NIST SPECIAL PUBLICATION 1800-1

Securing Electronic Health Records on Mobile Devices

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), How-To Guides (C), Standards and Controls Mapping (D), and Risk Assessment and Outcomes (E)

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

NIST SPECIAL PUBLICATION 1800-1

Securing Electronic Health Records on Mobile Devices

Includes Executive Summary (A); Approach, Architecture, and Security Characteristics (B), How-To Guides (C), Standards and Controls Mapping (D), and Risk Assessment and Security Outcomes (E)

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

July 2018

U.S. Department of Commerce
Wilbur Ross, Secretary

National Institute of Standards and Technology
Walter G. Copan, Under Secretary of Commerce for Standards and Technology and Director

NIST SPECIAL PUBLICATION 1800-1A

Securing Electronic Health Records on Mobile Devices

Volume A:
Executive Summary

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

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

Executive Summary

- Patient information in electronic health records (EHRs) 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 by using commercially available products.
- The example solution is described in the "How-To" guide, which provides organizations with detailed instructions to re-create it. 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 contained in the National Institute of Standards and Technology (NIST) Cybersecurity Framework and in the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. In areas where there are no standards, such as malware prevention and detection or antivirus, our solution uses best practices.

CHALLENGE

Healthcare providers increasingly use mobile devices to store, process, and transmit patient information. When health information is stolen, inappropriately made public, or altered, healthcare 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 EHR system.

In our lab at the NCCoE at NIST, we built an environment that simulates interaction among mobile devices and an EHR system that is supported by the information technology (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 EHR, the EHR system enables another physician to access the information through a mobile device as well. This guide does not address patients accessing their own data. In general, EHR systems are accessed by healthcare professionals only. Patients typically access their data via a patient portal, in which data is derived from the EHR system.

This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.1800-1

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 healthcare 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 IT 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 re-create our reference design in whole or in part

While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. Your organization's information security experts should identify the products that will best integrate with its existing tools and IT system infrastructure. The 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.

ASSESS YOUR RISK

All healthcare organizations need to fully understand the potential risk posed to their information systems, the bottom-line implications of those risks, and the lengths that attackers will go to exploit them. According to our analysis (NIST SP 1800-1B, Section 4.3, and NIST SP 1800-1E), and in the experience of many healthcare organizations, the combination of mobile devices and Protected Health Information can present unique risks in a healthcare organization's networks. At the 2012 Health and Human Services (HHS) 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 (http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/).

Assessing risks and making decisions about how to mitigate them should be continuous to account for the dynamic nature of business 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 for adopting this or other approaches that will

increase the security of EHRs. It is important for management to perform regular periodic risk review, as determined by the needs of the business.

SHARE YOUR FEEDBACK

You can view or download the guide at https://www.nccoe.nist.gov/projects/use-cases/health-it/ehr-on-mobile-devices. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the business processes associated with implementing it.

To learn more by arranging a demonstration of this reference solution, contact us at hit_nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified 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, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200

NIST SPECIAL PUBLICATION 1800-1B

Securing Electronic Health Records on Mobile Devices

Volume B:
Approach, Architecture, and Security Characteristics

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

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

DISCLAIMER

Certain commercial entities, equipment, products, 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, equipment, products, or materials 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, 35 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov/. To learn more about NIST, visit https://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 align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Healthcare 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 healthcare providers, mobile devices can introduce vulnerabilities in a healthcare organization's networks. At the 2012 HHS Mobile Devices Roundtable, participants stressed that many providers are using mobile devices for healthcare delivery before they have implemented safeguards for privacy and security [1].

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

KEYWORDS

EHR; electronic health records; HIPAA; mobile device security; patient health information; PHI; risk management; standards-based cybersecurity; stolen health records

ACKNOWLEDGMENTS

We would like to highlight and express our gratitude to Leah Kauffman, with NIST, who served as editor-in-chief of this guide.

We are grateful to the following individuals for their generous contributions of expertise and time.

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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. We worked with:

Technology Partner/Collaborator	Build Involvement
Cisco	Identity Services Engine (ISE), Adaptive Security Virtual Appliance (ASAv), and RV220W
IBM	MaaS360
Intel	Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI)
MedTech Enginuity	OpenEHR software
Ramparts	Risk assessment and security testing
RSA	Archer Governance, Risk & Compliance (GRC)
Symantec	Endpoint Protection

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 (EHRs) can be exploited in ways that can endanger patient health as well as compromise identity and privacy [2].
- EHRs shared on mobile devices are especially vulnerable to attack [3].

In response to the problem of securing electronic healthcare information on mobile devices, the National Cybersecurity Center of Excellence (NCCoE) has taken the following actions:

- The NCCoE developed an example solution to this problem by 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, have prompted healthcare groups to rapidly adopt EHR systems. Unfortunately, they have not adopted security measures at the same pace. Attackers are aware of vulnerabilities within these systems and are deploying increasingly sophisticated means to exploit information systems and devices. The Ponemon Institute reports 125% growth in the number of intentional attacks over a five-year period. Malicious hacks on healthcare organizations now outnumber accidental breaches [2].

According to a risk analysis described in Section 3.3, and in the experience of many healthcare providers, mobile devices can present vulnerabilities to a healthcare organization's networks. At the 2012 HHS 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 [3].

The negative impact of stolen health records is much higher when we factor in the costs that an organization incurs in responding to a breach. In addition to federal penalties, organizations pay for credit and identity theft monitoring for affected clients and for 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, and incorrect prescriptions. Costs are likely to increase as more breaches occur.

1.2 Challenge

Healthcare providers increasingly use mobile devices to receive, store, process, and transmit patient health information. (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.) Unfortunately, many organizations have not implemented safeguards to ensure the security of patient information when doctors, nurses, and other caregivers use mobile devices in conjunction with an EHR system [3]. As stated above, when patient health information is stolen, made public, or altered, healthcare 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 deliver healthcare more rapidly and effectively, 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 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 EHRs 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 we can imagine playing out hundreds or thousands of times a day in a real-world healthcare organization, is how to effectively secure patient health information when accessed by health practitioners who are using mobile devices, without degrading the efficiency of healthcare delivery.

1.3 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 security engineers and information technology professionals, using commercially available and open-source tools and technologies that are consistent with cybersecurity standards, can help healthcare organizations that use mobile devices share patients' health records more securely. We use a layered security strategy to achieve these improvements in protecting health information. Our focus is on devising a solution and not on selecting technologies.

Our solution uses commercially available tools. When there were no commercial products to address our needs, we used open-source products. For more information about the process that NCCoE uses to select products, visit the NCCoE website.

Using the guide, an 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 IT 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 easy 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. An organization's security experts should identify the standards-based products that will best integrate with its existing tools and IT system infrastructure. An organization can adopt this solution or one that adheres to these guidelines in whole or use this guide as a starting point for tailoring and implementing parts of a solution.

1.4 Assess Your Risk

All healthcare organizations need to fully understand their potential cybersecurity risks, the bottom-line implications of those vulnerabilities, and the lengths that 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 the business, the threat landscape, and the data itself. The guide describes our approach to risk assessment and provides a concrete example. We urge an organization to implement a continuous risk management process for itself as a starting point to adopting this or other approaches that will increase the security of EHRs. 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.

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 EHRs 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* [1], defines mobile devices as smartphones and tablets. They are characterized by small form factors, wireless networking capability, built-in data storage, limited operating systems, and multiple ways of accessing applications. While there are many types of mobile devices, we only used smartphones and tablets as examples for this project.

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–list of standards, best practices, and technologies used in creating this Practice Guide
- 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.

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

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

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 3), where we provide a detailed architecture and map security characteristics of this example solution to cybersecurity standards and best practices, and to HIPAA requirements
- Risk Management (Section 3.3), 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 and 4 explain what we did, and why, to address this cybersecurity challenge.
- NIST SP 1800-1C: How-To Guides cover all the products we employed in this reference design. We do not re-create 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: Section 3 Security Standards is a complete list of security standards used to create the architecture.
- NIST SP 1800-1E: Section 6 Risk Assessment Results 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 healthcare organizations. While we have used certain commercially available products, there may be comparable products that might better fit your an organization's particular IT systems and business processes. Regardless of which products and services your organization uses, 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 3-3 maps the representative products we used to the cybersecurity controls delivered by this reference design. Section 3.5 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. We seek feedback on its contents and welcome your input. Comments, suggestions, and success stories will improve subsequent versions of this guide. To contribute your thoughts or join our community of interest please email hit_nccoe@nist.gov.

2.1 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*
Bold	names of menus, options, command buttons, fields	Choose **File > Edit**
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov

3 Approach

Healthcare records have become one of the most sought-after types of information. A stolen medical record contains data that gives thieves access to a patient's medical or other identity, and to a healthcare organization's services. Theft of health information raises the cost of healthcare and can result in physical harm: if a person's healthcare record is altered, an unsafe drug interaction might result; if the record cannot be trusted, a patient might experience a delay in care [4].

