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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

PRACTICE GUIDE | Health IT
NIST SP 1800-1a

Securing Electronic Health Records on Mobile Devices

Executive Summary

- Patient information in electronic health records needs to be protected so it is not exploited to endanger patient health or compromise identity and privacy.[‡]
- If not protected, patient information collected, stored, processed, and transmitted on mobile devices is especially vulnerable to attack.[†]
- The National Cybersecurity Center of Excellence (NCCoE) developed an example solution to this problem using commercially available products.
- The example solution is packaged as a “How To” guide, providing organizations with the detailed instructions to recreate our example. The NCCoE’s approach secures patient information when practitioners access it with mobile devices.
- Organizations can use some, or all, of the guide to help them implement relevant standards and best practices in the NIST Framework for Improving Critical Infrastructure Cybersecurity and Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

The National Cybersecurity Center of Excellence helps organizations adopt advanced technologies that improve the security of their digital assets such as electronic health record systems and the patient information they contain.

BUSINESS CHALLENGE

Health care providers increasingly use mobile devices to store, process, and transmit patient information. When health information is stolen, inappropriately made public, or altered, health care organizations can face penalties and lose consumer trust, and patient care and safety may be compromised. The NCCoE helps organizations implement safeguards to ensure the security of patient information when doctors, nurses, and other caregivers use mobile devices in conjunction with an electronic health record (EHR) system.

In our lab at the NCCoE at the National Institute of Standards and Technology (NIST), we built an environment that simulates interaction among mobile devices and an EHR system supported by the IT infrastructure of a medical organization.

We considered a scenario in which a hypothetical primary care physician uses her mobile device to perform recurring activities such as sending a referral containing a patient’s clinical information to another physician, or sending an electronic prescription to a pharmacy. At least one mobile device is used in every transaction, each of which interacts with an EHR system. When a physician uses a mobile device to add patient information into an electronic health record, the EHR system enables another physician to access the information through a mobile device, as well.

THE SOLUTION

The NIST Cybersecurity Practice Guide "Securing Electronic Records on Mobile Devices" demonstrates how existing technologies can meet your organization's need to better protect the information in EHR systems. Specifically, we show how security engineers and IT professionals, using commercially available and open-source tools and technologies that are consistent with cybersecurity standards, can help health care organizations that use mobile devices share patients' health records more securely. We use a layered security strategy to achieve these results.

Using the guide, your organization may choose to adopt the same approach. Commercial and open-source standards-based products, like the ones we used, are easily available and interoperable with commonly used information technology infrastructure and investments.

The guide:

- maps security characteristics to standards and best practices from NIST and other standards organizations, and to the HIPAA Security Rule
- provides a detailed architecture and capabilities that address security controls
- facilitates ease of use through automated configuration of security controls
- addresses the need for different types of implementation, whether in-house or outsourced
- provides a how-to for implementers and security engineers seeking to recreate our reference design

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization's security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution that best meets your mission needs.

ASSESS YOUR RISK

All health care organizations need to fully understand their potential cybersecurity vulnerabilities, the bottom-line implications of those vulnerabilities, and the lengths attackers will go to exploit them. According to our risk analysis (NIST SP 1800-1b, Section 4.3 and NIST SP 1800-1e), and in the experience of many health care organizations, 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 "many health care providers are using mobile devices in health care delivery before they have appropriate privacy and security protections in place."[†]

Assessing risks and making decisions about how to mitigate them should be continuous to account for the dynamic nature of your businesses processes and technologies, the threat landscape, and the data itself. The guide describes our approach to risk assessment. We recommend that organizations implement a continuous risk management process as a starting point to adopting this or other approaches that will increase the security of electronic health records.

SHARE YOUR FEEDBACK

You can improve our guide by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to share your experience and advice with us.

- email HIT_NCCoE@nist.gov
- participate in our forums at http://nccoe.nist.gov/forums/health-it

Or learn more by arranging a demonstration of this example solution by contacting us at HIT_NCCoE@nist.gov.

TECHNOLOGY PARTNERS

The NCCoE issued a call in the Federal Register to invite technology providers with commercial products that matched our security characteristics to submit letters of interest describing their products' capabilities. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution.

The National Cybersecurity Center of Excellence at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based example solutions using commercially available technologies. The NCCoE seeks problems that are applicable to whole sectors, or across sectors. This cybersecurity challenge was brought to us by members of the health IT community. The center's work results in publicly available NIST Cybersecurity Practice Guides that provide modular, open, end-to-end reference designs.

LEARN MORE

Visit http://nccoe.nist.gov

ARRANGE A DEMONSTRATION

nccoe@nist.gov
240-314-6800

[‡] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015.

[†] HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians' Use of and Privacy & Security Good Practices for mHealth, http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/, accessed June 1, 2015.

NIST CYBERSECURITY PRACTICE GUIDE HEALTH IT

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Approach, Architecture, and Security Characteristics

For CIOs, CISOs, and Security Managers

Gavin O'Brien
Brett Pleasant
Colin Bowers
Sue Wang
Kangmin Zheng
Kyle Kamke
Nate Lesser

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1b
DRAFT

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST Special Publication 1800-1b

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

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

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 1800-1b
Natl. Inst. Stand. Technol. Spec. Publ. 1800-1b, 23 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 publicly 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 her mobile device to perform reoccurring activities such as sending a referral (e.g., clinical

[*] 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

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
Sally Edwards	MITRE
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 Summary

The key motivation for this practice guide is captured by the following two points:

- Electronic health records can be exploited in ways that can endanger patient health as well as compromise identity and privacy.[1]
- Electronic health records shared on mobile devices are especially vulnerable to attack.[2]

The National Cybersecurity Center of Excellence (NCCoE) response to the problem of securing electronic health care information on mobile devices has been to take the following actions:

- The NCCoE developed an example solution to this problem using commercially available products that conform to federal standards and best practices.
- This example solution is packaged as a “How To” guide. In addition to helping organizations comply with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, the guide demonstrates how to implement standards-based cybersecurity technologies in the real world, based on risk analysis.

1.1 Background

Cost and care efficiencies, as well as incentives from the Health Information Technology for Economic and Clinical Health Act (HITECH Act), have prompted health care groups to rapidly adopt electronic health record (EHR) systems. Unfortunately, organizations have not adopted security measures at the same pace. Attackers are aware of these vulnerabilities and are deploying increasingly sophisticated means to exploit information systems and devices. The Ponemon Institute reports 125% growth in the numbers of intentional attacks over a five-year period. Malicious hacks on health care organizations now outnumber accidental breaches.[3]

According to a risk analysis described in Section 4.3 below, and in the experience of many health care providers, mobile devices can present vulnerabilities to a health care organization’s networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that “many health care providers are using mobile devices in health care delivery before they have appropriate privacy and security protections in place.”[4]

The negative impact of stolen health records is much higher when you factor in the costs an organization incurs when responding to a breach. In addition to federal penalties, organizations

[1] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015.
[2] HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians’ Use of and Privacy & Security Good Practices for mHealth, http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/, accessed June 1, 2015.
[3] Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2015.
[4] HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians’ Use of and Privacy & Security Good Practices for mHealth, http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/, accessed June 1, 2015.

pay for credit and identity theft monitoring for affected clients, crisis communications, and they lose revenue due to loss of consumer and patient trust. In 2013, the Ponemon Institute calculated the cost of medical identity theft at $12 billion annually, along with consequences for patient safety in terms of misdiagnosis, delayed treatment, or incorrect prescriptions. Costs are likely to increase as more breaches occur.

1.2 Business Challenge

Health care providers increasingly use mobile devices to receive, store, process, and transmit patient health information[5]. Unfortunately, many organizations have not implemented safeguards to ensure the security of patient data when doctors, nurses, and other caregivers use mobile devices in conjunction with an EHR system. As stated above, when patient health information is stolen, made public, or altered, health care organizations can face fines and lose consumer trust, and patient care and safety may be compromised. The absence of effective safeguards, in the face of a need to leverage mobile device technologies to more rapidly and effectively deliver health care, poses a significant business challenge to providers.

In response to this challenge, the NCCoE at NIST built a laboratory environment that simulates interaction among mobile devices and an EHR system supported by the information technology (IT) infrastructure of a medical organization. The laboratory environment was used to support composition and demonstration of security platforms composed to address the challenge of securing electronic health records in mobile device environments.

The project considered a scenario in which a hypothetical primary care physician uses her mobile device to perform recurring activities such as sending a referral containing clinical information to another physician, or sending an electronic prescription to a pharmacy. At least one mobile device is used in every transaction, each of which interacts with an EHR system. When a physician uses a mobile device to add clinical information into an electronic health record, the EHR system enables another physician to access the clinical information through a mobile device as well.

The challenge in this scenario, which you can imagine playing out hundreds or thousands of times a day in a real-world health care organization, is that of how to effectively secure patient health information when accessed by health practitioners using mobile devices without degrading the efficiency of health care delivery.

1.3 The Solution

The NIST Cybersecurity Practice Guide “Securing Electronic Health Records on Mobile Devices” demonstrates how existing technology can meet an organization’s need to better protect these records. Specifically, we show how health care providers, using open source and commercially available tools and technologies that are consistent with cybersecurity standards

[5] 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.

and best practices, can more securely share electronic health records among caregivers who use mobile devices. We use a layered security strategy to achieve these improvements in protection of health information.

Using the guide, your organization is encouraged to adopt the same approach. Commercial and open-source standards-based products, like the ones we used, are available and interoperable with existing information technology infrastructure and investments.

The guide:

- maps security characteristics to standards and best practices from NIST and other standards organizations, and to the HIPAA Security Rules
- provides a detailed architecture and capabilities that address security controls
- facilitates ease of use through transparent, automated configuration of security controls
- addresses the need for different types of implementation, whether in-house or outsourced
- provides guidance for implementers and security engineers

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization’s security experts should identify the standards-based products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

1.3.1 Technology Partners

The NCCoE issued a call in the Federal Register to invite technology providers with commercial products that matched our security characteristics to submit letters of interest describing their products’ capabilities. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement (CRADA) with NIST, allowing them to participate in a consortium to build this example solution. The following companies contributed their products to this effort:

- Cisco
- Intel
- MedTech Enginuity
- MaaS360
- Ramparts
- RSA
- Symantec

For more details, see Section 4.6, Technologies.

1.4 Assess Your Risk

All health care organizations need to fully understand their potential cybersecurity vulnerabilities, the bottom-line implications of those vulnerabilities, and the lengths attackers will go to exploit vulnerabilities.

Assessing risks and making decisions about how to mitigate them should be a continuous process to account for the dynamic nature of your businesses, the threat landscape, and the data itself. The guide describes our approach to risk assessment. We urge you to implement a continuous risk management process for your own organization as a starting point to adopting this or other approaches that will increase the security of electronic health records. Additional information about mobile device risk and the security of health information is available from the Department of Health and Human Services at http://www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security.

1.5 Share Your Feedback

While our example solution has been evaluated by our consortium team members, you can improve it further by contributing feedback. As you review and adopt this solution for your own organization, we ask you and your colleagues to contribute your experience and advice to us by email at HIT_NCCoE@nist.gov, and by participating in our forums at http://nccoe.nist.gov/forums/health-it.

Or learn more by arranging a demonstration of this example solution by contacting us at HIT_NCCoE@nist.gov.

2 How to Use This Guide

This NIST Cybersecurity Practice Guide demonstrates 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. Mobile devices are defined variously across the IT community. NIST Special Publication 800-124, Guidelines for Managing the Security of Mobile Devices[6], defines mobile devices as smart phones and tablets. They are characterized by small form factors, wireless networking capability, built-in data storage, limited operating systems, and with multiple ways of accessing applications. For the purposes of this project, mobile devices are considered smart phones and tablets.

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** ⬅ **YOU ARE HERE**
- 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

[6] M. Souppaya, K. Scarfone, Guidelines for Managing the Security of Mobile Devices. NIST Special Publication 800-124, Rev. 1, http://csrc.nist.gov/publications/PubsSPs.html#800-124 [accessed July 15, 2015]. http://dx.doi.org/10.6028/NIST.SP.800-124r1

- NIST SP 1800-1e: Risk Assessment and Outcomes – risk assessment methodology, results, test, and evaluation

Depending on your role in your organization, you might use this guide in different ways.

Health care organization leaders, including chief security and technology officers will be interested in the Executive Summary, which provides:

- a summary of the challenge health care organizations face when utilizing mobile devices for patient interactions
- a description of the example solution built at the NCCoE
- an understanding of importance of adopting standards-based cybersecurity approaches to better protect your organization’s digital assets and the privacy of patients

Technology or security program managers who are responsible for managing technology portfolios and are concerned with how to identify, understand, assess, and mitigate risk might be interested in:

- The Approach (Section 4), where we provide a detailed architecture and map security characteristics of this example solution to cybersecurity standards and best practices, and HIPAA requirements
- Risk Management (Section 4.3), which is the foundation for this example solution

If your organization is already prioritizing cybersecurity, this guide can help increase confidence that the right security controls are in place.

IT professionals who want to implement an approach like this will find the whole practice guide useful. Specifically,

- NIST SP 1800-1b: Approach, Architecture, and Security, Sections 3 to 5 provide an explanation of what we did, and why, to address this cybersecurity challenge
- NIST SP 1800-1c: How-To Guides, covers all the products that we employed in this reference design. We do not recreate the product manufacturer’s documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment to create an example solution.
- NIST SP 1800-1d: Standards and Controls Mapping, Section 1 is a complete list of security standards used to create the architecture
- NIST SP 1800-1e: Risk Assessment and Outcomes, Section 1 shows, step-by-step, what happens when an adversary attempts to gain unauthorized access to our EHR system, as well as the ease with which an authorized user gains access.
- NIST SP 1800-1e: Risk Assessment and Outcomes, Section 2 describes the results of an independent test on the reference design detailed in this guide.

This guide assumes that the IT professionals who follow its example have experience implementing security products in health care organizations. While we have used certain commercially available products, there may be comparable products that might better fit your particular IT systems and business processes.[7] If you use substitute products, we recommend that, like us, you ensure that they are congruent with standards and best practices in health IT. To help you understand the characteristics you should look for in the components you use, Table 3 maps the representative products we used to the cybersecurity controls delivered by this reference design. Section 4.5 describes how we used appropriate standards to arrive at this list of controls.

A NIST Cybersecurity Practice Guide does not describe “the” solution, but a possible solution. This is a draft guide. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/health-it.

3 Introduction

Health care records have become one of the most sought-after types of information. A stolen medical record contains data that provides thieves with access to a patient’s medical or other identity, and to a health care organization’s services. Theft of health information raises the cost of health care and can result in physical harm: if a person’s health care record is altered, an unsafe drug interaction might result; if the record cannot be trusted, a patient might experience a delay in care.[8]

This guide demonstrates tools a health care organization can use to increase the security of health information as it is stored, processed, and transmitted on mobile devices. In particular, the scenarios in this guide focus on the medical providers who use mobile devices to review, update, and exchange electronic health records. Mobile devices used in this way are subject to the following security concerns, which are addressed in this guide:

- A health care worker might lose or misplace a mobile device containing private health information, or be a victim of exploitation or theft.
- Compromised mobile devices enable hackers to access the health care organization’s network.
- Untrusted networks using a man-in-the-middle strategy to obtain credentials to access the enterprise network.

[7] 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.

[8] Kaiser Health News, The Rise of Medical Identity Theft in Health Care, Stateline, March 7, 2014

- Interacting with other systems increases a health care worker's risk of compromising routine operations such as data synchronization and storage.

At the NCCoE, we set out to address needs expressed by health care organizations and to demonstrate how an organization can recreate and implement this reference design in whole or in part to improve information security. For this project, we built an environment that simulates interaction among mobile devices and an EHR system. In our simulation, the EHR system is assumed to be located in a mid- to large-sized[9] medical organization and is accessed from a small organization. We used this environment to replicate an example approach to better secure this type of electronic exchange and the important health and other data contained and stored in electronic medical records. We explored three configuration options:

1. organizations that provide wireless connections for mobile devices
2. organizations with outsourced support for system access (e.g., using the cloud for systems access)
3. organizations that provide access via a wholly external access point (e.g., virtual private network, VPN)

This guide explains how we assessed and mitigated risk, and implemented and evaluated a standards-based example solution. It contains a detailed architecture and clearly identifies the security characteristics your health care organization should ensure are in place within your overall enterprise. In addition, we provide instructions for the installation, configuration, and integration of each component used in the example implementation of these security characteristics.

4 APPROACH

The initial motivation for this project came from inquiries by members of the health care industry. We conducted a risk assessment to evaluate the challenges faced by health care organizations. This risk assessment initially evaluated the current and planned uses of electronic health care records. As indicated in the Introduction, this analysis revealed that current practice involving the use of mobile devices: a) provides real advances in speed and accuracy in the exchange and use of medical records, and b) involves significant threats to the confidentiality and integrity of those records. We found that realization of these threats can result in severe patient health and safety, litigation, and regulatory issues.

Based on the finding that use of mobile devices to exchange patient health records is needed, but carries high risk in the absence of improved security and privacy measures, we:

- derived requirements that support effective and efficient exchange of health records while maintaining the security and privacy of those records and complying with applicable regulations
- explored the availability of components to address the derived requirements

[9] In this case organizational size is used as a proxy for technical sophistication and cybersecurity maturity

- generated a formal use case description of the problem, the derived requirements, and a security platform composed of available components that could be demonstrated in a laboratory environment to address the requirements
- assembled a team of voluntary industry collaborators
- composed and demonstrated the security platform
- documented the requirements, example solution, and how the example solution may be used to address the requirements

The following description of our approach includes:

1. a description of the intended audience
2. the scope of the descriptive and instructive documentation
3. a brief summary of our risk management approach and findings
4. use case scenarios addressed in the context of a high-level architecture
5. the security characteristics that needed to be demonstrated to meet our derived requirements
6. the technical components we identified for laboratory demonstration of the necessary security characteristics.

4.1 Audience

This guide is intended for individuals responsible for implementing IT security solutions in health care organizations. For organizations that choose to use Internet service providers or cloud-based solutions, Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section 8, provides a checklist of questions to help you choose a secure solution.

4.2 Scope

This guide is limited in scope to the technological aspects of this cybersecurity challenge and the detail necessary to recreate our reference design. Our simulated health enterprise is focused on protecting the EHR system, the mobile devices using it, and the data in the electronic health records.

4.3 Risk Management

According to NIST IR 7298, Glossary of Key Information Security Terms, risk management is:

> The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and

(iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.[10]

Risk management is an ongoing organizational process. Our simulated environment does not operate continuously and does not include the organizational characteristics necessary to implement risk management processes (e.g. number and location of facilities, size of the staff, risk tolerance of the organization, etc). We did, however, conduct a system risk assessment in accordance with NIST Special Publication 800-30, Guide for Conducting Risk Assessments.

Our risk assessments focused on identifying threats that might lead to:

- loss of confidentiality – unauthorized disclosure of sensitive information
- loss of integrity – unintended or unauthorized modification of data or system functionality
- loss of availability – impact to system functionality and operational effectiveness

Based on our risk assessment, the major threats to confidentiality, integrity, and availability are:

- a lost or stolen mobile device
- a user who
    - walks away from logged-on mobile device
    - downloads viruses or other malware
    - uses an unsecure Wi-Fi network
- inadequate
    - access control and/or enforcement
    - change management
    - configuration management
    - data retention, backup, and recovery

More detail about our risk assessment can be found in Volume 1800-1e of this publication, Risk Assessment and Outcomes.

In order to demonstrate how to monitor and clearly communicate the relationship between technical risks and organizational risks, we used a governance, risk and compliance (GRC) tool to aggregate and visualize data. The details on how to install and setup the GRC tool can be found in Volume 1800-1c of this publication, How-To Guides, Section 10, “Governance, Risk and Compliance.”

4.4 The Use Case

In 2012, the NCCoE published the draft use case, “Mobile Devices: Secure Exchange of Electronic Health Information.”[11] The use case describes scenarios in which physicians use

[10] http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf,

mobile devices to refer patients to another physician or to issue an e-prescription. In addition, the use case contains a diagram (Figure 1) illustrating the flow of information from the physician to the EHR system, and then back to another physician.

[11] Final draft available at http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_HIT_MobileDevices_UseCase.pdf

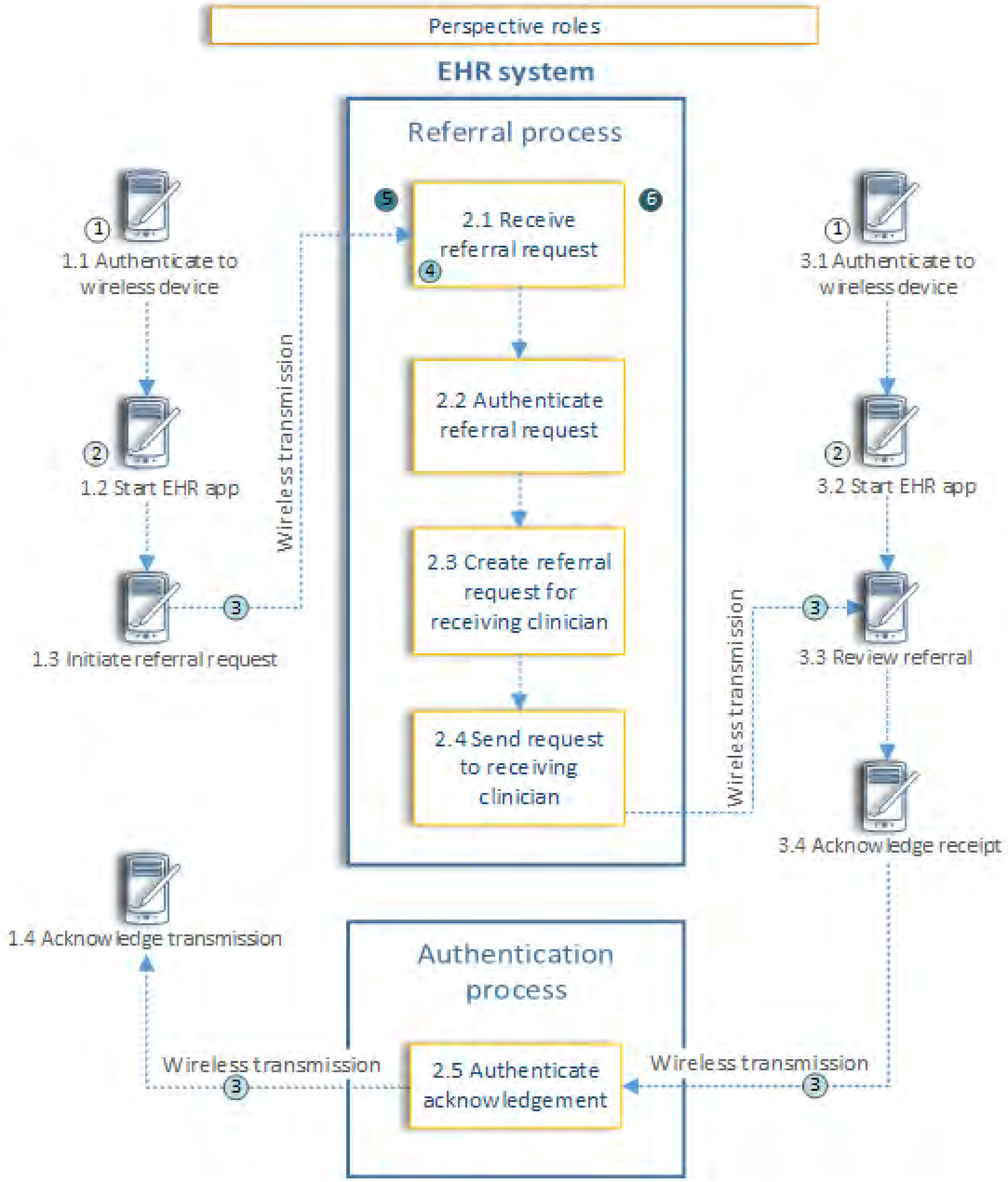

Perspective roles
EHR system
Referral process
5
6
2.1 Receive referral request
4
2.2 Authenticate referral request
2.3 Create referral request for receiving clinician
2.4 Send request to receiving clinician
1
1.1 Authenticate to wireless device
2
1.2 Start EHR app
3
1.3 Initiate referral request
Wireless transmission
1
3.1 Authenticate to wireless device
2
3.2 Start EHR app
3
3.3 Review referral
3.4 Acknowledge receipt
Wireless transmission
1.4 Acknowledge transmission
Authentication process
2.5 Authenticate acknowledgement
Wireless transmission
3
Wireless transmission
3

Figure 1: Security characteristics required to securely perform the transfer of electronic health records among mobile devices.1) wireless device security; 2) wireless device data security; 3) wireless device transmission security; 4) EHR message authentication; 5) EHR network security; and 6) EHR system security.

As we further developed the scenarios, we could not explore the security of a health care organization's EHR system and mobile devices without recreating within our lab the sort of enterprise infrastructure that an organization might rely upon. This practice guide implements a defense-in-depth strategy for securing the EHR, mobile devices, and patient information. In other words, these assets sit behind layers of security. Figure 2 shows the high-level architecture from the original use case with the organization's enterprise included.

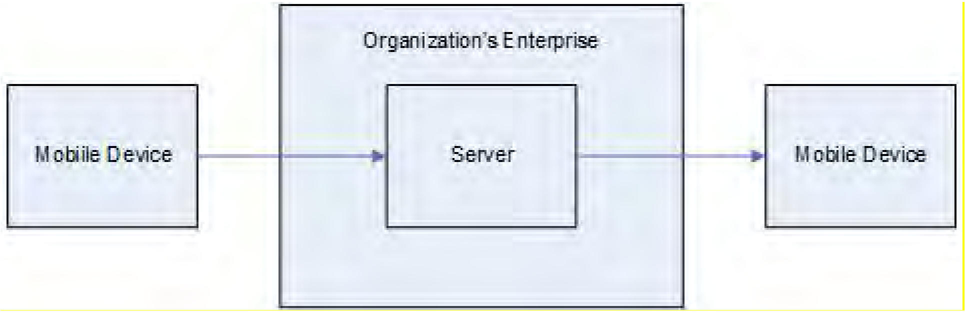


Figure 2: High-level architecture

From this use case scenario, we identified the architecture components that are likely in an organization's enterprise (see Table 1).

Table 1: Use Case Architecture Components

Mobile Devices	**Networks**	**Back End**[12]	**Secure Infrastructure**
mobile device	Wi-Fi	certified[13] electronic health record system	firewall
mobile device management client		storage encryption	VPN gateway
intrusion detection system		antivirus	authentication, authorization, and accounting (AAA) server
firewall software		intrusion detection system	certificate authority and enrollment
provisioning system for mobile devices client		provisioning system for mobile devices server	
health care mobile device application		mobile device management server	

[12] Back end systems are run from the organization's data center and support the data processing or core functions of the organization.

[13] ONC Health IT Certification Program, Certified Health IT Product List, http://www.healthit.gov/policy-researchers-implementers/certified-health-it-product-list-chpl

storage encryption		auditing mobile device	
antivirus		mobile device identity management	

4.5 Security Characteristics

From the use case scenarios we derived a set of security characteristics as the high-level requirements for our build. The security characteristics are:

- Access control – selective restriction of access to an individual or device
- Audit controls and monitoring – controls recording information about events occurring within the system
- Device integrity – maintaining and ensuring the accuracy and consistency of a device
- Person or entity authorization – the function of specifying access rights to people or entities
- Transmission security – the process of securing data transmissions from being infiltrated, exploited or intercepted by an individual, application, or device.

Table 2 shows the relationship between the security characteristics and the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the Cybersecurity Framework, or CSF) for critical infrastructure functions and categories and HIPAA requirements.

Table 2: Mapping Security Characteristics to the CSF and HIPAA

Security Characteristics	CSF Function	CSF Category	HIPAA Requirements
access control	Protect (PR)	Access Control (PR.AC)	§ 164.312 (a)
audit controls/ monitoring	Identify (ID)	Asset management (ID.AM)	§164.312(b)
		Risk Assessment (ID.RA)	§164.312(b)
	Detect (DE)	Security Continuous Monitoring (DE.CM)	§164.312(b)
device integrity	Protect (PR)	Access Control (PR.AC)	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Data Security (PR.DS)	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Information Protection Processes and Procedures (PR.IP)	(§ 164.312 (c))
		Protective Technology (PR.PT)	(§ 164.312 (c))
	Detect (DE)	Security Continuous Monitoring (DE.CM)	(§ 164.312 (c))
			(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
person or entity authentication	Protect (PR)	Access Control (PR.AC)	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
transmission security	Protect (PR)	Access Control (PR.AC)	§164.312 (e)
		Data Security (PR.DS)	§ 164.312 (e))

		Technology (PR.PT)	§ 164.312 (e))
Security incidents	Respond (RS)	Mitigation (RS.MI)	§ 164.308(a)(6)(ii)
Recover (RC)	Recover (RC)	Recovery Planning (RC.RP)	§ 164.308(a)(7)(ii)(A) § 164.308(a)(7)(ii)(B) § 164.308(a)(7)(ii)(C)

Volume 1800-1d of this publication, Standards and Controls Mapping, contains a complete description of the security characteristics and controls.

4.6 Technologies

In January 2013, the NCCoE issued a call in the Federal Register to invite technology providers with commercial products that could meet the desired security characteristics of the mobile device use case to submit letters of interest describing their products' relevant security capabilities. In April of 2013, the center hosted a meeting for interested companies to demonstrate their products and pose questions about the project. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, enabling them to participate in a consortium to build a reference design that addresses the challenge articulated in the use case.

Table 3 lists all products and the participating companies and open-source providers used to implement the security requirements in Table 2. The CSF aligns with existing methodologies and aids organizations in expressing their management of cybersecurity risk. The complete mapping of representative product to security controls can be found in NIST SP 1800-1d, Standards and Controls Mapping, Section 5.

Table 3: Participating Companies and Contributions Mapped to Controls

CSF Function	Company	Application/Product	Use
Identify (ID)	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
Protect (PR)	MedTech Enginuity	OpenEMR	web-based and open source electronic health record and supporting technologies
	open source	Apache Web Server	
	open source	PHP	
	open source	MySQL	
	open source	ModSecurity	Apache module extension, web application firewall (supporting OpenEMR)
	open source	OpenSSL[14]	cryptographically secures transmissions between mobile devices and the OpenEMR web portal service
	Various	mobile devices	Windows, IOS and Android tablets
	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	stateful inspection firewall
	open source	Root CA / Fedora PKI manager	cryptographically signs identity certificates to prove authenticity of users and devices
	open source	domain name system (DNS) and DNS encryption (DNSE) / Bind9	performs host or fully qualified domain resolution to IP addresses

[14] The Library is used by TLS.

	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	Cisco	local and remote mobile NAC (Identity Services Engine)	radius-based authentication, authorization and accounting management server
	Cisco	VPN server (ASAv 9.4)	enterprise class virtual private network server based on both TLS and IPSEC
	open source	URbackup	online remote backup system used to provide disaster recovery
	Cisco	wireless access point (RV220W)	Wi-Fi access point
Detect (DE)	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	stateful inspection firewall
	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	open source	intrusion detection server (Security Onion IDS)	monitors network for threats via mirrored switch ports
	open source	host-based security manager (freeware)	server client-based virus and malware scanner
	open source	vulnerability scanner (freeware)	cloud-based proactive network and system vulnerability scanning tool
Respond (RS)	open source	iptables firewall	stateful inspection firewall
	open source	secure configuration manager / Puppet Enterprise	creation, continuous monitoring, and maintenance of secure server and user hosts
	RSA	Archer GRC	centralized enterprise, risk and compliance management tool
Recover (RC)	open source	URbackup	online remote backup system used to provide disaster recovery
	RSA	Archer GRC	centralized enterprise, risk and compliance management tool

The architecture for this example solution (see Section 5) contains many applications supporting the security of the enterprise which, in turn, secure the EHR and mobile device systems. While the products that we used in our example solution are for reference purposes, organizations are encouraged to implement the security controls in this guide. We recognize that wholesale adoption of these security controls may not align with every organization's priorities, budget, or risk tolerance. This document is designed to be modular to provide guidance on implementation of any subset of the capabilities we used. In addition, organizations should check that the cloud provider secures their enterprise appropriately and consistently with the organization's risk assessment. See Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section 8, for a list of questions you can use with your third-party provider.

5 Architecture

In this section we show:

- high-level security strategies used to create our architecture
- the architecture diagram and how security characteristics map to the architecture
- important security features employed to achieve the target security characteristics

5.1 Methodologies

The following methodologies were used to select capabilities for this reference design.

5.1.1 Defense-In-Depth

A defense-in-depth strategy includes defending a system against attack using several independent methods. While these methods and security systems may, or may not, directly overlap security domains, they still provide a layered defense against threats. Our defense-in-depth strategy is focused on protecting the electronic health record management system.

5.1.2 Modular Networks and Systems

The design is modular to support change and growth in the enterprise, such as the addition of medical devices. The architecture is easily modified to allow for changes in products and technologies, and best practices. For example, if new security technologies emerge, the architecture can be altered with minimal effort.

5.1.3 Traditional Engineering Practices

The development of our architecture and the build of the reference design are based on traditional system engineering practices: identify a problem, gather requirements, perform a risk assessment, design, implement, and test.

5.2 Architecture Description

Figure 3 illustrates the project's simulated health IT enterprise for the Health Care Organization and its five main parts:

1. Data Center
2. Radiology Department
3. Dr. Jones Orthopedics (specialty practice)

4. Virtual private network
5. Third-party cloud services providers

The Data Center is the main data center for the organization and provides access to the Internet; the organizations and VPN are areas of the architecture where mobile devices are used internal or external to the Health Care Organization; and the third-party cloud services providers represent applications used in the cloud through the Internet. The overall architecture shows how health service providers access the IT enterprise.

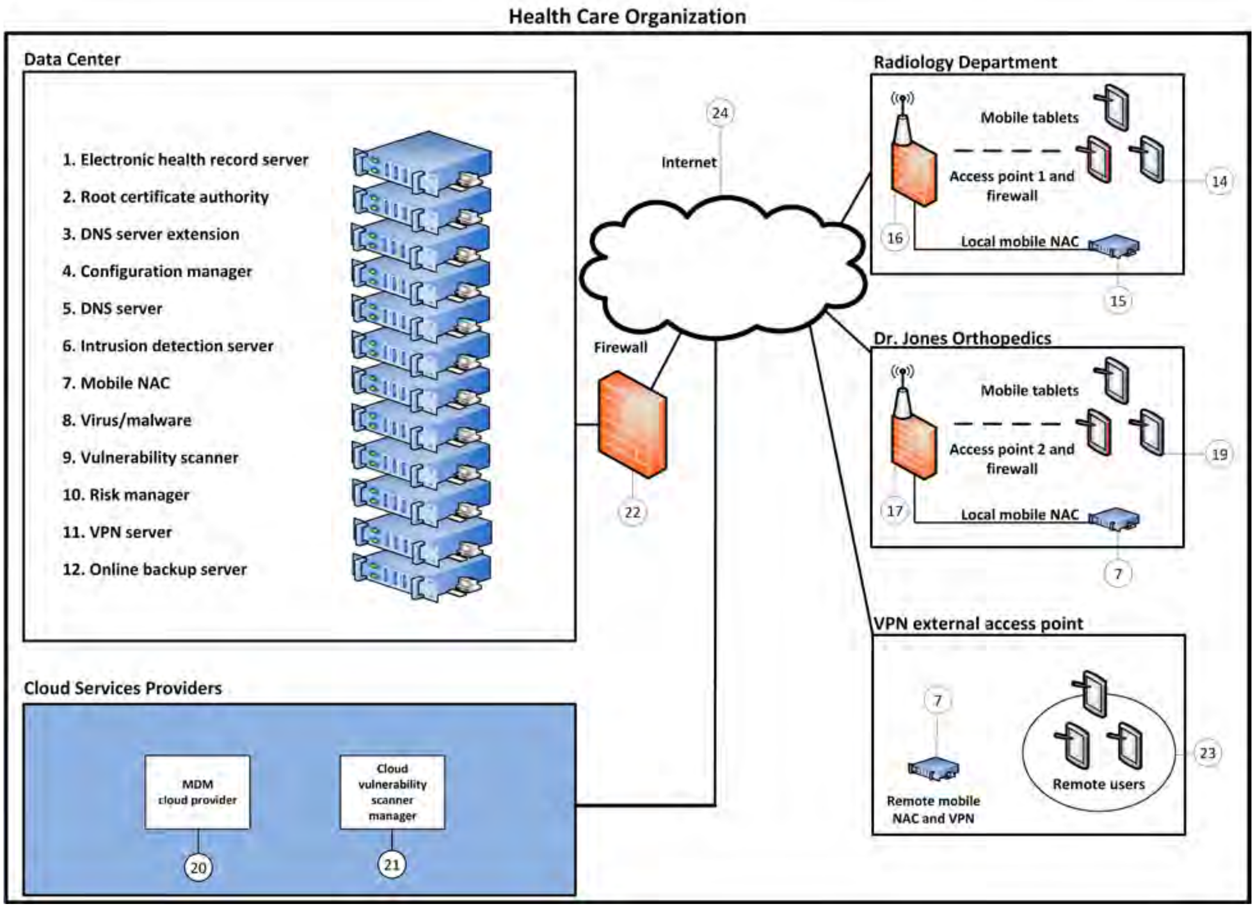


Figure 3: Architecture for the secure exchange of electronic health records on mobile devices in a health care organization

5.2.1 Organizational Architecture

Organizations that might implement this reference design vary. In the architecture, we consider both small practices and remote offices (e.g., Dr. Jones Orthopedics) and sub-organizations (e.g., a radiology department).

5.2.1.1 *The Server Room*

The Data Center represents the central computing facility for a health care organization. It typically performs the following services:

- electronic health record Web portal – provides the electronic health record server, i.e., OpenEMR service (#1)

- identity and access services – provides identity assurances and access to patient health information for users with a need to know through use of root certificate authorities, authentication, and authorization services (#2)
- domain name system (DNS) services – provides authoritative name resolution for the Data Center, Radiology Department, and Dr. Jones Orthopedics (#3 and #5)
- firewalls – provides perimeter and local system protection to ports and protocols both locally and for each health organization as a service, if needed (#22 is the main firewall)
- wireless access point (AP) policy decision point (PDP) services – provides remote enforcement and management of user access to access points (APs) (#16 and #17)
- mobile device management – provides remote cloud-based mobile device policy management (#20)
- host-based security – provides enterprise management of virus and malware protection (#8, virus/malware)
- remote VPN connectivity – provides strong identity and access controls, in addition to confidentiality of patient health information, using network encryption for transmissions. Used to facilitate secure and confidential communications between patients, doctors, and health care administrators who are not on premises (#11)
- configuration manager – facilitates an ability to create secure system configurations (#4)
- online backup manager – creates logical offsite backup for continuity of operations purposes (#12)
- intrusion detection system (IDS) – monitors network for known intrusions to the Data Center network, Radiology Department, and Dr. Jones Orthopedics (#6)
- remote mobile network access control (NAC) – remotely manages, authenticates, and authorizes identities and access for OpenEMR and wireless APs (#7)
- vulnerability scanner – scans all server systems for known vulnerabilities and risks (#9)
- risk manager – determines risk factors using Risk Management Framework,[15] NIST controls, HIPAA guidance, and physical device security posture (#10)

5.2.1.2 Radiology Department

In our simulated environment and scenarios, the Radiology Department wants to outsource some of its IT services, but may want to bring more services in-house as its IT expertise matures. The Data Center supports this department for some of its outsourced services.

