gain_Access_to_Access_Point13
1.54E-13	0.1	1.54E-14	Gain_Access_to_Access_Point11
1.71E-14	0.9	1.54E-14	DisconnectDevice00
1.71E-14	0.9	1.54E-14	Disconnect_OpenEMR3333
1.71E-14	0.9	1.54E-14	Disconnect_OpenEMR000

1.71E-14	0.9	1.54E-14	DisconnectDevice3333
1.54E-13	0.1	1.54E-14	Connect_as_OpenEMR23333
1.54E-13	0.1	1.54E-14	Connect_as_Device00
1.54E-13	0.1	1.54E-14	Connect_as_OpenEMR2000
1.54E-13	0.1	1.54E-14	Connect_as_Device3333
1.54E-13	0.1	1.54E-14	Connect_as_OpenEMR2
1.54E-13	0.1	1.54E-14	Connect_as_Device
1.71E-14	0.9	1.54E-14	Disconnect_OpenEMR
1.71E-14	0.9	1.54E-14	DisconnectDevice
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent311
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent777
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent877
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent711
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent477
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent377
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent677
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent611
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent411
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent811
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent211
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent277
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent3
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent7
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent6
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent4
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent8
1.54E-14	0.9	1.39E-14	Traffic___High_Volumes_Sent2
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall79
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall822
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall39
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall722
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall322

6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall89
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall422
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall69
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall622
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall49
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall29
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall222
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall72
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall62
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall82
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall42
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall32
6.36E-14	0.1	6.36E-15	Access_thru_HIT_Server_Room_Firewall22
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent422
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent322
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent622
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent89
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent29
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent39
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent222
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent69
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent822
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent79
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent49
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent722
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent62
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent82
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent72
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent32
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent42
6.29E-15	0.9	5.66E-15	Traffic___High_Volumes_Sent22
4.46E-14	0.1	4.46E-15	Coding_Malware9

4.46E-14	0.1	4.46E-15	Coding_Malware22
4.46E-14	0.1	4.46E-15	Coding_Malware
5.27E-14	0.01	5.27E-16	Access_from_AP_to_Mobile_Device4433
5.27E-14	0.01	5.27E-16	Access_from_AP_to_Mobile_Device4431
7.02E-16	0.75	5.27E-16	Malicious_Access_Point4431
5.85E-16	0.9	5.27E-16	Install_Device_Degrading_Malware4433
5.85E-16	0.9	5.27E-16	Install_Device_Degrading_Malware4431
7.02E-16	0.75	5.27E-16	Malicious_Access_Point4433
1.05E-15	0.5	5.27E-16	Mobile_Device_Attaches_to_Malicious_Access_Point4433
1.05E-15	0.5	5.27E-16	Mobile_Device_Attaches_to_Malicious_Access_Point4431
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR411
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR877
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR777
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR811
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR611
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR711
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR111
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR477
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR377
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR311
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR677
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR177
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR3
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR1
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR8
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR4
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR7
1.71E-15	0.1	1.71E-16	Access_to_Health_IT_OpenEMR6
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR622
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR822
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR69

6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR422
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR322
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR79
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR89
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR39
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR49
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR722
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR19
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR122
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR32
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR82
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR62
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR72
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR42
6.98E-16	0.1	6.98E-17	Access_to_Health_IT_OpenEMR12
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent833
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent81
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent30
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent40
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent60
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent61
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent80
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent333
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent73
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent41
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent83
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent70
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent31
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent71
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent63
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent43
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent433

9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent33
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent733
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent633
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent766
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent46
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent355
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent66
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent866
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent655
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent855
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent36
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent755
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent455
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent21
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent233
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent20
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent23
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent26
9.19E-20	0.9	8.27E-20	Traffic___High_Volumes_Sent255
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent63333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent43333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent83333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent73333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent33333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent700
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent800
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent600

8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent300
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent400
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent8111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent6111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent7111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent3444
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent4111
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent200
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2000
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent23333
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2222
8.18E-20	0.9	7.36E-20	Traffic___High_Volumes_Sent2444
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR63
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR833
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR43
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR71
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR733
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR61
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR83
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR41
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR31

1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR80
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR81
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR60
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR33
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR30
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR73
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR333
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR433
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR633
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR70
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR40
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR355
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR46
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR855
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR655
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR66
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR455
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR866
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR36
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR766
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR755
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR133
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR11
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR10
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR13
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR16
1.02E-20	0.1	1.02E-21	Access_to_Health_IT_OpenEMR155
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR83333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4000