This guide demonstrates tools that a healthcare organization can use to increase the security of health information as it is collected, 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 EHRs. Mobile devices used in this way are subject to the following security concerns, which are addressed in this guide:

- A healthcare worker might lose or misplace a mobile device containing patient health information, or be a victim of exploitation or theft.
- Compromised mobile devices enable hackers to access the healthcare organization's network.
- Untrusted networks may use a man-in-the-middle strategy to obtain credentials to access the enterprise network.
- Interacting with other systems increases a healthcare worker's risk of compromising routine operations such as data synchronization and storage.

At the NCCoE, we set out to address needs expressed by healthcare organizations and to demonstrate how an organization can re-create 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-size medical organization and is accessed by a healthcare provider from a small organization. In this case, we use organizational size as a proxy for technical sophistication and cybersecurity maturity. (Note that a patient accessing an EHR through a mobile device was not part of our use case and is outside the scope of our solution.) 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 health records. We explored three configuration options:

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

The initial motivation for this project came from inquiries by members of the healthcare industry. We conducted a risk assessment to evaluate the challenges faced by healthcare organizations. This risk assessment initially evaluated the current and planned uses of EHRs. As indicated in the Summary, 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. In our risk assessment, we found that availability when using mobile devices is a critical feature rather than a convenience.

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
- generated a 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 and 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

3.1 Audience

This guide is intended for individuals responsible for implementing IT security solutions in healthcare organizations. If an organization chooses to use Internet service providers or cloud-based solutions, Volume 1800-1E of this publication, Risk Questionnaire, Section 8 provides a checklist of questions to help you choose a secure solution.

3.2 Scope

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

3.3 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 [5].

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). 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 with respect to EHRs using mobility are:

- a lost or stolen mobile device
- deliberate misuse: a user who:
  - roots/jailbreaks device
  - walks away from logged-on mobile device
  - downloads viruses or other malware
  - uses an unsecure Wi-Fi network
- inadequate privilege management:
  - 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.

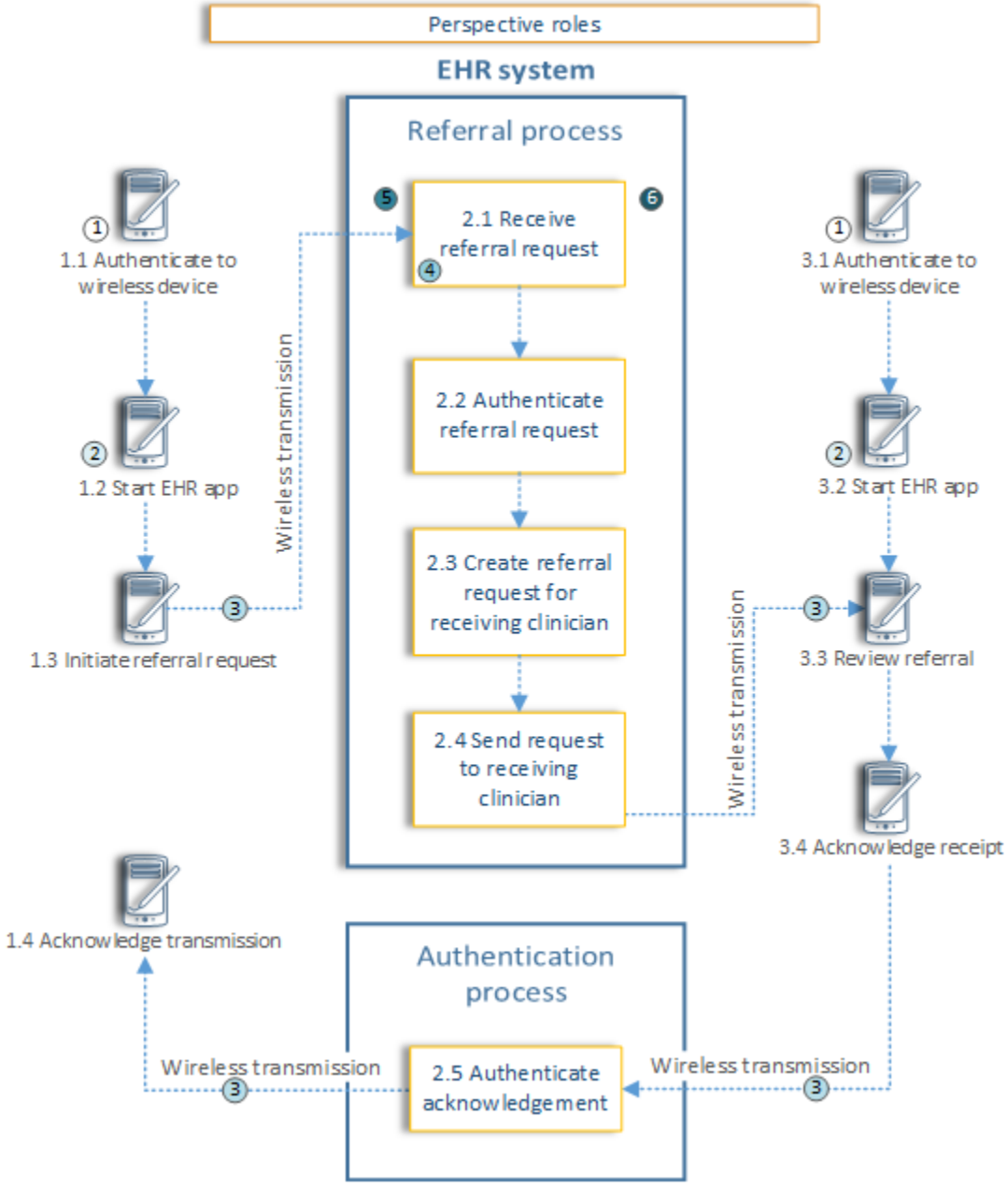
To demonstrate how to monitor and clearly communicate the relationship between technical risks and organizational risks, we used a governance, risk, and compliance (GRC) tool to aggregate and visualize data. The details on how to install and set up the GRC tool can be found in Volume 1800-1C of this publication, How-To Guides, Section 12, Governance, Risk, and Compliance.

3.4 The Use Case

In 2012, the NCCoE published the draft use case *Mobile Devices: Secure Exchange of Electronic Health Information* [6]. The use case describes scenarios in which physicians use mobile devices to refer patients to another physician or to issue an e-prescription. In addition, the use case contains a diagram (Figure 3-1) illustrating the flow of information from the physician to the EHR system, and then back to another physician.

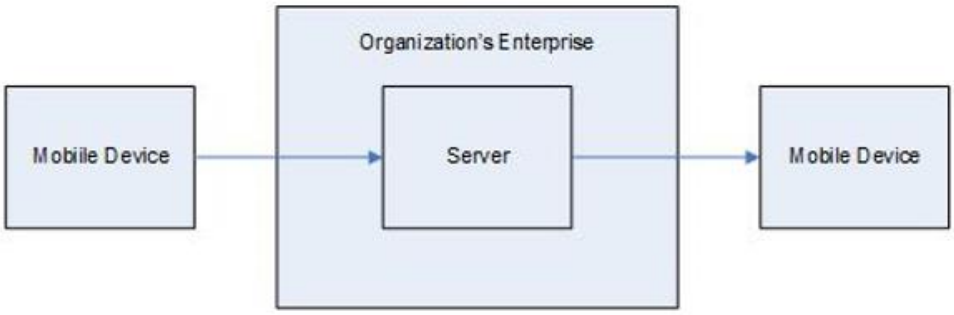
Figure 3-1 Security Characteristics Required to Securely Perform the Transfer of Electronic Health Records Among Mobile Devices

Legend: 1) wireless device security; 2) wireless device data security; 3) wireless device transmission security; 4) EHR message authentication



As we further developed the scenarios, we could not explore the security of a healthcare organization's EHR system and mobile devices without re-creating 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 3-2 shows the high-level architecture from the original use case [5] with the organization's enterprise included.

Figure 3-2 High-Level Architecture



The use case scenario was not intended to include a complete set of components but rather to start a discussion about the issue and to provide an opportunity for vendors of security products to participate in the solution.

From this use case scenario, we identified the architecture components that are likely in an organization's enterprise (see Table 3-1). The table also includes the security characteristics that we derived from the use case. These are the security characteristics that defined our problem.

Table 3-1 Use Case Architecture Components

Mobile Devices / Client Side	Networks	Back End / Server Side	Secure Infrastructure
mobile device	Wi-Fi	certified [7] EHR system	firewall
mobile device management client		storage encryption	VPN gateway
intrusion detection system		antivirus	authentication, authorization, and accounting server
firewall software		intrusion detection system	certificate authority and enrollment

Mobile Devices / Client Side	Networks	Back End / Server Side	Secure Infrastructure
provisioning system for mobile devices client		provisioning system for mobile devices server	
healthcare mobile device application		mobile device management server	
storage encryption		auditing mobile device	

3.5 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 – the absence of corruption in the hardware, firmware, and software of a device. A device has integrity if its software, firmware, and hardware configurations are in a state that is trusted by a relying party
- 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
- security incidents – the process of identifying and responding to suspected or known security incidents
- recovery – planning and executing data backup and disaster recovery

Table 3-2 shows the relationship between the security characteristics and the NIST Framework for Improving Critical Infrastructure Cybersecurity (also known as the NIST Cybersecurity Framework) for critical infrastructure functions and categories and HIPAA requirements. The security characteristics in Table 3-2 are also derived from our use case. In this use case, application security was implicit in device integrity. When we build our next use case, we may consider more security characteristics.