[15] Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, NIST Special Publication 800-37, Rev. 1,June 2014, http://dx.doi.org/10.6028/NIST.SP.800-37r1 [Accessed July 14, 2015].

The members of the Radiology Department have a general system administrator's understanding of IT networks. This organization has already implemented most of the traditional client server environment components, including domain, role-based access, file sharing, and printing services.

Members of this organization are capable of managing its current infrastructure, but any new or cutting-edge technologies are outsourced to consultants or cloud services.

The Radiology Department locally manages:

- identity and access services
- firewall (#16)
- wireless access points (#16)

The Radiology Department seeks consultants or uses cloud services for:

- mobile device management (MDM; #20)
- mobile device policy creation (#20)
- certificate authority (#2)
- virus and malware scanning (#8)
- remote VPN connectivity to OpenEMR

5.2.1.3 Dr. Jones Orthopedics

Dr. Jones Orthopedics out sources IT technology and services to an external organization. Dr. Jones would use the questionnaire in Volume 1800-1e of this publication, Risk Assessment and Outcomes, Section 8, as a means to assess and hold accountable its service provider for the implementation of security controls.

The services and servers below are managed offsite by the Data Center:

- identity and access services
- firewall
- wireless access points
    - mobile device policy creation
    - certificate authority
    - virus and malware scanning
    - remote VPN connectivity to OpenEMR

5.2.1.4 VPN

The virtual private network allows access from a public network to a private network by using a client server technology to extend the private network.

5.2.1.5 Third-Party Cloud Service Providers

Third-party cloud service providers serve the enterprise from the cloud. In this build, the MDM and the cloud vulnerability scanner manager are the two applications in the cloud.

5.3 Security Characteristics

This section provides additional details for each of the security characteristics.

5.3.1 Access Control

Below are important features that restrict access to a resource. Figure 4 shows user and system identity access controls.

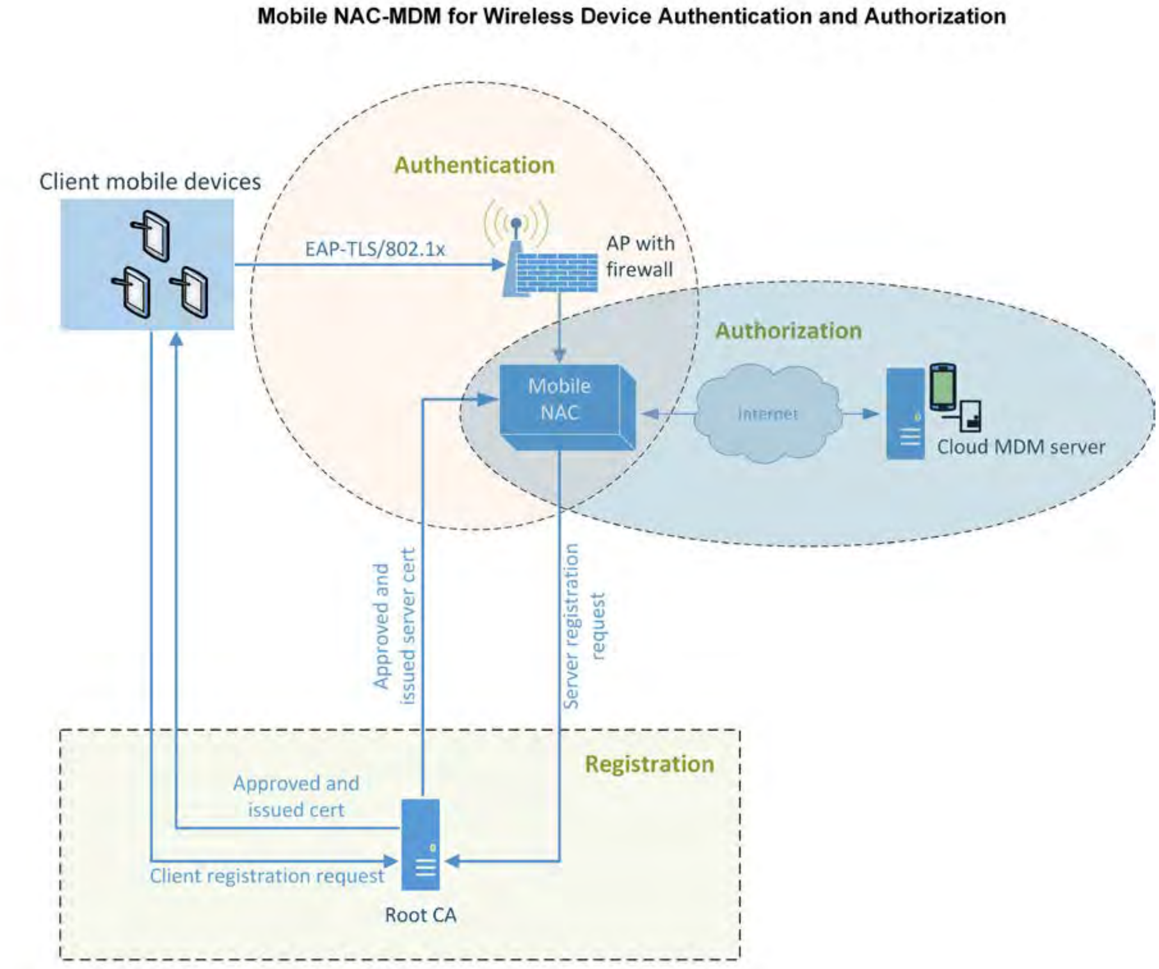


Figure 4: User and system identity access controls

- network access control – firewalling, application, or user roles are used to limit access to the needed resources for a notional administrator or patient to use the system at all segments and service components within the build architecture
- multifactor authentication – each system where a typical patient, doctor, or health IT administrator must interact with patient records, systems, or networks, requires at least a certificate, user name, and password to access
- least privilege access control for maximum security – a user of a system has enough rights to conduct authorized actions within a system. All other permissions are denied by default

In any build, every component can implement access control. In this particular build, the mobile devices, access points, firewalls, mobile NAC, certificate authority, and electronic health record server have access controls implemented. These access controls were implemented in the NCCoE reference design. How they are implemented in actual health care organizations can have an impact on system ease of use – which may require work-arounds for certain emergency situations.

5.3.2 Audit Controls and Monitoring

- user audit controls – simple audits are in place. While additional security incident and event managers (SIEM) and system log aggregation tools are recommended to maximize security event analysis capabilities, aggregation and analytics tools like these are considered out of scope for this iteration.
- system monitoring – each system is monitored for compliance with a secure configuration baseline. Each system is also monitored for risks to known good secure configurations by vulnerability scanning tools. Specific user activity monitoring for mobile devices was not a capability provided by the vendors participating in this project; however, the MDM tool can monitor changes in users' devices, in accordance with an organization's policy. The MDM device can also monitor the geographical location of users if a company policy dictates conformity with geospatial requirements. The auditing of data center staff was considered out of scope for this reference design since the absence of actual data center staff made auditing their behavior impractical.

5.3.3 Device Integrity

- server security baseline integrity – server service device integrity in the notional Data Center is achieved via creation and continuous monitoring of a secure baseline for each server. Mobile device integrity is achieved via continuous monitoring of the mobile policy implemented on each device by the MDM.
- encryption of data at rest – all systems that serve, manage, and protect systems that serve patient information use disk encryption. All archived patient information and server system files are stored offsite/remotely via encrypted communication with a backup service.

5.3.4 Person or Entity Authentication

NAC and application person or entity authentication – at each point where a typical patient, provider, or health IT administrator must access a network or information, the person or device entity is challenged using strong authentication methods.

5.3.5 Transmission Security

All communication between a typical patient, doctor, health IT administrator, and the electronic health record system is protected via Internet Protocol Security or secure sockets layer encryption (e.g., transport layer security, TLS).

NIST CYBERSECURITY PRACTICE GUIDE HEALTH IT

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

How-To Guides

For Security Engineers

Gavin O'Brien
Sue Wang

Brett Pleasant
Kangmin Zheng
Nate Lesser

Colin Bowers
Kyle Kamke

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1c

DRAFT

NIST Special Publication 1800-1c

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

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

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 1800-1c
Natl. Inst. Stand. Technol. Spec. Publ. 1800-1c, 82 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 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 publicly 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 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

mobile devices. The scenario considered is that of a hypothetical primary care physician using 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
Sallie Edwards	MITRE
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 demonstrates 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** ⬅ **YOU ARE HERE**
- 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

2 Introduction

The following guides show IT professionals and security engineers how we implemented this example solution for securing the transfer of electronic health records on mobile devices. We cover all the products employed in this reference design. We do not recreate the product manufacturer's documentation, which is presumed to be widely available. Rather, these guides show how we incorporated the products together in our environment.

These guides assume that you have experience implementing security products in a health care organization. While we have used the commercially available products described here, we assume that you have the knowledge and expertise to choose other products that might better fit your IT systems and business processes.[1] If you use substitute products, we hope you'll seek products that are congruent with standards and best practices in health IT, as we have. Refer to NIST SP 1800-1d: Standards and Controls Mapping, Section 5, Table 2, for a list of the products that we used mapped to the cybersecurity controls provided by this reference design, to understand the characteristics you should seek in alternate products. NIST SP 1800-1d, Section 4, Security Characteristics and Controls, Table 2 describes how we arrived at this list of controls.

This NIST Cybersecurity Practice Guide does not describe "the" solution, but a possible solution. This is a draft version. We are seeking feedback on its contents and welcome your

[1] 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.

input. Comments and suggestions will improve subsequent versions of this guide. Please contribute your thoughts to hit_nccoe@nist.gov, and join the discussion at http://nccoe.nist.gov/forums/health-it.

The National Cybersecurity Center of Excellence (NCCoE) response to the problem of securing electronic health care information on mobile devices has been to take the following actions:

- The NCCoE developed an example solution to this problem using commercially available products that conform to Federal standards and best practices.
- This example solution is packaged as a "How To" guide. In addition to helping organizations comply with Health Insurance Portability and Accountability Act (HIPAA), the guide demonstrates how to implement standards-based cybersecurity technologies in the real world, based on risk analysis.

Conventions

Filenames, pathnames, partitions, URLs, and program names are in italic text:

filename.conf

…/folder/filename.conf

http://nccoe.nist.gov

Commands and status codes are in `Courier`:

```
mkdir
```

Code that a user inputs is in **Courier bold**:

```
service sshd start
```

> This guidance is applicable to the build that the NCCoE completed. These are not comprehensive tutorials. There are many possible service and security configurations for these products that are out of scope for this reference design.

3 Basic Network Infrastructure Services

Basic network infrastructure services exist throughout the architecture and consists of all switching and routing protocols related to layer 2 and layer 3 of the Open Systems Interconnection (OSI) model. Additional fully qualified domain name (FQDN) resolution, and wireless access services are in this section of the network. These components facilitate network traffic throughout the enterprise and interconnect systems.

3.1 Hostnames

This section references all fully qualified domain names and IP addresses used in this build. The information here can be used to build an exact duplicate of the architecture used in this build.

You do not have to use this host-naming convention or IP structure to successfully deploy this example solution. If, however, you change any of the hostnames while setting up other products mentioned in this guide, you should make the appropriate hostname changes to the configuration files for those products.

Capability Name	Hostname/FQDN	IP
OpenEMR	openemr1.healthisp.com	192.168.200.80
Fedora PKI Manager	healthitca.healthisp.com	192.168.200.73
Bind DNS and DNSE	healthitdns.healthisp.com	192.168.200.86
	healthitdnse.healthisp.com	192.168.200.85
Puppet Enterprise	puppet.healthisp.com	192.168.200.88
Security Onion IDS	healthitids.healthisp.com	192.168.200.98
Cisco ISE 1 and 2	healthitise1.healthorg1.org	10.10.101.101
	healthitise2.healthorg2.org	192.168.100.87
Symantec Endpoint Protection	healthithostprotect.healthisp.com	192.168.200.93
Vulnerability Scanner	healthitscancon.healthisp.com	192.168.100.95
RSA Archer	healthitriskman.healthisp.com	192.168.200.200
VPN Server	healthitvpn.healthisp.com	192.168.200.250
Health ISP External Firewall	healthitfirewall.healthisp.com	192.168.200.254
		192.168.100.87
Cisco AP 1	healthitorg1fw.healthitorg1.org	192.168.100.101
		10.10.101.1
Cisco AP 2	healthitorg1fw.healthitorg1.org	192.168.100.102
		10.10.102.1
URBackup Server	healthitbackup.healthisp.com	192.168.200.99
HealthIT Organization #1 Mobile Devices		10.10.101.0/24
HealthIT Organization #2 Mobile Devices		10.10.102.0/24

3.2 Bind DNS and DNSE Installation and Hardening

The Bind DNS application is based on a distributed hierarchical naming system for computers, services, or any IP based system resource connected to a public or a private network. This build utilized both an internal and external DNS server. Each was named DNS for internal and DNSE for external host resolution. This implementation forms what is known as split-DNS or spilt-brained DNS. Use of this implementation approach provides security separation of name to IP resolution. Used effectively it will essentially protect a private (RFC-1918) network from being enumerated by unauthorized external users via DNS lookups. Additionally, if an external unauthorized user attacks the external DNS the internal DNS will continue to function.

This section will show you how to install and configure both DNS servers then integrate them with the internal firewall, puppet and all other hosts on this build that need FQDN resolution.

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 5.2, Puppet Enterprise Configuration

3.2.1 Bind DNS Setup

> You can install Bind in several ways, such as with Linux installers like *apt-get*, *yum* and *rpm*. We used *yum*. If you install Bind using *yum,* you must either have admin/root privilege or use `sudo` to run the following commands. We recommend that you run all commands with `sudo`, rather than at the root terminal.

To install Windows Dynamic updates to Bind, see *https://support.microsoft.com/en-us/kb/275866*

Install Bind DNS by entering the following:

```
> yum install bind bind-utils
```

Configure Bind by entering:

```
> cd /var/named
```

Create DNS zone files by entering:

```
> touch dynamic/healthisp.com, healthitorg1.org, healthitorg2.org
```

Edit the zone file for the Health ISP by entering:

```
> vi dynamic/healthisp.com
```

Paste the following into *dynamic/healthisp.com:*

```
        $TTL 1D
        @ IN SOA dns.healthisp.com. admin.healthisp.com. (
                                2 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H ) ; minimum
                NS dns.healthisp.com.
                A 192.168.100.87
    www         A 192.168.200.80
    healthitvpn         A 192.168.200.250
    healthitriskman             A 192.168.200.200
    healthitca          A 192.168.200.73
    openemr1            A 192.168.200.80
    healthitdns         A 192.168.200.86
    healthitdnse        A 192.168.200.85
    dns         A 192.168.200.86
    healthitconfman             A 192.168.200.88
    puppet              A 192.168.200.88
    healthitbackup              A 192.168.200.99
```

Create the zone file for Health IT Organization #1 by entering the following:

```
> vi healthitorg1.org
```

Paste the following into *healthitorg1.org:*

```
        $TTL 1D
        @ IN SOA @ rname.localhost. (
0 ; serial
1D ; refresh
1H ; retry
1W ; expire
3H ) ; minimum
    NS @
                                A 192.168.100.87
                        www             A 192.168.100.87
            healthitise1    A 10.10.101.101
```

Create the zone file for Health IT Organization #2 by entering the following:

```
> vi healthitorg2.org
```

Paste the following into *healthitorg2.org:*

```
          $TTL 1D
          @ IN SOA @ rname.localhost. (
              0 ; serial
 1D ; refresh
 1H ; retry
 1W ; expire
 3H ) ; minimum
       NS @
                                    A 192.168.100.87
                              www   A 192.168.100.87
                              healthitise2   A 192.168.100.87
```

Open the *named.conf* configuration file for DNS by entering the following:

```
> vi/etc/named.conf
```

Paste the following into the *named.conf* file, or edit the file to look like this:

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
 listen-on port 53 { 127.0.0.1; 192.168.200.86; };
 listen-on-v6 port 53 { ::1; };
 directory "/var/named";
 dump-file "/var/named/data/cache_dump.db";
 statistics-file "/var/named/data/named_stats.txt";
 memstatistics-file "/var/named/data/named_mem_stats.txt";
 allow-query { any;};

 /*
 - If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
 - If you are building a RECURSIVE (caching) DNS server, you need to enable
 recursion.
 - If your recursive DNS server has a public IP address, you MUST enable access
 control to limit queries to your legitimate users. Failing to do so will
 cause your server to become part of large scale DNS amplification
 attacks. Implementing BCP38 within your network would greatly
 reduce such attack surface
 */
 recursion yes;

 dnssec-enable yes;
 dnssec-validation yes;
 dnssec-lookaside auto;

 /* Path to ISC DLV key */
 bindkeys-file "/etc/named.iscdlv.key";

 managed-keys-directory "/var/named/dynamic";

 pid-file "/run/named/named.pid";
 session-keyfile "/run/named/session.key";
};

logging {
 channel default_debug {
 file "data/named.run";
 severity debug;
 };
};

zone "." IN {
 type hint;
 file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

Open the named*.rfc1912.zones* configuration file by entering the following:

```
> vi/etc/named.rfc1912.zones
```

Paste the following into the *named.rfc1912.zones* file, or edit the file to look like this:

```
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
// and http://www.ietf.org/internet-drafts/draft-ietf-dnsop-default-local-zones-02.txt
// (c)2007 R W Franks
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "localhost.localdomain" IN {
 type master;
 file "named.localhost";
 allow-update { none; };
};

zone "localhost" IN {
 type master;
 file "named.localhost";
 allow-update { none; };
};

zone "1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
 type master;
 file "named.loopback";
 allow-update { none; };
};

zone "1.0.0.127.in-addr.arpa" IN {
 type master;
 file "named.loopback";
 allow-update { none; };
};

zone "0.in-addr.arpa" IN {
 type master;
 file "named.empty";
 allow-update { none; };
};

// START CUSTOM DOMAINS FOR LAB


zone "healthitorg1.org" IN {
 type master;
 file "healthitorg1.org";
 allow-update { none; };
};

zone "healthitorg2.org" IN {
 type master;
 file "healthitorg2.org";
 allow-update { none; };
};

zone "healthisp.com" IN {
 type master;
 file "dynamic/healthisp.com";
 allow-update { 192.168.200.70; 192.168.200.71; 192.168.200.83; 192.168.200.93; 192.168.200.72; };
};

zone "_msdcs.healthisp.com" IN {
 type master;
 file "dynamic/_msdcs.healthisp.com";
 allow-update { 192.168.200.70; 192.168.200.71; 192.168.200.83; 192.168.200.93; 192.168.200.72;};
```

```
    };
```

3.3 Access Point: Cisco RV220W

This build uses the Cisco business class wireless access points (AP). These business class APs have additional functions beyond normal home use APs. As an example, the APs allow enterprise connection security to enable certificated based authentication to the AP. The APs assist in facilitating mobile device connectivity to each of the remote health organization networks. Each connected mobile device can then securely connect to the EHR server using the AP connection.

This section will describe how to configure the APs with IPs, MAC address filtering and certificate based access control.

System requirements

- Two Cisco RV220W APs
- At least version 1.0.6.6 and up firmware
- A PC to connect to and configure the Web-based interface

You will also need the following parts of this guide:

- Section 3.1, Hostnames
- Section 8.2.1, MDM Setup
- Section 9.1, Cisco Identity Services Engine

3.3.1 Cisco RV220 AP Setup

We assume that you have a functional Internet connection via Ethernet.

1. Connect the Ethernet cable from the Internet to the WAN port of the RV220W.
2. Connect one end of a different Ethernet cable to one of the LAN (Ethernet) ports on the back of the unit.
3. Connect the other end to an Ethernet port on the PC that will be used to run the Web-based device manager.
4. Connect the power line and turn on the power switch.

More detailed procedures for installing the Cisco® RV220W Network Security Firewall is available from the Cisco installation guide at *http://www.cisco.com/c/dam/en/us/td/docs/routers/csbr/rv220w/administration/guide/rv220w_ag_78-19743.pdf.*

3.3.2 Post-Setup Tasks

1. Use a PC to connect to a LAN port of the Cisco RV220W. If DHCP is enabled, the PC should receive an IP address and the PC becomes a DHCP client of the RV220W. Otherwise, you may need to configure the PC to obtain an IP address from a DHCP server.
2. From the PC, use a compatible browser (e.g. Firefox) to connect to the Cisco® RV220W administration portal using the default address (192.168.1.1) and the default credentials (username “cisco” and password “cisco”).

3. After logging in to the configuration utility, click Run Setup Wizard in the navigation tree to detect and configure the Internet setting automatically. In addition to setting up the Internet connection, the setup wizard will also request that the user change the default password.

4. Verify that the IPv4 WAN setting is correctly set, which should include the IP address of the device in the WAN with proper subnet mask, default gateway, and primary DNS server IP address. If the IPv4 WAN is not configured automatically, check with the Internet service provider to obtain these required parameters and configure the Internet connection under: *Networking > WAN (Internet) > IPv4WAN (Internet)*. Be sure to specify the correct Internet Connection Type: Static IP, DHCP or other types.

5. Verify the Cisco RV 220W has the latest firmware installed:

   - Navigate to the path: *Status > System Summary* to check the software version. The current version is 1.0.6.6. If your AP firmware version is lower than the current one, update the firmware by following these steps:

     - Download the firmware from https://software.cisco.com/download/release.html?mdfid=283118607&softwareid=282487380&release=1.0.2.4&rellifecycle, and save it to a file.

     - From the Cisco RV220W configuration utility, navigate to *Administration > Firmware Upgrade.*

     - Browse to the saved download file.

     - Press the Start Firmware Upgrade button and following the instruction from the installer.

3.3.3 Cisco RV220 AP Setup for EAP-TLS Authentication

3.3.3.1 To configure LAN for IPv4

1. Use 10.10.101.0 Org1 and 10.10.102.0 Org2

2. Navigate to the path from the Configuration Utility Portal: *Network > LAN (Local Network) > IPv4 LAN (Local Network)* to setup the IPv4 LAN.

3. Change the default setting to meet your specific requirements to include:

   - IP address for this device in the LAN (e.g. 10.10.101.1)
   - subnet mask (e.g. 255.255.255.0)
   - DHCP mode for assigning IP addresses to the client connect to this LAN (e.g. DHCP server)
   - domain name (e.g. HealthITOrg1)
   - starting IP address (e.g. 10.10.101.2)
   - ending IP address (e.g. 10.10.101.25)
   - primary DNS server (e.g. 192.168.100.87)

If you want to configure a static IP address and MAC address for a known computer:

1. Use the path: *Network > LAN (Local Network) > Static DHCP***.** This will reserve the IP addresses for a list of known computer devices linked to the LAN.

2. Click Add to add an IP address and the MAC address for each computer you wish to include.

3.3.3.2 Cisco RV220 AP Wireless Setup for IPv4 LAN

1. Navigate to the path from the Configuration Utility Portal by following the path *Wireless* > *Basic Setting.*
2. Enable one of the four default preset SSIDs in the wireless Basic Setting table setting:
   - assign an SSID Name
   - disable SSID broadcast
   - enable security mode
   - enabled the MAC filter
3. Edit Security Mode:
   - Navigate to Wireless > Basic Setting
   - Select a Wireless SSID to edit the security mode
   - Click Security Setting Mode
   - In the form for required security parameters, follow the guidance for enabling WPA2 Enterprise and Encryption AES
4. Edit MAC Filtering to block devices with MAC addresses that are not registered in the AP
   - Use the path Wireless > Basic Setting
   - Select a Wireless SSID to edit the security mode
   - Click Edit MAC Filtering and Add
   - Follow the form to add the MAC addresses that you want the AP to control

3.3.3.3 Cisco RV220 AP RADIUS Server Settings

NOTE: References to the RADIUS server are synonymous with the Cisco ISE server. The radius server is a subcomponent of the Cisco ISE AAA services (Authentication, Authorization, and Accounting).

1. Navigate to the path from the Configuration Utility Portal: *Security* > *RADIUS* Server to setup the AP to communicate with the authentication server
2. Fill out details in the RADIUS configuration pages, which normally includes:
   - Authentication Server IP address – the IP address of the authenticating RADIUS server (e.g. 10.10.101.101)
   - Authentication Port – the RADIUS authentication server's port number used to send RADIUS traffic (e.g. 1812)
   - Enter the pre-shared secret that will be used between the AP and the RADIUS authenticator server
   - Timeout – the timeout interval (in seconds) after which the RV220W re-authenticates with the RADIUS server

- Retries – the number of retries for the RV220W to re-authenticate with the RADIUS server. If the number of retries is exceeded, authentication of this device with the RADIUS server has failed

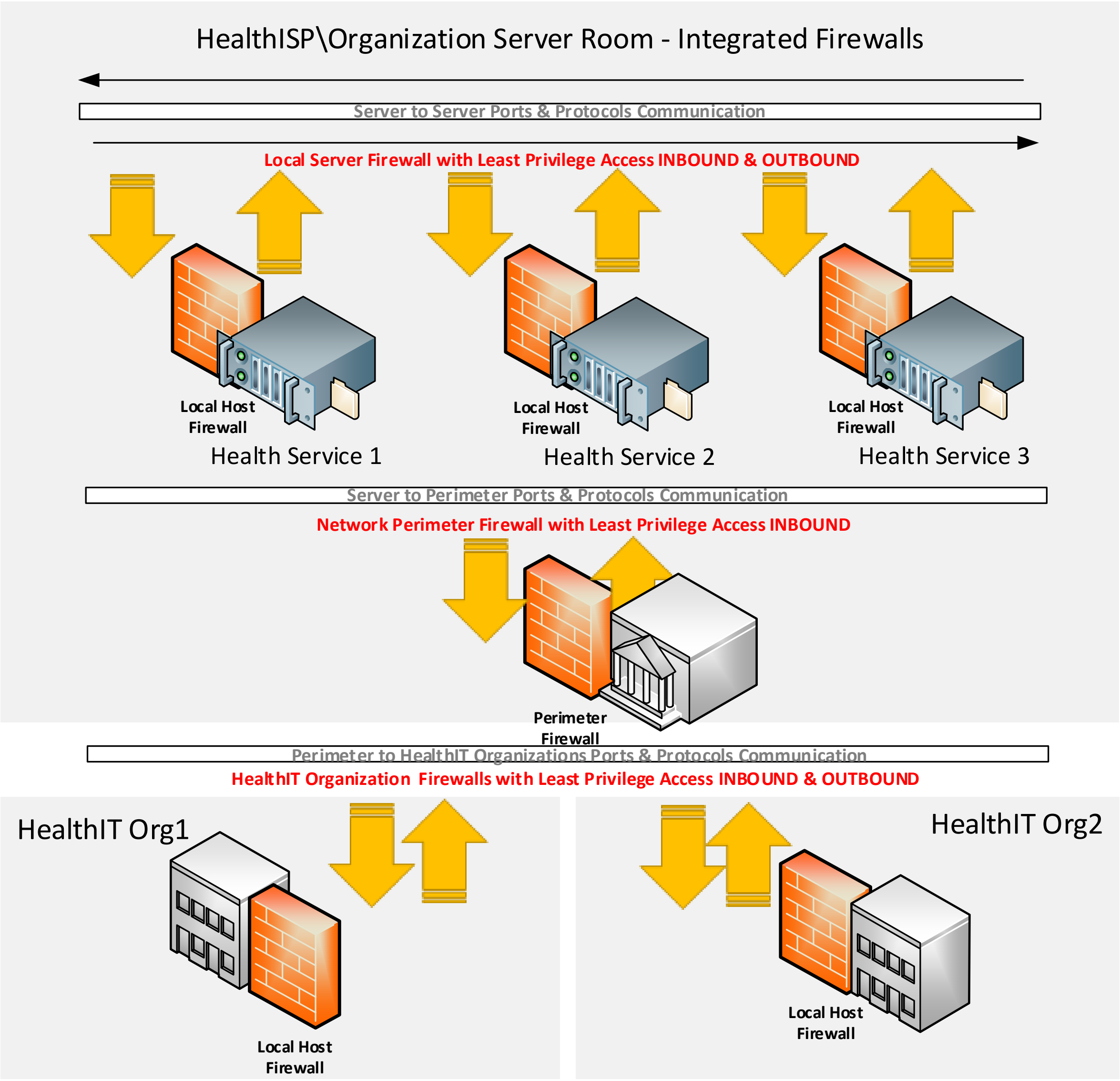
After the setup, you can use the diagnostic tools provided in the RV220W admin portal to test the connectivity between the AP and the RADIUS authentication server.

The firewall on the APs were set to the default setting for this install. This blocked all inbound traffic with exception to Internet Control Message Protocol (ICMP) traffic. All outbound traffic was allowed from internal clients. If the authentication server is installed in the cloud behind the corporate or AP firewall, you can use port forwarding to allow the AP to properly communicate with the RADIUS server. In this case, use the firewall network address as the authentication server IP address.

3.4 Firewalls: IPTables

A firewall is used to control egress and ingress network traffic between multiple subnets and or systems. A firewall will determine what traffic goes in which direction based on ip, tcp/ip or udp/ip ports and protocols. A firewall uses rules to allow or disallow traffic based on an organization’s security policy. The IPTables firewall is a Linux based firewall that uses stateful inspection to protect ports.

Each subnet and server host on this build has a firewall. The servers have local firewalls that follow a least privilege access approach for outbound and inbound traffic. Each subnet cross point between other subnets has a firewall to protect Internet traffic from traversing inbound to the internal network.


HealthISP\Organization Server Room - Integrated Firewalls
Server to Server Ports & Protocols Communication
Local Server Firewall with Least Privilege Access INBOUND & OUTBOUND
Local Host Firewall
Health Service 1
Local Host Firewall
Health Service 2
Local Host Firewall
Health Service 3
Server to Perimeter Ports & Protocols Communication
Network Perimeter Firewall with Least Privilege Access INBOUND
Perimeter Firewall
Perimeter to HealthIT Organizations Ports & Protocols Communication
HealthIT Organization Firewalls with Least Privilege Access INBOUND & OUTBOUND
HealthIT Org1
Local Host Firewall
HealthIT Org2
Local Host Firewall

System requirements

- Linux Operating System
- IPTables application installed (installed by default on most Linux systems)
- Most intel-based systems will support IPtables and Linux (see your Linux version hardware compatibility (HCL) list for more)
- If this is a system that protects multiple subnets then multiple network interface cards (NIC) for each subnet will be needed. (see your Linux OS HCL for more on multiple NIC compatibility)

You will also need the following parts of this guide:

- Section 11.2.2, Linux Post-Installation Tasks
- Section 3.1, Hostnames

IPTables Setup

Puppet Enterprise ensured the installation of IPTables and all Linux-based external firewalls for this build. No action is needed to install the local firewalls if the Puppet prerequisite has been followed below. Section 3.4 lists the files that contain the firewall rules for each Linux system used in our build.

4 Backup

The backup system is an important part of security as it assists with ensuring the architecture survives in the event of a disaster. Regular full and incremental backups provide a means of recovery in the event of a disaster. Remote online backups provide even more security as offsite backups are harder to tamper or lose in a local disaster to the architecture.

This section will show you how to install an online back-up system using URBackup.

4.1 URBackup

As described, URBackup is a remote backup system that will facilitate both full and incremental backups. It's a Web-based system designed to allow multiple administrators to manage backups to all Windows and Linux based systems

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 5.2, Puppet Enterprise Configuration

URBackup Setup

Follow these instructions to build, install, and set up UrBackup on Fedora20 Linux systems.

> If you want the URBackup Server itself to be backed up, follow this same guidance for the URBackup Server.

1. Follow Section 11.2, Linux Installation and Hardening.
2. Install the dependencies UrBackup needs:
   - If installing on Fedora 20, there is a WxWidgets app already installed. Please verify that its version is higher than 3.0.
   - On Fedora 20, you will use *yum* as your installer.
3. Input the following commands:

For this install, make sure you have allowed outbound port 80 and 443 only.

```
> yum install gcc-c++
> yum remove wxBase or wxBase3 # removes any current yum instantiations of wxBase3 so no conflicts
> yum install wxGTK3
> yum install wxGTK3-devel
> yum install wxBase3
> ln -s /usr/libexec/wxGTK3/wx-config /usr/bin/wx-config
> yum install cryptopp-devel
> wx-config # just to test if it works
> mkdir /usr/local/urbackup
> cd /usr/local/urbackup
> wget http://sourceforge.net/projects/urbackup/files/Client/1.4.7/urbackup-client-1.4.7.tar.gz/download
> mv download /usr/local/urbackup/urbackup-client-1.4.7.tar.gz
> cd /usr/local/urbackup/
> tar zxvf urbackup-client-1.4.7.tar.gz
> cd urbackup-client-1.4.7/
> ./configure --enable-headless # enable headless if you want to use the main server vs GUI on the client
```

4. Build the UrBackup client and install it:

```
> make
> make install
```

The program will return the following:

```
POST INSTALL NOTICE:
----------------------------------------------------------------------
Libraries have been installed in:
 /usr/local/lib
If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
 - add LIBDIR to the `LD_LIBRARY_PATH' environment variable
 during execution
 - add LIBDIR to the `LD_RUN_PATH' environment variable
 during linking
 - use the `-Wl,-rpath -Wl,LIBDIR' linker flag
 - have your system administrator add LIBDIR to `/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
/usr/bin/install -c -m 644 -D "./backup_client.db"
"/usr/local/var/urbackup/backup_client.db.template"
touch "/usr/local/var/urbackup/new.txt"
make[2]: Leaving directory `/usr/local/urbackup/urbackup-client-
1.4.7/urbackupclient'
make[1]: Leaving directory `/usr/local/urbackup/urbackup-client-
1.4.7/urbackupclient'
```

5. Setup communication with the server by opening *vi /usr/local/var/urbackup/data/settings.cfg* and add the following:

Make sure there are no spaces at the end of the line when you cut and paste this into the file.

```
internet_server=healthitbackup.healthisp.com
internet_server_port=55415
computername=<your backup client hostname>.healthisp.com
internet_authkey=foobar # See Note 2 in section 4 about this; remove this
                  comment when you cut and paste it in the file
internet_mode_enabled=true
```

6. Make sure that the UrBackup client can communicate with the server correctly. (Don't worry when you see authentication errors. We are only testing the ability for the client to communicate properly.)

```
> start_urbackup_client --loglevel debug --no_daemon --internetonly
```

It should connect and say "Successfully Connected" after a series of lines that fly by on the screen.

You will receive an authentication error that looks like the following:

```
2015-01-29 09:41:54: Successfully connected.
2015-01-29 09:41:54: ERROR: Internet server auth failed. Error: Unknown
client (healthitconfman.healthisp.com)
2015-01-29 09:41:54: InternetClient: Had an auth error
```

```
2015-01-29 09:41:54: ERROR: Internet server auth failed. Error: Unknown
client (healthitconfman.healthisp.com)
```

```
2015-01-29 09:41:54: InternetClient: Had an auth error
```

`> CTRL-C` to exit

Here is the fix:

UrBackup also allows manually adding clients and manually configuring the shared key. Follow these steps to add such a client:

- Log into the URBackup server via the Web link *http://yourhost.yourdomain.com:55414*
- Go to the “Status” screen.
- Under “Internet clients” enter the FQDN name of the laptop/PC you want to add. This must be the fully qualified computer name (i.e. the one you see in the advanced system settings) or the computer name configured on the client.
- After pressing “add” there will be a new client in the “Status” screen. Go to the "Settings" section then use the drop down "Client" menu to select the newly added client there.
- In the Internet settings view the authentication key for that client. Copy the key and go back to the client then edit the */usr/local/var/urbackup/data/settings.cfg* file on the client. Add the authentication key to the setting in that file.
- The server and client should now connect to each other. If it does not work the client shows what went wrong in the “Status” window.
- Test the fully authenticated connection again:

  ```
  > sudo start_urbackup_client --loglevel debug --no_daemon --
  internetonly
  ```

You should now see a success message. Just `CTRL-C` out of it and move to the next step.

7. Start the UrBackup client backend on startup using the following for Fedora20:

   ```
   > vi /lib/systemd/system/urbackup-client-backend.service
   ```

   Add the following to the file *urbackup-client-backend.service*

   ```
   [Unit]
   Description=Starting backend client services for URBackup client
   After=syslog.target network.target

   [Service]
   Type=forking
   NotifyAccess=all
   PIDFile=/run/urbackup_client.pid
   ExecStart=/usr/local/sbin/start_urbackup_client
   ExecStop=/usr/local/sbin/stop_urbackup_client
   ```

```
[Install]
WantedBy=multi-user.target
```

Change Permissions

```
> chmod 755 /lib/systemd/system/urbackup-client-backend.service
```

Create Stop Client Process File

```
> vi /usr/local/sbin/stop_urbackup_client
```

Add the following to the stop_urbackup_client file

```
#!/bin/bash

if [ -f /var/run/urbackup_client.pid ]; then
        /usr/bin/kill `cat /var/run/urbackup_client.pid`
else
        echo ""
         echo "URBackup Client is not running!!!"
         echo ""
fi
```

Make symbolic link

```
> cd /etc/systemd/system/
> ln -s /lib/systemd/system/urbackup-client-backend.service
```

Make systemd take notice of it

```
> systemctl daemon-reload
```

Activate a service immediately

```
> service urbackup-client-backend start
```

Or

```
> systemctl start urbackup-client-backend.service
```

Enable a service to be started on bootup

```
> chkconfig urbackup-client-backend on
```

Or

```
> systemctl enable urbackup-client-backend.service
```

8. Start the UrBackup client backend on startup using the following for CentOS and other Linux OSs that still use init scripts:

   Edit rc.local

   ```
   > vi /etc/rc.d/rc.local
   ```

Paste the following into that file

/usr/local/sbin/start_urbackup_client

To start immediately, run

```
> start_urbackup_client
```

9. Configure the client backup files, images, time intervals and increments, and custom backup locations and other settings for each client:
    - Log into the URBackup server Web portal.
    - Use the client dropdown menu and select the client you want to set custom settings for this configuration.
    - Select the "Separate settings for this client" radio button and begin edits.
    - Save your settings after each section you edit.