9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR700
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR63333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR800
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR600
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR73333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR400
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR43333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR300
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR33333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR4111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR7444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR8444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR6111
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR13333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR1000
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR1333
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR100
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR1444
9.08E-21	0.1	9.08E-22	Access_to_Health_IT_OpenEMR3222

431
7 Tests Performed in Security Controls Assessment

Test ID	CSF Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
1	PR.AC-1 Identities and credentials are managed for authorized devices and users	AC-2	Architecture accounts for multiple user roles the access privileges assigned to each role.	Log on to OpenEMR as an administrator to verify the account types specified that will allow the least privileged access necessary for a user to perform their job function.	The solution has the capability to allow multiple privilege and role levels.
2	PR.AC-1 Identities and credentials are managed for authorized devices and users	AC-2	Only currently authorized users are able to access the EHR data.	Test the system applies access controls: a) After verifying roles in OpenEMR, enter credentials for two users and two devices, no users for third device; b) show a user can access authorized device but not the third one; c) delete one user's credentials; d) show that user can no longer log in	- No EHR information can be accessed unless authorized credentials are used. - A mechanism exists for a privileged user to add/modify/remove access.
3	PR.AC-3 Remote access is managed	IA-3	Unknown devices are challenged when attempting to connect/unknown devices are unable to connect to the EHR system.	Test: a) attempt to access OpenEMR using a device that does not have a valid certificate.	The EHR system recognizes the device as an unknown and either deny access completely or demands additional authentication before establishing connectivity.

4	PR.AC-3 Remote access is managed	AC-17	Connection to the EHR system is permitted only through specific secure protocols.	Test: a) Using a mobile device, attempt to connect to the EHR application 1) via FTP, port 21; 2) via HTTP port 80.	The EHR system allows connections does not allow access via insecure connections. Only secured and appropriate connection protocols are used.
5	PR.AC-4 Access permissions are managed, incorporating the principles of least privilege and separation of duties.	AC-17, AC-6	System components are configured to allow only authorized access to information.	Inspect component settings (network ACLs, firewall rules, OS permissions, application settings) to verify that mechanisms exists to limit access to only authorized users and services. -Verify that those restricted settings are in place. -Verify that services have the least privileged settings necessary to perform their function and use a default deny approach.	Settings limit access to explicitly allowed systems and users.
6	PR.AC-4 Access permissions are managed, incorporating the principles of least privilege and separation of duties.	AC-6	The system will not allow a user greater access than their assigned role permits.	Test the system applies access controls: a) log in as a privileged user; logout. b) log in as a user with no special privileges, attempt to gain privileged access.	The non-privileged user does not gain additional privileges.
7	PR.AC-4 Access permissions are managed, incorporating the principles of least privilege and separation of duties.	IA-5	Application and system components contain a mechanism to allow the auditing of privileged functions.	Within the application, examine settings to identify whether the components used in the solution provide an audit capability that will indicate when privileged use has been employed.	An audit capability exists and can be employed when implemented in a production environment.

8	DE.CM-4: Malicious code is detected	SI-3	Malicious code (anti-virus software) protection is installed on mobile devices.	1) Examine mobile devices to verify that malicious code protection is installed. 2) Inspect the signature file to ensure that the code protection software is current.	Malicious code/anti-virus software is installed.
9	DE.CM-4: Malicious code is detected	SC-35	The EHR application will not permit malicious code to be uploaded.	1) Inspect the OS to ensure that malicious code protection is installed. 2) Test: Attempt to upload a European Institute for Computer Antivirus Research (EICAR) standard anti-virus test file within the application. Verify that the virus scanner responds as if it found a harmful virus. 3) Attempt to upload an EICAR test file that has been compressed. 4) Attempt to upload an EICAR test file that has been archived.	The application should detect/quarantine all attempts to upload malicious files.
10	DE.CM-5: Unauthorized mobile code is detected	SC-18	Verify that only mission appropriate content may be uploaded within the application.	Test: 1) Log in to the OpenEMR application. 2) Identify fields within the application requiring user input. 3) Attempt to upload multiple file types including those containing HTML and JavaScript that contain script code.	The application should employ functionality to restrict upload of file types to those expressly required for operations (e.g., TIFF, JPEG, and PDF).
11	PR.DS-1: Data-at-rest is protected	SC-28	Data within EHR is accessible only to authorized users and services.	Inspect: 1) Verify that encryption tools are employed by reviewing configuration settings or available logs or records to confirm that the installed encryption tools or software are operational. Document how it is implemented for the EHR data. 2) Indicate the encryption type in use and whether it is embedded in the EHR product or a separate mechanism. 3) Identify any non-cryptographic mechanisms employed to protect data (file share scanning, and integrity protection).	Data is protected during storage and processing.