Table 3-2 Mapping Security Characteristics to the NIST Cybersecurity Framework and HIPAA

Security Characteristics	NIST Cybersecurity Framework Function	NIST Cybersecurity Framework Category	HIPAA Security Rule [8]
access control	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
audit controls/monitoring	Detect (DE)	Security Continuous Monitoring (DE.CM)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(d), 164.312(e), 164.314(b)
device integrity	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
		Data Security (PR.DS)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e), 164.314(b), 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e), 164.314(b)
		Information Protection Processes and Procedures (PR.IP)	45 C.F.R. §§ 164.306(e), 164.308(a), 164.310(b), 164.312(a), 164.316(b)
		Protective Technology (PR.PT)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(e)
	Detect (DE)	Security Continuous Monitoring (DE.CM)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(d), 164.312(e), 164.314(b)

Security Characteristics	NIST Cybersecurity Framework Function	NIST Cybersecurity Framework Category	HIPAA Security Rule [8]
person or entity authentication	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
transmission security	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e)
		Data Security (PR.DS)	45 C.F.R. §§ 164.308(a), 164.308(b), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(c), 164.312(d), 164.312(e), 164.314(b)
		Protective Technology (PR.PT)	45 C.F.R. §§ 164.308(a), 164.310(a), 164.310(b), 164.310(c), 164.310(d), 164.312(a), 164.312(b), 164.312(e)
security incidents	Respond (RS)	Mitigation (RS.MI)	45 C.F.R. §§ 164.308(a)
	Recover (RC)	Recovery Planning (RC.RP)	45 C.F.R. §§ 164.308(a), 164.310(a)

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

3.6 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 2013, the NCCoE 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 3-3 lists all products and the participating companies and open-source providers used to implement the security requirements in Table 3-2. The NIST Cybersecurity Framework aligns with existing methodologies and aids organizations in describing how they manage cybersecurity risk. The complete mapping of representative product to security controls can be found in NIST SP 1800-1D, Technologies, Section 5.

Table 3-3 Participating Companies and Contributions Mapped to Controls

NIST Cybersecurity Framework Function	Company	Product	Use
Identify (ID)	RSA	Archer GRC	Centralized enterprise, risk, and compliance management tool
Protect (PR)	MedTech Enginuity	OpenEMR	Web-based and open-source EHR and supporting technologies
	open source	Apache Web Server	
	open source	OpenSSL	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	Fedora PKI Manager	Root certificate authority cryptographically signs identity certificates to prove authenticity of users and devices
	open source	BIND	Domain name system (DNS) server performs host or fully qualified domain resolution to internet protocol addresses
	open source	Puppet Enterprise	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
	Cisco	Identity Services Engine	Local and remote mobile network access control (NAC), radius-based authentication, authorization and accounting management server
	Cisco	ASAv	Enterprise-class VPN server based on both Transport Layer Security (TLS) and Internet Protocol Security (IPSec)
	open source	URbackup	Online remote backup system used to provide disaster recovery

NIST Cybersecurity Framework Function	Company	Product	Use
	Cisco	RV220W	Wi-Fi access point
Detect (DE)	Fiberlink	MaaS360	Cloud-based mobile device policy manager
	open source	iptables firewall	Stateful inspection firewall
	open source	Puppet Enterprise	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
	open source	Security Onion IDS	Intrusion detection server (IDS) monitors network for threats via mirrored switch ports
	open source	Host-based security manager (freeware)	Host-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	Puppet Enterprise	Secure configuration manager for 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 4) contains many applications supporting the security of the enterprise, which, in turn, secure the EHR and mobile device systems. While the products 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 their risk assessment. See Volume 1800-1E of this publication, Risk Questionnaire, Section 8, for a list of questions you can use with your third-party provider.

4 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

4.1 Methodologies

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

4.1.1 Defense-in-Depth

A defense-in-depth strategy includes defending a system against attack by 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 EHR management system.

4.1.2 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, technologies, and best practices. For example, if new security technologies emerge, the architecture can be altered with minimal effort.

4.1.3 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.

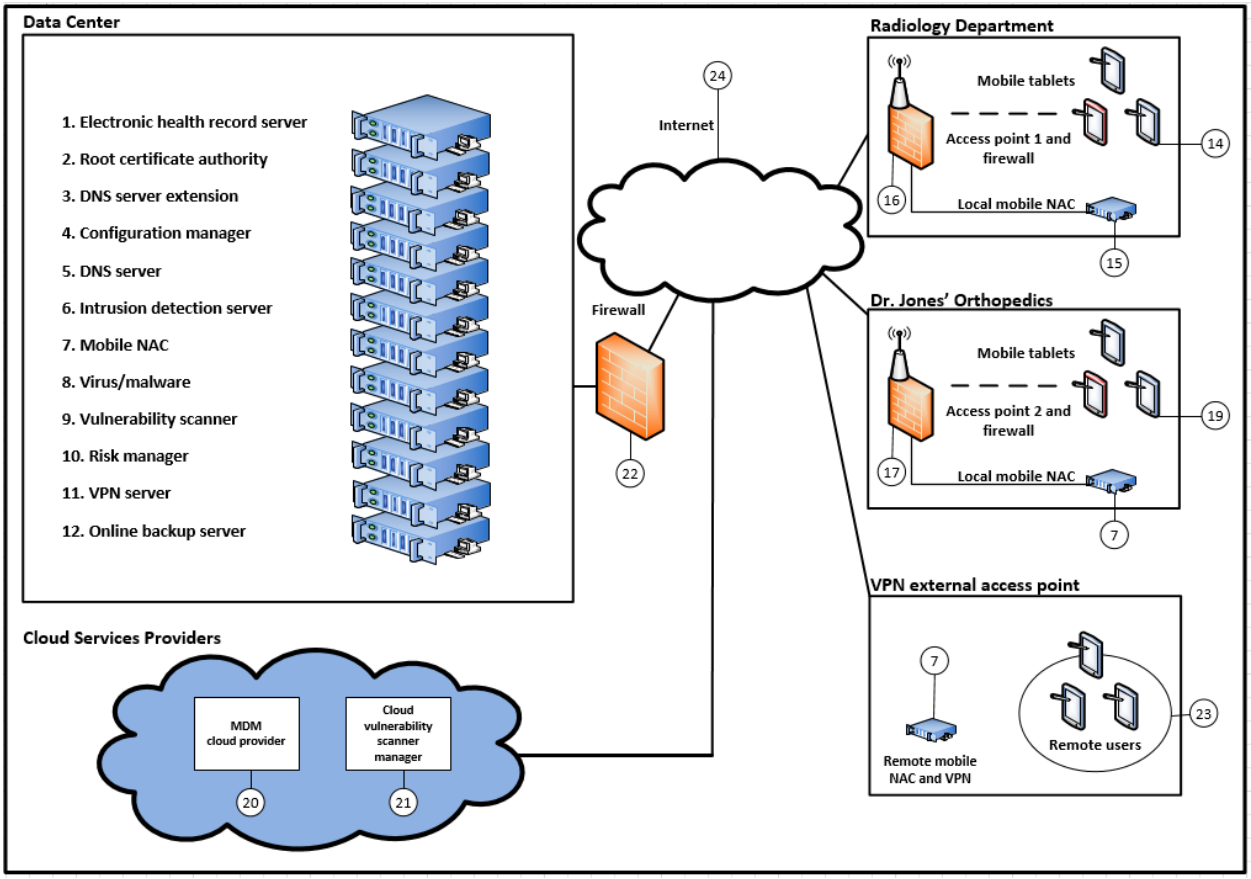
4.2 Architecture Description

Figure 4-1 illustrates the project's simulated health IT enterprise for the healthcare 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 healthcare 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 4-1 Architecture for the Secure Exchange of Electronic Health Records on Mobile Devices in a Healthcare Organization



4.2.1 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 suborganizations (e.g., a radiology department).

4.2.1.1 The Server Room/Data Center

The Data Center represents the central computing facility for a healthcare organization. It typically performs the following services: (Numbers in parentheses refer to Figure 4-1.)