10. Make sure local client firewall rules allow inbound and outbound for URBackup. Fedora 20 server clients and `iptables` command:

```
      /sbin/iptables -A OUTPUT -p tcp --dport 55415 -m state --state NEW -d
192.168.200.99 -j ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 35621 -m state --state NEW -s
192.168.200.99 -j ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 35623 -m state --state NEW -s
192.168.200.99 -j ACCEPT

      iptables -A INPUT -p icmp --icmp-type 8 -s 0/0 -m state --state
NEW,ESTABLISHED,RELATED -j    ACCEPT
```

11. Make sure URBackup Server has firewall rules to allow inbound and outbound rules

```
      /sbin/iptables -A OUTPUT -p tcp --dport 35621 -m state --state NEW -d
192.168.200.0/24 -j ACCEPT

      /sbin/iptables -A OUTPUT -p tcp --dport 35623 -m state --state NEW -d
192.168.200.0/24 -j ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 55415 -m state --state NEW -j
ACCEPT

      /sbin/iptables -A INPUT -p tcp --dport 55414 -m state --state NEW -j
ACCEPT
```

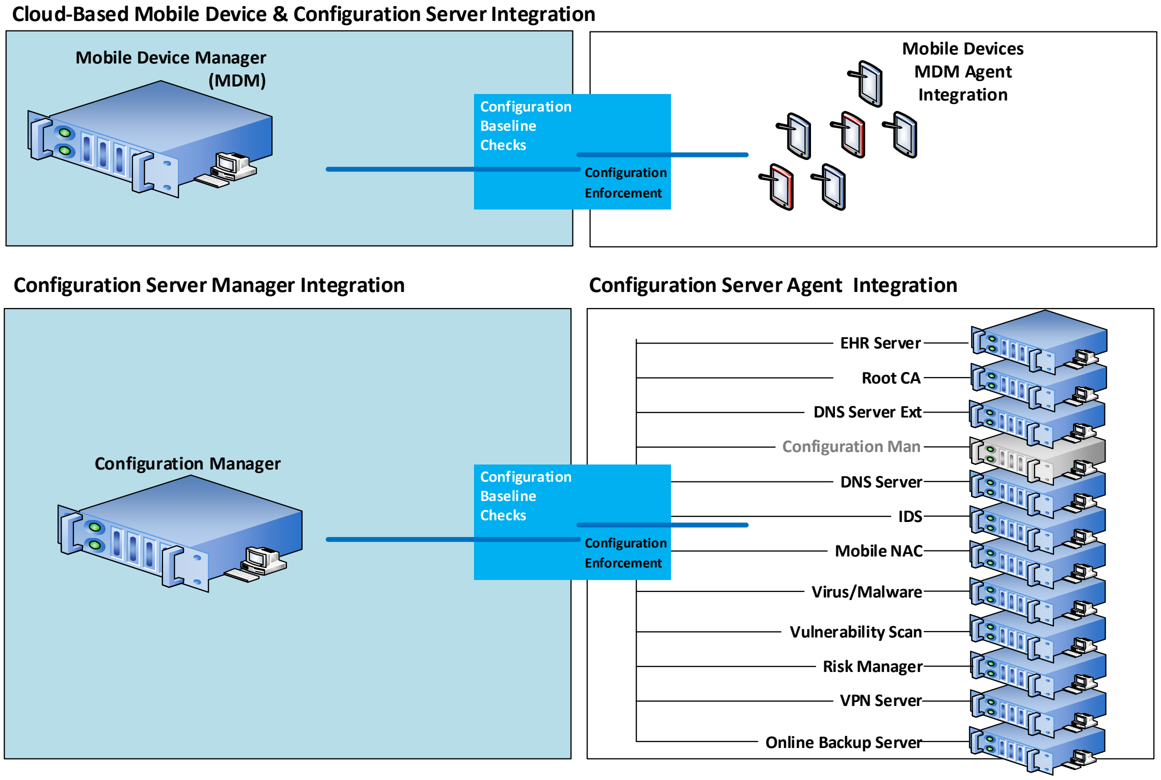
5 Configuration Management

Understanding, implementing and maintaining a secure baseline for all systems that process and store PHI is critical to its security. In the event that a configuration becomes corrupt or unusable the configuration management tool provides recovery capabilities. In addition the tool can periodically validate that a configuration is correct or unchanged from its known configuration. The configuration management tool selected for this build offers the following options:

- Secure Configuration Baseline Creation
- Automated Secure Configuration Baseline Maintenance

- Automated Secure Configuration Baseline Compliance
- Secure Configuration Baseline Reporting

System Security Baseline and Configuration Management System


Cloud-Based Mobile Device & Configuration Server Integration
Mobile Device Manager (MDM)
Configuration Baseline Checks
Configuration Enforcement
Mobile Devices MDM Agent Integration
Configuration Server Manager Integration
Configuration Server Agent Integration
Configuration Manager
Configuration Baseline Checks
Configuration Enforcement
EHR Server
Root CA
DNS Server Ext
Configuration Man
DNS Server
IDS
Mobile NAC
Virus/Malware
Vulnerability Scan
Risk Manager
VPN Server
Online Backup Server

System requirements

- Processor Minimum 1.4 GHz 64-bit processor
- RAM Minimum 8G
- Disk space Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames

5.1 Puppet Setup

This build uses an agent/master configuration with the default <puppet> hostname for the Puppet Master. We used the Web-based report interface in this build, although it is not normally installed with Puppet.

5.1.1 Pre-Install Tasks

Puppet Enterprise has some preparation tasks that need to be completed prior to install. For the steps to follow, see *https://docs.puppetlabs.com/guides/install_puppet/pre_install.html*

5.1.2 Install Instructions

This build used Puppet Enterprise on Fedora 20 Linux. Find install instructions for Fedora 20 at *https://docs.puppetlabs.com/guides/install_puppet/install_fedora.html*

5.1.3 Post-Install Tasks

Puppet has several post-installation tasks, including setting up its manifests, modules, and other files. Before starting the Puppet Master, follow the guidance in Section 5.2, Puppet Enterprise Configuration. We give specific guidance in Section 5.1.3 regarding changes to the Puppet Enterprise post-install documentation.

According to the post-install guidance in the Puppet Enterprise documentation, the following components can be installed as options.

> We recommend that you do NOT set up the following post-installs unless you are familiar with the security implications and advanced features.

- Automatic Puppet Master Certificate Processing – this has security implications. See note above
- Load Balancing – not needed unless your organization has a large group of agents to manage
- Puppet Manifests and Modules – This task will be completed later, but you should read this section in the Puppet Enterprise post-install documentation for the location of the directories and files needed to set up Puppet
- Configure Production Ready Web Server – this will be covered in Section 5.2.5 Puppet Enterprise Web-Based Reporting Installation and Configuration and Section 5.3, Production Web Server

5.2 Puppet Enterprise Configuration

> Puppet uses the *g* file, manifests, and modules to configure itself and other systems. While there are other files that assist with configuration of Puppet, these are the main areas where specific system configuration control is executed. This build also made use of Puppet templates to assist with creation of Linux-based files to be used in configuration management and secure baseline controls.

5.2.1 Puppet.conf

The *puppet.conf* file for the Puppet Master is in the */etc/puppet* directory. This build requires the following configuration. Cut and paste the Puppet Master *puppet.conf* configuration below into */etc/puppet/puppet.conf.*

```
[main]
    # The Puppet log directory.
    # The default value is '$vardir/log'.
    logdir = /var/log/puppet

    # Where Puppet PID files are kept.
    # The default value is '$vardir/run'.
    rundir = /var/run/puppet

    # Where TLS certificates are kept.
    # The default value is '$confdir/tls'.
    tlsdir = $vardir/tls
        server = puppet.healthisp.com
[agent]
    # The file in which puppet stores a list of the classes
    # associated with the retrieved configuration. Can be loaded in
    # the separate ``puppet`` executable using the ``--loadclasses``
    # option.
    # The default value is '$confdir/classes.txt'.
    classfile = $vardir/classes.txt

    # Where puppetd caches the local configuration. An
    # extension indicating the cache format is added automatically.
    # The default value is '$confdir/localconfig'.
    localconfig = $vardir/localconfig
    report=true
[master]
    reports=store,http
    reporturl=http://puppet.healthisp.com:3000/reports/upload
```

5.2.2 Manifests

Manifests are files that consist of Puppet application code language. Those familiar with functions and classes in other programming languages may find the code in Puppet familiar.

Learn more about manifests at *https://docs.puppetlabs.com/pe/latest/puppet_modules_manifests.html*

The following list describes each manifest used in this build. The specific files can be found in the online file repository for this use case at *https://nccoe.nist.gov/sites/default/files/nccoe/manifests.zip*.

Once downloaded, the files should be moved to the */etc/puppet/manifests* directory of Puppet Master. The files will not work if the hostnames for each system have been changed from the hostnames provided in the Section 3.1, Hostnames.

The following customized Puppet enterprise manifests were configured and installed in this build:

site.pp – this is the main configuration file for Puppet. This is the launch point for all other manifests. There are custom class entries in this file for specific Windows configurations. However, most of this file consists of manifests imports and calls to predefined classes created in each manifest.

- *accounts.pp* - this allows control over users who can log in and also controls the password. If an attacker changes any of the information in the *passwd* file then Puppet will change back based on the entries in this file.
- *crontabconfig.pp* - this file creates tasks that run automatically at set intervals. In this case there are four tasks that are executed to secure Linux.
  - *Logoutall.sh* - this task will run every few seconds and kill all other user tasks with exception of root. This effectively removes normal users from all the Linux systems while they are in production mode
  - *puppetagent.config.base.sh* – this task will periodically run the Puppet agent to update any changes to the configuration of the local system based on a remote Puppet Master configuration change.
  - *yum.config.base.sh* – this task will force the local system to update itself during set a time every day.
  - *harden.os.single.commands.sh* – this is a series of single commands to ensure changes to permissions on critical system files, disable root console or other one line commands are issued.
- *firewall_rules.pp* - this creates and enforces individual *iptables* rules on each local Linux host in accordance with the least access needed in or out of the system.
- *grub2fedora20.pp* - this build implemented versions of Fedora 20 with the Grub2 bootloader. The bootloader assists with starting the Linux operating system and allowing the operator to make special configurations prior to the system boot process. This access can be dangerous because it will allow an attacker to boot the system into single user mode or make other changes prior to the boot process. The changes made with this Puppet manifest file create a Grub2 password challenge.
- *openemr.pp* - this will use both the `apache` and `concat` modules to configure the EHR OpenEMR Web server. It will enable TLS and OCSP.
- *openemrconcat.pp* – this file augments the *openemr.pp* file by setting up the ModSecurity Web application firewall.
- *packages.pp* - this ensures that less secure applications are removed and only the applications needed to run the service are installed on the local system.

- *passwdfile.pp* - this cleans the *passwd* file of standard users that come with the Fedora 20 Linux distro. It also cleans the group file.
- *puppet.pp* – this sets up the Puppet reporting feature.
- *securettyfile.pp* - this creates a new *securetty* file in the local system that prevents root from logging into a console session.
- *ssh.pp* - this hardens the encrypted remote management service for Linux.
- *time.pp* - this forces the local system to use a time server for accurate time. This creates accurately time-stamped logs.
- *warningbanners.pp* - this creates warning banners at the console and remote login sessions that warn users that their sessions should be authorized and monitored. This banner should act as a deterrent for good people accidentally doing bad things. It will in no way stop a determined attacker under any circumstances.

5.2.3 *Templates*

Puppet templates are used in this build to create configuration files for systems. As an example, if the *sshd_config* file already existed on a Linux system running *ssh*, Puppet would recreate the *sshd_config* file according to our templates. Another example is that all of the local system and Health ISP perimeter firewall rules are in the templates directory. If new rules or policies for all systems managed by Puppet need to be changed, the templates can be updated in one central location. Puppet templates can be configured with the *erb* Puppet language. This build used simple text commands that are native to the application configured by the template. For example, the *iptables* template uses *iptables* configuration language to configure the firewall on each system.

All of the templates used this this build can be downloaded from the following link: *https://nccoe.nist.gov/sites/default/files/nccoe/templates.zip*.

Once you download the templates, move them to the */var/lib/puppet/templates* directory. The templates directory may need to be created using the `mkdir` command.

The following list provides descriptions of each template file.

- puppet agent cron – periodic tasks to run Puppet agent
  - *puppetagent_config_base.erb*
  - *logoutall_CENTOS_config_base.erb*
  - *logoutall_config_base.erb*
  - *logoutall_daytime_config_base.erb*
  - *government_motd_motd_file.erb*
  - *government_motd_issue_file.erb*
  - *passwd_group_file_edit_data.erb*
- account lockout – locks out certain non-root users during production run time
- message of the day - unauthorized use warning banner
- password file clean up **–** removes default users and groups from Linux
  - *passwd_group_remove_script.erb*

- boot lockdown – adds grub password to system boot up and prevents single sign-on ability
  - *grub_lockdown_password.erb*
  - *grub2_lockdown_password.erb*
- single line hardening commands - a series of permissions and other changes to the system to harden it against attacks
  - *harden_os_single_commands.erb*
- local and perimeter firewall rules – all firewall rules for each system used in this build
  - *dns_firewall_base_rules.erb*
  - *dnse_firewall_base_rules.erb*
  - *healthitbackup_firewall_base_rules.erb*
  - *openemr1_firewall_base_rules.erb*
  - *puppet_firewall_base_rules.erb*
  - *healthitca_firewall_base_rules.erb*
  - *healthitfirewall_firewall_base_rules.erb*
- root console login deny – prevents root from logging in at the local console and an attacker from attempting a brute-force attack at the console
  - *securetty_devicelogin_config.erb*
- linux system updates - creates script for *cron* to run *yum* updates to Linux systems
  - *yum_config_base.erb*

5.2.4 Modules

Multiple manifests combine to make up modules in Puppet. There are communities of people who maintain a large array of Puppet modules. When installed via the following process, Modules are stored in the */etc/puppet/modules* directory.

They can be found at *https://forge.puppetlabs.com/.*

Modules can also be viewed, downloaded, and installed by the Puppet Master using the following commands at the Puppet Master command line interface:

```
> puppet module list
# Lists all installed modules

> puppet module search apache
# puppet will search and list Apache modules.

> puppet module install puppetlabs-apache –version
# puppet will install here
```

Learn more about Modules at *https://docs.puppetlabs.com/pe/latest/puppet_modules_manifests.html*

Our example solution used the following Puppet modules. Use the commands above to install them.

- *puppetlabs-apache* – streamlined creation of Web services using Apache

- *puppetlabs-mysql* – streamlined edits of *mysql* with minimal configuration
- *puppetlabs-concat* - allows creation of configuration files based on concatenation
- *puppetlabs-ntp* – provides an ability to manage standard time on systems
- *puppetlabs-registry* – allows edits to the Windows registry for configuration
- *puppetlabs-stdlib* – this is the standard library for resources on Puppet

5.2.5 Puppet Enterprise Web-Based Reporting Installation and Configuration

Find the full installation documentation at *https://docs.puppetlabs.com/dashboard/manual/1.2/configuring.html*

Short Version:

Run the following on your Puppet Master:

```
> yum install puppet-dashboard
```

Add the following to *puppet.conf* on each Puppet Agent:

```
[agent]
        report = true
```

Add the following to *puppet.conf* on the Puppet Master

```
[master]
 reports = store, http
 reporturl = http://dashboard.example.com:3000/reports/upload
```

Run the following commands on the Puppet Master:

```
> puppet-dashboard rake cert:create_key_pair
> puppet-dashboard rake cert:request
> puppet-dashboard rake cert:retrieve
```

5.3 Production Web Server

These instructions are for a non-production environment like ours. Because a production-ready reporting server is a best practice, it may be beneficial to learn more about that once you become familiar with Puppet Enterprise. Visit the following link: *https://docs.puppetlabs.com/guides/install_puppet/post_install.html#configure-a-production-ready-web-server.*

6 Intrusion Detection System (IDS)

An Intrusion Detection Server monitors a network for known threats to an organizations network. It will examine every packet it sees, then deconstruct the packet looking for header and/or payload threats. Usually, most IDS servers will utilize a packet reassembly mechanism to limit the effects of fragmented attacks as well as normal TCP transmission analysis.

6.1 Security Onion

Security Onion is the IDS selected for this build. It was selected based on its track record in the open source community for its support to SNORT and built in Web-based administration functions.

IDS Supporting Applications and Services

- **Squert** – a Web application that is used to query and view event data stored in a Sguil database (typically IDS alert data). Squert is a visual tool that attempts to provide additional context to events through the use of metadata, time series representations and weighted and logically grouped result sets. The hope is that these views will prompt questions that otherwise may not have been asked.
- **Sguil** – used as a database for IDS alerts
- **ELSA** – adds and ability to normalize logs and assists in searching a large set of alerts
- **Snorby** – integrates with Snort and allows reporting of sensor data on a daily, weekly and monthly basis.

System requirements

- The Security Onion IDS runs on Ubuntu Linux
- Hardware requirements can be found at https://code.google.com/p/security-onion/wiki/Hardware
- Find the ISO image full version at https://code.google.com/p/security-onion/wiki/QuickISOImage
- Find the Install Version for Ubuntu Linux at https://code.google.com/p/security-onion/wiki/InstallingOnUbuntu

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames

Security Onion Setup

We followed the documentation provided by Security Onion:

- Introduction *https://code.google.com/p/security-onion/wiki/IntroductionToSecurityOnion*
- Production install steps *https://code.google.com/p/security-onion/wiki/ProductionDeployment*

- Booting issues
  https://code.google.com/p/security-onion/wiki/TroubleBooting
- Post-Installation
  https://code.google.com/p/security-onion/wiki/PostInstallation

7 Certificate Authority

The certificate authority uses the OpenSSL cryptographic libraries to create then sign soft certificates for use in identifying mobile devices that would ultimately connect to both the AP and the OpenEMR server. The certificate authority is also the trusted signatory of the OpenEMR Web server certificate. In a transaction where a certificate is used as an identity, all participants must ultimately trust the signatory of the presented certificate. This build relies heavily on a certificate authority. Using a Public Key Infrastructure approach is among the strongest methods to assure proper identity and access control for PHI.

7.1 Fedora PKI

The certificate authority used for this build is based on a Linux PKI Manger used in Fedora, RedHat Enterprise and other production class Linux distros.

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 3.2, Bind DNS and DNSE Installation and Hardening
- Section 5.2, Puppet Enterprise Configuration

Fedora PKI Installation

Fedora PKI Manager Installation instructions can be found at *http://pki.fedoraproject.org/wiki/Quick_Start*

7.2 Post-Installation

Fedora PKI Manager Administrator set-up instructions can be found at *http://pki.fedoraproject.org/wiki/CA_Admin_Setup*.

To manually create user/device certificates, follow the steps in Section 8, Mobile Device Manager, or the instructions at *http://pki.fedoraproject.org/wiki/User_Certificate*.

To approve the certificate request, use the Web administrator's interface, as described below. You can use the command line, instead, if you are familiar with that method.

1. Navigate to Web Approval at *https://<your certificate authority host.domain>.com:8443*
2. Go to *Admin Services* > *Agent Services*
3. This should default to the List Requests tab. If not, click that tab on the left navigation pane.

4. Click the Find button. Once the Find page loads, there were be a list of pending requests. Select the number to approve the request.
5. Scroll to the bottom of the page, then approve or deny the request.

To retrieve the client/device certificate:

1. Navigate to *http://<your certificate authority host.domain>.com:8080*
2. Click on End Users Services.
3. Click on Retrieval Tab. This will connect to the Check Request Status Tab.
4. Enter in your certificate request reference number created during the registration request process.
5. Scroll to the bottom of the page and download

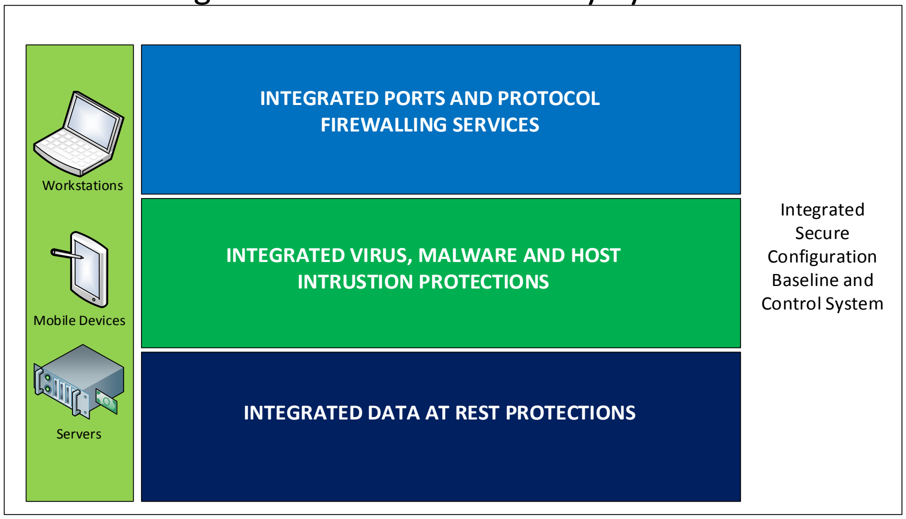
   OR

   Copy and paste the certificate information to the mobile device desktop and follow Section 8, “Mobile Device Management” for details on how to install the certificate.

8 Hosts and Mobile Device Security

Hosts and Mobile Devices combine with the basic network architecture to create the HealthIT environment used to move PHI to and from its origin. Each host on the build network is a server that provides a specific service to either secure or facilitate authorized PHI data sharing. Mobile devices are used by authorized health care professionals and patients to add, change, read or remove PHI.

Integrated Host Based Security System


Workstations
Mobile Devices
Servers
INTEGRATED PORTS AND PROTOCOL FIREWALLING SERVICES
INTEGRATED VIRUS, MALWARE AND HOST INTRUSTION PROTECTIONS
INTEGRATED DATA AT REST PROTECTIONS
Integrated Secure Configuration Baseline and Control System

This section will show you how to build and configure hosts and mobile devices securely.

8.1 Mobile Devices

The main purpose of this Practice Guide is to demonstrate how mobile devices can be used in a practical and effective cybersecurity architecture with PHI. The mobile devices in this build allow an authorized user to remotely access to PHI from anywhere. These devices must be secured so that they both protect themselves and the PHI data transmitted or stored on them.

This section will show you how to configure both Apple and Android mobile devices to successfully connect and securely protect PHI. This section will also show you how to setup the mobile devices to communicate and their security policy configurations managed by the Maas360 MDM.

System requirements

- Android device: Android operating system 4.1 and up, screen size 7” and up, and Wi-Fi enabled
- Apple devices: Apple iOS 7 and up, screen size 7” and up, with Wi-Fi enabled

You will also need the following parts of this guide:

- Section 3.3, Access Point: Cisco RV220W
- Section 7.1, Fedora PKI
- Section 8.2.1, MDM Setup
- Section 9.1, Cisco Identity Services Engine

8.1.1 Mobile Device Setup

This guide assumes that MaaS360 has been configured and applicable policies and rules for Android devices have been established. We also assumed that you have the corporate identifier for your MaaS360 and your Google account name and Google account password.

8.1.1.1 Register Device to MDM (Fiberlink MaaS360)

Prepare Mobile Device for MDM enrollment

1. Perform factory reset - This step is optional. If factory reset is necessary for an Android device, be sure to check the options for backing up and restoring your data (*https://support.google.com/android-one/answer/2819582*). Follow these steps to perform the factory reset:
    - On your mobile device, open the Settings menu.
    - Under Personal, tap on Backup & Reset.
    - Under Personal data, tap on Factory Data Reset.
    - After pressing Reset Device, the device will start to reboot into recovery mode and begin to wipe the tablet and return the device to its factory conditions.
    - Startup the device and follow the instructions on the screen to set up the device for a new user. Be sure the Date and Time setting is correct. Otherwise, the wrong date and time could affect the process for validating the certificates for authentication.
2. Passcode protection - Passcode protection is required for Android devices to be encrypted and enroll into the MDM. To set the passcode, follow these steps:
    - On your mobile device, open the Setting menu.
    - Under Personal, touch Security.
    - Under Screen Security, navigate to Screen Lock.

- Select the Password option.
- Follow the instructions on the screen to complete the passcode set up and record it in a safe location.

3. Device encryption - Our NCCoE security policy defined in the MDM requires the device to be encrypted for protecting data at rest. It is recommended that the device is encrypted before enrolling the device to MDM. Perform encryption using these steps:

    - Plug in the device to a power cable and allow the battery to charge. Keep the power cable connected during the encryption process.
    - On your mobile device, open the Settings menu.
    - Under Personal, touch Security.
    - Scroll to the Encrypt Tablet option.
    - Press the Encrypt Tablet button.
    - The device will reboot several times during the encryption process.
    - On completion, the device will prompt you to enter your password.

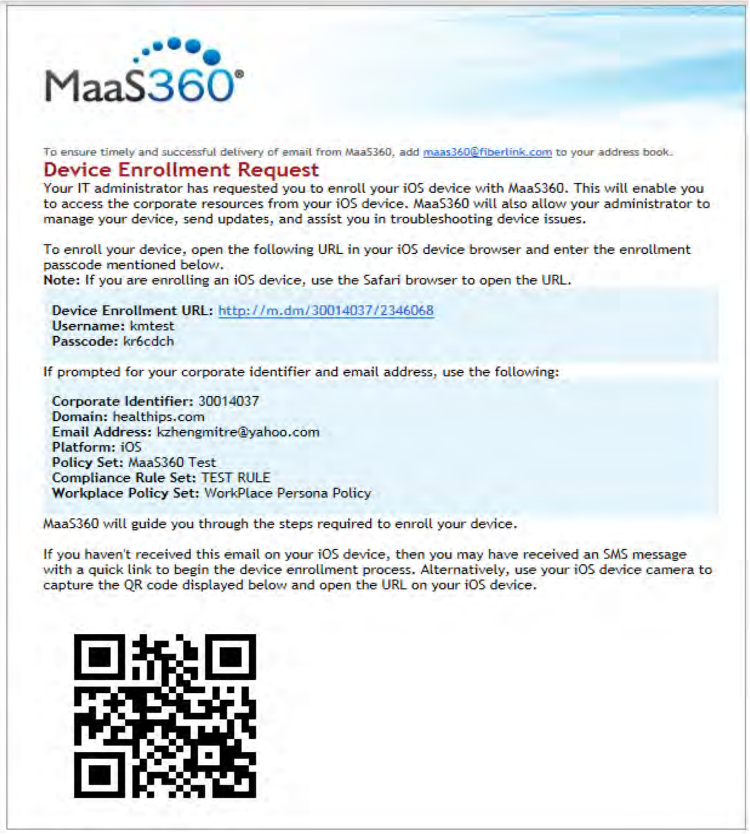
4. Wi-Fi configuration - In our NCCoE build, a dedicated Wi-Fi with SSID HealthITOrg1Reg was established in the wireless access point to allow the device to connect to the Internet for MDM enrollment and for connecting to the Certificate Authority server for requesting and importing device certificates. This Wi-Fi is protected using the WPA2 security protocol. This Wi-Fi SSID is not broadcast. Configure the device to connect to Wi-Fi using these steps:

    - On your mobile device, open the Settings menu.
    - Go to Wireless & Networks.
    - If Wi-Fi is unchecked, tap the empty box.
    - Since the SSID is not broadcast, use Add New Action to create a new Wi-Fi connection.
    - Type in all the details and be sure to select the WPA2 as the protocol and enter the correct password.
    - Check Internet connection using a public Web site such as http://*www.google.com*.

MDM enrollment - It is assumed that the device enrollment request has been done and the enrollment notification has been received via email.

1. For enrollment application:

    - Use your device to open the enrollment email as shown below:



MaaS360®

To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Device Enrollment Request

Your IT administrator has requested you to enroll your iOS device with MaaS360. This will enable you to access the corporate resources from your iOS device. MaaS360 will also allow your administrator to manage your device, send updates, and assist you in troubleshooting device issues.

To enroll your device, open the following URL in your iOS device browser and enter the enrollment passcode mentioned below.
Note: If you are enrolling an iOS device, use the Safari browser to open the URL.

Device Enrollment URL: http://m.dm/30014037/2346068
Username: kmtest
Passcode: kr6cdch

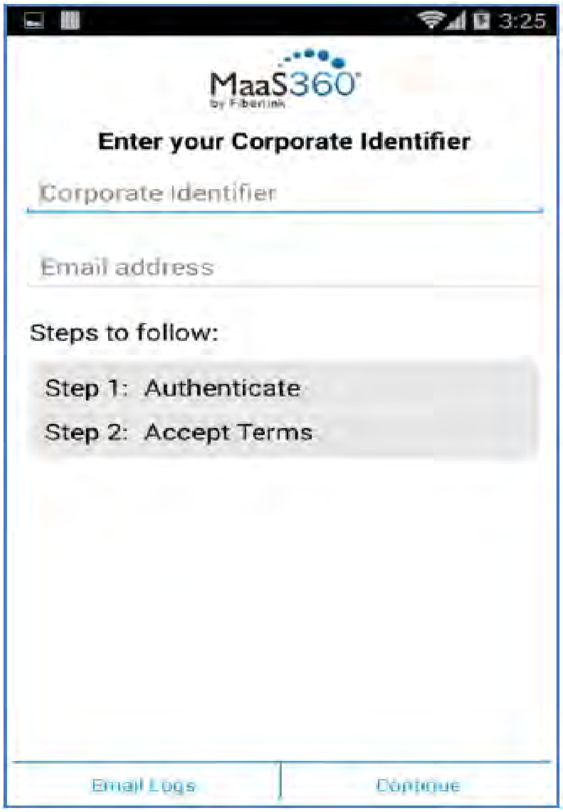
If prompted for your corporate identifier and email address, use the following:

Corporate Identifier: 30014037
Domain: healthips.com
Email Address: kzhengmitre@yahoo.com
Platform: iOS
Policy Set: MaaS360 Test
Compliance Rule Set: TEST RULE
Workplace Policy Set: WorkPlace Persona Policy

MaaS360 will guide you through the steps required to enroll your device.

If you haven't received this email on your iOS device, then you may have received an SMS message with a quick link to begin the device enrollment process. Alternatively, use your iOS device camera to capture the QR code displayed below and open the URL on your iOS device.

- Click the Device Enrollment URL to start the enrollment process, which includes these steps:
  - Download and install the MaaS360 MDM for Android app to the device.
  - Click to open the MaaS360 MDM for Android app



Enter your Corporate Identifier

Corporate Identifier

Email address

Steps to follow:

Step 1: Authenticate

Step 2: Accept Terms

- Fill in the Corporate Identifier and Email address as shown in the device enrollment request email.
- Press Continue to open the agreement page and select the Checkbox and press to continue.
- Press Activate to enroll the device to MDM.
- Install all the required apps.
- Apply policy and rule - Make sure the correct version of policy and rule are applied to the device.
- Verify compliance - Verify the device is compliant with all the security requirements. If not, from the Uncompliant list, click the uncompliant item to correct the problem.

8.1.1.2 Register Device in AP for MAC Address Filtering

Add MAC address and set the static IP address. Make sure the device MAC address is registered in the AP for MAC filtering service. Follow Section 3.3, Access Point: Cisco RV220W for adding a Device MAC address for MAC filtering service.

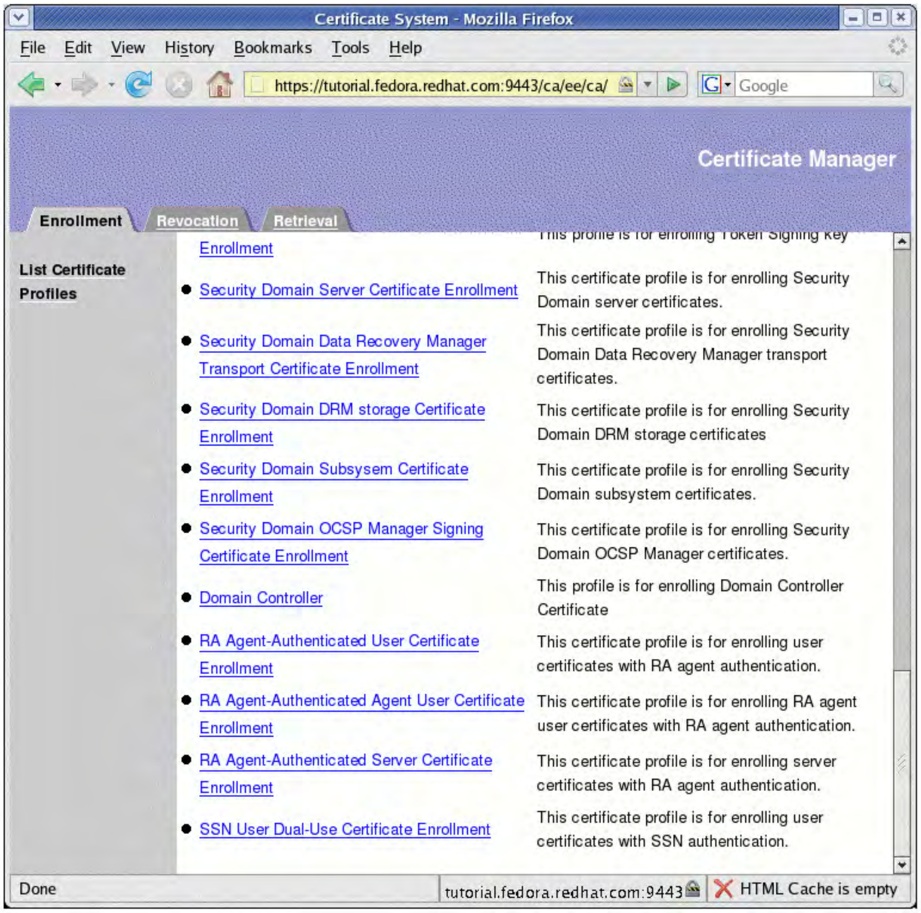
8.1.1.3 Install CA Trusted Certificates

Import certificates on Android devices - Most Android devices will import certificates from an internal or external SD card. Android OS has Credential Storage under the Settings/Security. Some old Android versions cannot recognize certain certificate formats, so additional steps are required to convert the certificate to the format being recognized by the device. For some newer versions of Android devices, directly importing and installing the certificate using a supported support browsers is possible. Below is the list of options that can be used to install a PKI certificate to the device.

Option 1. Directly install the certificate from a browser

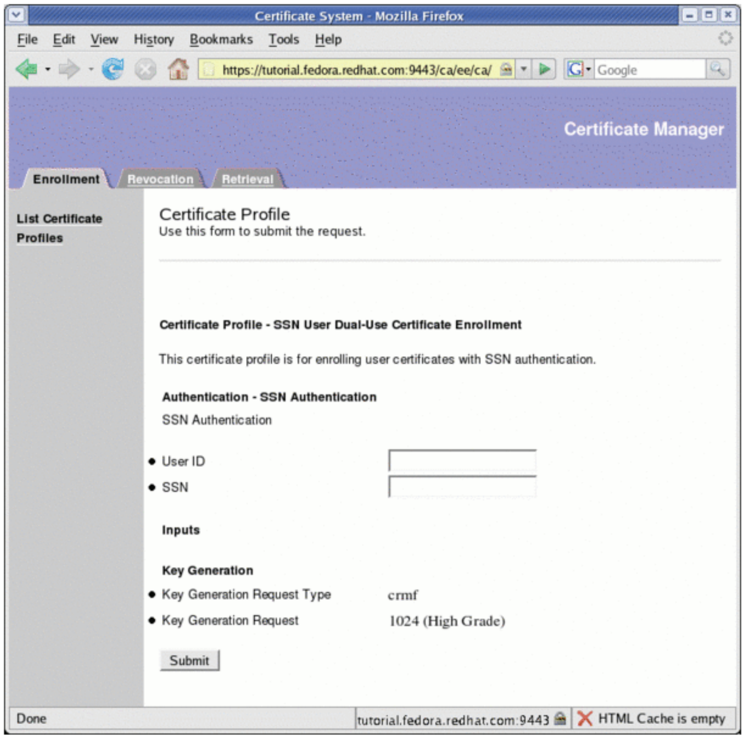
The CA Certificate Authority server provides a browser-based interface for requesting and retrieving device certificates.

- From your device, launch a browser
- Type the URL *https://<PKI hostname>:<PKI secure EE port>* into the browser to list the CA Certificate Profiles:


Certificate System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles
Done
tutorial.fedora.redhat.com:9443
HTML Cache is empty

Enrollment	This profile is for enrolling Token Signing key
● Security Domain Server Certificate Enrollment	This certificate profile is for enrolling Security Domain server certificates.
● Security Domain Data Recovery Manager Transport Certificate Enrollment	This certificate profile is for enrolling Security Domain Data Recovery Manager transport certificates.
● Security Domain DRM storage Certificate Enrollment	This certificate profile is for enrolling Security Domain DRM storage certificates
● Security Domain Subsysem Certificate Enrollment	This certificate profile is for enrolling Security Domain subsystem certificates.
● Security Domain OCSP Manager Signing Certificate Enrollment	This certificate profile is for enrolling Security Domain OCSP Manager certificates.
● Domain Controller	This profile is for enrolling Domain Controller Certificate
● RA Agent-Authenticated User Certificate Enrollment	This certificate profile is for enrolling user certificates with RA agent authentication.
● RA Agent-Authenticated Agent User Certificate Enrollment	This certificate profile is for enrolling RA agent user certificates with RA agent authentication.
● RA Agent-Authenticated Server Certificate Enrollment	This certificate profile is for enrolling server certificates with RA agent authentication.
● SSN User Dual-Use Certificate Enrollment	This certificate profile is for enrolling user certificates with SSN authentication.

- Select an Enrollment link and fill in the device identity in the Common Name field as shown the in page below:


Certificate System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles
Submit
Done
tutorial.fedora.redhat.com:9443
HTML Cache is empty

Certificate Profile
Use this form to submit the request.

Certificate Profile - SSN User Dual-Use Certificate Enrollment

This certificate profile is for enrolling user certificates with SSN authentication.

Authentication - SSN Authentication

SSN Authentication

- User ID
- SSN

Inputs

Key Generation

- Key Generation Request Type: crmf
- Key Generation Request: 1024 (High Grade)

- Press Submit to request the device certificate
- If successful, a request number will be given. Record this number for later use
- The CA Authority Administrator will use the Certificate system to approve or disapprove the request. (Refer to Section 7 for details.)
- Once approved, use the same interface as shown to select the Retrieval Tab.
- Enter the request number to retrieve the certificate. If successful, the certificate will be displayed on the screen with the Import button for importing the certificate to the device.
- If successful, a valid certificate will be installed to the Android device in the location at *Setting/Security/Trusted Credentials*.