12	PR.AC-3 Remote access is managed	AC-17(1)	Remote access to the EHR is monitored and controlled by access type, preventing unauthorized connections	Test: 1) Have user A (above) log in via the Internet; logout 2) Have user A try to log in via dial-up. This should fail. 3) Have user B above try to log in via the Internet; this should fail. 4) Have user B log in via dial-up from the authorized source location; logout 5) have user B try to log in via dial-up from an unauthorized source location; this should fail 6) Have users A and C above log in via Internet. Both users attempt to perform a privileged function. Only user C should be successful. 7) Have users B and C log in via dial-up from authorized source locations. Both users attempt to perform a privileged function. Only user D should be successful. 8) Have an unauthorized user X attempt to access the EHR server remotely via dial-up from an authorized location (the location from which user B above is authorized to dial in); this should fail.	Attempted logins and use of privileged functions is successful or fails as noted in preceding column. This demonstrates that the mechanisms for restricting access based on remote access type are enforced correctly by the EHR server.
13	PR.AC-3 Remote access is managed	AC-17	Only devices with authorized MAC addresses will be granted access to the network.	1) Use an authorized mobile device to log an authorized user into the EHR. 2) Configure that otherwise legitimate mobile device to have a MAC address that is not authorized to access the network and attempt to log on. 3) Verify that the log in attempt will fail.	MAC address checking is performed.
14	PR.AC-5 Network Integrity is protected, incorporating network segregation where appropriate	AC-4	Information flow control policy is enforced to control the flow of info between the designated mobile devices and the EHR server.	Test: 1) Attempt to send EHR information from one mobile device directly to the other via the EHR application. 2) Attempt to perform IP spoofing on the server OS. Command for evaluating on Linux: ls /proc/sys/net/ipv4/conf/*/rp_filter cat /proc/sys/net/ipv4/conf/*/rp_filter grep rp_filter /etc/sysctl.conf	1) EHR information will not be accessible directly from device to device. 2) The system is protected from packets transmitted from a masquerading server.

15	PR.DS-2: Data-in-transit is protected	SC-8 SC-13	The confidentiality and integrity of EHR information is protected while in transit (SC-8) using a cryptographic mechanism	Examine transmission settings. Verify the encryption mechanisms in place when transmitting data. Test: 1) Set up Wireshark to eavesdrop on link between mobile device and EHR server and start capturing packets (A hub can be placed between the wireless access point and the wired network and Wireshark run on a computer connected to the hub.) 2) Send EHR info from mobile device to EHR server 3) Turn off packet capture 4) Examine packet capture to verify that a digital signature was sent with the EHR info transmitted. 5) Calculate what the digital signature should be for this EHR and verify that it is the same as the value that was transmitted. 6) Verify that the packets containing health information are encrypted exactly as they should be given the encryption algorithm used.	FIPS 140-2 compliant mechanism is used to secure data in transit.
16	PR.PT-4:Communication and control networks are protected	SC-7	All Wi-Fi-related products in the system conform to IEEE 802.11i and IEEE 802.1X standards.	Consult WiFi Alliance online list of Wi-Fi Certified products to verify that all mobile devices and access points used in the system are Wi-Fi Alliance certified in the three security areas of: 1) WPA2™ (Wi-Fi Protected Access® 2) EAP (Extensible Authentication Protocol), and 3) Protected Management Frames.	Devices in use are Wi-Fi Certified.
17	PR.PT-4: Communications and control networks are protected	SC-7	Wired network is hardened (EHR server is protected by a firewall, antivirus software, and an IDS, and all patching is up-to-date)	Inspect wired network to verify presence of firewall, antivirus software, and an IDS. Confirm that all patching is up-to-date	Wired network has listed security components installed.
18	PR.PT-4: Communications and control networks are protected	SC-7	Mobile Device (wireless client) is hardened in general.	Mobile Device has a firewall, antivirus software, and an IDS installed, its patching is up-to-date, 802.11 ad hoc mode is disabled, and Bluetooth is turned off by default.	Mobile device has listed security components installed

19	PR.PT-4: Communications and control networks are protected	SC-7	The application accepts connections from only those devices hardened in compliance with security policy.	1. Use a mobile device to successfully log in to OpenEMR. Log out. 2) Turn Bluetooth on that mobile device and attempt to log in to the EHR. 3) Verify that the mobile device can no longer login to the EHR server.	Non-compliant mobile devices may not access the OpenEMR application.
20	PR.PT-4: Communications and control networks are protected	SC-7	A mobile device's configuration goes out of compliance while logged in.	1) Use a mobile device to successfully log in to OpenEMR. 2) While logged in to the OpenEMR, turn on Bluetooth for that mobile device. 3) Verify that the mobile device is not visible to other devices	Mobile devices outside of the EHR application are unable to connect to a mobile device accessing OpenEMR.