- EHR web portal – provides the EHR server (i.e., OpenEMR service) (#1)
- identity and access services – provide 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)

- DNS services – provide authoritative name resolution for the Data Center, Radiology Department, and Dr. Jones' Orthopedics (#3 and #5)
- firewalls – provide 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 services – provide remote enforcement and management of user access to 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)
- remote VPN connectivity – provides strong identity and access controls, in addition to confidentiality of patient health information, using network encryption for transmissions. Facilitates secure and confidential communications among patients, doctors, and healthcare administrators who are not on premises (#11)
- configuration manager – facilitates creating secure system configurations (#4)
- online backup manager – creates logical offsite backup for continuity of operations (#12)
- IDS – monitors network for known intrusions to the Data Center network, Radiology Department, and Dr. Jones' Orthopedics (#6)
- remote mobile 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 by using Risk Management Framework [9], NIST controls, HIPAA guidance, and physical device security posture (#10)

4.2.1.2 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.

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 (#15)
- 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 connectivity to OpenEMR (#1)

4.2.1.3 Dr. Jones' Orthopedics

Dr. Jones' Orthopedics outsources IT technology and services to an external organization. Dr. Jones would use the questionnaire in Volume 1800-1E of this publication, Risk Questionnaire, Section 8, to assess and hold its service provider accountable for the implementation of security controls.

The services and servers below are managed off-site by the Data Center:

- identity and access services (#7)
- firewall (#17 and #22)
- wireless access points (#17)
- mobile device policy creation (#20)
- certificate authority (#2)
- virus and malware scanning (#8)
- remote connectivity to OpenEMR (#1)

4.2.1.4 VPN

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

The services and servers below are managed off-site by the Data Center:

- identity and access services (#7)
- firewall (#22)

- mobile device policy creation (#20)
- certificate authority (#2)
- virus and malware scanning (#8)
- remote VPN (#11) connectivity to OpenEMR (#1)

4.2.1.5 Third-Party Cloud Services Providers

Third-party cloud services 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.

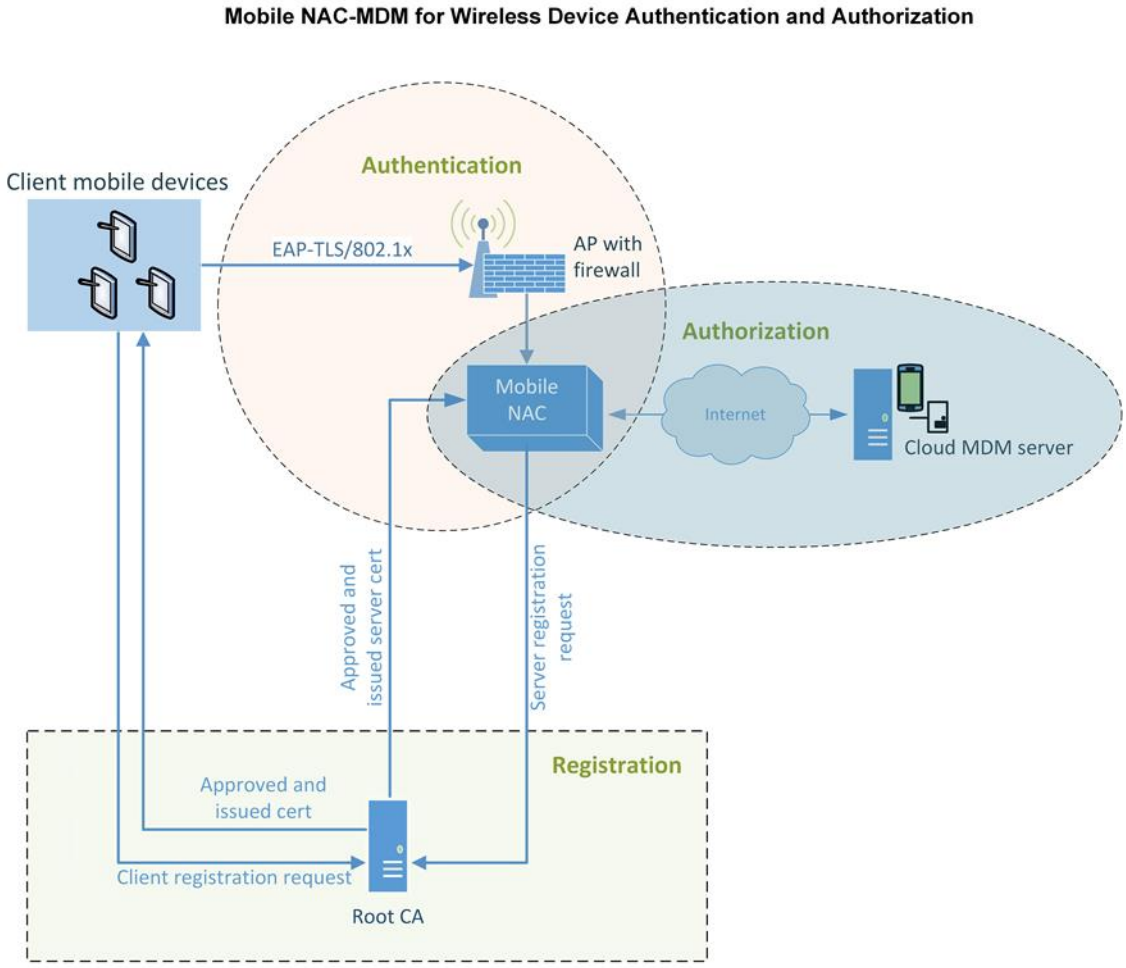
4.3 Security Characteristics

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

4.3.1 Access Control

Below are important features that restrict access to a resource. Figure 4-2 shows user and system identity access controls.

Figure 4-2 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, username, 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 EHR server have access controls implemented. These access controls were implemented in the NCCoE reference design. How they are

implemented in actual healthcare organizations can have an effect on easy use of the system—which may require work-arounds for certain emergency situations.

4.3.2 Audit Controls and Monitoring

- user audit controls – simple audits are in place. While additional security incident and event managers 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 by vulnerability scanning tools for risks to known good secure configurations. The vendors participating in this project did not provide specific user activity monitoring for mobile devices; however, the MDM tool can monitor changes in users' devices, in accordance with an organization's policy. The MDM device can also monitor the geographic location of users if an organization's policy dictates conformity with geospatial requirements. The auditing of data center staff was considered out of scope for this reference design because the absence of actual data center staff made auditing their behavior impractical.

4.3.3 Device Integrity

- server security baseline integrity – server service device integrity in the notional Data Center is achieved via creating and continuously monitoring 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 off-site/remotely via encrypted communication with a backup service.

4.3.4 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 by using strong authentication methods.

4.3.5 Transmission Security

All communication among a typical patient, doctor, health IT administrator, and the electronic health record system is protected via end-to-end encryption by using IPSec, TLS, or similar technology. Federal agencies should verify that all components using Extensible Authentication Protocol (EAP) Transport Layer Security (TLS) are Federal Information Processing Standard (FIPS) 140-2 validated. In our implementation, because we used such a varied set of products, not all of the products were FIPS 140-2 validated.

Appendix A References

[1] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication 800-124 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf [accessed 4/24/2018].

[2] *Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data*, Ponemon Institute, May 2015, https://media.scmagazine.com/documents/121/healthcare_privacy_security_be_30019.pdf [accessed 4/24/2018].

[3] J. Pritts, *HHS Mobile Devices Roundtable: Health Care Delivery Experts Discuss Clinicians' Use of and Privacy & Security Good Practices for mHealth*, The Office of the National Coordinator for Health Information Technology, Department of Health and Human Services [Website], http://www.healthit.gov/buzz-blog/privacy-and-security-of-ehrs/mobile-devices-roundtable/ [accessed 4/24/2018].

[4] R. Kissel, *Glossary of Key Information Security Terms*, NISTIR 7298 Revision 2, National Institute of Standards and Technology, Gaithersburg, Maryland, May 2013, http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf [accessed 4/24/2018].

[5] *Mobile Devices – Secure Exchange of Electronic Health Information*, Final Draft, National Cybersecurity Center of Excellence, National Institute of Standards and Technology, Gaithersburg, Maryland, November 2014, https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-ehr-project-description-final.pdf [accessed 4/24/2018].

[6] *ONC Health IT Certification Program*, The Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, [Website], https://www.healthit.gov/policy-researchers-implementers/onc-health-it-certification-program [accessed 4/24/2018].

[7] *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, February 2016, https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf [accessed 4/24/2018].

[8] K. Marchesini, *Mobile Devices Roundtable: Safeguarding Health Information: Real World Usages and Real World Privacy & Security Practices*, The Office of the National Coordinator for Health Information Technology, Department of Health and Human Services, Washington, D.C., March 16, 2012, https://www.healthit.gov/sites/default/files/onc_ocpo_mobile_device_roundtable_slides_3_16_12.pdf [accessed 4/24/2018].

[9] *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2014, http://doi.org/10.6028/NIST.SP.800-37r1 [accessed 4/24/2018].

NIST SPECIAL PUBLICATION 1800-1C

Securing Electronic Health Records on Mobile Devices

Volume C:
How-To Guides

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

Brett Pleasant
Sue Wang
Kangmin Zheng
Marc Schneider
The MITRE Corporation
McLean, VA

Colin Bowers
Kyle Kamke
Ramparts, LLC
Clarksville, MD

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

DISCLAIMER

Certain commercial entities, equipment, products, or materials may be identified in this document 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, equipment, products, or materials 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, 103 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://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 align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Healthcare 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 healthcare providers, mobile devices can introduce vulnerabilities in a healthcare organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that many providers are using mobile devices for healthcare delivery before they have implemented safeguards for privacy and security [1].