> The retrieving interface provides an IMPORT action button for importing and installing the certificate to the device directly. You should use the same browser that you used for submitting the certificate request to perform this importing since the private key generally accompanies the browser.

Option 2. Use internal storage or an external SD card to install the certificate

Download an exported certificate to internal storage or an external SD card and install the certificate from there.

The exported certificate can be copied or downloaded to the internal storage or an external SD card of the device. Android devices provide a tool in the Settings/Security for installing the certificate from internal or external storage. This method will be suitable for installing the root certificate to the device.

- Go to the Settings of your Android device.
- Select Security.
- From the Credentials Storage, select Install from Storage Device to install the certificate.

Option 3. Use OpenSSL utility tool

If Option 1 or 2 does not work, there is a possibility that the specific Android device requires a special certificate format. You can use tools such as OpenSSL to generate a proper certificate and copy it to the SD card for installation. The TLS protocol utility functions provided by the open source OpenSSL may be used to handle conversion of the certificate from one format to another suitable format.

The process for acquiring the CA signed certificate using the OpenSSL command line tool is (Using CN=nccoe525 as an example):

1. Use a Linux server where the OpenSSL Utility is installed
2. Generate a new private key and Certificate Signing Request:

   openssl req –newkey rsa:4096 –days 365 keyout nccoe525.key –out nccoe525.csr –subj "/CN=nccoe525"

3. Have CA sign the certificate. The certificate request you just created in the file "*certreq.tx*" will have a blob of data looking something like this: "-----BEGIN NEW CERTIFICATE REQUEST----- ……. -----END NEW CERTIFICATE REQUEST-----". Copy the Blob to a clipboard
4. Proceed to the CA main page at *https://example.host.com:9443/ca/services* and click on "SSL End Users Services".
5. Select the certificate profile "Manual Administrator Certificate Enrollment".
6. Paste the blob to the large edit box while accepting the default format 'PKCS#10".
7. Add the subject name: example, *CN=nccoe525*
8. Click Submit**.**
9. If successful, a request number will be displayed for future retrieval of the approved certificate.
10. CA admin will verify the request and approve the certificate.
11. Retrieve the approved certificate using the Retrieval tab in the CA main page and save it as a certificate file. In the Retrieval tab, fill in the request number and submit it to get the certificate content. From the opening Certificate content, copy this under the Base 64 encoded certificate from the line "-----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----".
12. Use the copied blob to create a certificate file, e.g *nccoe525.crt*. If there is a *.txt* extension associated with this file, remove it.
13. Move this file to the Linux server in the location where the private key file is located.
14. Use the OpenSSL command to bind the signed certificate with the private key file and convert the certificate to a p12 file so that it may be installed in most browsers:

```
openssl pkcs12 -export -clcerts -in nccoe525.crt -inkey
   nccoe526.key -out nccoe526.p12
```

15. Save this file and transfer it to the device's internal or external storage.
16. Install the certificate as shown in Option 2.

8.1.1.4 Configure Wi-Fi for EAP-TLS authentication

With the certificates in place, you are ready to connect to the wireless network that requires the certificate as the authentication mechanism. Use the following steps to setup Wi-Fi in an Android device with EAP-TLS authentication:

1. Go to Wi-Fi settings for the Android device
2. Enter the following items:
    - EAP method: TLS
    - Phase 2 authentication: None
    - CA certificate: Name of your RootCA
    - User certificate: Name of your device certificate
3. Click Save. You should be now connected to the network using EAP-TLS authentication.
4. In this build, we used a protected website, *https://www.healthisp.com*, to verify whether the EAP-TLS authentication was successful or not.

8.1.2 Setup Apple Mobile Devices to Support EAP-TLS Authentication

It is assumed that the MaaS360 has been configured and applicable policies and rules for Apple iOS devices have been established. It is also assumed that you have the corporate identifier for your MaaS360 and your Apple ID for the device.

8.1.2.1 Register Device to MDM (Fiberlink MaaS360)

Prepare Device for MDM enrollment

1. Perform factory reset - This step sets the device to its factory default setting for a new owner and erases the original settings, data, and applications to prevent unknown and harmful applications remaining on the device. If a factory reset is necessary for an Apple device, be sure to check options for backing up and restoring your data (*https://support.apple.com/en-us/HT203977*). Following these steps to perform the factory reset:
    - On your Apple device, open the Settings menu.
    - Under General, tap on Reset.
    - Under Reset, tap on Erase All Content and Settings.
    - You will have to confirm your selection to set your device to the factory default.
    - After you confirm your choice, the device will begin the reset process.
    - Restart your device and follow the on screen instructions to setup the device for a new owner.
2. Passcode protection and device encryption **-** Passcode code protection is required for iOS devices to be encrypted and enroll into the MDM. Setting a passcode in the iOS device will also enable encryption on the device. To set the passcode, follow

these steps:

- On your mobile device, open the Settings menu.
- Under General, go to Passcode Lock and press Turn Passcode On.
- Under Screen Security, navigate to Screen Lock.
- When you turn on the passcode, you also enable encryption on your iOS devices.

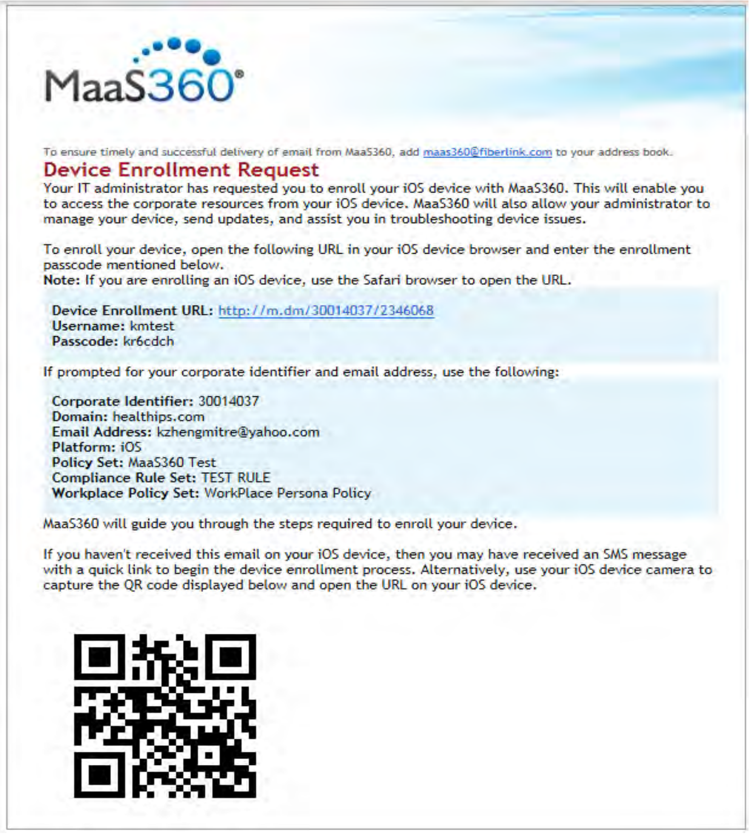
3. Wi-Fi configuration - In our NCCoE build, a dedicated Wi-Fi with SSID HealthITOrg1Reg was established in the wireless Access Point to allow a device to connect to the Internet for MDM enrollment and to the CA certificate Authority server to request and import device certificates. This Wi-Fi is protected using the WPA2 security protocol. This Wi-Fi SSID is not broadcast. Configure the device to connect to Wi-Fi using these steps:

   - On your mobile device, open the Settings menu.
   - Tap Wi-Fi.
   - When Wi-Fi is on, the device will automatically search for available Wi-Fi networks.
   - Join the hidden Wi-Fi network with no broadcast SSID: Under the Choose a Network section, tap on Other.
   - In Name, put the exact Wi-Fi network SSID you want to connect.
   - Tap on Security and choose the type of network encryption used. (For the NCCoE build, WPA2 is used).
   - Return back to the primary connection screen.
   - Enter the Wi-Fi SSID password and tap on Join to connect to the hidden wireless network.

MDM Enrollment - It is assumed that the device enrollment request has been completed and the enrollment notification has been received via email.

1. For enrollment application

   - Enroll your iOS device using the URL provided to you via the enrollment email from MaaS360 (an example is shown below). Click the URL provided. Alternatively, you can open the Safari browser on the device and enter the URL manually.



To ensure timely and successful delivery of email from MaaS360, add maas360@fiberlink.com to your address book.

Device Enrollment Request

Your IT administrator has requested you to enroll your iOS device with MaaS360. This will enable you to access the corporate resources from your iOS device. MaaS360 will also allow your administrator to manage your device, send updates, and assist you in troubleshooting device issues.

To enroll your device, open the following URL in your iOS device browser and enter the enrollment passcode mentioned below.
Note: If you are enrolling an iOS device, use the Safari browser to open the URL.

Device Enrollment URL: http://m.dm/30014037/2346068
Username: kmtest
Passcode: kr6cdch

If prompted for your corporate identifier and email address, use the following:

Corporate Identifier: 30014037
Domain: healthips.com
Email Address: kzhengmitre@yahoo.com
Platform: iOS
Policy Set: MaaS360 Test
Compliance Rule Set: TEST RULE
Workplace Policy Set: WorkPlace Persona Policy

MaaS360 will guide you through the steps required to enroll your device.

If you haven't received this email on your iOS device, then you may have received an SMS message with a quick link to begin the device enrollment process. Alternatively, use your iOS device camera to capture the QR code displayed below and open the URL on your iOS device.

- Clicking the Device Enrollment URL will start the enrollment process.
- The enrollment steps include Authenticate, Accept Terms, Download & Install Profile, and Install MaaS360 for iOS App to the device.
- Click Continue to proceed and follow the instructions to provide necessary authentication information from the enrollment email, such as passcode and Corporation Identifier.
- Accept terms. You must agree to the Fiberlink end user agreement to enroll your device.
- The device will start to install the MDM Profile. Press Continue. The profile will enable the MaaS360 Administrator to manage the device using MaaS360. Click Install to install the profile and accept any prompts for profile installation to continue with the enrollment.
- After the profile is installed, you will be prompted to install the required MaaS360 app from the Apple App Store.
- Return to the home screen and locate the MaaS360 app. Tap the MaaS360 icon to install the Fiberlink MDM for iOS app.
- The installation may request permission to use your location information and your permission to send you push notifications. Accept these requests by clicking the OK button.
- You device is enrolled in MaaS360 now.

- Apply policy and rule - From the home screen, locate the MaaS360 icon. Tap on it to display the device general information and the device policy. Make sure the correct versions of policy and rules are applied to the device.
- Verify compliance - Verify the device is compliant with all the security requirements. If not, from the uncompliant list, click the uncompliant item to correct the problem.

8.1.2.2 Register Device in AP for MAC Address Filtering

Add MAC address and set the static IP address. Make sure the device MAC address is registered in the AP for MAC filtering service. Follow Section 3.3, Access Point: Cisco RV220WM for adding a Device MAC address for MAC filtering service.

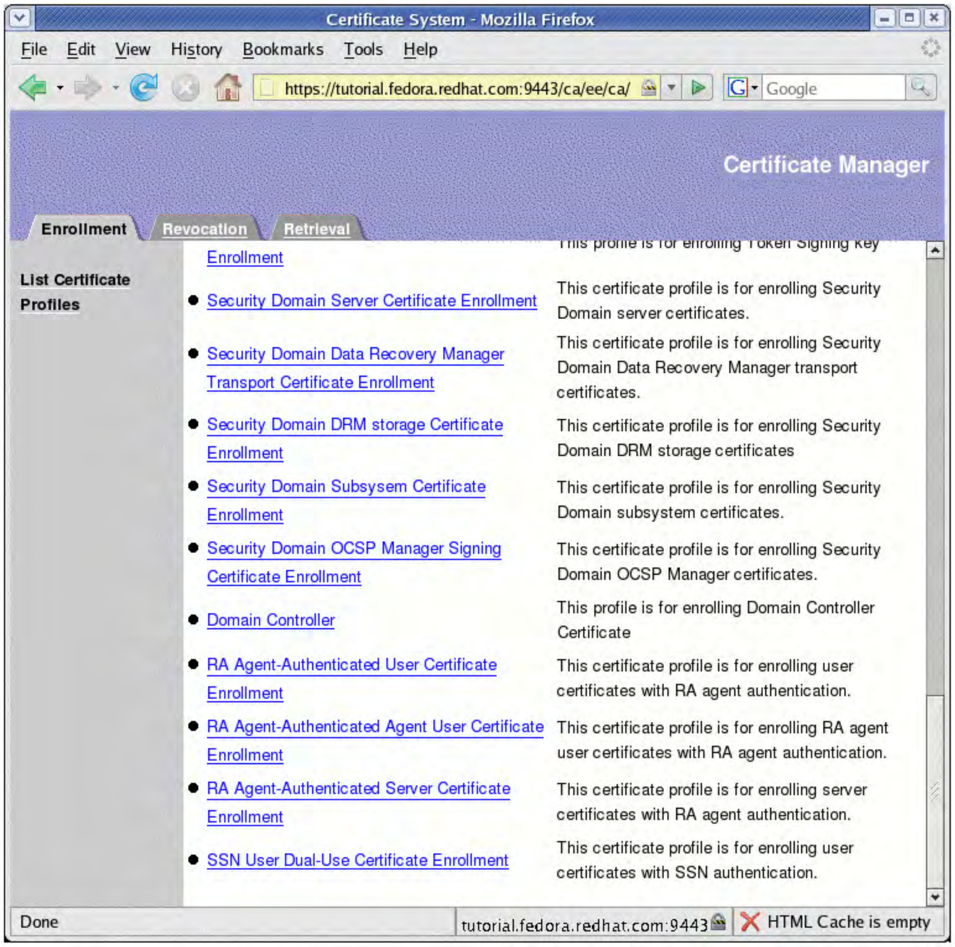
8.1.2.3 Install CA Trusted Certificates

Import certificates on iOS Devices - Most of the iOS devices will import certificates from *.*p12* or **pfx* files sent to your device as an attachment in an email. We recommend this email is encrypted using TLS. Below is the list of options that can be used to install a PKI certificate to the device.

Option 1. Directly install the certificate from browser

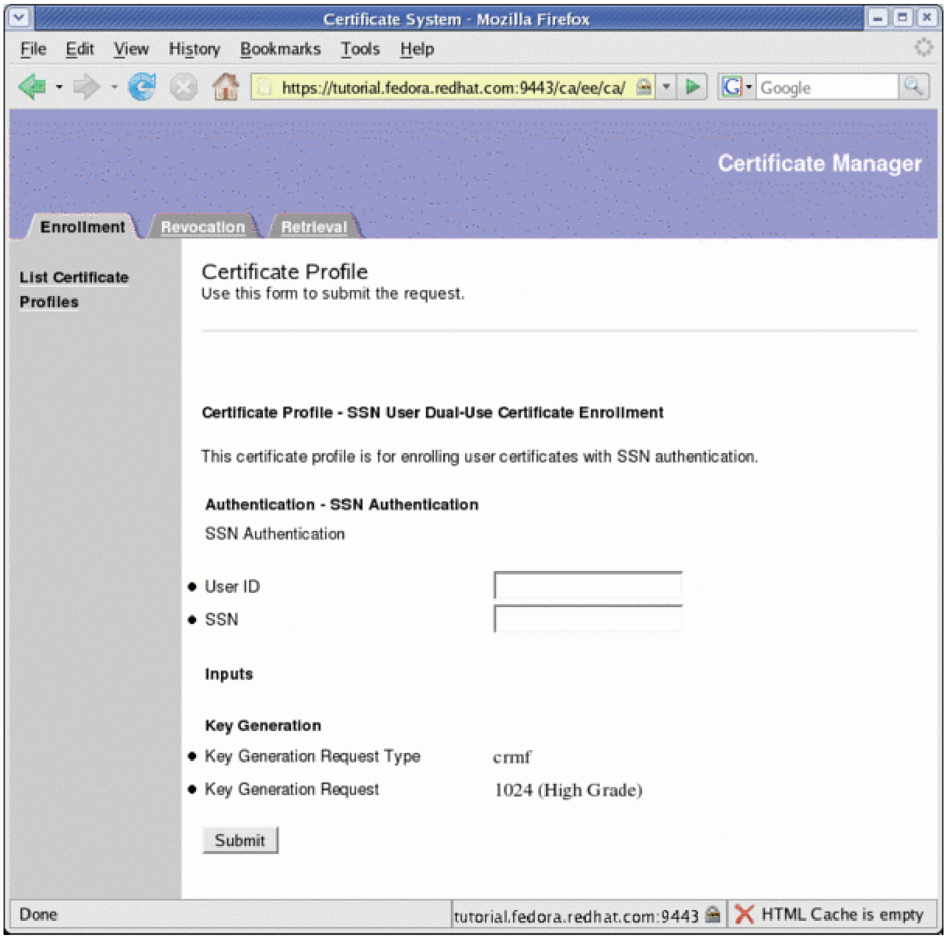
The CA Certificate Authority server provides a browser-based interface for requesting and retrieving device certificates.

- From your device, launch a browser
- Type the URL *https://<PKI hostname>:<PKI secure EE port>* into the browser to list the CA Certificate Profiles:


Certificate System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles
Done
tutorial.fedora.redhat.com:9443
HTML Cache is empty

Enrollment	This profile is for enrolling Token Signing key
● Security Domain Server Certificate Enrollment	This certificate profile is for enrolling Security Domain server certificates.
● Security Domain Data Recovery Manager Transport Certificate Enrollment	This certificate profile is for enrolling Security Domain Data Recovery Manager transport certificates.
● Security Domain DRM storage Certificate Enrollment	This certificate profile is for enrolling Security Domain DRM storage certificates
● Security Domain Subsysem Certificate Enrollment	This certificate profile is for enrolling Security Domain subsystem certificates.
● Security Domain OCSP Manager Signing Certificate Enrollment	This certificate profile is for enrolling Security Domain OCSP Manager certificates.
● Domain Controller	This profile is for enrolling Domain Controller Certificate
● RA Agent-Authenticated User Certificate Enrollment	This certificate profile is for enrolling user certificates with RA agent authentication.
● RA Agent-Authenticated Agent User Certificate Enrollment	This certificate profile is for enrolling RA agent user certificates with RA agent authentication.
● RA Agent-Authenticated Server Certificate Enrollment	This certificate profile is for enrolling server certificates with RA agent authentication.
● SSN User Dual-Use Certificate Enrollment	This certificate profile is for enrolling user certificates with SSN authentication.

- Select an Enrollment link and fill in the device identity in the Common Name field as shown the in page below:


Certificate System - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://tutorial.fedora.redhat.com:9443/ca/ee/ca/
Google
Certificate Manager
Enrollment
Revocation
Retrieval
List Certificate Profiles
Submit
Done
tutorial.fedora.redhat.com:9443
HTML Cache is empty

Certificate Profile
Use this form to submit the request.

Certificate Profile - SSN User Dual-Use Certificate Enrollment

This certificate profile is for enrolling user certificates with SSN authentication.

Authentication - SSN Authentication
SSN Authentication

- User ID
- SSN

Inputs

Key Generation

- Key Generation Request Type crmf
- Key Generation Request 1024 (High Grade)

- Then press Submit to request the device certificate.
- If successful, a request number will be given. Record this number for later use.
- The CA Authority Administrator will use the Certificate system to approve or disapprove the request. (Refer to Section 7 for details.)
- Once approved, use the same interface as shown to select the Retrieval Tab.
- Enter the request number to retrieve the certificate. If successful, the certificate will be displayed on the screen with the Import button for importing the certificate to the device.
- If successful, a valid certificate will be installed to the iOS device in the location at *Setting/General/Profile & Device Management*.

The retrieving interface provides an IMPORT action button for importing and installing the certificate to the device directly. You should use the same browser as you used for submitting the certificate request to perform this importing since the private key generally accompanies the browser.

Option 2. Use email attachment to install the certificate

- Open the certificate file from an email with the certificate as the attachment. The install process will start.
- At the Install Profile screen, press the Install button.
- If you are prompted with a warning messaging saying: “Installing this profile will change settings on your iPhone,” press the Install Now button.
- You may need to enter the passcode that you set for the device.
- Once the certificate installation has finished, you will see a screen showing your certificate.
- Press Done to exit the installation process.

Option 3. Use OpenSSL utility tool

You can use tools such as OpenSSL to generate a proper certificate and copy it to the SD for installation. In case the above methods do not work, there is a possibility that the specific device requires a special certificate format. The TLS protocol utility functions provided by the open source OpenSSL may be used to handle conversion of the certificate from one format to another suitable format so installation of a certificate on this device becomes possible.

The process for acquiring the CA signed certificate using the OpenSSL command line tool is (using CN=nccoe525 as an example) :

1. Use a Linux server where the OpenSSL Utility is installed
2. Generate a new private key and Certificate Signing Request:

   openssl req –newkey rsa:4096 –days 365 keyout nccoe525.key –out nccoe525.csr –subj “/CN=nccoe525”

3. Have CA sign the certificate. The certificate request you just created in the file "certreq.tx" will have a blob of data looking something like this: “-----BEGIN NEW CERTIFICATE REQUEST----- ……. -----END NEW CERTIFICATE REQUEST-----“. Copy the Blob to a clipboard
4. Proceed to the CA main page at *https://example.host.com:9443/ca/services* and click on “SSL End Users Services”.
5. Select the certificate profile “Manual Administrator Certificate Enrollment”.
6. Paste the blob to the large edit box while accepting the default format ‘PKCS#10”.
7. Add the subject name: example, *CN=nccoe525*
8. Click Submit**.**
9. If successful, a request number will be displayed for future retrieval of the approved certificate.
10. CA admin will verify the request and approve the certificate.

11. Retrieve the approved certificate using the Retrieval tab in the CA main page and save it as a certificate file. In the Retrieval tab, fill in the request number and submit it to get the certificate content. From the opening Certificate content, copy this under the Base 64 encoded certificate from the line "-----BEGIN CERTIFICATE----- to -----END CERTIFICATE-----".
12. Use the copied blob to create a certificate file, e.g *nccoe525.crt*. If there is a *.txt* extension associated with this file, remove it.
13. Move this file to the Linux server in the location where the private key file is located.
14. Using the OpenSSL command to bind the signed certificate with the private key file and convert the certificate to a p12 file so that it may be installed in most browsers:

```
openssl pkcs12 -export -clcerts -in nccoe525.crt -inkey
   nccoe526.key -out nccoe526.p12
```

15. Save this file and transfer it to the iOS device using secure email.
16. Install the certificate as shown in Option 2.

8.1.2.4 Configure Wi-Fi for EAP-TLS Authentication

With the certificates in place (CA Root certificate and the device certificate), you are ready to connect your iOS device to the wireless network that requires the certificate as the authentication mechanism. Use the following steps to setup Wi-Fi in an iOS device with EAP-TLS authentication

1. Go to the Wi-Fi settings for the iOS device
2. Click Other Network to enter the following items:
   - Name of the SSID
   - Security: WPA2 Enterprise
   - Return to Other Network page
   - Click Mode
   - Select EAP-TLS as the Mode
   - Return to Other Network page
   - Enter the Username that has been assigned to this device
   - Click Identify to list all the certificates
   - Select the one registered for the device
   - Click Join to connect to the network
3. You should be now connected to the network using EAP-TLS authentication
4. In this build, we used the protected website *https://www.healthisp.com* to verify if the EAP-TLS authentication was successful

8.2 MaaS360

The MDM selected for this build is based on the MaaS360 product. Maas360 is a cloud based solution that is responsible for managing polices on each mobile device. An administrator can enforce the corporate mobile policies without logging into each device. This action will manage one or more centralized policies for distribution to all devices with the Maas360 agent installed. MaaS360 can group policies, users, and mobile devices, then distribute unique policies based on their roles.

This section will show you how to install one of our predefined policies

System Requirements

- A computer system for accessing the cloud version of MaaS360 Administration Portal
- Internet connectivity and Internet browsers installed
- Windows Phone Company Hub certificate

You will also need the following parts of this guide:

- Section 3.3, Access Point: Cisco RV220W
- Section 7.1, Fedora PKI
- Section 8.2.1, MDM Setup
- Section 9.1, Cisco Identity Services Engine

8.2.1 MDM Setup

8.2.1.1 Enable Mobile Device Management Service

It is assumed that a MaaS360 account has been established with Fiberlink. If no account has been established, contact Fiberlink for more information on how to request a user account (*http://www.maas360.com/*). It is also assumed that the required Windows Phone Company Hub and the Apple APNS certificates have been acquired. For detailed information on how to acquire these required certificates, please refer to the document *(http://content.maas360.com/www/support/mdm/assets/APNS_CertRenewalGuide.pdf*) for Apple MDM certificate and the document (*http://content.maas360.com/www/pdf/Win%20Phone%208%20Company%20Hub.pdf*) for MaaS360 Windows Phone 8 Company Hub Certificate.

1. Add the Apple MDM Certificate for managing Apple devices
   - Log on to MaaS360 dashboard using *https://logon.maas360.com*
   - Navigate to *Setup* > *Services***,** click *Mobile Device Management***.**
   - Click Apple MDM Certificate and use the Browser to load the certificate file.
2. Add Windows Phone Company Hub certificate for managing Windows Phones
   - Log on to MaaS360 dashboard using *https://logon.maas360.com*
   - Navigate to *Setup* > *Services*, click *Mobile Device Management*.
   - Expand the Windows Phone Company Hub certificate by pressing the “+” symbol.
   - Use the browser to load and install the certificate to the MDM.

8.2.1.2 Enable Security Policies for Mobile Devices

1. Create a new policy for a type of device

- Log on to the MaaS360 dashboard using *https://logon.maas360.com*
- Navigate to *Security* > *Polices*, click *Add Policy*
- Add a Name, e.g**.** Lab_Only_ISO
- Add Description
- Select a Type from the dropdown list: (e.g. IOS MDM)
- Use a Start From dropdown list to copy an existing policy for this new policy
- Click Continue to create a new policy for the type of device.

2. Edit and refine the created policies
   - Log on to MaaS360 dashboard using *https://logon.maas360.com*
   - Navigate to Setup > Policies.
   - From the Policy list, click View to view a selected Policy.
   - Review each item in the policy to make sure they are set per your security policy and business requirement.
   - If the policy settings do not meet your security requirement, click the Edit button to enter the edit mode.
   - Change the values to your desired values.
   - Click Save to save the changes or click Save and Publish to save and publish the new policy.
   - Enter the password and press Continue.
   - Click Confirm Publish to complete this edition and the new policy will be assigned with a new version number. You can use this version number to verify that the devices controlled by this policy are enforced by this version of the policy.

If the policy is set to be extremely restrictive, it can lock you out of the mobile device and make it very difficult to unlock.

8.2.1.3 Enable Security Compliance Rule for Mobile Devices

1. Create a new rule set
   - Log on to MaaS360 dashboard using *https://logon.maas360.com*
   - Navigate to *Security* > *Compliance Rules*, click *Add Rule Set*
   - Add a Name, e.g. HIT-RULE
   - Copy an existing rule set for the new rule from the Copy From dropdown list
   - Click Continue to create a new rule.
2. Edit and refine the newly created rule
   - Log on to theMaaS360 dashboard using *https://logon.maas360.com*

- Navigate to *Security > Compliance Rules*
- Click Edit for the selected rule you want to review and edit
- From the Basic Settings, under Select Applicable Platforms, check the checkbox next to an OS's name to Enable the Real-Time Compliance for OS's.
- In the Event Notification Recipients fill in the emails you want to notified in case of noncompliance.
- Use the navigation tree to view and set other rules per your security and operational requirements.
- Click Save to save the newly set rules.

8.2.1.4 Add Applications to be Distributed to Mobile Devices

1. Add App to App Catalog
    - Log on to MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *APPS > Catalog***,** click *Add* to select Apps from different app stores.
    - In the popup page, type a key word for the App in the search box to list the available Apps.
    - Select the app you want and click Add button to add the app into the category.
2. Add App to Bundles for Distribution
    - Log on to the MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *APPS > Bundles*, click *Add App Bundles* to open the App Bundle window.
    - In the popup page, enter a Bundle Name and Description for the bundle. Then enter the App Names in the App Name field. Use a comma to separate the apps.
    - Click Add button to add the App Bundle.
    - From the App Bundle list, click Distribute button to set the distribution Target.

8.2.1.5 Add Device Group to Manage Mobile Devices

1. Add Device Group
    - Log on to MaaS360 dashboard using *https://logon.maas360.com*
    - Navigate to *Users > Groups***,** click *Create Device Group* to create a new Group.
    - Enter a group name and description from the Device Group Details window and specify the group Type.
    - Click Save to save the setting.
2. Configure Group
    - The group can be configured to include devices, policy, rules, etc. Devices in the same group will share the same settings as configured for the group.

- Detailed settings for group properties can be referenced in the MDM manual. *http://content.fiberlink.com/www/support/assets/MaaS360ServicesUserGuide.pdf*

8.2.1.6 Device Enrollment

- iOS MDM Enrollment is described in Section 0
- Android MDM Enrollment is described in Section 8.2.1.6

8.3 Host Based Security

Both the notional Data Center and the HealthIT Organizations in this build have systems that need protection from viruses and malware. As with most of the capabilities selected for this build, the Symantec Endpoint Protection service provides an enterprise class ability to manage host security policy for multiple systems. These managed systems could be local to the server or remotely across the world. An organization with the proper skilled resources on staff could manage traditional servers and hosts or allow an ISP like the notional Data Center in this build.

8.3.1 Symantec Endpoint Protection Suite

The Symantec Endpoint Protection server provides the following options:

- Local Host Intrusion Prevention System(IPS) will block traffic before it traverses the network
- Utilizes a global intelligence network service to remain current on threats
- Supports Windows, Linux and Mac systems
- Centralized management console

The Data Center in this build only manages the local servers in the Data Center. Symantec will be working with the NCCOE team in future iterations of this build to integrate mobile device malware and virus management with its Endpoint Protection product.

System requirements

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8G
Disk space	Minimum 150 GB

You will also need the following parts of this guide:

- Section 11.1, Windows Installation and Hardening
- Section 3.1, Hostnames

Symantec Setup

To set up Symantec Endpoint Protection, follow the installation and Administration guide at *https://support.symantec.com/en_US/article.DOC7698.html*

9 Identity and Access Control

This build utilizes a radius server integrated with our CA and AP which combines to create the full identity and access control function. A radius server uses the AAA protocol to manage network access via authentication, authorization and accounting. Authentication and authorization are of particular focus in the identity and access process used in this build. The authentication mechanism is integrated with the root certificate authority as a recipient of a signed root cert and OCSP communication. The authorization mechanism is integrated with the MDM to check mobile device policy for compliance.

9.1 Cisco Identity Services Engine

The Cisco Identity Services Engine (ISE) provides the ability to do the following:

- Centralize and unify identity and access policy management
- Visibility and more assured device identification through certificate challenges
- Organizations can use business rules to segment access to sections of the network
- Even with more assured and stronger authentication, the user experience during the challenge process is made seamless

System requirements

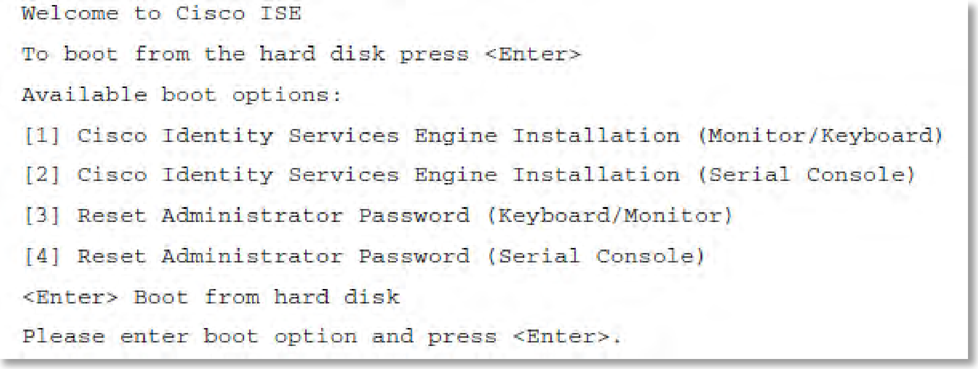
- Virtual Hypervisor (VH) capable of housing virtual machines (VMs)
- VM with CPU: Single Quad-core; 2.0 GHz or faster
- VM with minimum 4 GB memory
- VM with minimum 200 GB disk space

You will also need the following parts of this guide:

- Section 7.1, Fedora PKI
- Section 8.2.1, MDM Setup

Cisco ISE Setup

1. Download the Cisco ISE 1.2 ISO from *https://software.cisco.com/download/release.html?mdfid=283801620&softwareid=283802505&release=1.2*. Either use the ISO image or burn the ISO image on a DVD, and use it to install Cisco ISE 1.2 on a virtual machine
2. Follow the guidance from your VM vendor to boot the DVD or ISO and start the install process
3. Once the system boots up, follow the console display to select one of the installation options shown below:



```
Welcome to Cisco ISE
To boot from the hard disk press <Enter>
Available boot options:
[1] Cisco Identity Services Engine Installation (Monitor/Keyboard)
[2] Cisco Identity Services Engine Installation (Serial Console)
[3] Reset Administrator Password (Keyboard/Monitor)
[4] Reset Administrator Password (Serial Console)
<Enter> Boot from hard disk
Please enter boot option and press <Enter>.
```

4. Select Option 1 to start the installation.
5. Once the installation is complete, the system prompts for the network setup through the

command-line interface (CLI).

6. Enter the required parameters, below, to configure the network. If you would like to use our IP and hostname address scheme, refer to Section 3.1, Hostnames.
    - Hostname
    - Ethernet interface address
    - Default gateway
    - DNS domain name
    - Primary name server
    - Username and Password for use for the command line interface (CLI) and the admin portal access are provided by the Cisco ISE

More detailed procedures for installing the Cisco ISE is available from the installation guide provided by Cisco, available at *http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/installation_guide/ise_ig/ ise_vmware.html#pgfId-1057864*

9.2 Cisco ISE Post-Installation Tasks

> Management of the Cisco ISE should be executed with a web browser unless you intend to administer via command line. All instructions in this guide for managing the Cisco ISE product relate to use of the graphical user interface.

1. Using a web browser and the Cisco ISE host address, log on to the Cisco ISE Administration Portal. You will use the credentials (username and password) created during the installation procedure.
2. From the Administration Portal, click the Setup Assistant.
3. Follow the wizard interface to set up the basic operating configuration and default settings for authentication, authorization, profiling, posture, client provisioning, guest services, and support for personal devices.

9.3 Configure CISCO ISE to Support EAP-TLS Authentication

9.3.1 Set ISE to support RADIUS authentication

The following steps are used to set up a communication connection from Cisco ISE to the network device (Access Point) used as the authenticator in the RADIUS authentication:

1. From the Admin Portal, navigate to the path: *Administration* > *Network Resources* > *Network Devices*. Then select *Add*.
2. Fill out the required parameters as indicated in the form:
    - The name of the network device,
    - The IP Address of the device with its subnet mask,
    - Select the RADIUS protocol as the selected protocol, and
    - Enter the shared secret that is configured on the network device.

There are many advanced optional RADIUS settings in the ISE network device definition. For example, KeyWrap helps increase RADIUS communication security via use of the AES KeyWrap algorithm. However, you should be experienced with Cisco ISE and confident that your network device supports this configuration.

9.3.2 Enable PKI in Cisco ISE

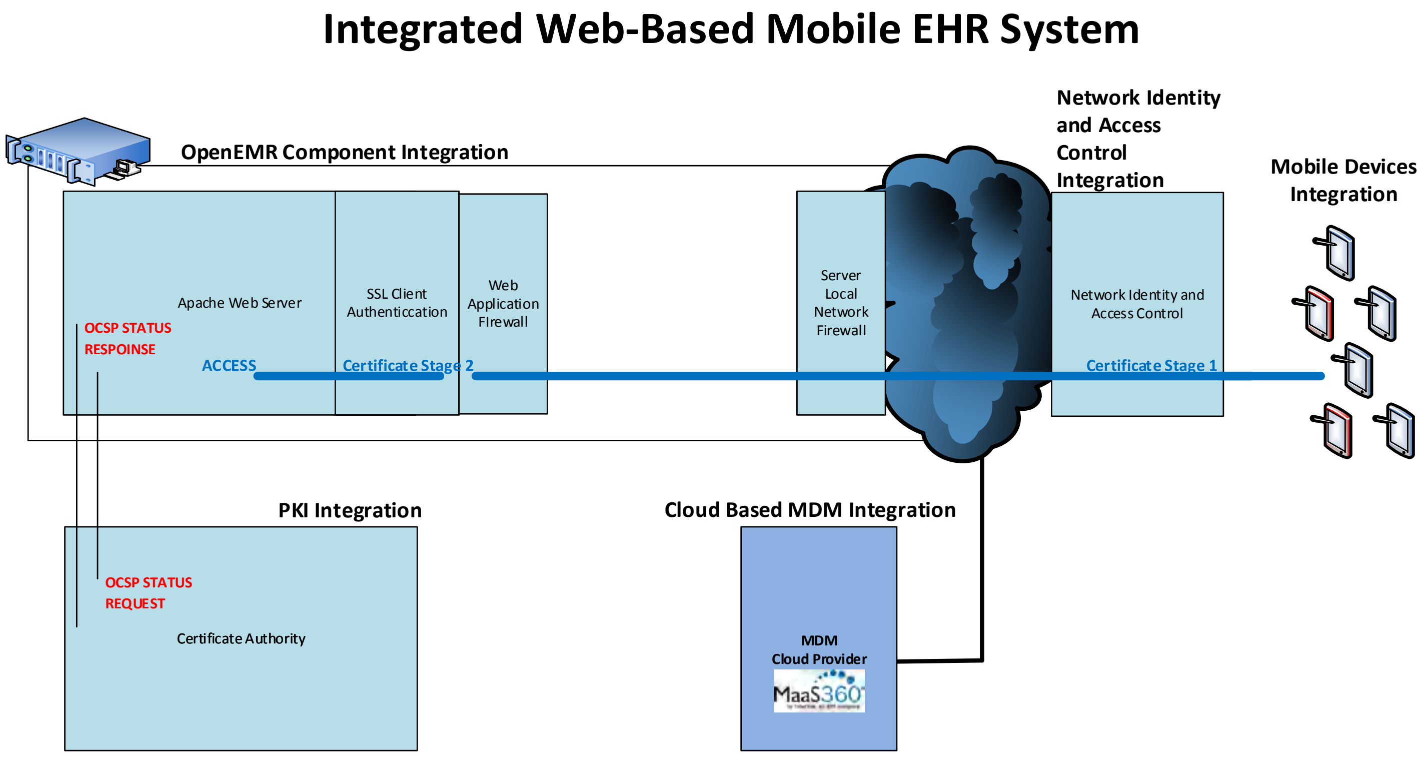
We replaced the Cisco ISE default self-signed certificate with the CA-signed certificate issued through our Certificate Authority. The steps are:

1. Generate a certificate signing request (CSR) through the Cisco ISE navigation path *Administration > System > Certificates > Local Certificates*.