8 Risk Questionnaire for Health Care Organizations Selecting a Cloud-Based Electronic Health Record Provider

8.1 Introduction

Health care organizations with limited resources and capital may, based on their individual enterprise risk assessment, choose cloud-based services to provide health care IT for clinicians and administrators. Since cloud computing resources are often shared by multiple tenants and hosted outside a health care organization's perimeters, and data is transmitted through the public Internet, health care organizations should become educated about the potential risks of using the cloud for their health care IT needs.

The functionalities provided, service levels offered, and the ability to achieve compliance with legal, regulatory, and security related standards and requirements might differ significantly among different cloud computing vendors. The Office of the National Coordinator for Health Information Technology provides a questionnaire[13] to help health care organizations shop for a cloud vendor that provides security for health care information and personal privacy along with supports for technical and legal compliance.

The questionnaire should not be viewed as an exhaustive arbiter of security when shopping for a cloud provider. Rather, it is intended to help organizations address security concerns in the early stages so that potential threats and vulnerabilities can be mitigated and minimized in the future. We strongly recommended that each organization perform a thoroughly risk assessment before moving to cloud-based health care IT services, and make a strategic decision based on their organization's financial, business operation, and legal and regulatory requirements. We also recommend regular re-assessments when there are significant changes to the organization's environment.

8.2 Security Questionnaire

1. Vendor Agreements
    a. Is the EHR system vendor willing to sign a comprehensive business service agreement?
    b. Is the EHR system vendor willing to confirm compliance with HIPAA Privacy and Security Rules, and willing to be audited, if requested?
2. Third-party Application Integration
    a. Does the health care organization need to integrate the cloud-based EHR system with other in-house products, such as practice management software, billing systems, and email systems?

[13] Security Risk Assessment Tool, Office of the National Coordinator for Health Information Technology, http://www.healthit.gov/providers-professionals/security-risk-assessment [accessed July 15, 2015].

   b. If integration of the cloud-based EHR system to in-house applications is needed, what are the implementation procedures and techniques used? What security features protect the data communicated among different systems?

3. Personal or Device Authentication and Authorization
   a. Does the EHR system vendor restrict the type of mobile devices that can access the system?
   b. Are mobile devices subject to some kind of mobile device management control for enforcing device security compliance?
   c. Are there any security compliance polices for using a client's own device to access the cloud-based EHR system?
   d. If a device is lost, stolen, or found to be hacked, are there any countermeasures in place to avoid protected data from becoming compromised?
   e. Does the cloud-based EHR system require a user to be authenticated prior to obtaining access to patient health information?
      i. What are the authentication mechanisms used for accessing the system?
      ii. Are user IDs uniquely identifiable?
      iii. Is multifactor authentication used? Which factors?
      iv. If passwords are used, does the vendor enforce strong passwords and specify the lifecycle of the password?
   f. Does the system offer a role-based access control approach to restrict system access to authorized users to different data sources?
   g. Is the least privilege policy used? (A user of a system has only enough rights to conduct an authorized action within a system, and all other permissions are denied by default.)
4. Data Protection
   a. What measures are used to protect the data stored in the cloud?
   b. What measures are used to protect the data from loss, theft, and hacking?
   c. Does the system back up an exact copy of protect data? Are these backup files kept in a different location, well protected, and easily restored?
   d. Does the system encrypt the protected data while at rest?
   e. What happens if the EHR system vendor goes out of business? Will all clinical data and information be retrievable?
   f. Does the EHR system vendor have security procedures and policies for decommissioning used IT equipment and storage devices which contained or processed sensitive information?
5. Security of Data in Transmission
   a. How does the network provide security for data in transmission?
   b. What capabilities are available for encrypting health information as it is transmitted from one point to another?

   c. What reasonable and appropriate steps are taken to reduce the risk that patient health information can be intercepted or modified when it is being sent electronically?

6. Monitoring and Auditing
   a. Are systems and networks monitored continuously for security events?
   b. Does the EHR vendor log all the authorized and unauthorized access sessions and offer auditing?
   c. Does the system have audit control mechanisms that can monitor, record, and/or examine information system activities that create, store, modify, and transmit patient health information?
   d. Does the system retain copies of its audit/access records?
   e. How does the EHR system vendor identify, respond to, handle, and report suspected security incidents?
7. Emergencies
   a. Does the EHR system vendor offer the ability to activate emergency access to its information system in the event of a disaster?
   b. Does the EHR system vendor have policies and procedures to identify the role of the individual responsible for accessing and activating emergency access settings, when necessary?
   c. Is the EHR system designed to provide recovery from an emergency and resume normal operations and access to patient health information during a disaster?
8. Customer and Technical Support
   a. What is included in the customer support / IT support contract and relevant service level agreements?
   b. Can the HER system vendor provide a written copy of their security and privacy policies and procedures (including disaster recover)?
   c. How often are new features released? How are they deployed?