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

KEYWORDS

EHR; electronic health records; HIPAA; mobile device security; patient health information; PHI; risk management; standards-based cybersecurity; stolen health records

ACKNOWLEDGMENTS

We would like to highlight and express our gratitude to Leah Kauffman, with NIST, who served as editor-in-chief of this guide.

We are grateful to the following individuals for their generous contributions of expertise and time.

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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. We worked with:

Technology Partner/Collaborator	Build Involvement
Cisco	Identity Services Engine (ISE), Adaptive Security Virtual Appliance (ASAv), and RV220W
IBM	MaaS360
Intel	Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI)
MedTech Enginuity	OpenEHR software
Ramparts	Risk assessment and security testing
RSA	Archer Governance, Risk & Compliance (GRC)
Symantec	Endpoint Protection

Contents

List of Figures

List of Tables

1 Introduction

The following guides show information technology (IT) professionals and security engineers how the NCCoE implemented this example solution for securing the transfer of electronic health records (EHRs) on mobile devices. We cover all the products in the selected versions 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 into our environment.

These guides assume that you have experience implementing security products in a healthcare 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. 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 done. Refer to National Institute of Standards and Technology (NIST) Special Publication (SP) 1800-1D: Standards and Controls Mapping, Section 4, 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 alternative products. NIST SP 1800-1D, Section 4, Security Characteristics and Controls, Table 2, describes how we arrived at this list of controls.

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

- The NCCoE developed an example solution to this problem by 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), the guide demonstrates how to implement standards-based cybersecurity technologies in the real world, based on risk analysis.

1.1 Practice Guide Structure

This guide assumes that IT professionals have experience implementing security products within the enterprise. While we have used a suite of commercial products to address this challenge, this guide does not endorse these particular products. 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. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. We hope you will seek products that are congruent with applicable standards and best practices.

A NIST Cybersecurity Practice Guide does not describe "the" solution but a possible solution. We seek feedback on this guide's 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.

Note: *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.*

1.2 Typographic Conventions

The following table presents typographic conventions used in this volume.

Typeface/Symbol	Meaning	Example
Italics	filenames and pathnames references to documents that are not hyperlinks, new terms, and placeholders	For detailed definitions of terms, see the *NCCoE Glossary*.
Bold	names of menus, options, command buttons and fields	Choose **File > Edit**.
`Monospace`	command-line input, on-screen computer output, sample code examples, status codes	`mkdir`
`Monospace Bold`	command-line user input contrasted with computer output	**`service sshd start`**
blue text	link to other parts of the document, a web URL, or an email address	All publications from NIST's National Cybersecurity Center of Excellence are available at https://www.nccoe.nist.gov.

2 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.

2.1 Windows Installation and Hardening

2.1.1 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 GB
Disk space	Minimum 150 GB

2.1.2 Windows Installation

We assume you purchased the appropriate Microsoft operating system (OS) and that you have both the compact disc and product key.

If you are not familiar with Microsoft's command line or nongraphical management, we recommend that 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
- 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.

2.1.3 Windows Post-Installation Tasks

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

2.1.4 Windows Security Hardening

2.1.4.1 Using Puppet

We employed Windows OS 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 of 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 that Windows updates are on.

2.1.4.2 Using Security Technical Implementation Guides (STIGs)

The Department of Defense's (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 to be important, that the STIG 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.

2.2 Linux Installation and Hardening

2.2.1 Linux Installation

We downloaded the Fedora 20 image from the following links:

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

We 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 implementing 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 EHR application should have its own partition or disk.

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

2.2.2 Linux Post-Installation Tasks

Install the Puppet agent by following the Puppet Enterprise installation instructions in Section 4.2.

Follow the instructions in Section 4.2, Puppet Enterprise Configuration, to configure the hostname in the *site.pp* file.

Install the backup agent by following the UrBackup instructions in Section 5.

2.2.3 Linux Security Hardening

Use the Puppet Enterprise configuration tool for all Linux OS 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 of 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, four tasks 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 the systems 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 a set 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 online 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 accurate time-stamped logs.

warningbanners.pp – creates warning banners at the console and remote login sessions that warn users that their sessions will 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.

3 Basic Network Infrastructure Services

Basic network infrastructure services exist throughout the architecture and consist of all switching and routing protocols related to layer 2 and layer 3 of the Open Systems Interconnection 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 internet protocol (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 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.

Table 3-1 Qualified Domain Names and IP Addresses Used in This Build

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	192.168.200.252
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

Capability Name	Hostname/FQDN	IP
HealthIT Organization #1 Mobile Devices		10.10.101.0/24
HealthIT Organization #2 Mobile Devices		10.10.102.0/24

3.2 Bind Domain Name System (DNS) and Domain Names Search Engine (DNSE) Installation and Hardening

The 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 split-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 8 GB
- Disk space Minimum 150 GB

You will also need the following parts of this guide:

- Section 2.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 4.2, 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.

Install Bind DNS by using root or sudo by entering the following (procedures are the same for Internal DNS and External DNS):

```
> 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 Internet Service Provider (ISP) by entering:

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

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

```
> vi healthitorg1.org
```

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