Ensure the CN field matches the Fully Qualified Domain Name of the Cisco ISE server.

2. Export the Certificate Signing Request from the navigation path *Administration > System > Certificates >Certificate Signing Requests,* then select *Export*
3. Save and submit the Certificate Signing Request file to a Certificate Authority. From there, the content of the CSR described in the text from “-----BEGIN CERTIFICATE REQUEST-----” through “-----END CERTIFICATE REQUEST-----.” is used for generating the signed certificate in CA for the specific server.
4. The process for signing the CSR is described in Section 7, Certificate Authority
5. Use the ISE Administration interface to bind the acquired CA-signed certificate with its private key using the path *Administration > System > Certificates > Local Certificates then Add>Bind CA Signed Certificate*

If you intend to use this certificate for client EA-TLS authentication, as we did in the NCCoE build, designate the certificate for EAP-TLS use when binding the certificate. The client needs this certificate to identify the Cisco ISE server for EAP protocols.



Architecture

9.3.3 Populate Certificate Store with Required CA-signed Certificates

The CA-signed root certificate, as well as the certificate for Fiberlink MaaS360 MDM server, are required by the Certificate Store. You will need to have the CA root certificate in PEM or DER format.

To import the CA-signed root certificates to the certificate store:

1. Obtain a CA-signed root certificate from the Trusted CA Administrator. The procedure for generating the root cert is described in Section 7, Certificate Authority
2. From the ISE Administration Portal, use the navigation path *Administration* > *System* > *Certificates* > *Certificate Store* to perform the import action.

Follow Steps 1 and 2 to import the Fiberlink MaaS360 MDM certificate to Cisco ISE so that ISE can communicate with Fiberlink MaaS360 MDM.

9.3.4 Set Identity Source for Client Certificate Authentication

No internal or external identity source is required for the EAP-TLS certificate-based authentication method, since the identity is validated based on the trusted certificate in the PKI. However, you must set up the Certificate Authentication Profile in the ISE as the external identity source. Instead of authenticating via the traditional username and password, Cisco ISE compares a certificate received from a client with one in the server to verify the authenticity of a user or device. Note that although internal or external identity sources are not needed for TLS authentication, internal or external identity sources can be added and used for authorization of a policy condition, if desired.

To create a Certificate Authentication Profile:

1. Use the Administration Portal to navigate to the path *Administration* > *Identity Management* > *External Identity Sources* > *Certificate Authentication Profile* and click *Add*.
2. Fill out the form with proper parameters. Be sure to select the Subject Name as the Principal Username X509 attribute because it is the field that will be used to validate the authenticity of the client.

9.3.5 Set Authentication Protocols

Cisco ISE uses authentication protocols to communicate with external identity sources. Cisco ISE supports many authentication protocols such as the Password Authentication Protocol (PAP), Protected Extensible Authentication Protocol (PEAP), and the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS). For this build, we used the EAP-TLS protocol for user and machine authentication.

To specify the allowed protocols services in Cisco ISE:

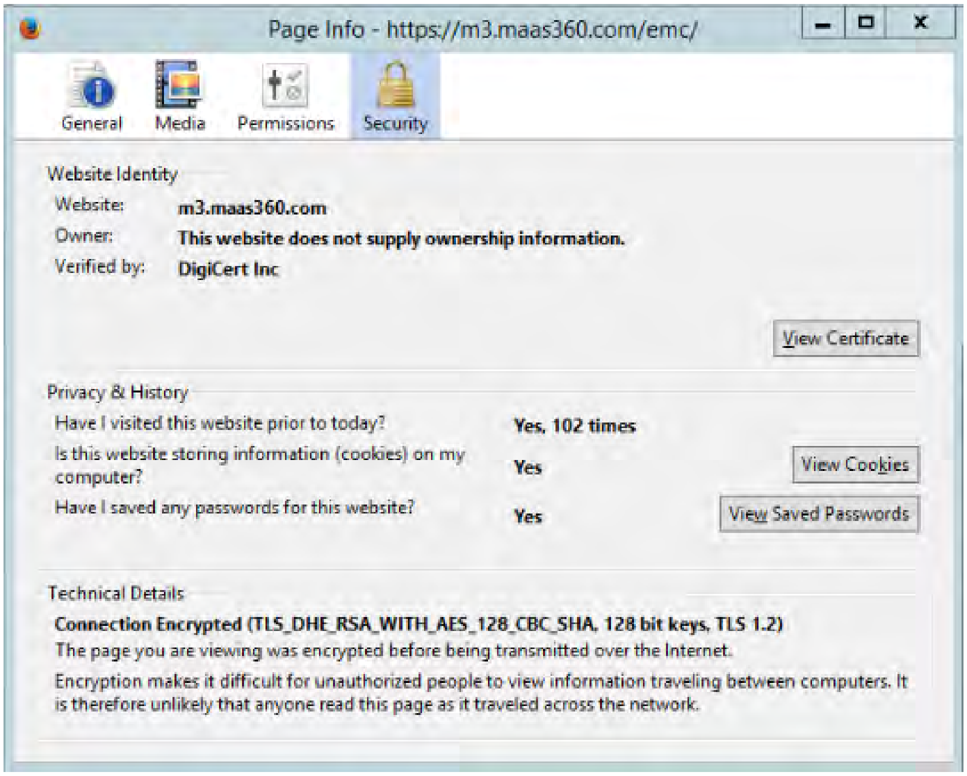
1. From the Administration Portal navigate to the path *Policy >Policy Elements* > *Results >Authentication* > *Allowed Protocols* > *Add*
2. Select the preferred protocol or list of protocols. In this build, the *EAP_TLS* is selected as the allowed authentication protocol.

9.3.6 Configure Cisco ISE to Integrate with Fiberlink MaaS360

1. Establish basic connectivity between the Cisco ISE server and the Fiberlink MaaS360 MDM server. As indicated in the architecture diagram, firewalls are installed between the

ISE and the Fiberlink MaaS360 in the cloud. The firewall should be configured to allow an HTTPS session from the ISE to the Fiberlink MaaS360 server located in the public Internet. The session is established outbound from ISE towards the MDM, where ISE takes the client role.

2. Import the MDM digital certificate for ISE
3. Export the MDM site digital certificate. One simple approach is to use one of the Internet browsers to do this. Depending on the browser selected, the importing and exporting procedures are slightly different. Here the Firefox browser is used.
    - From the browser, log on to the MaaS360: *https://logon.maas360.com*
    - In the Browser next to the URL, there is a lock symbol. Click that symbol. Open a security information page as shown below:

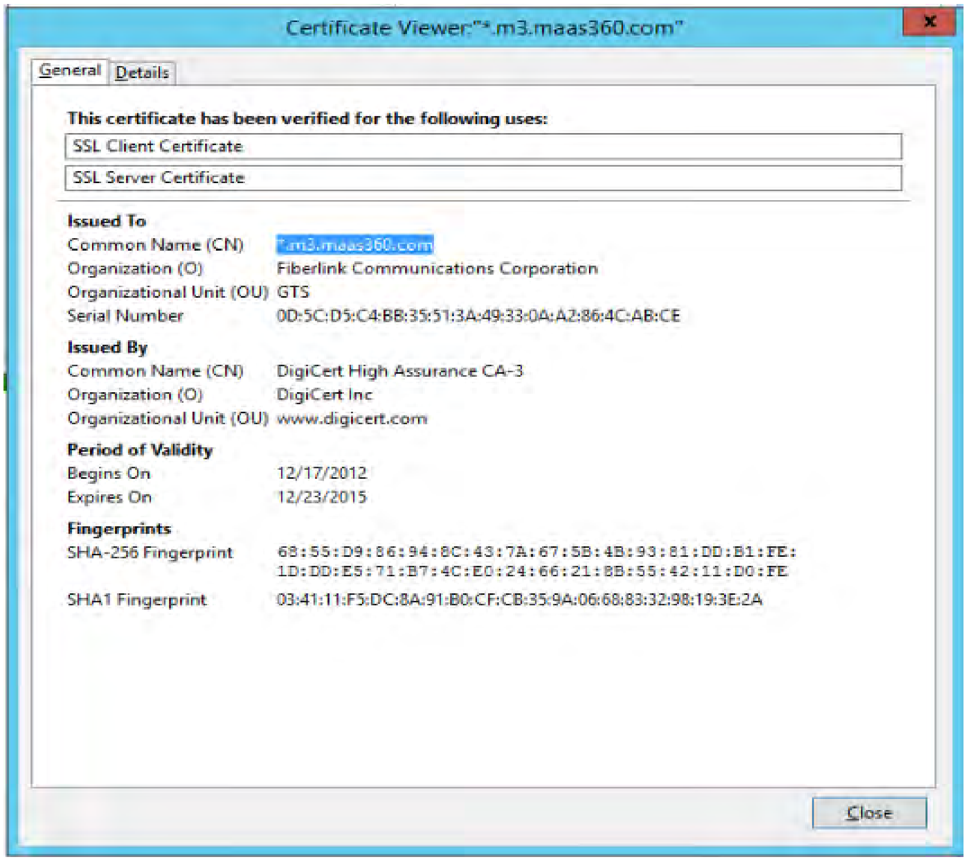


Website Identity
Website: m3.maas360.com
Owner: This website does not supply ownership information.
Verified by: DigiCert Inc

Privacy & History
Have I visited this website prior to today? Yes, 102 times
Is this website storing information (cookies) on my computer? Yes
Have I saved any passwords for this website? Yes

Technical Details
Connection Encrypted (TLS_DHE_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

- Click the View Certificate button to view the certificate



This certificate has been verified for the following uses:

SSL Client Certificate

SSL Server Certificate

Issued To

Common Name (CN)	*.m3.maas360.com
Organization (O)	Fiberlink Communications Corporation
Organizational Unit (OU)	GTS
Serial Number	0D:5C:D5:C4:BB:35:51:3A:49:33:0A:A2:86:4C:AB:CE

Issued By

Common Name (CN)	DigiCert High Assurance CA-3
Organization (O)	DigiCert Inc
Organizational Unit (OU)	www.digicert.com

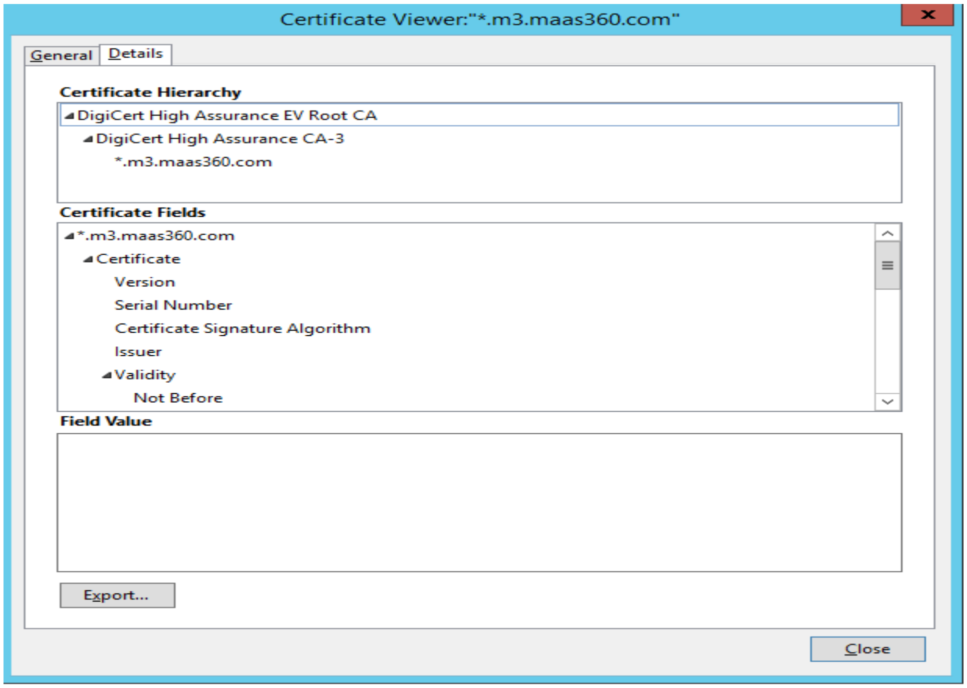
Period of Validity

Begins On	12/17/2012
Expires On	12/23/2015

Fingerprints

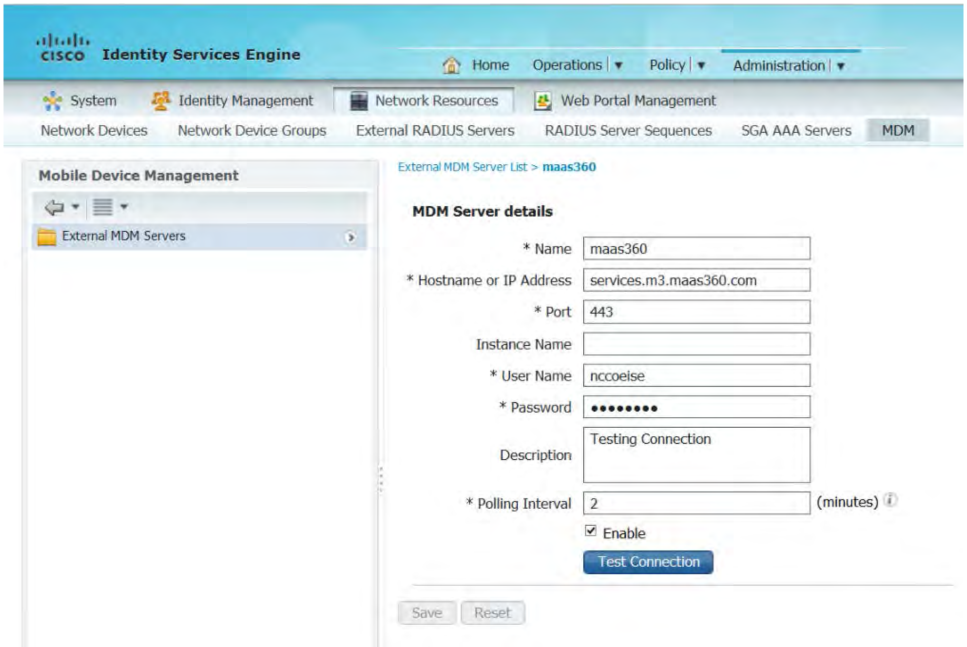
SHA-256 Fingerprint	68:55:D9:86:94:8C:43:7A:67:5B:4B:93:81:DD:B1:FE: 1D:DD:E5:71:B7:4C:E0:24:66:21:8B:55:42:11:D0:FE
SHA1 Fingerprint	03:41:11:F5:DC:8A:91:B0:CF:CB:35:9A:06:68:83:32:98:19:3E:2A

- Select the Detail to view the detail certificate information and from there you should have an Export button to export the certificate.



- Save the certificate to a file.

4. Import the certificate into the local cert store in ISE.
   - From the ISE Administration Portal, use the navigation path *Administration* > *System* > *Certificates* > *Certificate Store* to perform the import action.
   - Grant ISE Access to the Fiberlink MaaS360 API
5. Create a Fiberlink MaaS360 administrator account with an API role
   - Log on the MaaS360 with an Administrator Account
   - Navigate to *Setup* > *Administrators* and click Add Administrator.
   - Enter the new user name and a corporate email address and click Next
   - Enter Roles for the newly created administrator and click Next
   - Verify the setting and press Save.
6. Add MDM Server to ISE
   - Use the MaaS360 MDM admin account created above
   - Configure Cisco ISE to integrate with the MaaS360: *Administration* > *MDM* > *External MDM Server*, then click *Add*.
   - Fill out the required information using the account created in Step 5 and the hostname or IP address provided by Fiberlink. A sample result is given below:



External MDM Server List > maas360

MDM Server details

* Name: maas360
* Hostname or IP Address: services.m3.maas360.com
* Port: 443
Instance Name:
* User Name: nccoeise
* Password: ••••••••
Description: Testing Connection
* Polling Interval: 2 (minutes)
☑ Enable

   - The Test Connection button can be used to test the connection between the Cisco ISE and the cloud MaaS360. A successful message will be displayed if connection succeeds.

9.3.7 Configure Cisco ISE to Authorization Policy

Configure ISE Authorization Policies to include an MDM Compliance Check.

1. Configure Cisco ISE to allow network access for registered and compliant mobile devices
   - From the Cisco Administration Portal, navigate to *Policy* > *Authorization*
   - Create the rule as

     Name: *MDM Registered_Compliant*
     Condition: *If MDM:DeviceCompliantStatus Equals Compliant*
     And
     MDM:DeviceRegisterStatus Equals Registered
     Permissions: PermitAccess

2. Configure Cisco ISE to deny network access for unregistered or uncompliant mobile devices
   - From the Cisco Administration Portal, navigate to *Policy* > *Authorization*
   - Create a second rule as

     Name: *MDM UnRegistered_UnCompliant*
     Condition: *If MDM:DeviceCompliantStatus Equals UnCompliant*
     Or
     MDM:DeviceRegisterStatus Equals UnRegistered
     Permissions: *DenyAccess*

3. Configure Cisco ISE to deny network access for all Others
   - From the Cisco Administration Portal, navigate to *Policy* > *Authorization*
   - Create a third rule as

     Name: *Default*
     Condition: *If no matches*
     Permissions: *DenyAccess*

10 Governance, Risk, and Compliance (GRC)

Governance, Risk, and Compliance (GRC) allows an organization to link strategy and risk, adjusting strategy when risk changes, while remaining in compliance with laws and regulations. We used RSA Archer GRC to perform risk assessment and management.

10.1 RSA Archer GRC

10.1.1 System Requirements

This build requires the user to install a single-host RSA Archer GRC Platform node on a VMware virtual machine with the Microsoft Windows Server 2012R2 operating system to provide the risk management services needed.

> All components, features, and configurations presented in this guide reflect what we used based on vendors’ best practices and requirements. Please refer to vendors’ official documentation for complete instruction for other options.

10.1.2 Pre-installation

We chose the single-host deployment option for installing and configuring the GRC platform on a single VM under the Microsoft Windows Server 2012R2. All components, the Web application, services, and instance databases are running under a single server. Below are the pre-installation tasks that we performed prior the RSA Archer installation:

- Operating System: Windows Server 2012R2 Enterprise
  - Refer to Section 11.1, Windows Installation and Hardening for system requirements and installation.
- Database: Microsoft SQL Server 2012 Enterprise (x64)

Follow Microsoft's installation guidelines and steps to install the SQL Server Database Engine and SQL Server Management tools. Refer *to https://msdn.microsoft.com/en-us/library/bb500395(v=sql.110).aspx* for additional details.

We used the following configuration settings during the installation and configuration process. We also created the required database instances and users for the RSA Archer installation. Test the database instances by using different users to verify the login permissions on all database instances and configuration databases to ensure database owners have sufficient privileges and correct user mappings.

Setting	Value
Collation Settings set to case insensitive for instance database	SQL_Latin1_general_CP1_CI_AS
SQL Compatibility level set appropriately	SQL Server 2012 110
Locale set	English (United States)
Database server time zone	EST
Platform language	English
Create both the instance and configuration databases. For migration, create only the configuration database.	Database names: *grc-content* grc-config
User Account set to Database Owner role	*grc-content-user* grc-config-user
Recovery Model	Simple (configuration and instance databases)
Auto Shrink	False (configuration database)
Auto-Growth	Set it for (instance database)
Max Degree of Parallelism	1 (configuration and instance databases)

Web and Services

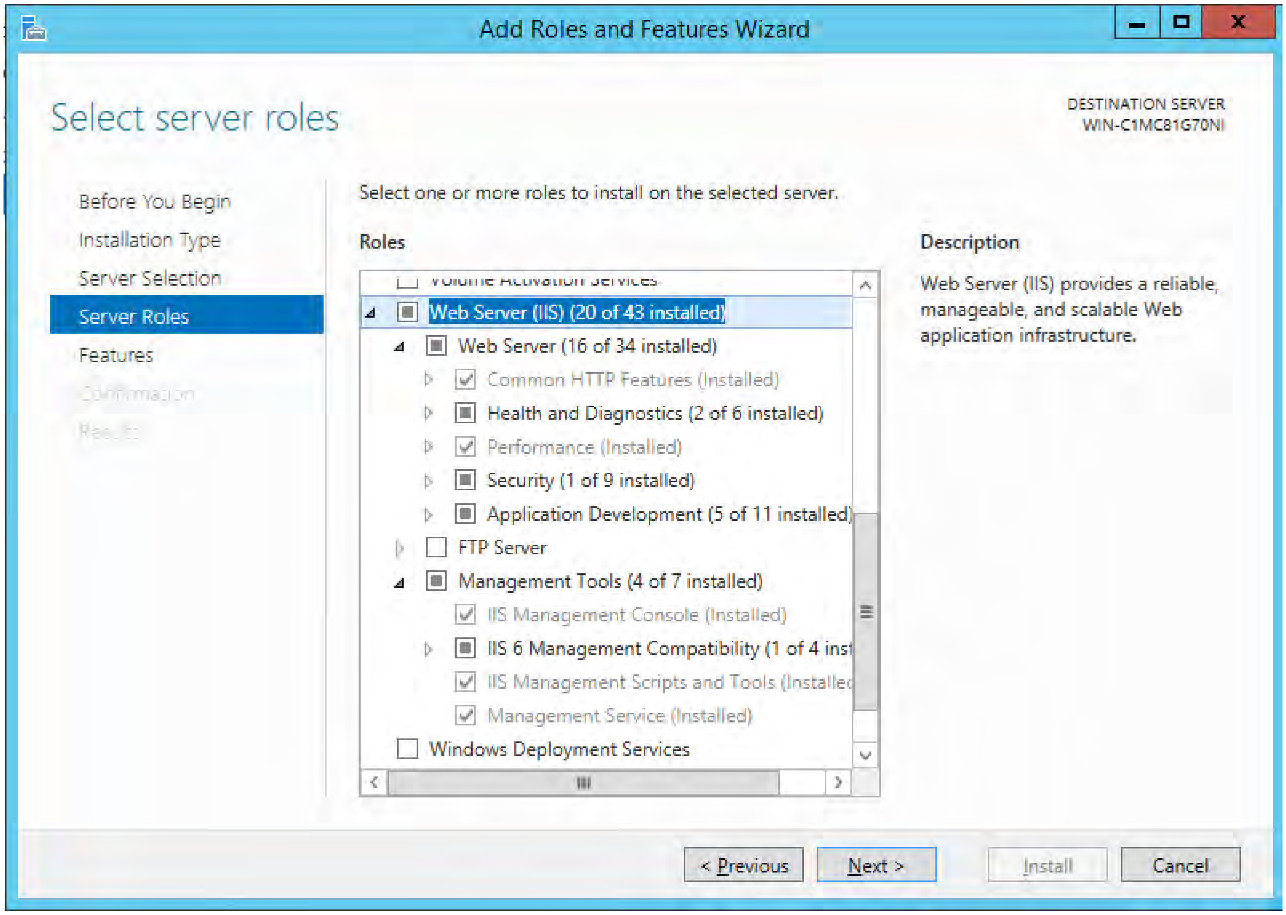
- Microsoft Internet Information Services (IIS) 8
- Microsoft .NET Framework 4.5

Use Server Manager for installing IIS and *.NET* Framework, referring to *http://www.iis.net/learn/get-started/whats-new-in-iis-8/installing-iis-8-on-windows-server-2012* for detailed steps and corresponding screenshots.

Please install IIS first and then install the *.NET* Framework.

The table below summarizes the required IIS components and *.NET* Framework features followed by the screenshots.

Required Option	Value
IIS	
Common HTTP Features	Default Document Directory Browsing HTTP Errors Static Content
Health and Diagnostics	HTTP Logging
Application Development	.NET Extensibility 4.5 ASP .NET 4.5 ISAPI Extensions ISAPI Filters
Security	Request Filtering
Management Tools	IIS Management Console
.NET Framework	
.NET Framework 4.5 Features	.NET Framework 4.5 ASP.NET 4.5
WCF Services	HTTP Activation TCP Port Sharing



Add Roles and Features Wizard

Select server roles

DESTINATION SERVER
WIN-C1MC81G70NI

Select one or more roles to install on the selected server.

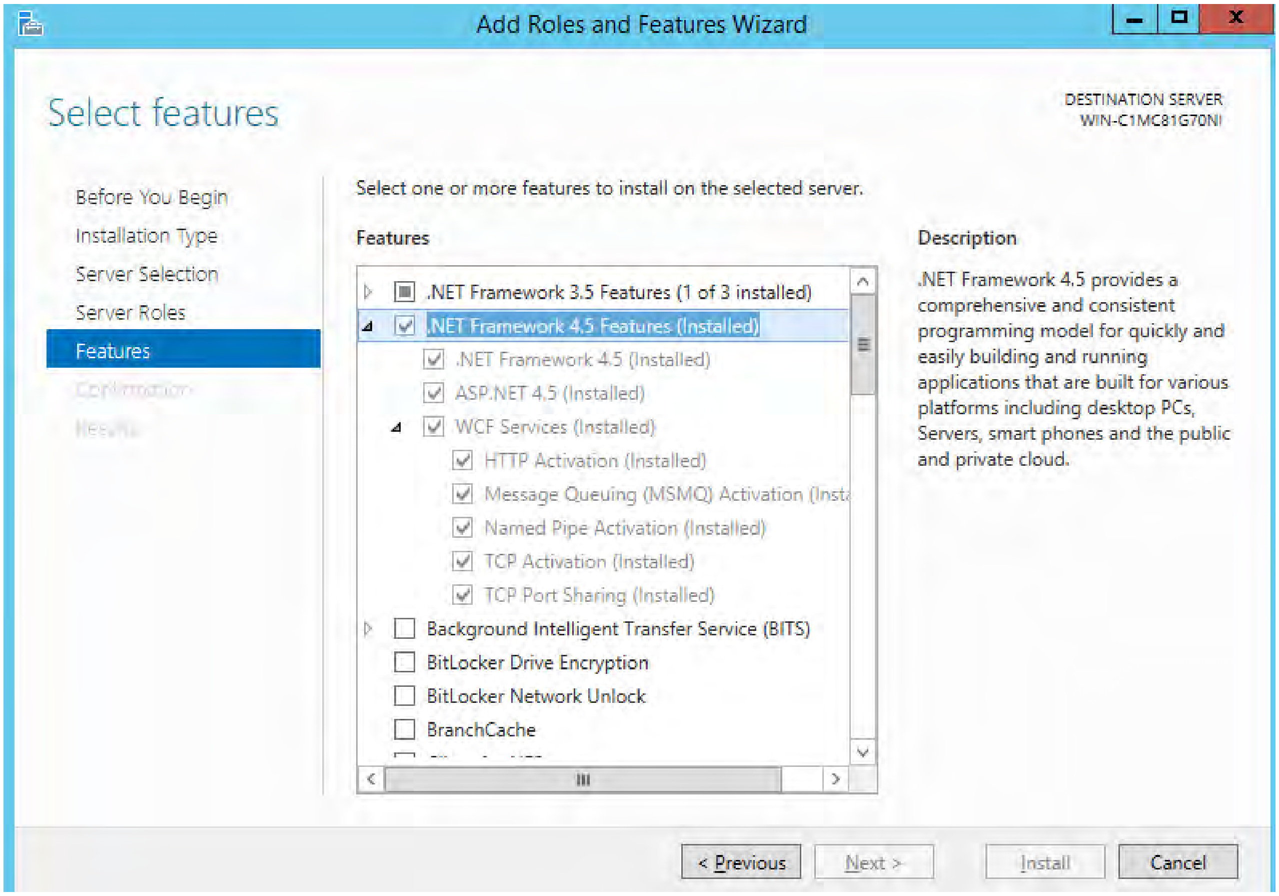
Roles

- □ Volume Activation Services
- ▣ Web Server (IIS) (20 of 43 installed)
  - ▣ Web Server (16 of 34 installed)
    - ☑ Common HTTP Features (Installed)
    - ▣ Health and Diagnostics (2 of 6 installed)
    - ☑ Performance (Installed)
    - ▣ Security (1 of 9 installed)
    - ▣ Application Development (5 of 11 installed)
  - □ FTP Server
  - ▣ Management Tools (4 of 7 installed)
    - ☑ IIS Management Console (Installed)
    - ▣ IIS 6 Management Compatibility (1 of 4 inst
    - ☑ IIS Management Scripts and Tools (Installed
    - ☑ Management Service (Installed)
- □ Windows Deployment Services

Description

Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.

Figure 1: Web Server (IIS) Components Selection Screenshot



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-C1MC81G70NI

Select one or more features to install on the selected server.

Features

- ▣ .NET Framework 3.5 Features (1 of 3 installed)
- ☑ .NET Framework 4.5 Features (Installed)
  - ☑ .NET Framework 4.5 (Installed)
  - ☑ ASP.NET 4.5 (Installed)
  - ☑ WCF Services (Installed)
    - ☑ HTTP Activation (Installed)
    - ☑ Message Queuing (MSMQ) Activation (Insta
    - ☑ Named Pipe Activation (Installed)
    - ☑ TCP Activation (Installed)
    - ☑ TCP Port Sharing (Installed)
- □ Background Intelligent Transfer Service (BITS)
- □ BitLocker Drive Encryption
- □ BitLocker Network Unlock
- □ BranchCache

Description

.NET Framework 4.5 provides a comprehensive and consistent programming model for quickly and easily building and running applications that are built for various platforms including desktop PCs, Servers, smart phones and the public and private cloud.

Figure 2: .NET Framework 4.5 Features Selection Screenshot

Microsoft Office 2013 Filter Packs

Download it from Microsoft website (*http://www.microsoft.com/en-us/download/details.aspx?id=40229*) and install it.

Java Runtime Environment (JRE) 8

Download and install JRE 8 refer to *http://www.oracle.com/technetwork/java/javase/install-windows-64-142952.html* for details.

> All pre-installation software must be installed and configured before installing RSA Archer.

10.1.3 Installation

1. Create folders *C:\ArcherFiles\Indexes* and *C:\ArcherFiles\Logging*(will be used later).
2. Obtain/Download the installer package from RSA; extract the installation package.
3. Run installer
   - Open installation folder, right-click on *ArcherInstall.exe*

- Select Run as Administrator
- Click OK to Run the Installer
- Follow the prompts from the installer for each step, set the value and click Next
- Select all components (Web Application, Services, Instance Database) for installation; then click Next
- Specify the X.509 Certification by selecting it from the checklist (create new cert or use existing cert)
- Set the Configuration Database options with the following properties:

SQL Server:	local
Login Name:	######
Password:	######
Database:	*grc-config* (this is the configuration database we created during the pre-installation process)

- Set the Configuration Web Application options with the following properties:

Website:	Default Website
Destination Directory:	select "Install in an IIS application" option with "RSAarcher" as the value

- Set the Configuration of the Service Credentials

  Select "Use the Local System Account to Run All" option from the checklist

- Set the Services and Application Files paths with the following properties:

  Services: use the default value "*C:\Program Files\RSA Archer\Services\*"

  Application Files: use the default value "*C:\Program Files\RSA Archer*"

- Set the Log File Path to *C:\ArcherFiles\Logging*
- Perform the installation by clicking Install, wait for the installer to complete installing all components, then click Finish. The RSA Archer Control Panel opens.

10.1.4 Post-Installation

10.1.4.1 Configure the Installation Settings

Verify and set the configurations for the following by clicking on RSA Archer Control Panel > Installation Settings, then select corresponding sections:

1. Logging Section
   - Path: *Archer Files\Logging*
   - Level: Error
2. Locale and Time Zone Section
   - Locale: English (United States)
   - Time Zone: (UTC-05:00) Eastern Time (US & Canada)

On the Toolbar, click Save.

3. Create the Default GRC Platform Instance
   - Start the RSA Archer Queuing Service
   - *Server Manager* > *Local Services* or *All Services* > *Locate RSA Archer Queuing* in the list under the *“SERVICES” section* > *Right-click RSA Archer Queuing* and click Start
   - Add a new instance
   - *RSA Archer Control Panel* > *Instance Management* > *Add New Instance*, enter “EHR1” as the Instance Name, then click Go. Complete the properties as needed.
   - Configure the Database Connection Properties
   - *RSA Archer Control Panel* > *Instance Management* > *under All Instances*, click on EHR1
   - In the Database tab setup the following:
     - SQL Server: (local)
     - Login name: xxxxxx
     - Password: xxxxxx
     - Database: grc-config
4. Click on the “Test Connection” link to make sure the “Success” message appears.
5. Configure the General Properties
   - *RSA Archer Control Panel* > *Instance Management* > *under All Instances, click on EHR1*
   - In the General tab, setup the following:
     - File Repository section – Path *C:\ArcherFiles\Indexes*
     - Search Index section - Content Indexing:Check on Index design language only; Path: *C:\ArcherFiles\Indexes\EHR1*
6. Configure the Web Properties
   - *RSA Archer Control Panel* > *Instance Management* > under *All Instances*, click on EHR1
   - In the Web tab, setup the following:
     - Base URL: *http://localhost/RSAArcher/*
     - Authentication URL: *default.aspx*
7. Change SysAdmin and Service Account passwords
   - *RSA Archer Control Panel* > *Instance Management* > *under All Instances, click on EHR1*
   - Change the password on the page by using a strong password
   - Complete Default GRC Platform Instance Creation by clicking Save on the

toolbar.

8. Register the Instance
   - *RSA Archer Control Panel > Instance Management > under All Instances, right-click on EHR1, select Update Licensing, enter the following info, then click on Active*

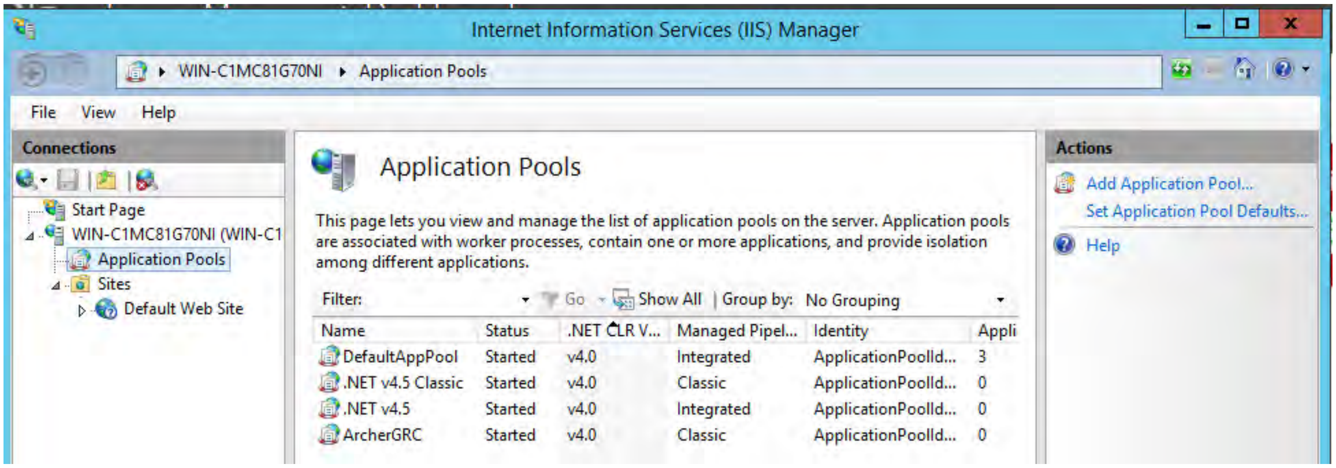
     Serial Number (obtained from RSA)

     Contact Info (First Name, Last Name, Company, etc)

     Activation Method (select Automated)

9. Activate the Archer Instance
   - Start the RSA Archer Services
   - *Server Manager > Local Services or All Services > Locate the following services > Right-click on that service and click Start*
     - RSA Archer Configuration
     - RSA Archer Job Engine
     - RSA Archer LDAP Synchronization
   - Restart the RSA Archer Queuing Service
   - *Server Manager > Local Services or All Services > Locate RSA Archer Queuing > Right-click RSA Archer Queuing and click Restart*
   - Rebuild the Archer Search Index
   - *RSA Archer Control Panel > Instance Management > under All Instances, right-click on EHR1, then click on Rebuild Search Index*

10. Configure and Activate the Web Role (IIS)
    - Setup Application Pools
    - *Server Manager > Tools > IIS Manager > Application Pools (in the left side bar) > right-click to add applications (.NET, ArcherGRC etc.),* example screenshot below

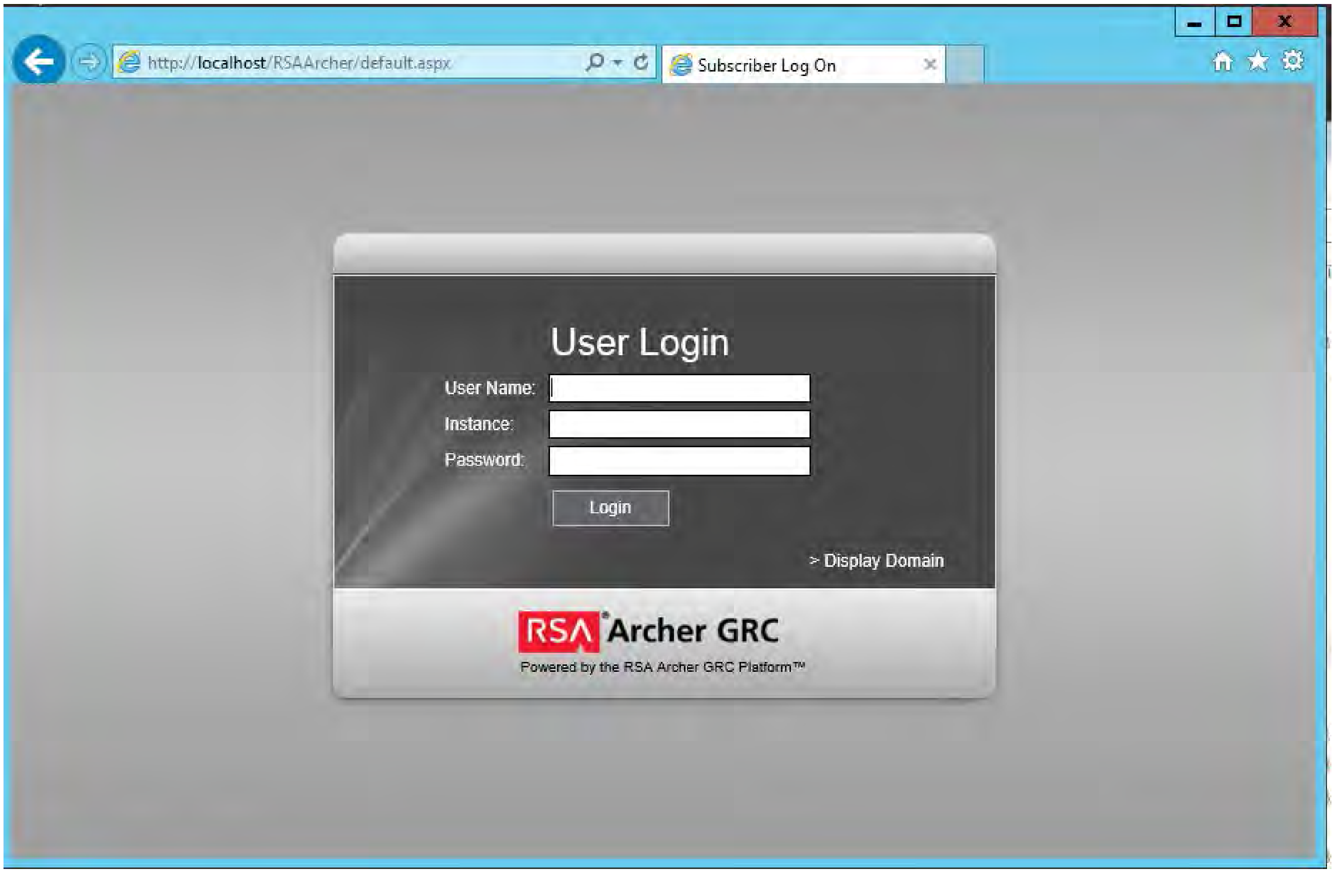


This page lets you view and manage the list of application pools on the server. Application pools are associated with worker processes, contain one or more applications, and provide isolation among different applications.

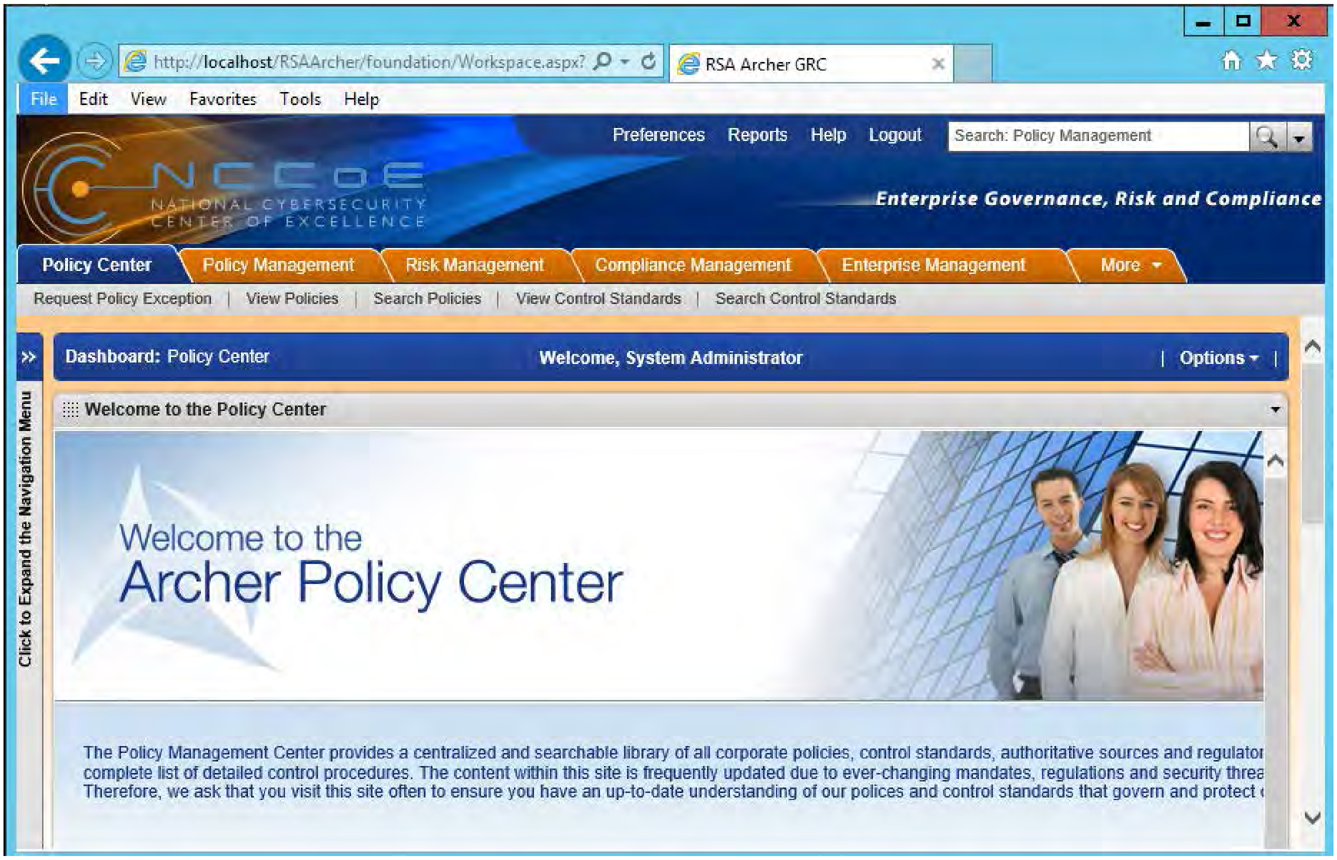
Name	Status	.NET CLR V...	Managed Pipel...	Identity	Appli
DefaultAppPool	Started	v4.0	Integrated	ApplicationPoolId...	3
.NET v4.5 Classic	Started	v4.0	Classic	ApplicationPoolId...	0
.NET v4.5	Started	v4.0	Integrated	ApplicationPoolId...	0
ArcherGRC	Started	v4.0	Classic	ApplicationPoolId...	0

- Restart IIS

11. Test Run for installed RSA Archer GRC and make sure you get the RSA Archer GRC Login screen.



12. Log in to EHR1 Instance.


http://localhost/RSAArcher/foundation/Workspace.aspx?
RSA Archer GRC
File Edit View Favorites Tools Help
Preferences Reports Help Logout
Search: Policy Management
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Enterprise Governance, Risk and Compliance
Policy Center
Policy Management
Risk Management
Compliance Management
Enterprise Management
More
Request Policy Exception | View Policies | Search Policies | View Control Standards | Search Control Standards
Click to Expand the Navigation Menu
Dashboard: Policy Center
Welcome, System Administrator
Options
Welcome to the Policy Center
Welcome to the
Archer Policy Center

The Policy Management Center provides a centralized and searchable library of all corporate policies, control standards, authoritative sources and regulator complete list of detailed control procedures. The content within this site is frequently updated due to ever-changing mandates, regulations and security threa Therefore, we ask that you visit this site often to ensure you have an up-to-date understanding of our polices and control standards that govern and protect

13. Now you are ready to set up the contents and establish the GRC processes detailed in the next section.

10.1.5 Content Setup for establishing GRC process

In order to demonstrate how to monitor and clearly communicate the relationship between technical risks and organizational risks, we used a GRC tool to aggregate and visualize data. We configured the RSA Archer GRC tool to ingest data from various sources and provide information about the implementation of security controls used to address the target security characteristics.

Table 1: Content Sources for GRC Tool

Source	Description
NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF)	• Used as the focal point for mapping the use case's security characteristics to Cybersecurity Standards and Best Practices (i.e., NIST SP-800-53r4) and Sector Specific Standards and Best Practices (i.e., HIPAA)
HIPAA Security Rule – Technical Safeguards	• Used as the core authoritative source for defining the objectives, policies, control standards and selecting the relevant control procedures
NIST SP 800-66 rev1	• Utilized the Security Rule Goals and Objectives in section 2.1.1 for defining the Corporate Objectives. • Used Table 4. HIPAA Standards and Implementation Specifications Catalog for defining the control standards and selecting the control procedures from SP 800-53

NIST SP 800-53r4	• Selected controls for HIPAA Security Rule – Technical Safeguards (based on NIST SP 800-66 mapping)
HHS-ONC SRA Tool Technical Safeguards	• Used Questionnaire for doing assessments
Results of Risk Assessment	• Used identified risks and their levels as the input for the risk register, a library of risks that can be utilized by the entire organization

RSA provided the NCCoE with all the core modules. However, this build uses the following modules:

- Enterprise Management
- Policy Management
- Risk Management
- Compliance Management

High Level Structure and Process Steps for NCCoE HIT Mobil Device Use Case GRC Program

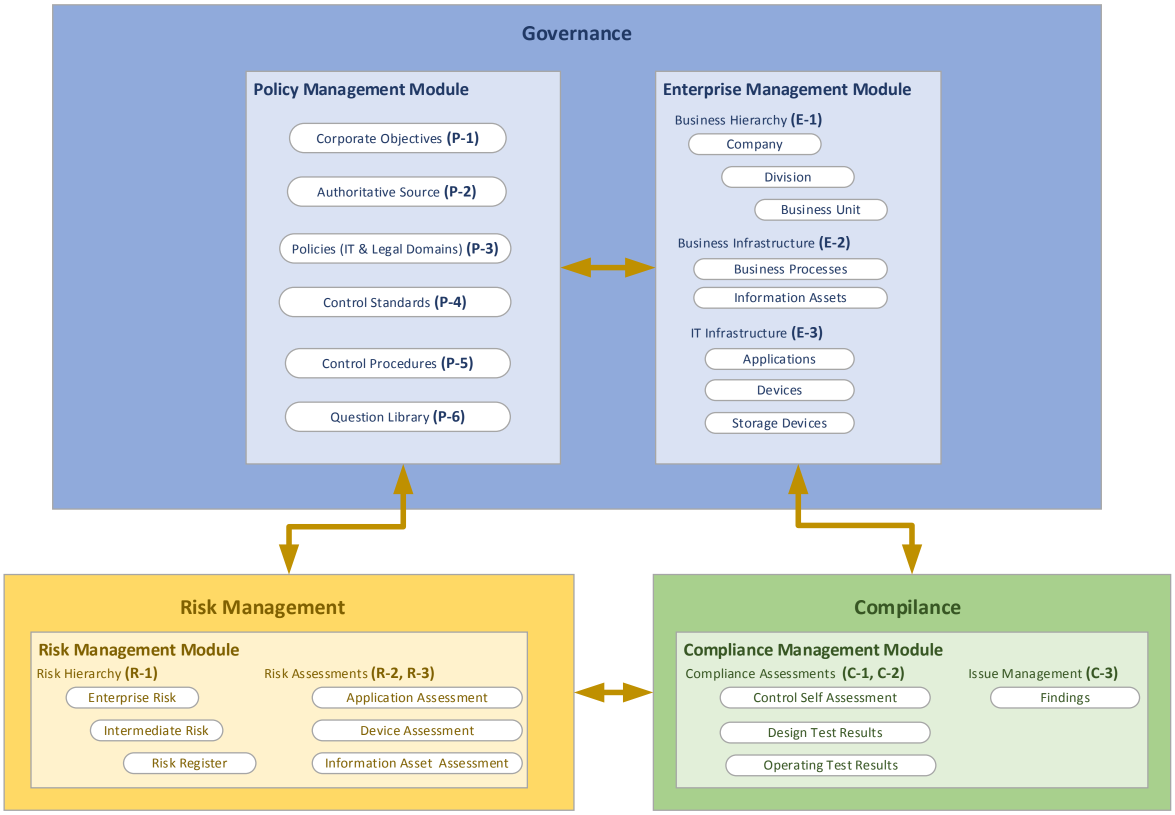


Table 2: High Level Process Steps summarizes the tasks that are conducted for this use case. For most of the tasks, the sequential order is not necessary. The task step is used as the content correlator within this guide. The techniques and relevant content sources are outlined as references. The column of "RM Tool Required?" is an indicator to the organizations, even

without an integrated risk management tool, accomplishes levels of risk management. Also, the manually prepared risk management contents (i.e., using spreadsheets) can be valuable inputs to the risk management tool, if an organization chooses to do so in a later stage.

Table 2: High Level Process Steps

Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
P-1	Define Corporate Objectives	Each organization has its own objectives for conducting the business. The objectives can be classified into different categories, such as strategic, operational, reporting and compliance etc. The objectives can be related to the defined policies and risks. Through those associations, Archer supports an organization to track policies and monitoring related risks and key performance indicators. For the demonstration purpose, this use case select a single objective from SP 800-66. **Primary Source:** NIST SP 800-66	**Archer Module:** Policy Management **Archer App:** Corporate Objectives **Actions:** use the Archer UI to create/update the corporate objectives and associate the objective to necessary existing policies, organizations, risks.	No
P-2	Select/Define Authoritative Source	In order to scope down the set of relevant controls, NCCoE takes the advantage of Archer's content library for the HIPAA Security as the authoritative source, but remap them to the set of control standards that are specifically created for HIPAA Security (P-4 & P-5). **Primary Source:** HIPAA/Archer content library, NCCoE	**Archer Module:** Policy Management **Archer App:** Authoritative Sources **Actions:** Created new report for Authoritative Sources for the target subset of the authoritative source. **To create new report:** Policy Management (tab) > Authoritative Source (side menu) > Reports > New > > Select reporting fields > Enter filters (for HIPAA security technical safeguards) > Enter sort option > Enter display option > Save report **To access to the new report:** Policy Management (tab) > Authoritative Source (side menu) > Records (side menu) > Reports (icon) > HIPAA Security Technical Safeguard Compliance (Select Report popup)	Yes
P-3	Select/Define related Policies			
P-4	Create relevant Control Standards	The NIST SP 800-66 is used as the guidance for NCCoE to create a set of Control Standards that are directly mapped to the HIPAA Security, Technical Safeguard (see Figure: Control Standards). Relevant SP 800-53r4 controls are also being created and mapped to the HIPAA related control standards (see Figure: Control Procedures – NCCoE) **Primary Source:** HIPAA Security, Technical Safeguards, NIST SP 800-	**Archer Module:** Policy Management **Archer App:** Control Standards **Actions:** use the Archer UI to create/update the control standards that corresponding to relevant source. **To create new control standard:** Policy Management (tab) > Control Standards (side menu) > New Record > enter data > Save **Archer App:** Control Procedures **Actions:** use the Archer UI to import pre-defined data from spreadsheet. **To import control procedures:**	No
P-5	Select SP800-53 control procedures			

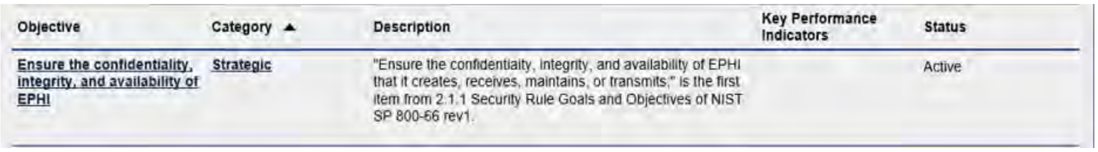
Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
		66, and NIST SP 800-53-r4	Policy Management (tab) > Control Procedures (side menu) > Data Import > Follow the Data Import Wizard to Select data file, select format option, perform data mapping, and import data.	
P-6	Create questionnaires by importing questions	The Security Risk Assessment Tool from the Office of the National Coordinator for Health Information Technology (ONC) is adopted for populating the questionnaires. **Primary Source:** HHS/ONC SRA tool	**Archer Module:** Policy Management **Archer App:** Question Library **Actions:** use the Archer UI to import pre-defined data from spreadsheet. **To import questionnaires:** Policy Management (tab) > Question Library (side menu) > Data Import > Follow the Data Import Wizard to Select data file, select format option, perform data mapping, and import data.	No
E-1	Define/Import Business Hierarchy	Pseudo organizations are used for presenting the organizations that defined in lab environment. **Primary Source:** NCCoE HIT EHR Mobile Device Use Case	**Archer Module:** Enterprise Management **Archer App:** Business Hierarchy **Actions:** use the Archer UI to create/update the business hierarchy and associate them to necessary existing policies, objectives, risks, and etc. **To create new company/division/business unit:** Enterprise Management (tab) > Business Hierarchy (side menu) > Company/Division/Business Unit > New Record.	No
E-2	Define/Import Business Infrastructure	With the pseudo organization and lab environment setting, this use case only defines Business Process and Information Assets in this group. **Primary Source:** NCCoE HIT EHR Mobile Device Use Case	**Archer Module:** Enterprise Management **Archer App:** Business Infrastructure **Actions:** use the Archer UI to create/update the Business Processes and Information Assets and associate them to necessary existing policies, organizations, objectives, risks, and etc. **To create new business processes/information assets:** Enterprise Management (tab) > Business Infrastructure (side menu) > Business Processes/Information Assets > New Record.	No
E-3	Define/Import IT Infrastructure	With the pseudo organization and lab environment setting, this use case defines Applications and Devices in this group. **Primary Source:** NCCoE HIT EHR Mobile Device Use Case (inventory list, device scanning list, etc.)	**Archer Module:** Enterprise Management **Archer App:** IT Infrastructure **Actions:** use the Archer UI to import pre-defined data from spreadsheets and then use Archer UI to associate them to necessary existing policies, organizations, objectives, risks, and etc. **To import applications/devices:** Enterprise Management (tab) > IT Infrastructure (side menu) > Applications/Devices > Data Import > Follow the Data Import Wizard to Select data file,	No

Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
			select format option, perform data mapping, and import data.	
R-1	Identify and rating risks and define risk hierarchy	Three-level Risk Hierarchy enables organization to roll-up their risk register from detailed risk records to an Intermediate summary level, and to an Enterprise level. Based on the NIST SP 800-30 (see diagram below), a study was conducted for identifying the risks in the NCCoE HIT Mobile Device use case environment based on the identified Threat Sources and Events, vulnerabilities, likelihood and impact. Refer to RAM section for details on the risk identification procedures. **Primary Source:** Identified Risks from the risk assessment exercise	**Archer Module:** Risk Management **Archer App:** Risk Hierarchy/Risk Register **Actions:** use the Archer UI to create risk hierarchy and risk register with all the risk assessment results. Then associate them to necessary existing policies, organizations, objectives, risks, devices, applications, and etc. **To create new risk hierarchy/risk register:** Risk Management (tab) > Risk Hierarchy/Risk Register (side menu) > New Record.	No
R-2	Design and conduct risk assessment for Applications, Devices and Info Asset	Modify the existing Archer assessment app for Application, Device and Information Asset by incorporating corresponding questionnaires form HHS/ONC SRA tool. Then conduct the assessments for required applications, devices, and information assets. The assessment results are aggregated and used throughout all associated objects (i.e., other asset type, business unit, business process, and objectives etc.) Business impacts can also be captured during the assessment process. **Primary Source:** HHS/ONC SRA tool and Archer Content Library	**Archer Module:** Risk Management **Archer App:** Risk Assessments **Actions:** use the Archer UI to modify existing assessment app; use the Archer UI to conduct assessments **To modify existing assessment apps:** Risk Management (tab) > Administration (side menu) > Manage Questionnaires (pop-up menu) > Application Assessment/Device Assessment/Information Asset Assessment (list on screen) > click Edit icon under Action > Field (tab) import ONC questionnaires > Layout (tab) to add additional sections with corresponding questions > Save. **To conduct risk assessment:** Risk Management (tab) > Risk Assessments (side menu) > Application Assessment/Device Assessment/Information Asset Assessment (side submenu) > select record > conduct assessment > Save.	Yes
R-3	Risk Assessment result/impact analysis and decision making	Various reports and charts can be accessed for viewing the assessment results and conducting the impact analysis at different levels and different modules. **Primary Source:** NCCoE	**Archer Module:** all used modules **Archer App:** any app that has risk management tab to be associated or reports that on the dashboard. **Actions:** various – see sample screenshots	Yes
C-1	Compliance Assessment	Various assessments can be used for checking the compliance to HIPAA, control standards, and control procedures **Primary Source:** HIPAA, HHS/ONC	**Archer Module:** Compliance Management **Archer App:** Compliance Assessments **Actions:** use the Archer UI to conduct assessments **To conduct compliance assessment:**	Yes

Task Step #	Task	Description & Primary Source	Techniques / Steps in using Archer	RM Tool Required?
		SRA tool, Archer content library	Compliance Management (tab) > Compliance Assessments (side menu) > Select type of assessment (side submenu) > select record > conduct assessment > Save.	
C-2	Compliance Assessment result/impact analysis and decision making	Create customized and use existing reports and charts to view assessment results and conducting the impact analysis at different levels and different modules. **Primary Source:** NCCoE	**Archer Module:** all used modules **Archer App:** any app that has compliance management tab to be associated or reports that on the dashboard. **Actions:** various – see sample screenshots	Yes
C-3	Issue Management	Issue Management module is embed in other modules, such as Risk Management, Compliance Management, and others. All related activities, such as assessments, imported scanning results and other tests produce “Findings”, which can be managed as issues. **Primary Source:** NCCoE	**Archer Module:** Issue Management **Archer App:** Findings. **Actions:** various – see sample screenshots **To access “Finding reports”:** Risk/Compliance Management (tab) > Issue Management (side menu) > Findings (side submenu) > Report icon > select report from drop-down list > view report (drill down to for other actions).	Yes
Final	Integrate with external data sources and customize reports and dashboards	Utilizing the Data Feed feature to setup the		Yes

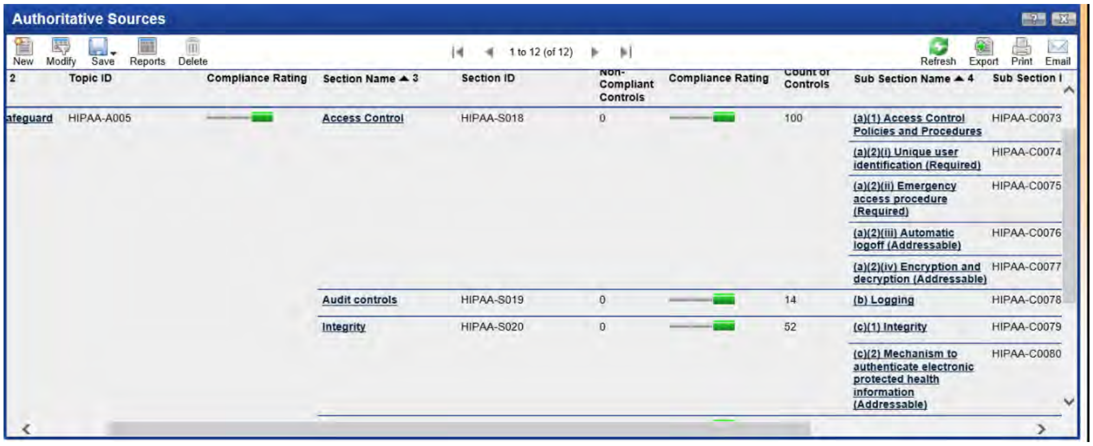
Below are sample screenshots for the steps defined in the table above:

P-1) Define Corporate Objectives



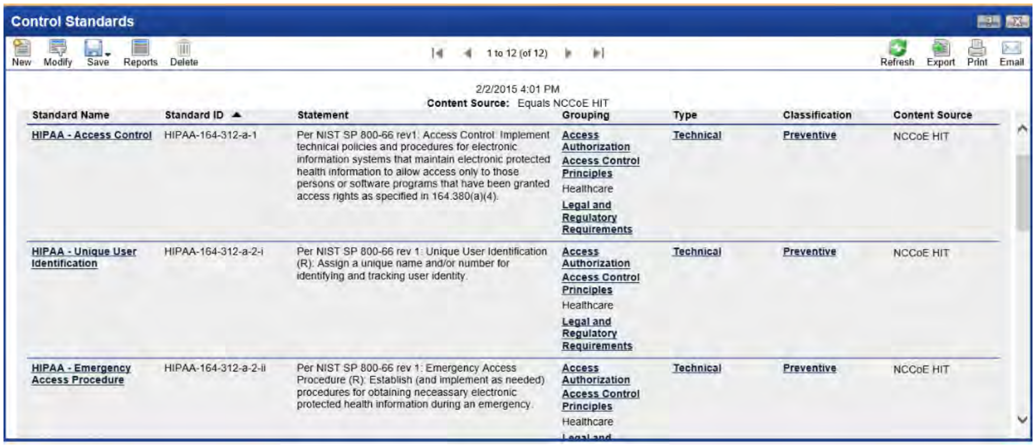
Objective	Category ▲	Description	Key Performance Indicators	Status
Ensure the confidentiality, integrity, and availability of EPHI	Strategic	"Ensure the confidentiaity, integrity, and availability of EPHI that it creates, receives, maintains, or transmits;" is the first item from 2.1.1 Security Rule Goals and Objectives of NIST SP 800-66 rev1.		Active

P-2) & P-3) Select/Define Authoritative Source (HIPAA Security) and related Policies



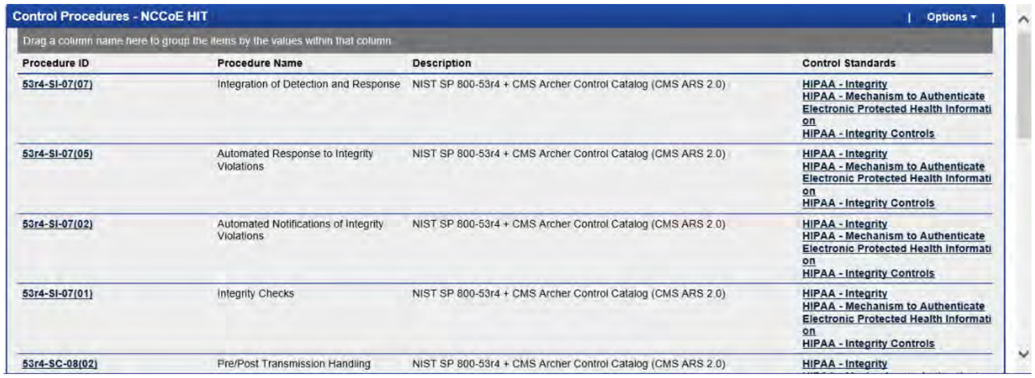
2	Topic ID	Compliance Rating	Section Name ▲ 3	Section ID	Non-Compliant Controls	Compliance Rating	Count of Controls	Sub Section Name ▲ 4	Sub Section I
afeguard	HIPAA-A005	🟩	Access Control	HIPAA-S018	0	🟩	100	(a)(1) Access Control Policies and Procedures	HIPAA-C0073
								(a)(2)(i) Unique user identification (Required)	HIPAA-C0074
								(a)(2)(ii) Emergency access procedure (Required)	HIPAA-C0075
								(a)(2)(iii) Automatic logoff (Addressable)	HIPAA-C0076
								(a)(2)(iv) Encryption and decryption (Addressable)	HIPAA-C0077
			Audit controls	HIPAA-S019	0	🟩	14	(b) Logging	HIPAA-C0078
			Integrity	HIPAA-S020	0	🟩	52	(c)(1) Integrity	HIPAA-C0079
								(c)(2) Mechanism to authenticate electronic protected health information (Addressable)	HIPAA-C0080

P-4) & P-5) Create relevant Control Standards and Select SP800-53 control procedures (focus on HIPAA Security, Technical Safeguards)



2/2/2015 4:01 PM
Content Source: Equals NCCoE HIT

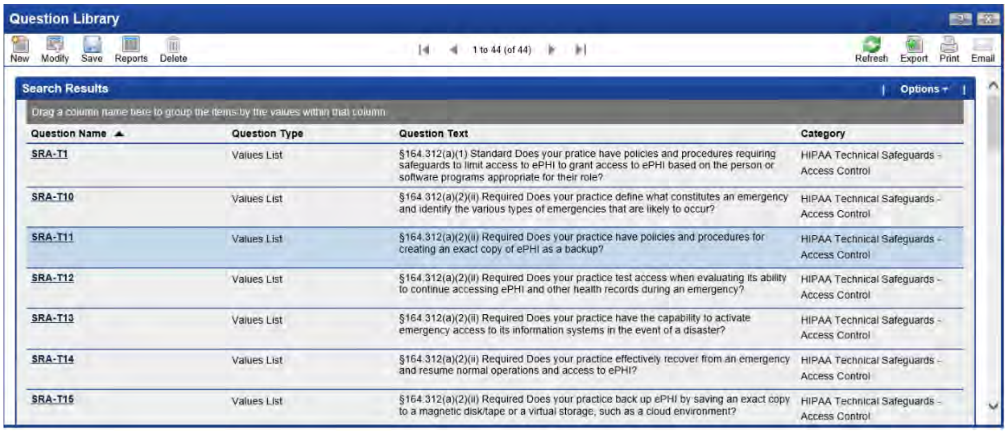
Standard Name	Standard ID ▲	Statement	Grouping	Type	Classification	Content Source
HIPAA - Access Control	HIPAA-164-312-a-1	Per NIST SP 800-66 rev1: Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in 164.380(a)(4).	Access Authorization Access Control Principles Healthcare Legal and Regulatory Requirements	Technical	Preventive	NCCoE HIT
HIPAA - Unique User Identification	HIPAA-164-312-a-2-i	Per NIST SP 800-66 rev 1: Unique User Identification (R): Assign a unique name and/or number for identifying and tracking user identity.	Access Authorization Access Control Principles Healthcare Legal and Regulatory Requirements	Technical	Preventive	NCCoE HIT
HIPAA - Emergency Access Procedure	HIPAA-164-312-a-2-ii	Per NIST SP 800-66 rev 1: Emergency Access Procedure (R): Establish (and implement as needed) procedures for obtaining neceassary electronic protected health information during an emergency.	Access Authorization Access Control Principles Healthcare Legal and	Technical	Preventive	NCCoE HIT



Control Procedures - NCCoE HIT
Options
Drag a column name here to group the items by the values within that column.

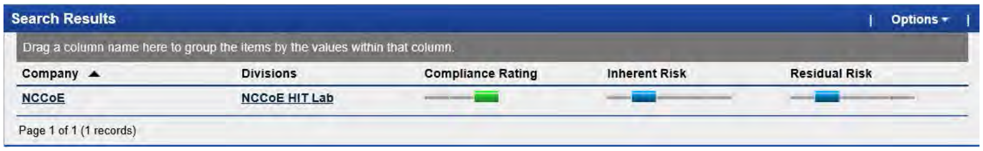
Procedure ID	Procedure Name	Description	Control Standards
53r4-SI-07(07)	Integration of Detection and Response	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Information HIPAA - Integrity Controls
53r4-SI-07(05)	Automated Response to Integrity Violations	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Information HIPAA - Integrity Controls
53r4-SI-07(02)	Automated Notifications of Integrity Violations	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Information HIPAA - Integrity Controls
53r4-SI-07(01)	Integrity Checks	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity HIPAA - Mechanism to Authenticate Electronic Protected Health Information HIPAA - Integrity Controls
53r4-SC-08(02)	Pre/Post Transmission Handling	NIST SP 800-53r4 + CMS Archer Control Catalog (CMS ARS 2.0)	HIPAA - Integrity

P-6) Create questionnaires by importing questions from HHS/ONC SRA tool



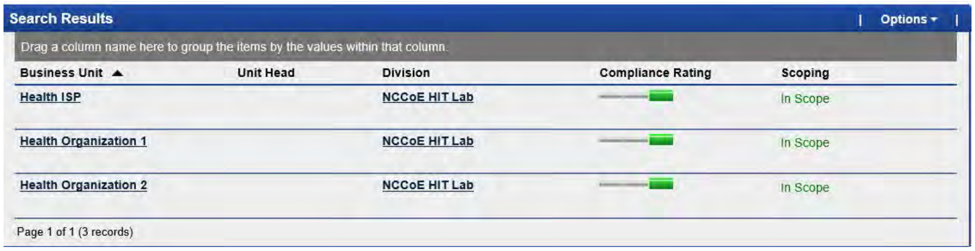
Question Name ▲	Question Type	Question Text	Category
SRA-T1	Values List	§164.312(a)(1) Standard Does your pratice have policies and procedures requiring safeguards to limit access to ePHI to grant access to ePHI based on the person or software programs appropriate for their role?	HIPAA Technical Safeguards - Access Control
SRA-T10	Values List	§164.312(a)(2)(ii) Required Does your practice define what constitutes an emergency and identify the various types of emergencies that are likely to occur?	HIPAA Technical Safeguards - Access Control
SRA-T11	Values List	§164.312(a)(2)(ii) Required Does your practice have policies and procedures for creating an exact copy of ePHI as a backup?	HIPAA Technical Safeguards - Access Control
SRA-T12	Values List	§164.312(a)(2)(ii) Required Does your practice test access when evaluating its ability to continue accessing ePHI and other health records during an emergency?	HIPAA Technical Safeguards - Access Control
SRA-T13	Values List	§164.312(a)(2)(ii) Required Does your practice have the capability to activate emergency access to its information systems in the event of a disaster?	HIPAA Technical Safeguards - Access Control
SRA-T14	Values List	§164.312(a)(2)(ii) Required Does your practice effectively recover from an emergency and resume normal operations and access to ePHI?	HIPAA Technical Safeguards - Access Control
SRA-T15	Values List	§164.312(a)(2)(ii) Required Does your practice back up ePHI by saving an exact copy to a magnetic disk/tape or a virtual storage, such as a cloud environment?	HIPAA Technical Safeguards - Access Control

E-1) Define/Import Business Hierarchy


Search Results
Options
Drag a column name here to group the items by the values within that column.

Company ▲	Divisions	Compliance Rating	Inherent Risk	Residual Risk
NCCoE	NCCoE HIT Lab	🟩	🟦	🟦

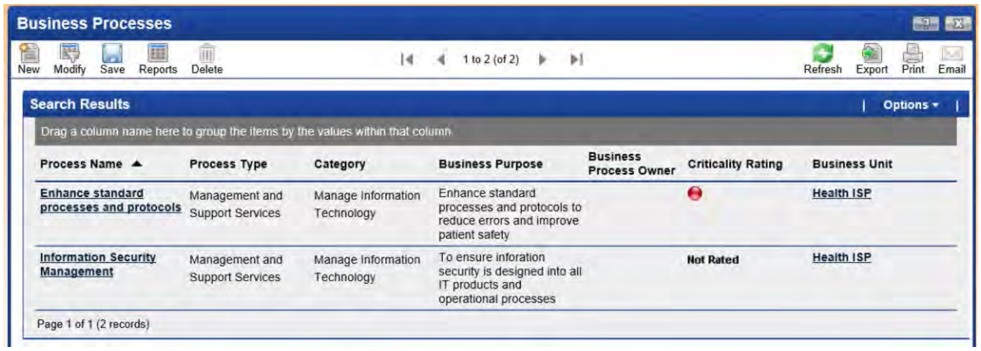
Page 1 of 1 (1 records)


Search Results
Options
Drag a column name here to group the items by the values within that column.

Business Unit ▲	Unit Head	Division	Compliance Rating	Scoping
Health ISP		NCCoE HIT Lab	🟩	In Scope
Health Organization 1		NCCoE HIT Lab	🟩	In Scope
Health Organization 2		NCCoE HIT Lab	🟩	In Scope

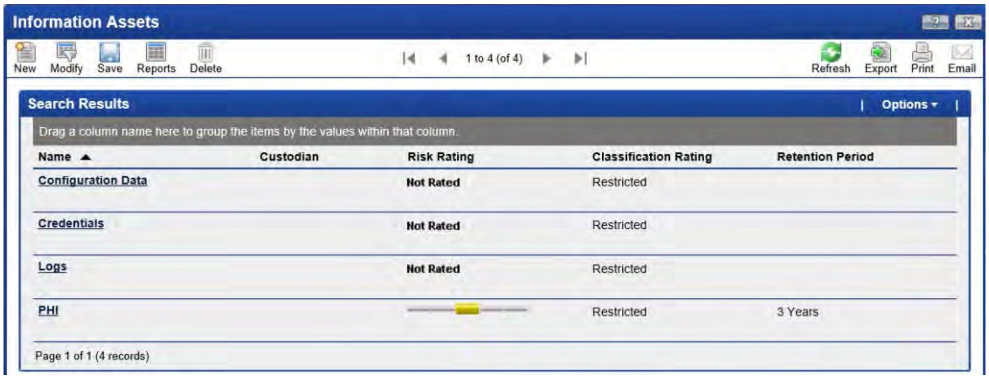
Page 1 of 1 (3 records)

E-2) Define/Import Business Infrastructure



Process Name ▲	Process Type	Category	Business Purpose	Business Process Owner	Criticality Rating	Business Unit
Enhance standard processes and protocols	Management and Support Services	Manage Information Technology	Enhance standard processes and protocols to reduce errors and improve patient safety		🔴	Health ISP
Information Security Management	Management and Support Services	Manage Information Technology	To ensure inforation security is designed into all IT products and operational processes		Not Rated	Health ISP

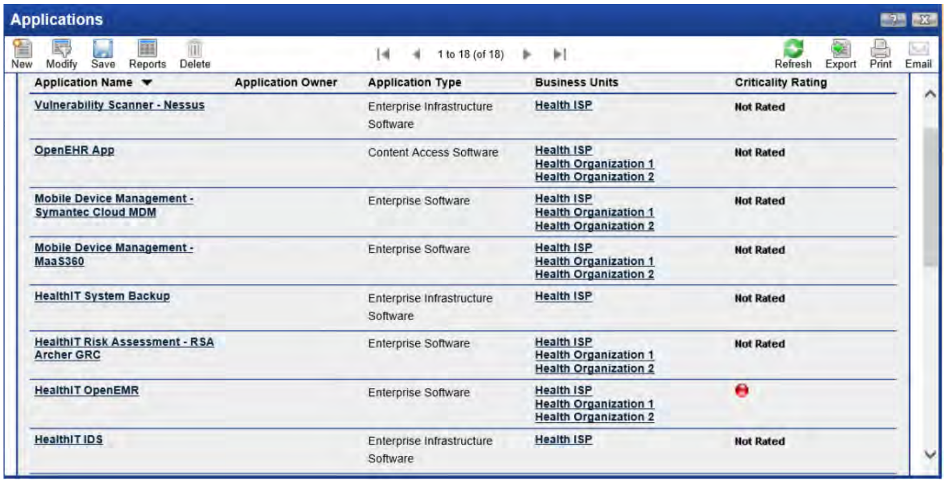
Page 1 of 1 (2 records)



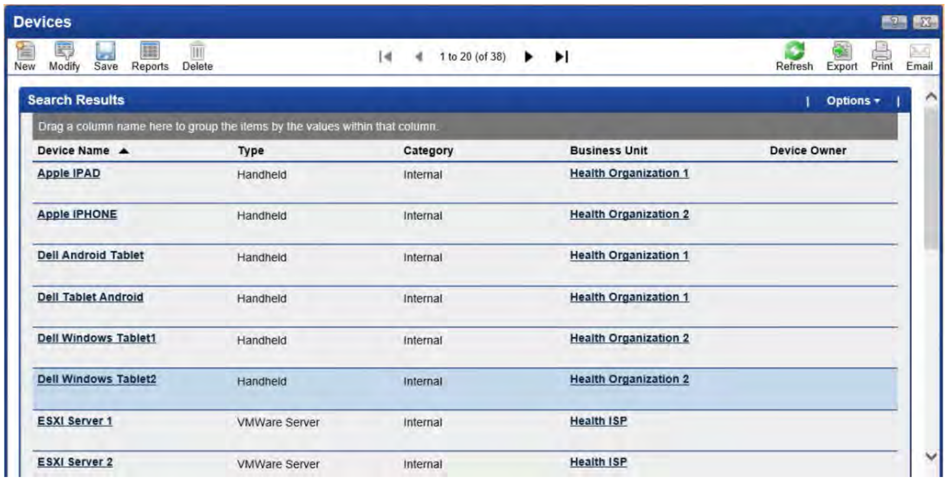
Name ▲	Custodian	Risk Rating	Classification Rating	Retention Period
Configuration Data		Not Rated	Restricted	
Credentials		Not Rated	Restricted	
Logs		Not Rated	Restricted	
PHI		🟨	Restricted	3 Years

Page 1 of 1 (4 records)

E-3) Define/Import IT Infrastructure



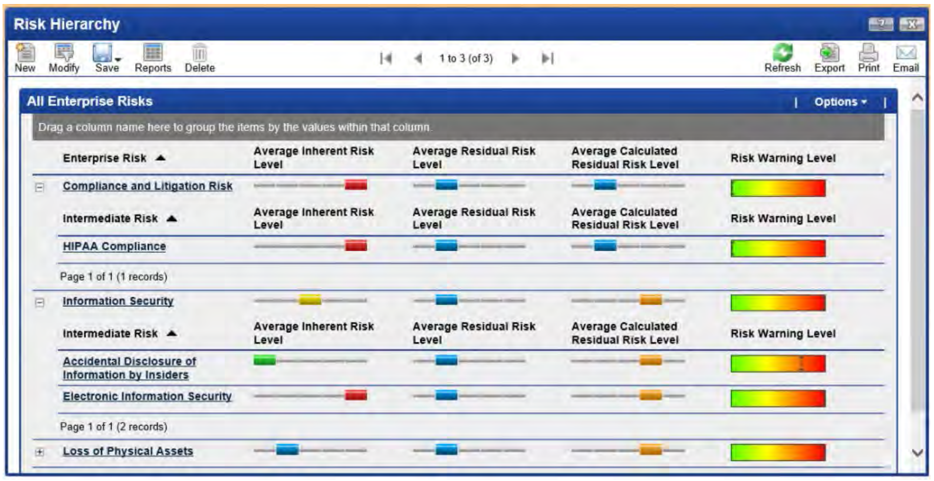
Application Name ▼	Application Owner	Application Type	Business Units	Criticality Rating
Vulnerability Scanner - Nessus		Enterprise Infrastructure Software	Health ISP	Not Rated
OpenEHR App		Content Access Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
Mobile Device Management - Symantec Cloud MDM		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
Mobile Device Management - MaaS360		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
HealthIT System Backup		Enterprise Infrastructure Software	Health ISP	Not Rated
HealthIT Risk Assessment - RSA Archer GRC		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	Not Rated
HealthIT OpenEMR		Enterprise Software	Health ISP Health Organization 1 Health Organization 2	●
HealthIT IDS		Enterprise Infrastructure Software	Health ISP	Not Rated



Drag a column name here to group the items by the values within that column.