```
> vi healthitorg2.org
```

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

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

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

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

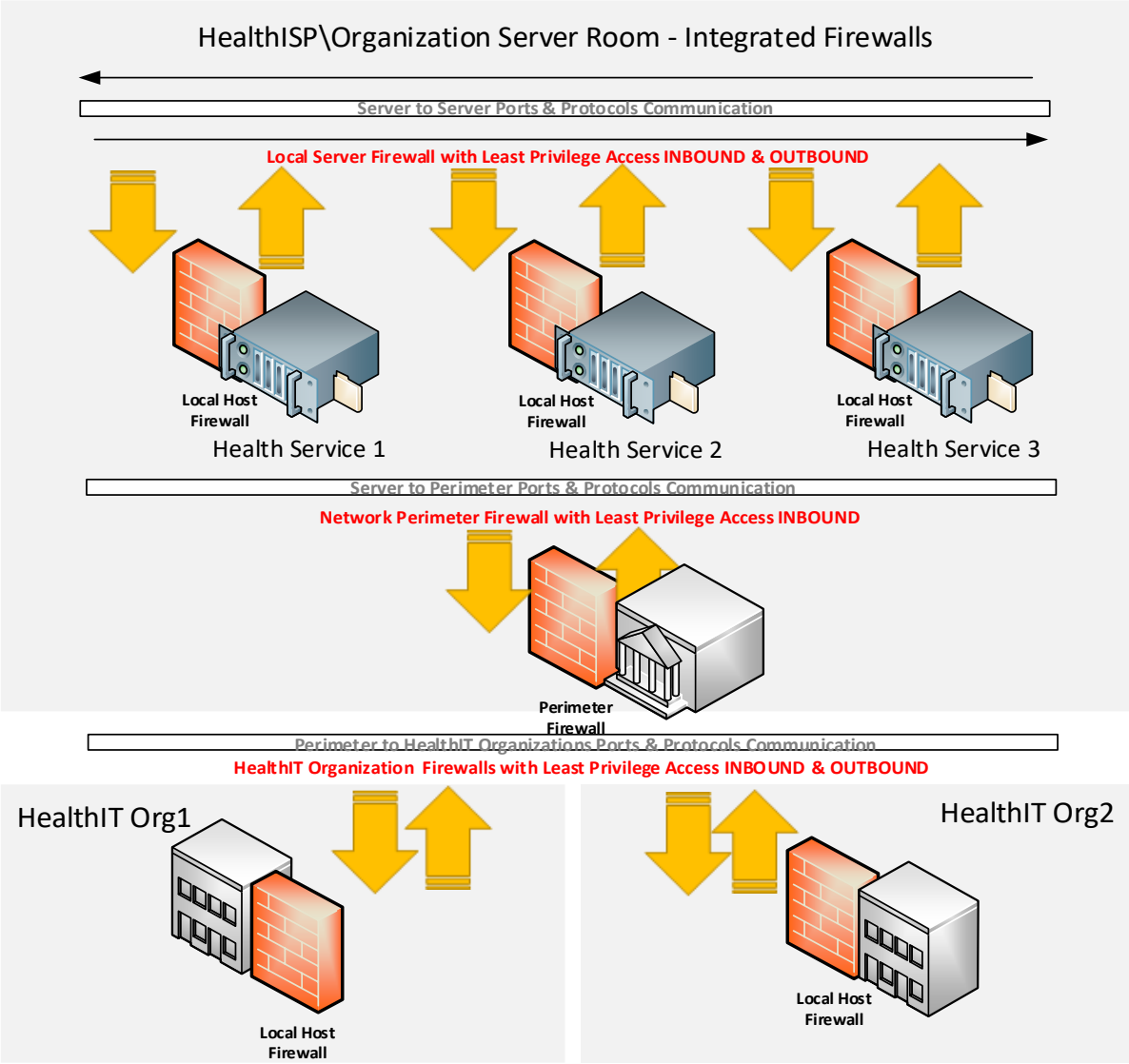
Sample DNS files used in this build can be found in the online file repository for this use case at https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.zip.

3.3 Firewalls: IP Tables

A firewall is used to control egress and ingress network traffic among multiple subnets and/or systems. A firewall will determine what traffic goes in what 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 among other subnets has a firewall to protect internet traffic from traversing inbound to the internal network.

Figure 3-1 Integrated Firewalls



System requirements

- Linux OS
- 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 list [HCL] for more)
- If this is a system that protects multiple subnets, then multiple network interface cards (NICs) 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 2.2.2, 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 below has been followed.

3.4 Intrusion Detection System (IDS)

An IDS monitors a network for known threats to an organization's 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 transmission control protocol (TCP) transmission analysis.

3.4.1 Security Onion

Security Onion is the IDS selected for this build. It was selected based on its record in the open-source community for its support of 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 might not have been asked.
- **Sguil** – used as a database for IDS alerts.
- **ELSA** – allows the user 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://github.com/security-onion-solutions/security-onion/wiki/Hardware.
- Find the ISO (International Standards Organization) image full version at https://github.com/security-onion-solutions/security-onion/wiki/quickISOimage.
- Find the Install Version for Ubuntu Linux at https://github.com/security-onion-solutions/security-onion/wiki/InstallingOnUbuntu.

You will also need the following parts of this guide:

- Section 2.2, Linux Installation and Hardening
- Section 3.1, Hostnames

Security Onion setup

We followed the documentation provided by Security Onion:

- Introduction https://github.com/security-onion-solutions/security-onion/wiki/IntroductionToSecurityOnion

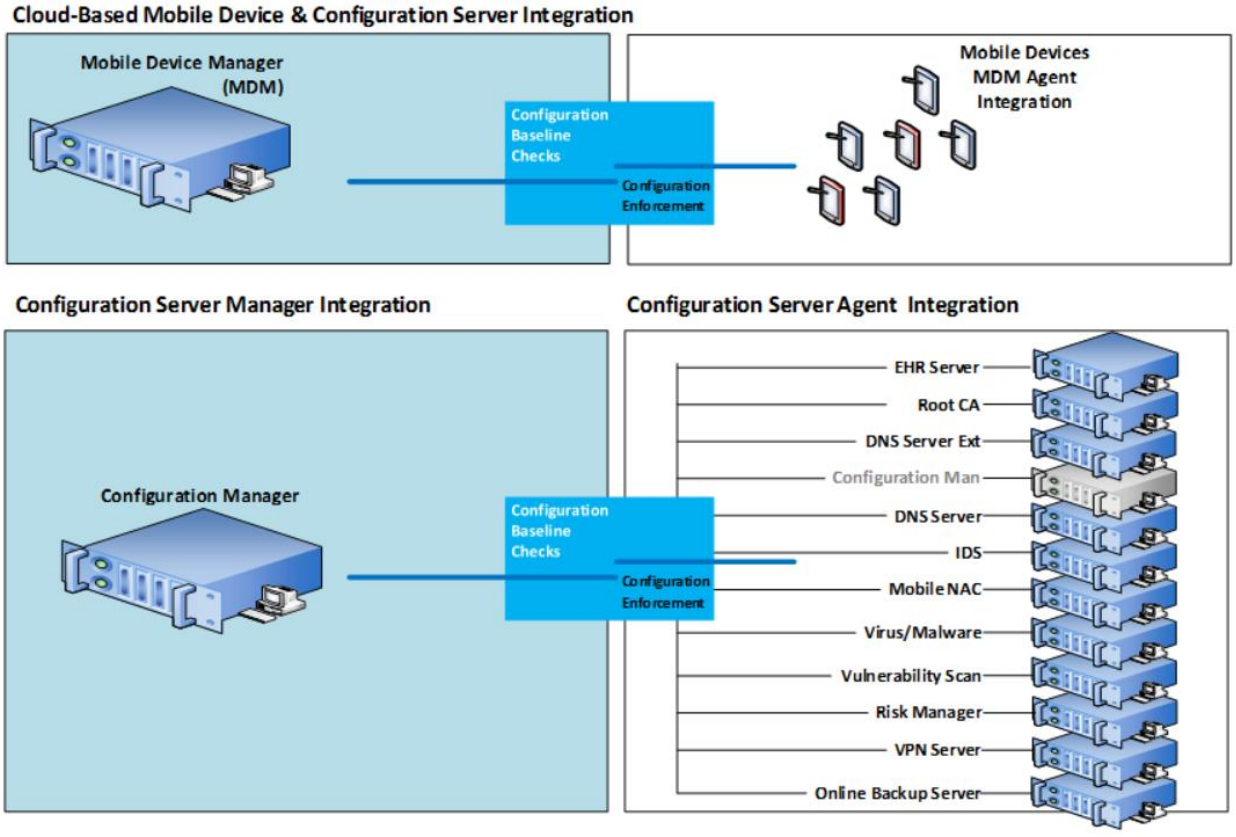
- Production installation steps
  https://github.com/security-onion-solutions/security-onion/wiki/ProductionDeployment
- Booting issues
  https://github.com/security-onion-solutions/security-onion/wiki/TroubleBooting
- Post-installation
  https://code.google.com/p/security-onion/wiki/PostInstallation

4 Configuration Management

Understanding, implementing, and maintaining a secure baseline for all systems that process and store protected health information (PHI) is critical to the systems' 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

Figure 4-1 System Security Baseline and Configuration Management System



System requirements

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

You will also need the following parts of this guide:

- Section 2.2, Linux Installation and Hardening
- Section 3.1, Hostnames

4.1 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.

4.1.1 Pre-installation Tasks

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

4.1.2 Installation Instructions

This build used Puppet Enterprise on Fedora 20 Linux. Find install instructions for Puppet Enterprise at Fedora 20.

4.1.3 Post-Installation 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 4.2, Puppet Enterprise Configuration. We give specific guidance in Section 4.2.3 regarding changes to the Puppet Enterprise post-installation documentation.

According to the post-installation 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-installations unless you are familiar with the security implications and advanced features.

- Automatic Puppet Master Certificate Processing – this has security implications.
- 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-installation 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 4.2.5, Puppet Enterprise Web-Based Reporting Installation and Configuration; and in Section 4.3, Production Web Server.

4.2 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 used Puppet templates to assist with creating Linux-based files to be used in configuration management and secure baseline controls.

4.2.1 Puppet.conf

The *puppet.conf* file for the Puppet Master is located in the */etc/puppet* directory. The configuration file for this build can be found at https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.zip. Once downloaded, the file should be moved to the */etc/puppet/puppet.conf* directory of Puppet Master.

4.2.2 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/projects/use_cases/medical_devices.

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 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 manifest imports and calls to predefined classes created in each manifest.
- *accounts.pp* – this file 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 it back based on the entries in this file.
- *crontabconfig.pp* – this file creates tasks that run automatically at set intervals. In this case, four tasks 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 the systems 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 a set time every day.

- *harden.os.single.commands.sh* – this is a series of single commands to ensure that changes to permissions on critical system files and 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 OS 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 Transport Layer Security (TLS) and Online Certificate Status Protocol (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 accurate time-stamped logs.
- *warningbanners.pp* – this creates warning banners at the console and remote login sessions that warn users that their sessions will be authorized and monitored. This banner should deter good people from accidentally doing bad things. It will in no way stop a determined attacker under any circumstances.

4.2.3 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 re-create 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 in this build can be downloaded from this page: https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.zip.

Once you download the templates, move them to the */var/lib/puppet/templates* directory. The templates directory may need to be created by 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 nonroot 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*

4.2.4 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 by 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
```

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

- *puppetlabs-apache* – streamlined creation of web services by using Apache
- *puppetlabs-mysql* – streamlined edits of *mysql* with minimal configuration
- *puppetlabs-concat* – allows creation of configuration files based on concatenation
- *puppetlabs-ntp* – allows the user to manage standard time on systems
- *puppetlabs-registry* – allows edits to the Windows registry for configuration
- *puppetlabs-stdlib* – the standard library for resources on Puppet

4.2.5 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:

After downloading the puppet-dashboard package, 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.<YourOrganization>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
```

4.3 Production Web Server

These instructions are for a nonproduction 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.

5 Backup

The backup system is an important part of security, as it assists with ensuring that 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 off-site backups are harder to tamper with or lose in a local disaster to the architecture.

This section will show you how to install an online backup system by using UrBackup.

UrBackup is a remote backup system that will facilitate both full and incremental backups. It is 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 8 GB
- Disk space Minimum 150 GB

You will also need the following parts of this guide:

- Section 2.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 4.2, Puppet Enterprise Configuration

5.1 UrBackup Server Setup

Baring details on http://urbackup.org/download.html, download software and compile the server:

1. Download the *UrBackup server* source tarball and extract it.
2. Install the dependencies. Those are *gcc*, *g++*, *make*, *libcrypto++*, and *libcurl* (as development versions).
3. Compile and install the server via `./configure`, `make`, and `make install`.
4. Run the server with `start_urbackup_server`.
5. Add */usr/sbin/start_urbackup_server* to your */etc/rc.local* to start the *UrBackup server* on server start-up.

After you have installed the UrBackup Server, perform the following steps:

1. Go to the user settings and add an admin account. If you do not do this, everybody who can access the server will be able to see all backups.

a. Set up the mail server by entering the appropriate mail server settings.

b. If you want the clients to be able to back up via the internet and not only via local network, configure the public server name or IP of the server in the internet settings.

2. If you want to get logs of failed backups go the Logs screen and configure the reports for your email address.

Change any other setting according to your usage scenario.

5.2 UrBackup Client Setup

Follow these instructions to build, install, and set up UrBackup on Fedora 20 Linux systems.

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

1. Follow Section 2.2, Linux Installation and Hardening.

2. Install the dependencies UrBackup needs:

   a. If installing on Fedora 20, there should be a WxWidgets application already installed. If not, download the WxWidgets and install it according to the installation instruction. Please verify that its version is higher than 3.0 by using the command `wx-config--version`.

   b. On Fedora 20, you will use *yum* as your installer.

3. Input the following commands:

```
> 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 path name 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. Set up 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
   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 of 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 to resolve the above authentication error:

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

a. Log in to the UrBackup Server via the web link http://<yourhost.yourdomain.com>:55414.

b. Go to the Status screen.

c. Under Internet Clients enter the FQDN name of the laptop/personal computer (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.

d. 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.

e. In 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.

f. 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.

g. 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 back end on start-up by using the following for Fedora 20:

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

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

```
[Unit]
Description=Starting back end 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 boot-up:

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

Or

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

8. Start the UrBackup client back end on start-up by 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:
    a. Log in to the UrBackup Server web portal.
    b. Use the client dropdown menu and select the client for whom you want to set custom settings for this configuration.
    c. Select the Separate Settings for This Client radio button and begin edits.
    d. 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 -- 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
```

6 Certificate Authority

The certificate authority (CA) uses the OpenSSL cryptographic libraries to create and then sign soft certificates for use in identifying mobile devices that would ultimately connect to both the access point (AP) and the OpenEMR server. The CA 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 CA. Using a public key infrastructure (PKI) approach is among the strongest methods to ensure proper identity and access control for PHI.

6.1 Fedora PKI Manager

The CA used for this build is based on a Linux PKI Manager used in Fedora, RedHat Enterprise, and other production-class Linux distros.

System requirements

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

You will also need the following parts of this guide:

- Section 2.2, Linux Installation and Hardening
- Section 3.1, Hostnames
- Section 3.2, Bind Domain Name System (DNS) and Domain Names Search Engine (DNSE) Installation and Hardening
- Section 4.2, Puppet Enterprise Configuration

Fedora PKI Manager Installation

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

6.2 Post-Installation

Fedora PKI Manager Administrator setup instructions can be found at http://pki.fedoraproject.org/wiki/CA_Admin_Setup.

To manually create user/device certificates, follow the steps in Section 10.1, Mobile Devices, 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 will be a list of pending requests. Write down the request number for use later in the process. 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 your certificate request reference number that was created during the registration request process.
5. Scroll to the bottom of the page and download.

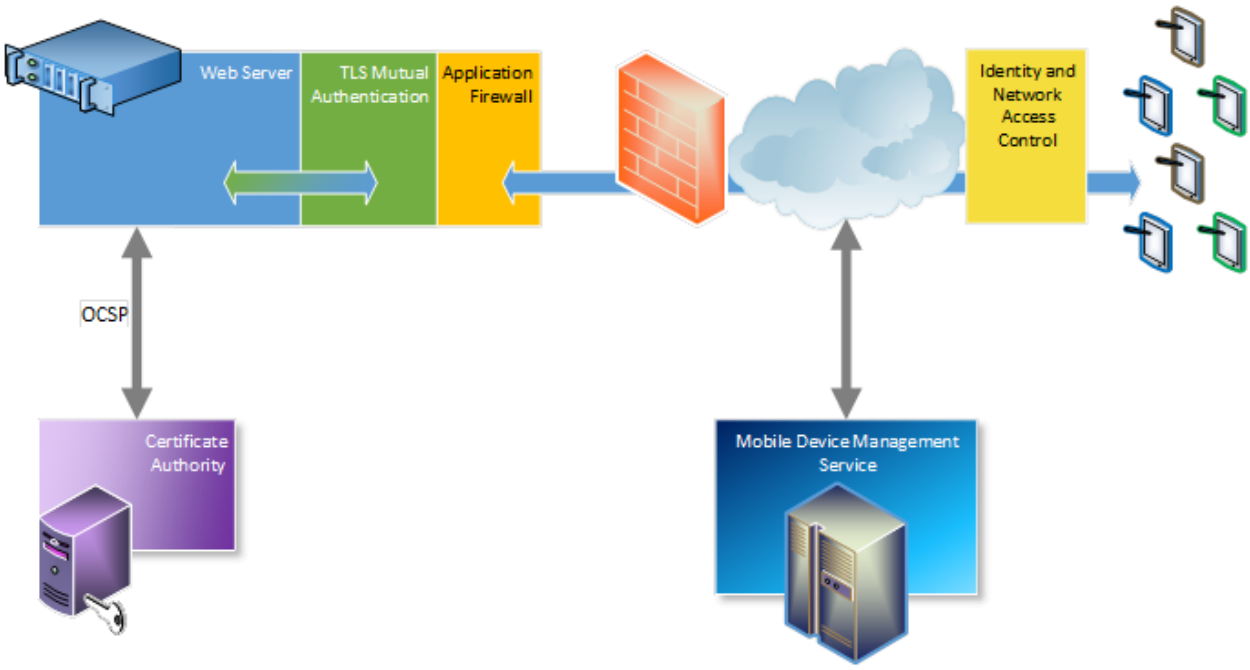
Or

Copy and paste the certificate information to the mobile device desktop and follow Section 10.1 for details on how to install the certificate.

7 Identity and Access Controls

This build utilizes a RADIUS server integrated with our CA and AP, which combine to create the full identity and access control function. A RADIUS server uses the authentication, authorization, and accounting (AAA) protocol to manage network access via those functions. 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 CA as a recipient of a signed root certificate and OCSP communication. The authorization mechanism is integrated with the mobile device manager to check mobile device policy for compliance.

Figure 7-1 Integrated Web-Based Mobile EHR System Architecture



7.1 Cisco Identity Services Engine

Benefits of the Cisco Identity Services Engine (ISE):

- Identity and access policy management are centralized and unified.
- Certificate challenges provide visibility and more assured device identification.
- Organizations can use business rules to segment access to sections of the network.
- The user experience during the challenge process is made seamless.

System requirements

- Virtual Hypervisor (VH) capable of housing virtual machines (VMs)
- VM with central processing unit (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 6.1, Fedora PKI Manager
- Section 10.2.1, 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 VM.
2. Follow the guidance from your VM vendor to boot the DVD or ISO and start the installation 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 with the CLI and the admin portal access are provided by the Cisco ISE

More detailed procedures for installing the Cisco ISE are available from the installation guide provided by Cisco, available at https://www.cisco.com/c/en/us/td/docs/security/ise/1-2/installation_guide/ise_ig/ise_pref.html.

7.2 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.

7.3 Configure Cisco ISE to Support EAP-TLS Authentication

7.3.1 Set ISE to support RADIUS authentication

The following steps are used to set up a communication connection from Cisco ISE to the network device (AP) 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.
    - 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 Advanced Encryption Standard (AES) Key Wrap algorithm. However, you should be experienced with Cisco ISE and confident that your network device supports this configuration.

7.3.2 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 Common Name (CN) field matches the FQDN of the Cisco ISE server.

2. Export the CSR from the navigation path **Administration > System > Certificates > Certificate Signing Requests,** then select **Export.**

3. Save and submit the CSR file to a CA. 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 6, Certificate Authority.

5. Use the ISE Administration interface to bind the acquired CA-signed certificate with its private key by using the path **Administration > System > Certificates > Local Certificates,** then **Add > Bind CA Signed Certificate.**

If you intend to use this certificate for client Extensible Authentication Protocol-Transport Layer Security (EAP-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.

7.3.3 Populate Certificate Store with Required CA-Signed Certificates

The CA-signed root certificate and the certificate for Fiberlink MaaS360 MDM server are required by the certificate store. You will need to have the CA root certificate in Privacy Enhanced Mail (PEM) or Distinguished Encoding Rules (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 6, 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.

7.3.4 Set Identity Source for Client Certificate Authentication

No internal or external identity source is required for the EAP-TLS certificate-based authentication method because 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.