Device Name ▲	Type	Category	Business Unit	Device Owner
Apple IPAD	Handheld	Internal	Health Organization 1	
Apple IPHONE	Handheld	Internal	Health Organization 2	
Dell Android Tablet	Handheld	Internal	Health Organization 1	
Dell Tablet Android	Handheld	Internal	Health Organization 1	
Dell Windows Tablet1	Handheld	Internal	Health Organization 2	
Dell Windows Tablet2	Handheld	Internal	Health Organization 2	
ESXI Server 1	VMWare Server	Internal	Health ISP	
ESXI Server 2	VMWare Server	Internal	Health ISP	

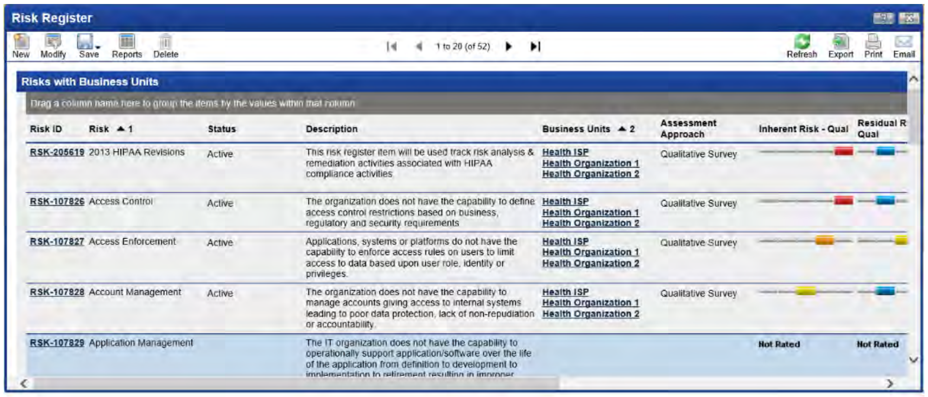
R-1) Identify and rating risks and define risk hierarchy



Drag a column name here to group the items by the values within that column.

Enterprise Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
⊟ Compliance and Litigation Risk	🟥	🟦	🟦	
Intermediate Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
HIPAA Compliance	🟥	🟦	🟦	
Page 1 of 1 (1 records)				
⊟ Information Security	🟨	🟦	🟧	
Intermediate Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
Accidental Disclosure of Information by Insiders	🟩	🟦	🟧	
Electronic Information Security	🟥	🟦	🟧	
Page 1 of 1 (2 records)				
⊞ Loss of Physical Assets	🟦	🟦	🟧	

Risk Register



Risk Register

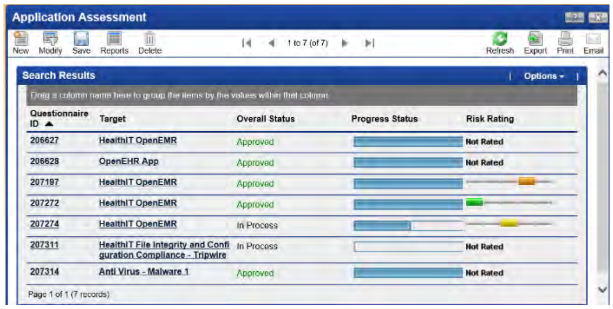
New Modify Save Reports Delete | 1 to 20 (of 52) | Refresh Export Print Email

Risks with Business Units

Drag a column name here to group the items by the values within that column

Risk ID	Risk ▲ 1	Status	Description	Business Units ▲ 2	Assessment Approach	Inherent Risk - Qual	Residual R Qual
RSK-205619	2013 HIPAA Revisions	Active	This risk register item will be used track risk analysis & remediation activities associated with HIPAA compliance activities	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟥	🟦
RSK-107826	Access Control	Active	The organization does not have the capability to define access control restrictions based on business, regulatory and security requirements	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟥	🟦
RSK-107827	Access Enforcement	Active	Applications, systems or platforms do not have the capability to enforce access rules on users to limit access to data based upon user role, identity or privileges.	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟧	🟨
RSK-107828	Account Management	Active	The organization does not have the capability to manage accounts giving access to internal systems leading to poor data protection, lack of non-repudiation or accountability.	Health ISP Health Organization 1 Health Organization 2	Qualitative Survey	🟨	🟦
RSK-107829	Application Management		The IT organization does not have the capability to operationally support application/software over the life of the application from definition to development to implementation to retirement resulting in improper			Not Rated	Not Rated

R-2) & R-3) Perform risk assessment, result/impact analysis and decision making for Applications, Devices and Info Asset



Application Assessment

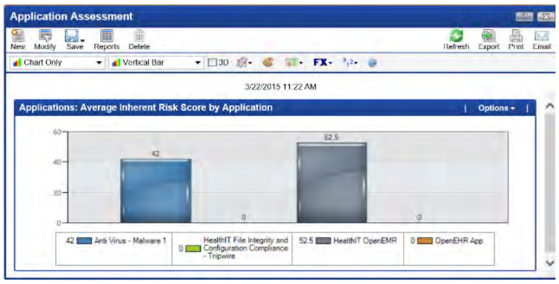
New Modify Save Reports Delete | 1 to 7 (of 7) | Refresh Export Print Email

Search Results | Options ▾ |

Drag a column name here to group the items by the values within that column.

Questionnaire ID ▲	Target	Overall Status	Progress Status	Risk Rating
206627	HealthIT OpenEMR	Approved		Not Rated
206628	OpenEHR App	Approved		Not Rated
207197	HealthIT OpenEMR	Approved		🟧
207272	HealthIT OpenEMR	Approved		🟩
207274	HealthIT OpenEMR	In Process		🟨
207311	HealthIT File Integrity and Confi guration Compliance - Tripwire	In Process		Not Rated
207314	Anti Virus - Malware 1	Approved		Not Rated

Page 1 of 1 (7 records)



Application Assessment

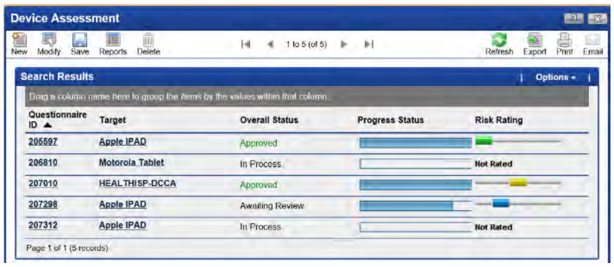
New Modify Save Reports Delete | Refresh Export Print Email

Chart Only ▾ | Vertical Bar ▾ | □3D | FX▾

3/22/2015 11:22 AM

Applications: Average Inherent Risk Score by Application | Options ▾ |

60
40
20
0
42
0
52.5
0
42 Anti Virus - Malware 1
0 HealthIT File Integrity and Configuration Compliance - Tripwire
52.5 HealthIT OpenEMR
0 OpenEHR App



Device Assessment

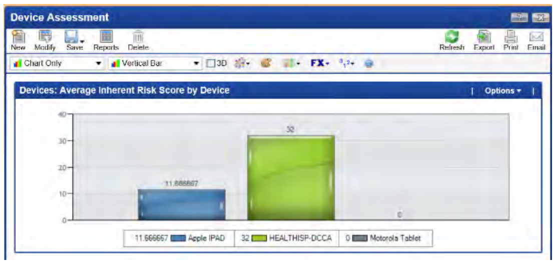
New Modify Save Reports Delete | 1 to 5 (of 5) | Refresh Export Print Email

Search Results | Options ▾ |

Drag a column name here to group the items by the values within that column.

Questionnaire ID ▲	Target	Overall Status	Progress Status	Risk Rating
205597	Apple IPAD	Approved		🟩
206810	Motorola Tablet	In Process		Not Rated
207010	HEALTHISP-DCCA	Approved		🟨
207298	Apple IPAD	Awaiting Review		🟦
207312	Apple IPAD	In Process		Not Rated

Page 1 of 1 (5 records)

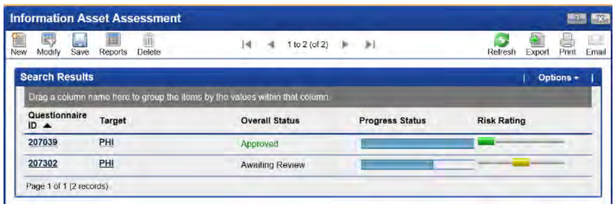


Device Assessment

New Modify Save Reports Delete | Refresh Export Print Email

Chart Only ▾ | Vertical Bar ▾ | □3D | FX▾

Devices: Average Inherent Risk Score by Device | Options ▾ |



Information Asset Assessment

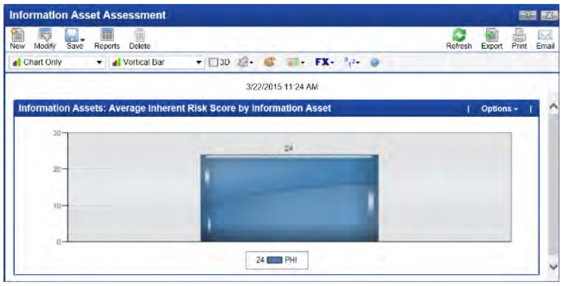
New Modify Save Reports Delete | 1 to 2 (of 2) | Refresh Export Print Email

Search Results | Options ▾ |

Drag a column name here to group the items by the values within that column.

Questionnaire ID ▲	Target	Overall Status	Progress Status	Risk Rating
207039	PHI	Approved		🟩
207302	PHI	Awaiting Review		🟨

Page 1 of 1 (2 records)



Information Asset Assessment

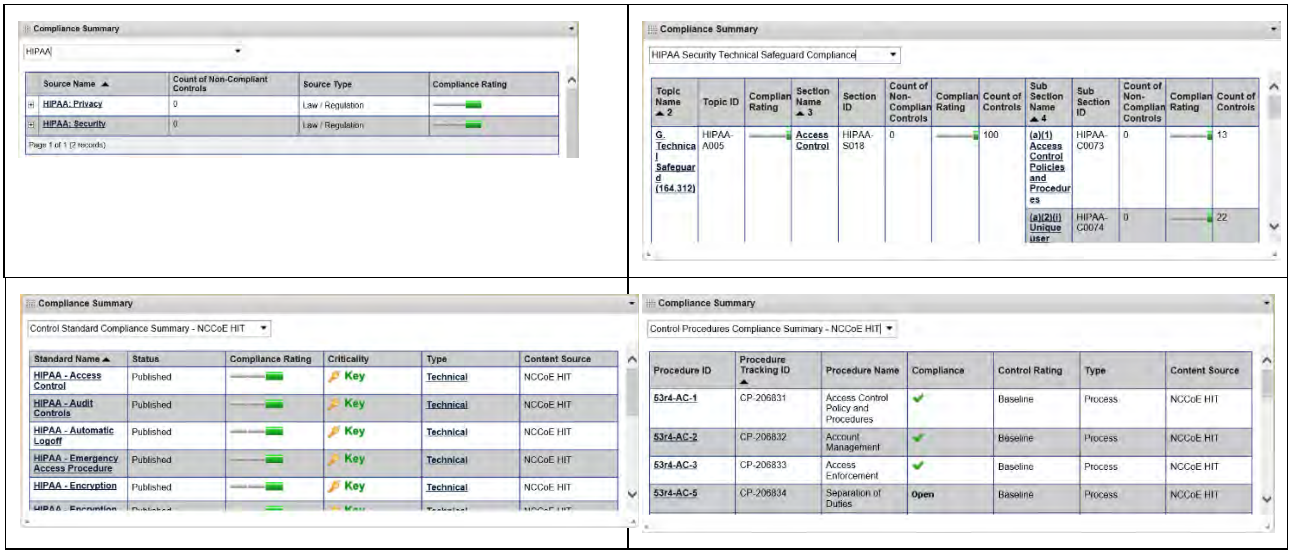
New Modify Save Reports Delete | Refresh Export Print Email

Chart Only ▾ | Vertical Bar ▾ | □3D | FX▾

3/22/2015 11:24 AM

Information Assets: Average Inherent Risk Score by Information Asset | Options ▾ |

C-1) & C-2) Perform compliance assessment, result/impact analysis and decision making



HIPAA

	Source Name ▲	Count of Non-Compliant Controls	Source Type	Compliance Rating
⊞	HIPAA: Privacy	0	Law / Regulation	
⊞	HIPAA: Security	0	Law / Regulation	

Page 1 of 1 (2 records)

HIPAA Security Technical Safeguard Compliance

Topic Name ▲ 2	Topic ID	Complian Rating	Section Name ▲ 3	Section ID	Count of Non-Complian Controls	Complian Rating	Count of Controls	Sub Section Name ▲ 4	Sub Section ID	Count of Non-Complian Controls	Complian Rating	Count of Controls
G. Technical Safeguard (164.312)	HIPAA-A005		Access Control	HIPAA-S018	0		100	(a)(1) Access Control Policies and Procedures	HIPAA-C0073	0		13
								(a)(2)(i) Unique user	HIPAA-C0074	0		22

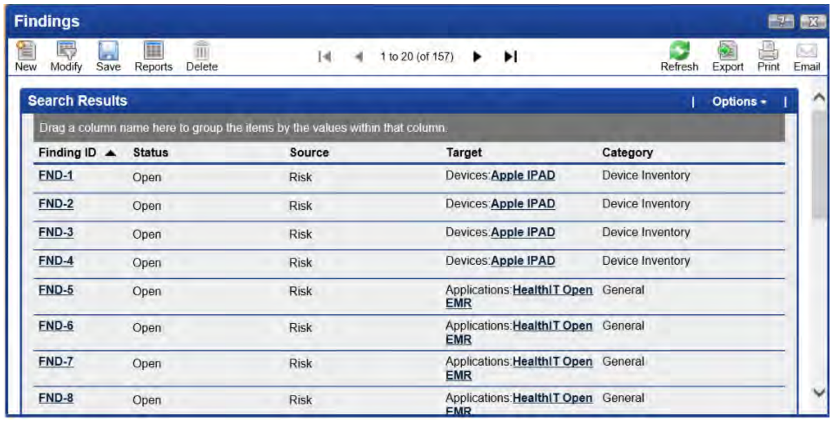
Control Standard Compliance Summary - NCCoE HIT

Standard Name ▲	Status	Compliance Rating	Criticality	Type	Content Source
HIPAA - Access Control	Published		Key	Technical	NCCoE HIT
HIPAA - Audit Controls	Published		Key	Technical	NCCoE HIT
HIPAA - Automatic Logoff	Published		Key	Technical	NCCoE HIT
HIPAA - Emergency Access Procedure	Published		Key	Technical	NCCoE HIT
HIPAA - Encryption	Published		Key	Technical	NCCoE HIT
HIPAA - Encryption	Published		Key	Technical	NCCoE HIT

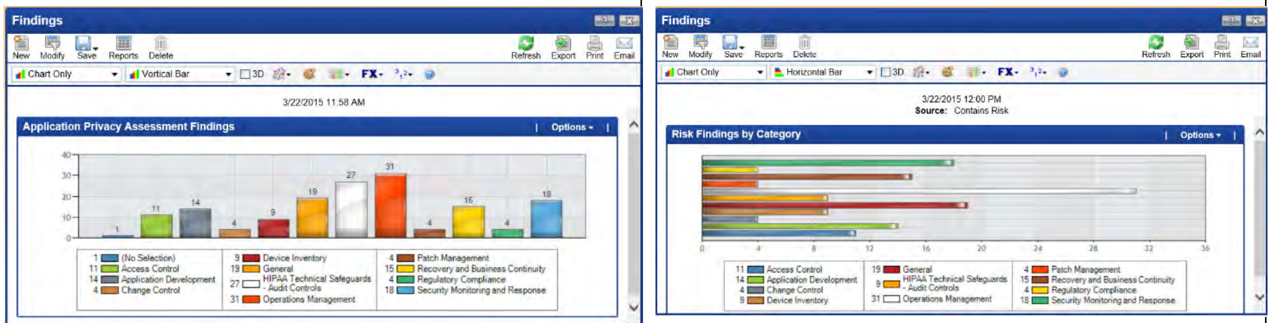
Control Procedures Compliance Summary - NCCoE HIT

Procedure ID	Procedure Tracking ID ▲	Procedure Name	Compliance	Control Rating	Type	Content Source
53r4-AC-1	CP-206831	Access Control Policy and Procedures	✓	Baseline	Process	NCCoE HIT
53r4-AC-2	CP-206832	Account Management	✓	Baseline	Process	NCCoE HIT
53r4-AC-3	CP-206833	Access Enforcement	✓	Baseline	Process	NCCoE HIT
53r4-AC-5	CP-206834	Separation of Duties	Open	Baseline	Process	NCCoE HIT

C-3) Manage Issues (Findings)

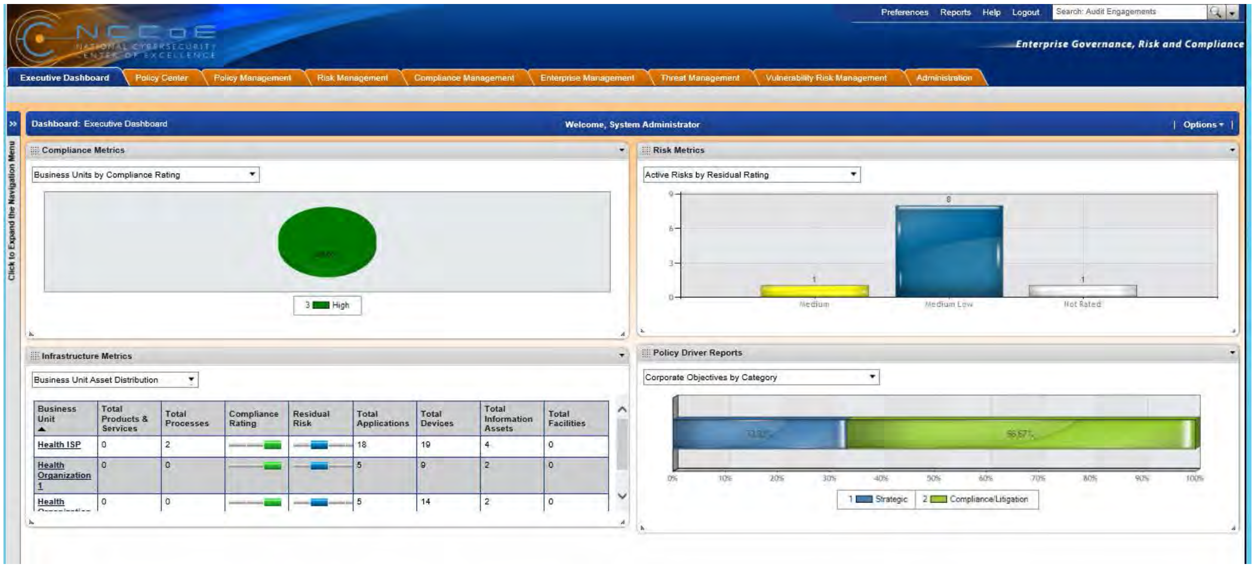


Finding ID ▲	Status	Source	Target	Category
FND-1	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-2	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-3	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-4	Open	Risk	Devices:Apple IPAD	Device Inventory
FND-5	Open	Risk	Applications:HealthIT Open EMR	General
FND-6	Open	Risk	Applications:HealthIT Open EMR	General
FND-7	Open	Risk	Applications:HealthIT Open EMR	General
FND-8	Open	Risk	Applications:HealthIT Open EMR	General



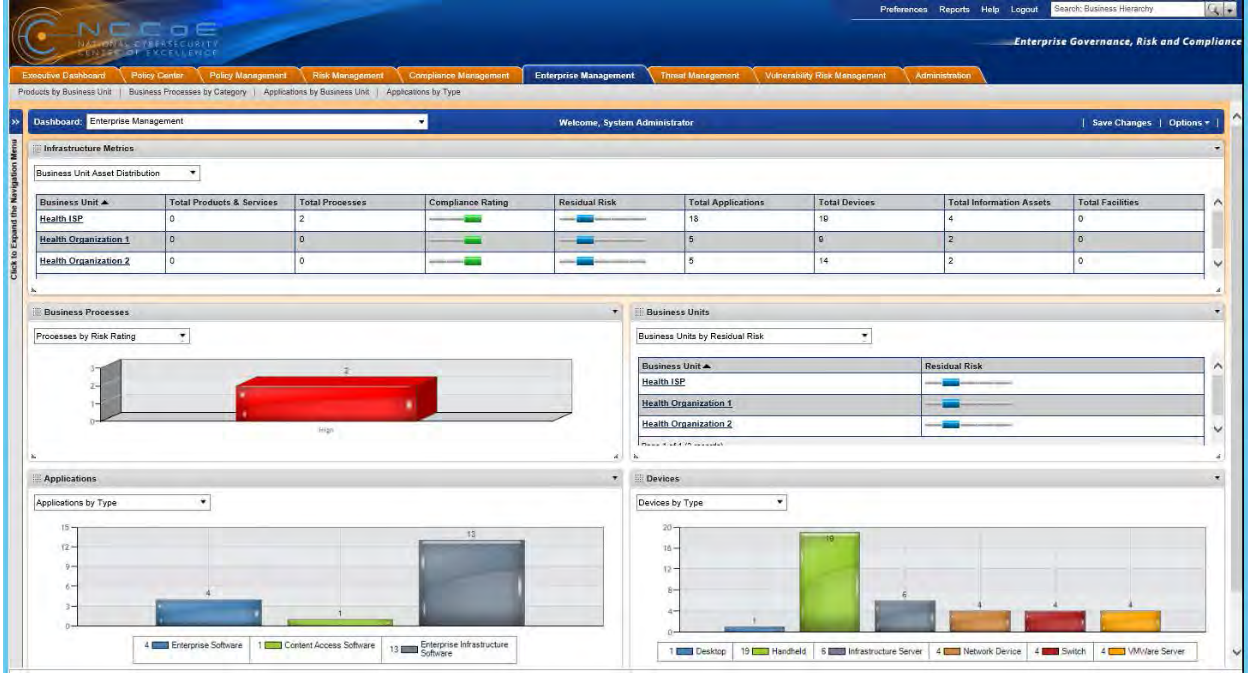
Final) Customized reports and dashboards creation samples

Executive Dashboard


Preferences
Reports
Help
Logout
Search: Audit Engagements
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Enterprise Governance, Risk and Compliance
Executive Dashboard
Policy Center
Policy Management
Risk Management
Compliance Management
Enterprise Management
Threat Management
Vulnerability Risk Management
Administration
Click to Expand the Navigation Menu
Dashboard: Executive Dashboard
Welcome, System Administrator
Options
Compliance Metrics
Business Units by Compliance Rating
3 High
Risk Metrics
Active Risks by Residual Rating
9
6
3
0
1
8
1
Medium
Medium Low
Not Rated
Infrastructure Metrics
Business Unit Asset Distribution
Policy Driver Reports
Corporate Objectives by Category
33.33%
66.67%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
1 Strategic
2 Compliance/Litigation

Business Unit ▲	Total Products & Services	Total Processes	Compliance Rating	Residual Risk	Total Applications	Total Devices	Total Information Assets	Total Facilities
Health ISP	0	2			18	19	4	0
Health Organization 1	0	0			5	9	2	0
Health	0	0			5	14	2	0

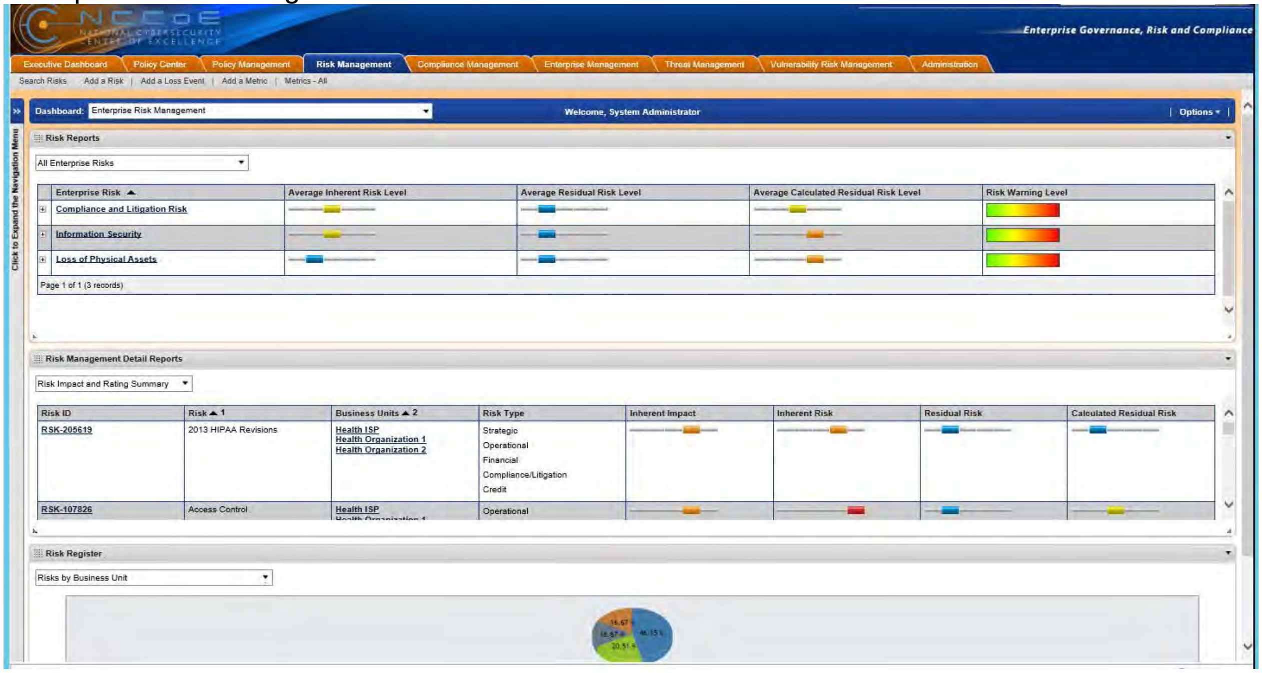
Enterprise Management Dashboard



Business Unit ▲	Total Products & Services	Total Processes	Compliance Rating	Residual Risk	Total Applications	Total Devices	Total Information Assets	Total Facilities
Health ISP	0	2			18	19	4	0
Health Organization 1	0	0			5	9	2	0
Health Organization 2	0	0			5	14	2	0

Business Unit ▲	Residual Risk
Health ISP	
Health Organization 1	
Health Organization 2	

Enterprise Risk Management Dashboard


NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Enterprise Governance, Risk and Compliance
Executive Dashboard
Policy Center
Policy Management
Risk Management
Compliance Management
Enterprise Management
Threat Management
Vulnerability Risk Management
Administration
Search Risks
Add a Risk | Add a Loss Event | Add a Metric | Metrics - All
Welcome, System Administrator
| Options ▾ |
Click to Expand the Navigation Menu
16.67 %
16.67 %
46.15 %
20.51 %

Dashboard: Enterprise Risk Management

Risk Reports

All Enterprise Risks

Enterprise Risk ▲	Average Inherent Risk Level	Average Residual Risk Level	Average Calculated Residual Risk Level	Risk Warning Level
Compliance and Litigation Risk	🟨	🟦	🟨	🟩🟨🟥
Information Security	🟨	🟦	🟧	🟩🟨🟥
Loss of Physical Assets	🟦	🟦	🟧	🟩🟨🟥

Page 1 of 1 (3 records)

Risk Management Detail Reports

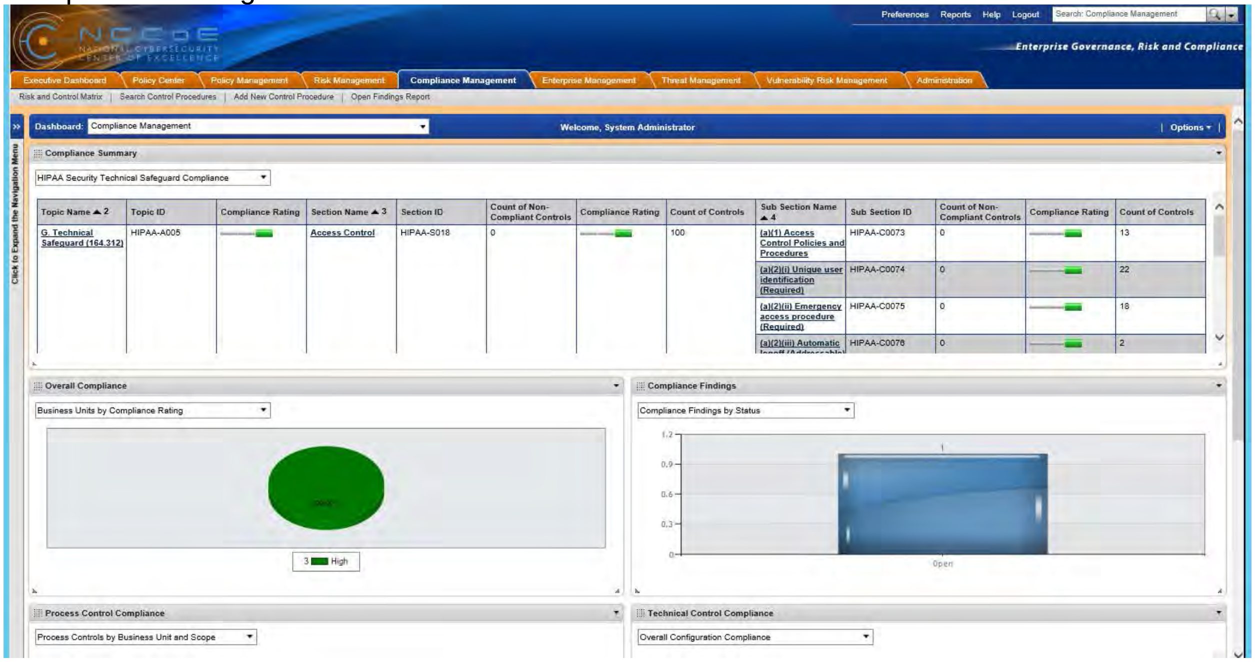
Risk Impact and Rating Summary

Risk ID	Risk ▲ 1	Business Units ▲ 2	Risk Type	Inherent Impact	Inherent Risk	Residual Risk	Calculated Residual Risk
RSK-205619	2013 HIPAA Revisions	Health ISP Health Organization 1 Health Organization 2	Strategic Operational Financial Compliance/Litigation Credit	🟧	🟧	🟦	🟦
RSK-107826	Access Control	Health ISP Health Organization 1	Operational	🟧	🟥	🟦	🟨

Risk Register

Risks by Business Unit

Compliance Management Dashboard


Preferences
Reports
Help
Logout
Search: Compliance Management
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Enterprise Governance, Risk and Compliance
Executive Dashboard
Policy Center
Policy Management
Risk Management
Compliance Management
Enterprise Management
Threat Management
Vulnerability Risk Management
Administration
Risk and Control Matrix | Search Control Procedures | Add New Control Procedure | Open Findings Report
Welcome, System Administrator
| Options ▾ |
Click to Expand the Navigation Menu
3 High
1.2
0.9
0.6
0.3
0
1
Open

Dashboard: Compliance Management

Compliance Summary

HIPAA Security Technical Safeguard Compliance

Topic Name ▲ 2	Topic ID	Compliance Rating	Section Name ▲ 3	Section ID	Count of Non-Compliant Controls	Compliance Rating	Count of Controls	Sub Section Name ▲ 4	Sub Section ID	Count of Non-Compliant Controls	Compliance Rating	Count of Controls
G. Technical Safeguard (164.312)	HIPAA-A005	🟩	Access Control	HIPAA-S018	0	🟩	100	(a)(1) Access Control Policies and Procedures	HIPAA-C0073	0	🟩	13
								(a)(2)(i) Unique user identification (Required)	HIPAA-C0074	0	🟩	22
								(a)(2)(ii) Emergency access procedure (Required)	HIPAA-C0075	0	🟩	18
								(a)(2)(iii) Automatic logoff (Addressable)	HIPAA-C0076	0	🟩	2

Overall Compliance

Business Units by Compliance Rating

Compliance Findings

Compliance Findings by Status

Process Control Compliance

Process Controls by Business Unit and Scope

Technical Control Compliance

Overall Configuration Compliance

11 Operating Systems

We used two types of operating systems, Windows-based and Unix-based. These choices were driven by the commercial products used in this example solution. Typically, open-source products run on open-source Unix-based operating systems.

11.1 Windows Installation and Hardening

11.1.1 Windows System Requirements

This build requires purchase and installation of the Windows 2012 Server and Windows 7 and 8.1 for workstations. You will also need the following:

Processor	Minimum 1.4 GHz 64-bit processor
RAM	Minimum 8 G
Disk space	Minimum 150 GB

11.1.2 Windows Installation

We assume you purchased the appropriate Microsoft OS and that you have both the CD and product key.

If you are not familiar with Microsoft's command line or non-graphical management, we recommend you first select the Desktop Experience option to make the installation process easier.

> Microsoft recommends Server Core as the most secure installation of Windows 2012.[2] In this build, however, we recommend a known interface—Desktop Experience—to help those unfamiliar with Server Core to navigate. We feel our defense in depth strategy addresses some of the risks. As you become more familiar with Server Core, you should opt for that.

Boot the system with the installation disk and follow the onscreen instructions to enable:

- Desktop Experience Installation (Windows 2012 Server only) for Windows 2012, versions 7 and 8.1

[2] According to Microsoft, “The Server Core Installation option reduces the space required on disk, the potential attack surface, and especially the servicing requirements, so [Microsoft] recommends that you choose the Server Core installation unless you have a particular need for the additional user interface elements and graphical management tools that are included in the ‘Server with a GUI’ option. An intermediate state is possible where you start with a Server with a GUI installation and then remove Server Graphical Shell, resulting in a server that comprises the ‘Minimal Server Interface,’ Microsoft Management Console (MMC), Server Manager, and a subset of Control Panel.” https://technet.microsoft.com/en-us/library/hh831786.aspx

- Local firewall – all unneeded ports and protocols blocked inbound and outbound
- Windows update – on and in a regularly scheduled state
- Bitlocker – full disk encryption enabled
- IPV6 – off, unless absolutely needed for your environment
- Roles and features – install only the roles and features needed to provide the production feature needed to serve your organization; remove all others if possible

See Section 3.1, Hostnames for hostnames to use.

> If you opt to change your organization's hostnames, you should make note of any changes for comparison and make necessary changes to the implementation of other products described here.

11.1.3 Windows Post-Installation Tasks

- Install the Puppet agent by following the Puppet Enterprise instructions in Section 5.
- Install the backup agent by following the URBackup instructions in Section 4.

11.1.4 Windows Security Hardening

11.1.4.1 Using Puppet

We employed Windows operating system hardening tasks that use the Puppet Enterprise Configuration Tool. At the least, each Windows system should be configured to receive base and custom sets of configuration enforcement instructions from Puppet. Puppet uses configuration files called manifests to house configuration enforcement instructions. The list of base Windows configuration manifests is below, along with a short explanation on why each was implemented on the Windows systems in this build.

Puppet Manifests

accounts.pp - allows control over users who can log in and their passwords. If an attacker changes any information, puppet will change settings back based on the entries in this file.

> We configured this feature, but did not use it, for Windows. In this case, organizations that wish to implement it can view this file as a demonstration.

site.pp – the build described in this practice guide uses the *site.pp* file as a main launch point for all of the various classes in the manifests file. In this case, there is one class in the *site.pp* file itself that configures Windows systems to enable firewalls, deny reboots with logged in users, and ensure Windows updates are on.

11.1.4.2 Using Security Technical Implementation Guides (STIGs)

The Department of Defense (DoD) Defense Information Systems Agency created and manages a series of technical security best practice guides that assist DoD services and agencies with hardening their systems. Many of the STIG documents are based on the NIST 800 series guidance and controls recommended for systems security. Organizations implementing Windows systems similar to the architecture described in this document should use these guides as ancillary references on how to secure their systems. Because the DoD considers protection from nation-state threats regarding unauthorized access to personally identifiable information, government secrets, and health information important, that may not be practical or functional in a private sector health organization.

The STIG process, specific operating system guidance, and automated assessment files can be downloaded at *http://iase.disa.mil/stigs/os/Pages/index.aspx*.

11.2 Linux Installation and Hardening

11.2.1 Linux Installation

Download the Fedora 20 image from the following links:

- 64 bit - *http://archive.fedoraproject.org/pub/fedora/linux/releases/20/Images/x86_64/*
- 32 bit - *http://archive.fedoraproject.org/pub/fedora/linux/releases/20/Images/i386/*

Download the Fedora 20 installation guides:

- PDF: *http://docs.fedoraproject.org/en-US/Fedora/20/pdf/Installation_Guide/Fedora-20-Installation_Guide-en-US.pdf*
- HTML: *http://docs.fedoraproject.org/en-US/Fedora/20/html/Installation_Guide/*

See Section 3.1, Hostnames for hostnames to use.

If you opt to change your organization's hostnames, you should make note of any changes for comparison and make necessary changes to the implementation of other products described here.

Use full disk file encryption on all Linux systems as described in the Fedora 20 installation guides.

Use separate disk partitions or hard disks to create the *root, var, usr* and *etc* partitions as described in the Fedora 20 installation guides. The electronic health record application should have its own partition or disk.

Use a 100G disk, at least, to allow for system and other logs.

11.2.2 Linux Post-Installation Tasks

Install the Puppet agent by following the Puppet Enterprise installation instructions in Section 5.

Ensure that all the base system files recommended in Section 11.2, Linux Installation and Hardening are configured in Puppet Master for this host.

Follow the instructions in Section 5.2, Puppet Enterprise Configuration to configure the hostname in the *site.pp* file.

Install the backup agent by following the URBackup instructions in Section 4.1.

11.2.3 Linux Security Hardening

Use the Puppet Enterprise configuration tool for all Linux operating system hardening tasks. Configure each Linux system to receive base and custom sets of configuration enforcement instructions from Puppet. Puppet uses configuration files called manifests to house configuration enforcement instructions. The base Linux configuration manifests list is below, along with a short explanation on why they were implemented on all Linux systems used in this build.

Puppet Manifests

accounts.pp – allows control over users who can log in and also controls the password. If an attacker changes any information in the password file, Puppet will change settings back based on the entries in this file

crontabconfig.pp – creates tasks that run automatically at set intervals. In this case, there are four tasks that are executed to secure Linux:

1. logoutall.sh – runs every few seconds and kills all other user tasks with exception of root, effectively removing normal users from all the Linux systems while they are in production mode
2. puppetagent.config.base.sh – periodically runs the Puppet agent to update any changes to the configuration of the local system based on a remote Puppet Master configuration change
3. yum.config.base.sh – forces the local system to update itself during set a time every day
4. harden.os.single.commands.sh – a series of single commands to ensure changes to permissions on critical system files that disable root console or other one-line commands

firewallrules.pp – creates and enforces individual *IPtables* rules on each local Linux host in accordance with the least access needed in or out of the system

grub2fedora20.pp – this build implemented versions of Fedora 20 with the Grub2 bootloader. The bootloader assists with starting the Linux operating system and allowing the operator to make special configurations prior to the system boot process. This access can be dangerous because it will allow an attacker to boot the system into single user mode or make other changes prior to the boot process. The changes made with this Puppet manifest file create a Grub2 password challenge

packages.pp – ensures that less secure applications are removed and only the applications needed to run the service are installed on the local system

passwdfile.pp – cleans password file of standard users that come with the Fedora 20 Linux distro. It also cleans the group file

securettyfile.pp – creates a new security file in the local system that prevents root from logging into a console session

ssh.pp – hardens the encrypted remote management service for Linux *time.pp* – forces the local system to use a time server for accurate time; creates accurately time-stamped logs

warningbanners.pp – creates warning banners at the console and remote login sessions that warn users that their sessions should be authorized and monitored. This banner should deter good people from accidentally doing bad things. It will not stop a determined attacker under any circumstances

NIST CYBERSECURITY PRACTICE GUIDE HEALTH IT

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Standards and Controls Mapping

Gavin O'Brien
Brett Pleasant
Colin Bowers
Sue Wang
Kangmin Zheng
Kyle Kamke
Nate Lesser

Leah Kauffman, Editor-in-Chief

NIST SPECIAL PUBLICATION 1800-1d

DRAFT

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

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

NIST Special Publication 1800-1d

SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES

Health IT Sector

DRAFT

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

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 1800-1d
Natl. Inst. Stand. Technol. Spec. Publ. 1800-1d, 16 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 publicly 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 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

[*] 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

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
Sally Edwards	MITRE
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 demonstrates 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**

  YOU ARE HERE
- NIST SP 1800-1e: Risk Assessment and Outcomes – risk assessment methodology, results, test and evaluation

2 Introduction

NIST SP 1800-1d, Standards and Control Mapping, provides a detailed listing of the standards and best practices used in the creation of the practice guide. This volume is broken into three sections:

- Security Standards – the standards and best practices considered in development of this practice guide
- Security Characteristics and Controls – mapping of the security characteristics described in NIST SP 1800-1b: Approach, Architecture, and Security Characteristics, section 4.5, to the relevant security controls
- Technologies – mapping of the technologies and products used in the reference design to the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the Cybersecurity Framework, or CSF) and relevant security controls

3 Security Standards

In addition to using the CSF and the Risk Management Framework,[1] it is important to consider industry-specific security standards and best practices, where possible. Table 1 is a list of security standards used to create this architecture.

[1] NIST Special Publication 800-37, *Guide for Applying the Risk Management Framework*.

Table 1: Related Security Standards

Related Technology	Relevant Standards	URL
Cybersecurity - general	NIST Cybersecurity Framework - Standards, guidelines, and best practices to promote the protection of critical infrastructure	http://www.nist.gov/itl/cyberframework.cfm
	NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 53r4
	ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls	http://www.iso.org/iso/catalogue_detail?csnumber=54533
	20 Critical Security Controls	http://www.sans.org/critical-security-controls/
Health care related	Health Insurance Portability and Accountability Act (HIPAA) Security Rule	http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
	NIST SP 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule	http://www.nist.gov/customcf/get_pdf.cfm?pub_id=890098
	U.S. Department of Health and Human Services (HHS) The Office of the National Coordinator for Health Information Technology (ONC) Security Risk Assessment (SRA) Tool Technical Safeguards	http://www.healthit.gov/sites/default/files/20140320_sratool_content_-_technical_volume_v1.docx
Mobile Wireless Security	NIST SP 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)	http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
	NIST SP 800-124r1, Guidelines for Managing the Security of Mobile Devices in the Enterprise	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
	NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i	http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf
	NIST SP 800-48 rev1, Guide to Securing Legacy IEEE 802.11 Wireless Networks	http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf
Network Security (Firewall)	NIST SP 800-41 rev1, Guidelines on Firewalls and Firewall Policy	http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf
Network	NIST SP 800-114, User's Guide to Securing External Devices for	http://csrc.nist.gov/publications/nistpubs/800-57/sp800-

Security (Remote Access)	Telework and Remote Access	57_part1_rev3_general.pdf
	NIST SP 800-46 rev1, Guide to Enterprise Telework and Remote Access Security	http://csrc.nist.gov/publications/nistpubs/800-46-rev1/sp800-46r1.pdf
Network Security (VPN)	NIST SP 800-77, Guide to IPsec VPNs	http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf
	NIST SP 800-52, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
Protocol (RADIUS)	RFC 2138, Remote Authentication Dial In User Service (RADIUS)	http://tools.ietf.org/html/rfc2138
	RFC 2139, RADIUS Accounting	http://tools.ietf.org/html/rfc2139
	RFC 2865, Remote Authentication Dial In User Service (RADIUS)	http://tools.ietf.org/html/rfc2865
	RFC 2866, RADIUS Accounting	http://tools.ietf.org/html/rfc2866
	RFC 2867, RADIUS Accounting for Tunnel Protocol Support	http://tools.ietf.org/html/rfc2867
	RFC 2869, RADIUS Extensions	http://tools.ietf.org/html/rfc2869
Protocol (PPP)	RFC 2284, Point-to-Point Protocol (PPP) EAP	http://tools.ietf.org/html/rfc2284
	RFC 2716, PPP EAP-TLS Authentication Protocol	http://tools.ietf.org/html/rfc2716
Protocol (TLS)	NIST SP 800-52 rev1, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r1.pdf
	RFC 2246, TLS Protocol 1.0	http://tools.ietf.org/html/rfc2246
	RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1	http://tools.ietf.org/html/rfc4346
	RFC 5246, The Transport Layer Security (TLS) Protocol Version 1.2	https://tools.ietf.org/html/rfc5246
Protocol (EAP)	RFC 3748, Extensible Authentication Protocol (EAP)	http://tools.ietf.org/html/rfc3748
	RCF 5247, Extensible Authentication Protocol (EAP) Key Management Framework	http://tools.ietf.org/html/rfc5247
	RFC 5216, The EAP-TLS Authentication Protocol	http://tools.ietf.org/html/rfc5216
Key Management	NIST SP 800-57 Part 1 – rev3, Recommendation for Key Management: Part 1: General (Revision 3)	http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
	NIST SP 800-57 Part 2, Recommendation for Key Management: Part 2: Best Practices for Key Management Organization	http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

	NIST SP 800-53 Part 3 rev1, Recommendation for Key Management: Part 3 - Application-Specific Key Management Guidance	http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf
	NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure	http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
Risk Management	NIST SP 800-30, Guide for Conducting Risk Assessments	http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
	NIST SP 800-39, Managing Information Security Risk Organization, Mission, and Information System View	http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf
	NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems A Security Life Cycle Approach	http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

4 Security Characteristics and Controls

To establish the architectural boundaries of the use case, we mapped the components to the CSF, relevant NIST standards, industry standards, and best practices. From this map, we identified the set of security characteristics that our example solution would address. We then cross-referenced the characteristics to the security controls in NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Information Technology – Security techniques – Code of practice for information security management (ISO/IEC 27002) ,[2] the SANS Institute, Critical Security Controls,[3] and The Health Insurance Portability and Accountability Act of 1996.[4]

By mapping each of the more general security characteristics to specific and multiple security controls, we define each characteristic more granularly and understand safeguards necessary to implement the characteristic. Another benefit of results from these mappings is traceability from a security characteristic to the evaluation of its security control. NIST SP 1800-1e, Section 4, Security Controls Assessment, builds on these mappings by illustrating tests of each countermeasure.

[2] ISO/IEC 27002:2005, http://www.iso27001security.com/html/27002.html

[3] SANS CAG20 https://www.sans.org/critical-security-controls/

[4] HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996

Table 2: Security Characteristics Mapped to Cybersecurity Standards and Best Practices, and HIPAA

Security Characteristics	Cybersecurity Standards and Best Practices						HIPAA Requirements
	CSF Function	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev4**	**IEC/ISO27002**	**SANS CAG20**	
access control	Protect (PR)	Access Control (PR.AC)	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-2, IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-9	§ 164.312 (a)
			PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2	CSC-17	§ 164.312 (a)
			PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16	6.1.3, 7.2.2, 8.1.1, 8.3.3, 10.1.3, 10.8.1, 11.1.1, 11.2.1, 11.2.2, 11.2.4, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2, 12.4.3, 15.2.1	CSC-9	§ 164.312 (a)

audit controls/ monitoring	Detect (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-1: The network is monitored to detect potential cybersecurity events	AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	6.1.8, 6.2.1, 8.3.3, 10.1.1, 10.1.2, 10.3.1, 10.3.2, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 10.10.1, 10.10.2, 10.10.4, 10.10.5, 11.2.1, 11.2.2, 11.2.4, 11.4.5, 11.4.6, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-2, CSC-3, CSC-5, CSC-6, CSC-11	§164.312(b)
			DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	6.1.8, 8.3.3, 10.10.1, 10.10.4, 10.10.5, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 15.2.2	CSC-6, CSC-11	§164.312(b)
			DE.CM-4: Malicious code is detected	SI-3	10.4.1	CSC-7	§164.312(b)
			DE.CM-5: Unauthorized mobile code is detected	SC-18, SI-4. SC-44	10.4.2, 10.10.2, 13.1.1, 13.1.2	CSC-5, CSC-6	§164.312(b)

			DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	6.1.8, 6.1.5, 6.2.1, 6.2.3, 8.1.1, 8.1.3, 8.2.1, 10.2.1, 10.2.2, 10.2.3, 10.6.2, 10.8.2, 10.10.2, 12.1.1, 12.5.5, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-5, CSC-6, CSC-7	§164.312(b)
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	6.1.8, 7.1.1, 7.1.2, 9.1.1, 9.1.2, 9.1.3, 9.1.5, 9.1.6, 10.1.1, 10.1.2, 10.3.2, 10.10.1, 10.10.2, 10.10.4, 10.10.5, 11.3.2, 11.4.4, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-1, CSC-2, CSC-5, CSC-6, CSC-7	§164.312(b)
			DE.CM-8: Vulnerability scans are performed	RA-5	12.6.1, 15.2.2	CSC-7, CSC-10	§164.312(b)
device integrity	Protect (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC‑17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2	CSC-5, CSC-6, CSC-8, CSC-14	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)

		Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	SC-28	None	CSC-15	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
			PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	CM-8, MP-6, PE-16	7.1.1, 7.1.2, 9.1.6, 9.2.6, 9.2.7, 10.7.1, 10.7.2, 10.7.3	CSC-1, CSC-2	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
			PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	10.4.1, 12.2.2, 12.2.3	CSC-3	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)
		Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained	CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	12.4.1, 10.1.4, 10.1.1, 10.1.2, 10.3.2, 12.4.1, 12.5.1, 12.5.2,12.5.3, 10.1.2, 10.3.2, 12.4.1, 12.5.2, 12.5.3, 10.1.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.3, 6.1.3. 7.1.1, 7.1.2, 8.1.1, 10.1.1, 10.1.2, 10.3.2,12.4.1, 12.4.3, 12.5.1, 12.5.2, 12.5.3	CSC-2, CSC-3, CSC-4, CSC-7, CSC-13	(§ 164.312 (c))

		Protective Technology (PR.PT)	PR.PT-2: Removable media is protected and its use restricted according to policy	SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, PL-8	6.1.3, 7.1.1, 7.1.2, 8.1.1, 10.1.1, 10.1.2, 10.1.4, 10.3.2, 11.1.1, 11.6.1, 12.4.1, 12.4.3, 12.5.1, 12.5.2, 12.5.3	CSC-3, CSC-7	(§ 164.312 (c))
	Detect (DE)	Security Continuous Monitoring (DE.CM)	DE.CM-5: Unauthorized mobile code is detected	SC-18, SI-4. SC-44	10.4.2, 9.10.2, 13.1.1, 13.1.2	CSC-5, CSC-6, CSC-12, CSC-14	(§ 164.312 (c))
			DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	CA-7, PS-7, SA-4, SA-9, SI-4	6.1.5, 6.1.8, 6.2.1, 6.2.3, 8.1.1, 8.1.3, 8.2.1, 10.2.1, 10.2.2, 10.2.3, 10.6.2, 10.8.2, 9.10.2, 12.1.1, 12.5.5, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-3, CSC-5, CSC-6, CSC-7, CSC-14, CSC-15, CSC-17	(§ 164.312 (c))
			DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	6.1.8, 7.1.1, 7.1.2, 9.1.1, 9.1.2, 9.1.3, 9.1.5, 9.1.6, 9.1.1, 9.1.2, 9.10.1, 9.10.2, 9.10.4, 9.10.5, 10.3.2, 11.4.4, 12.4.1, 12.5.1, 12.5.2, 12.5.3, 13.1.1, 13.1.2, 15.2.1, 15.2.2	CSC-1, CSC-2, CSC-3, CSC-4, CSC-5, CSC-6, CSC-14, CSC-17	(§ 164.312 (c)), §164.308 (a)(5)(ii)(B)

person or entity authentication	Protect (PR)	Access Control (PR.AC)	PR.AC-1: Identities and credentials are managed for authorized devices and users	AC-2, IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-5, CSC-9, CSC-11	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
			PR.AC-3: Remote access is managed	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	9.1.1, 9.1.2, 9.1.3, 9.1.4, 9.1.5, 9.1.6, 9.2.2, 9.2.3, 10.6.1, 11.2.1, 11.2.2, 11.2.4, 11.3.2, 11.4.4		§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
			PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	AC-2, AC-3, AC-5, AC-6, AC-16	6.1.3, 7.2.2, 8.1.1, 8.3.3, 10.1.3, 10.8.1, 11.1.1, 11.2.1, 11.2.2, 11.2.4, 11.4.1, 11.4.4, 11.4.6, 11.5.4, 11.6.1, 12.4.2, 12.4.3, 15.2.1	CSC-8, CSC-9	§164.312(d), §164.308 (a)(5)(ii)(D), §164.312 (a)(2)(i)
transmission security	Protect (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC-17, AC-19, AC-20	7.1.3, 8.1.1, 8.1.3, 10.4.1, 10.6.1, 10.8.1, 11.1.1, 11.4.1, 11.4.2, 11.4.3, 11.4.4, 11.4.6, 11.4.7, 11.7.1, 11.7.2	CSC-5, CSC-6, CSC-8, CSC-14	§164.312 (e)

			PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	AC-4, SC-7	6.2.1, 10.4.1, 10.4.2, 10.6.1, 10.8.1, 10.9.1, 10.9.2, 11.4.5, 11.4.6, 11.4.7, 11.7.2, 12.4.2, 12.5.4	CSC-4, CSC-5, CSC-9, CSC-13, CSC-15, CSC-16	§164.312 (e)
		Data Security (PR.DS)	PR.DS-2: Data-in-transit is protected	SC-8	10.4.2, 10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.2.3,12.3.1		§ 164.312 (e))
		Technology (PR.PT)	PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7	9.1.4, 10.4.2, 10.6.1, 10.6.2, 10.8.1, 10.9.1, 10.9.2, 11.1.1, 11.4.1, 11.4.2, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.7.1, 11.7.2, 12.2.3, 12.3.1, 12.4.2, 12.5.4, 14.1.3		§ 164.312 (e))

5 TECHNOLOGIES

In order to build an example solution (reference design), we needed to use multiple commercially available and open source technologies. Table 3 shows how the products used in creation of the reference design are mapped to security controls and architectural components listed in Figure 1.

Figure 1: Architecture for the Secure Exchange of Electronic Health Records on Mobile Devices in a Health Care Organization

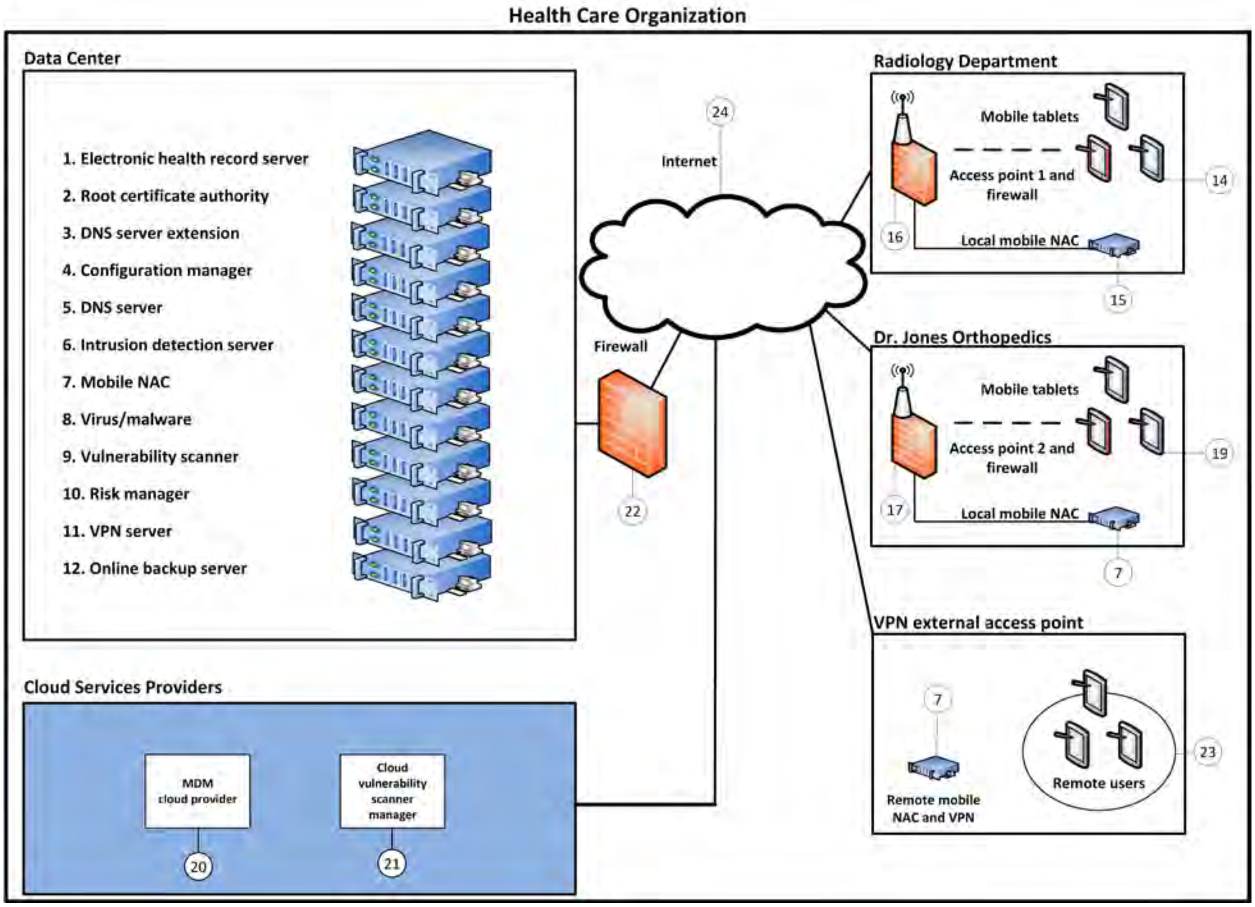


Table 3. Products and Technologies Used in the Secure Exchange of Electronic Health Records on Mobile Devices Reference Design

CSF Function	Reference to NIST 800-53 rev4 Controls	Company	Application / Product	V.	Architecture Element (see Figure 1)	Use
Identify (ID)	CA-2, CA-7, CA-8, CM-8, CP-2, PM-4, PM-9, PM-11, PM-12, PM-15, PM-16, RA-2, RA-3, RA-5, SA-5, SA-11, SA-14, SI-2, SI-4, SI-5	RSA	Archer GRC	5.5	10	centralized enterprise, risk and compliance management tool
Protect (PR)	AC-2, AC-3, AC-4, AC-5, AC-6, AC-16, AC-17, AC-18, AC-19, AC-20, AU-12, CA-7, CM-2, CM-3, , CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CP-4, CP-6, CP-8, CP-9, IA Family, MP-6, PE-3, PE-6,PE-16, PE-20, SA-10, SC-7, SC-8, SC-12, SC-18, SC-20, SC-21, SC-22, SC-23, SC-28, SC-44, SI-4, SI-7	MedTech Enginuity	OpenEMR	4.1.2	1	Web-based and open source electronic health record and supporting technologies
		open source	Apache Web Server	2.4	1	
		open source	PHP	5.5	1	
		open source	MySQL	5.x	1	
		open source	ModSecurity	2.9.0	1	Apache module extension, Web application firewall (supporting OpenEMR)
		open source	OpenSSL	1.0.1e-fips	1, 3 ,4	cryptographically secures transmissions between mobile devices and the OpenEMR Web portal service
		various	mobile devices		14, 19, 23	Windows, IOS and Android tablets
		Fiberlink	MaaS360	Curr-ent	20	Cloud-based mobile device policy manager

		open source	*iptables* firewall	1.4	1, 2, 3, 4, 5, 22	stateful inspection firewall
		open source	Root CA / Fedora PKI manager	9	2	cryptographically signs identity certificates to prove authenticity of users and devices
		open source	domain name system (DNS) and DNS encryption (DNSE) / Bind9	9.9.4	3, 5	performs host or fully qualified domain resolution to IP addresses
		open source	secure configuration manager / Puppet Enterprise	3.7	5	creation, continuous monitoring, and maintenance of secure server and user hosts
		Cisco	local and remote mobile NAC (Identity Services Engine)	1.2	7, 15	radius-based authentication, authorization and accounting management server
		Cisco	VPN server (ASAv 9.4)			enterprise class virtual private network server based on both TLS and IPSEC
		open source	URbackup	1.4.8	12	online remote backup system used to provide disaster recovery
		Cisco	wireless access point (RV220W)	6.0.4	16, 17	Wi-Fi access point

Detect (DE)	AC-2, AC-4, AU-12, CA-3, CA-7, CM-2, CM-3, CM-8, PE-3, PE-6, PE-20, RA-5, SC-5, SC-7, SI-3, SI-4	open source	*iptables* firewall	1.4	1, 2, 3, 4, 5, 22	stateful inspection firewall
		open source	secure configuration manager / Puppet Enterprise	3.7	5	creation, continuous monitoring, and maintenance of secure server and user hosts
		open source	intrusion detection server (Security Onion IDS)	12.04	6	monitors network for threats via mirrored switch ports
		open source	host-based security manager (freeware0		8	server client-based virus and malware scanner
		open source	vulnerability scanner (freeware)	Current	9	cloud-based proactive network and system vulnerability scanning tool

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

NIST 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 publicly 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.

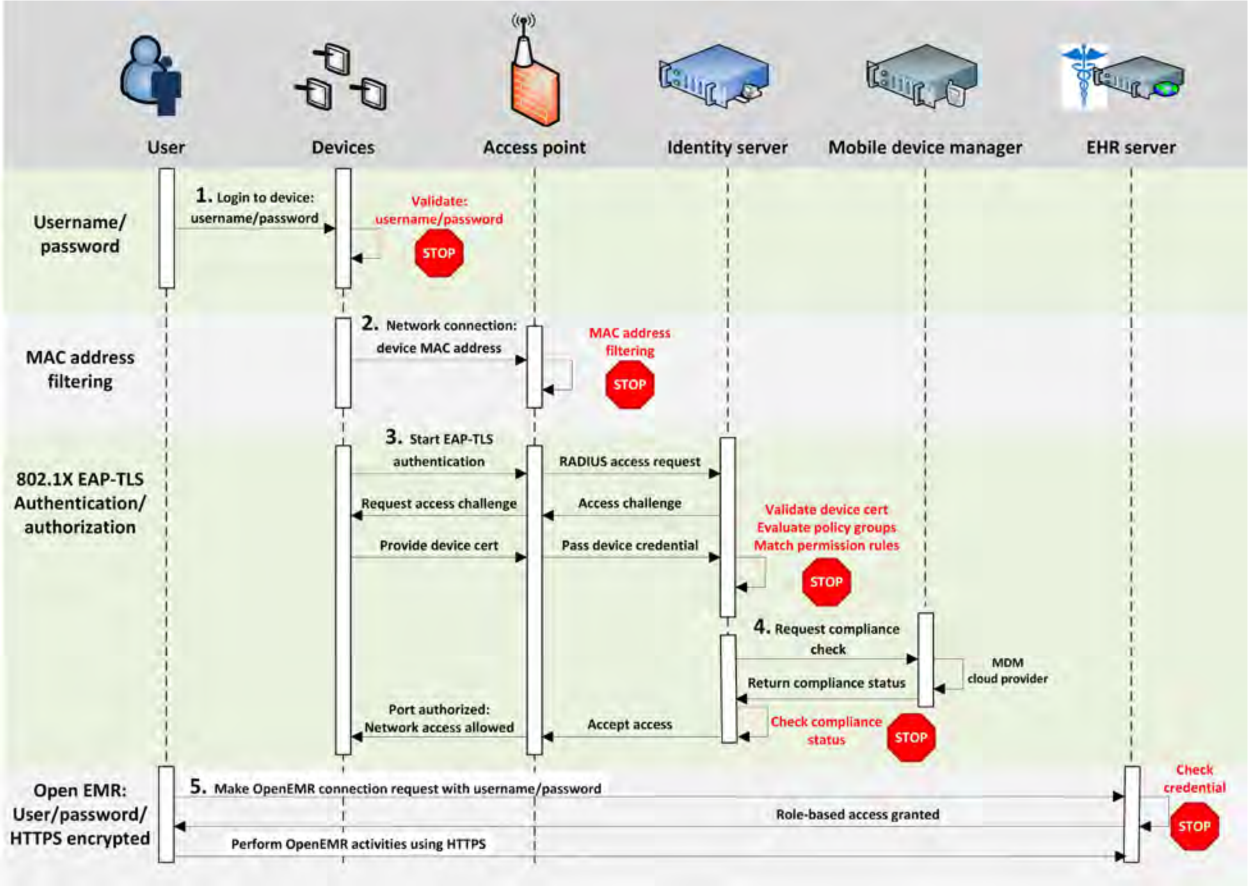


Figure 1: The steps necessary for a user and device to gain access to the electronic health record server.

[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.

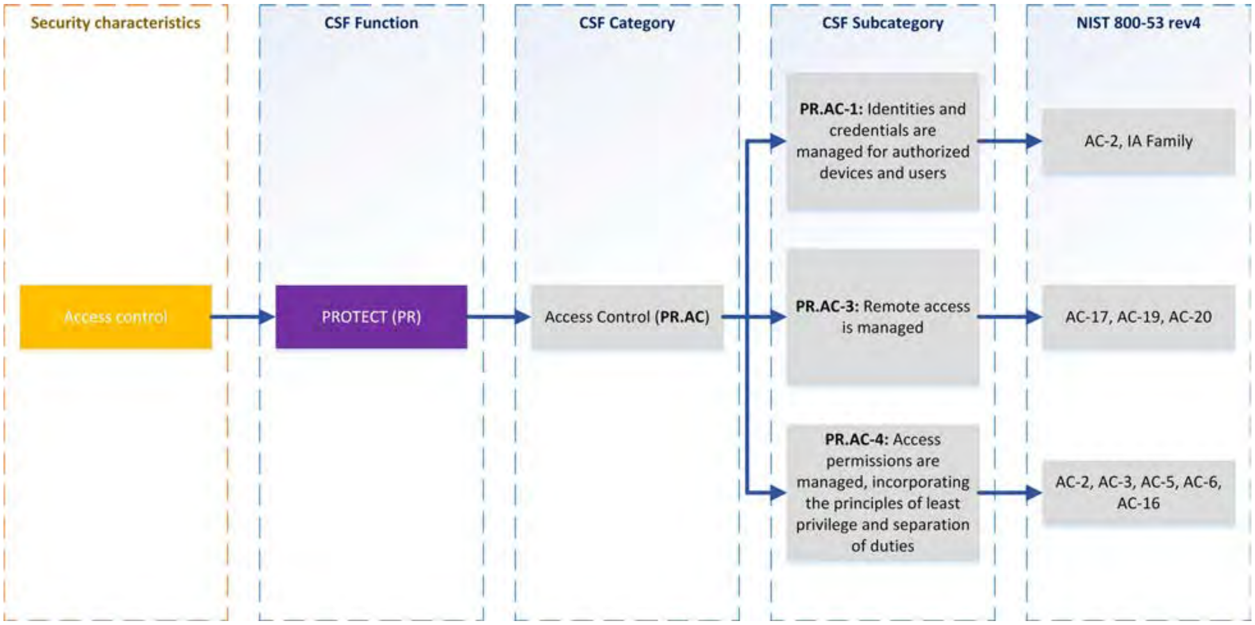

Security characteristics
CSF Function
CSF Category
CSF Subcategory
NIST 800-53 rev4
Access control
PROTECT (PR)
Access Control (PR.AC)
PR.AC-1: Identities and credentials are managed for authorized devices and users
PR.AC-3: Remote access is managed
PR.AC-4: Access permissions are managed, incorporating 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.

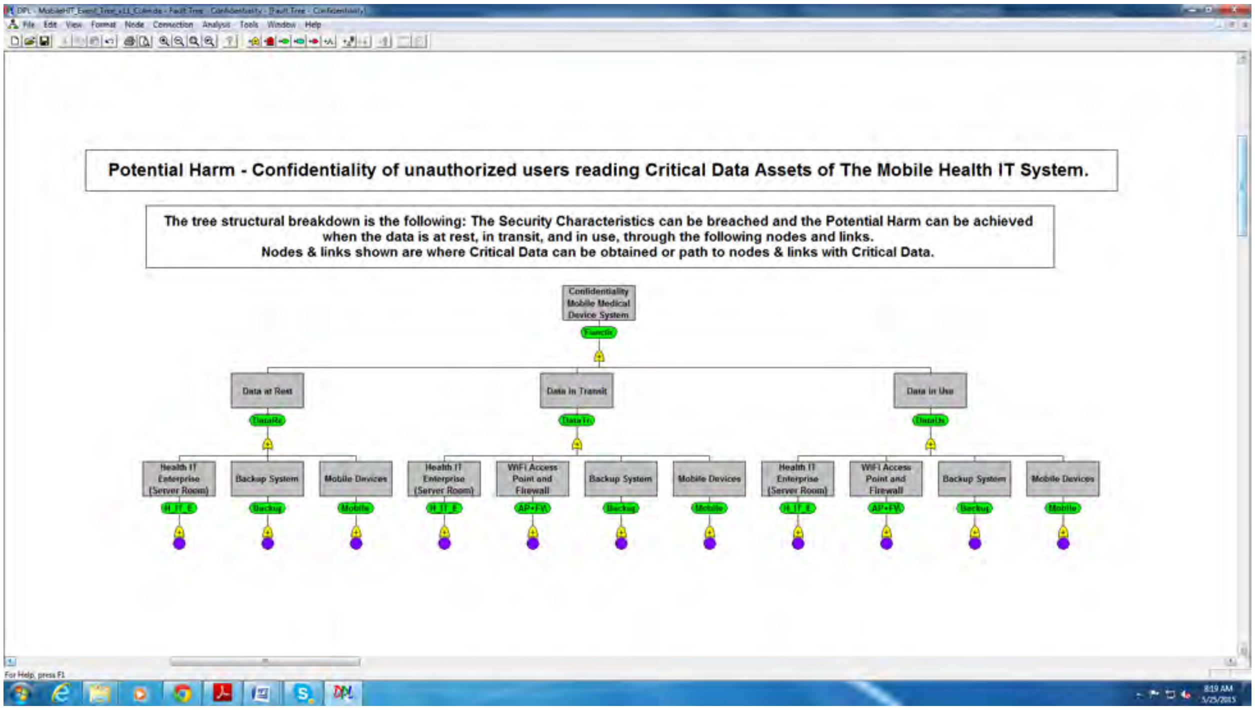
Step-2: Create Attack Event Trees (Attack Scenarios) with Countermeasures and Safeguards

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.

File Edit View Format Node Connection Analysis Tools Window Help
Confidentiality Mobile Medical Device System
Fxanclx
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
WiFi Access Point and Firewall
AP+FW
For Help, press F1

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.

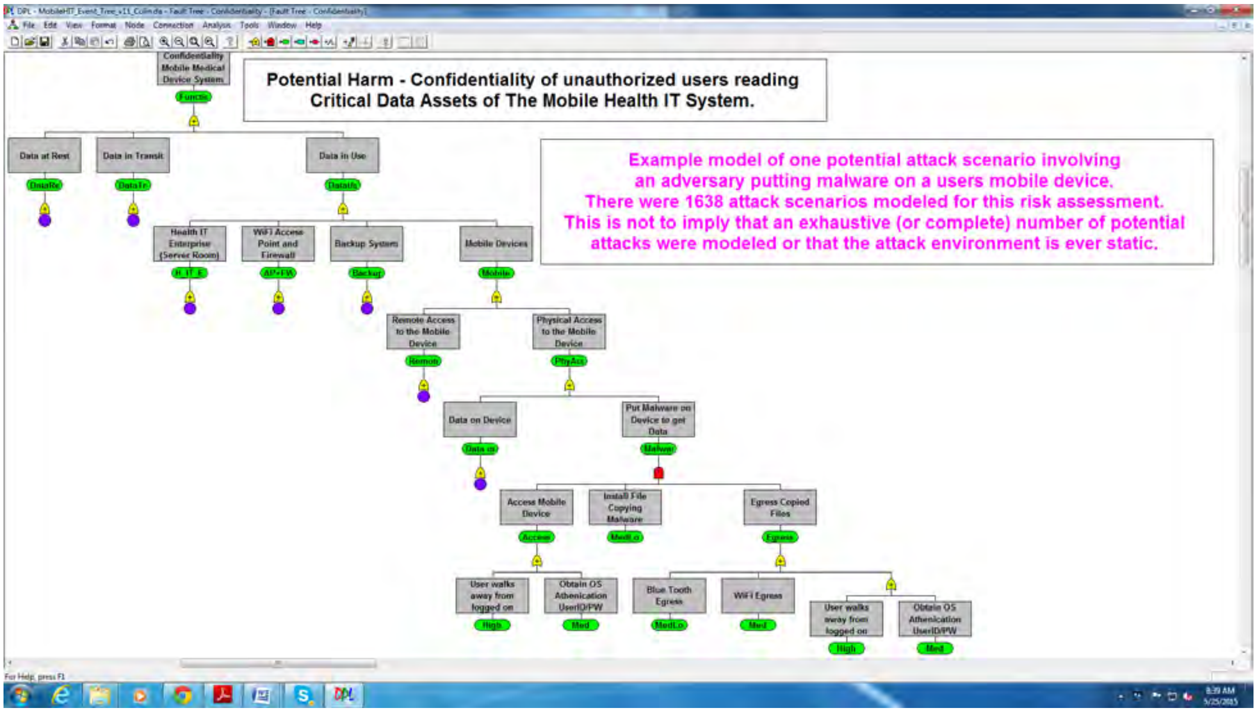
   This assessment is giving equal weight to the adversary's likelihood of success and not being detected. One goal of any organization providing good security is to make the resources an adversary would need to accomplish their cost prohibitive objective. For this assessment we have assumed those same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



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.

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
Functio
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
Remote
Physical Access to the Mobile Device
PhyAcc
Data on Device
Data on
Put Malware on Device to get Data
Malwar
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

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

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?