7.3.5 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, Protected Extensible Authentication Protocol, and the EAP-TLS. For this build, we used the EAP-TLS protocol for user and machine authentication.

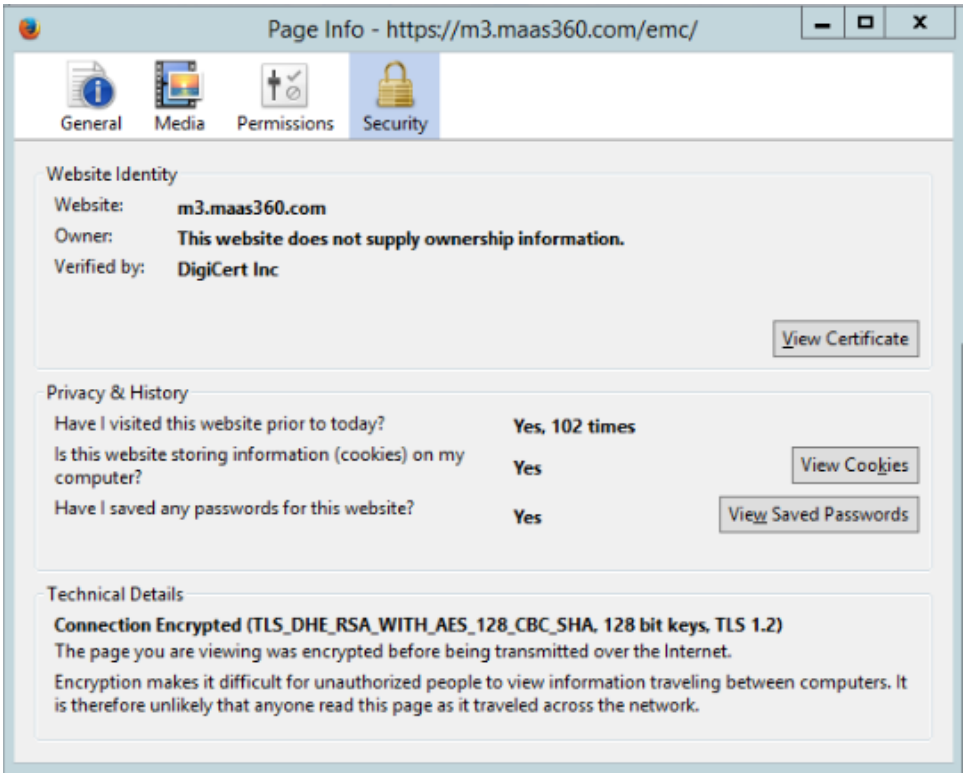
To specify the allowed protocols services in Cisco ISE:

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.

7.3.6 Configure Cisco ISE to Integrate with Fiberlink MaaS360

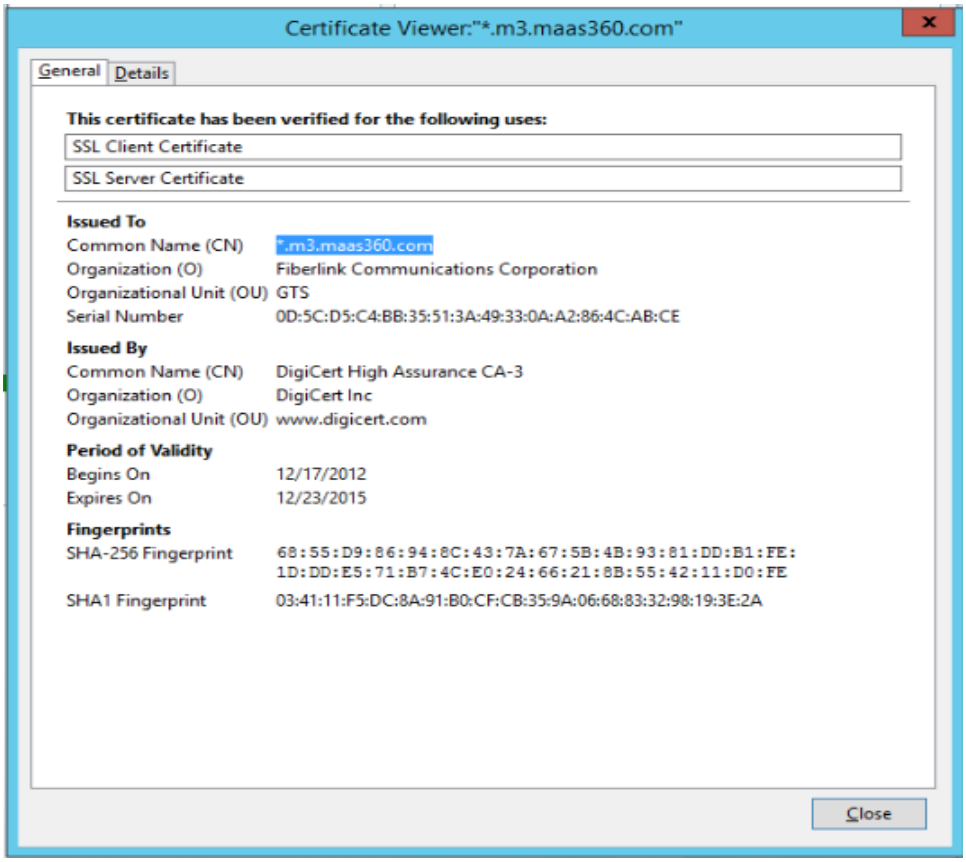
1. Establish basic connectivity between the Cisco ISE server and the Fiberlink MaaS360 MDM server. As indicated in the architecture diagram, firewalls are installed between the ISE and the Fiberlink MaaS360 in the cloud. The firewall should be configured to allow a Hypertext Transfer Protocol Secure (HTTPS) session from the ISE to the Fiberlink MaaS360 server located in the public internet. The session is established outbound from ISE toward 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.
    a. From the browser, log on to the MaaS360: https://login.maas360.com.
    b. In the browser next to the URL, there is a lock symbol. Click that symbol. Open a security information page as shown below:

Figure 7-2 Page Info Window



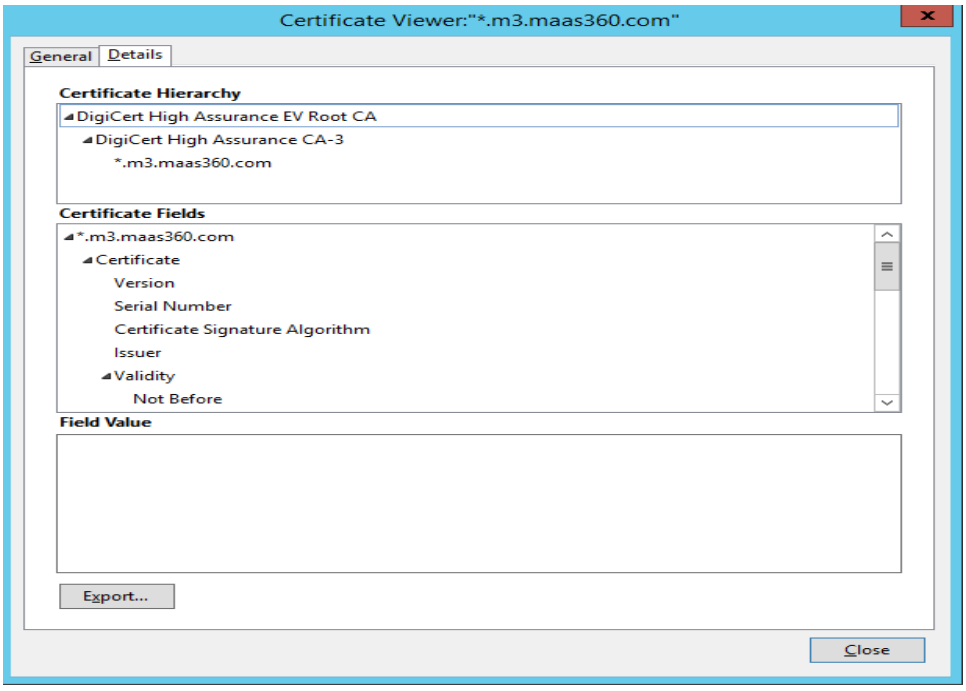
c. Click the **View Certificate** button to view the certificate.

Figure 7-3 Certificate Viewer – General



d. Select the **Details** tab to view the detailed certificate information. From there you should have an **Export** button to export the certificate.

Figure 7-4 Certificate Viewer – Details



e. **Save** the certificate to a file.

4. Import the certificate into the local certificate store in ISE.

    a. From the ISE Administration Portal, use the navigation path **Administration > System > Certificates > Certificate Store** to perform the import action.

    b. Grant ISE Access to the Fiberlink MaaS360 Application Programming Interface (API).

5. Create a Fiberlink MaaS360 administrator account with an API role.

    a. Log on to the MaaS360 with an Administrator Account.

    b. Navigate to **Setup > Administrators** and click **Add Administrator.**

    c. Enter the *new username* and a *corporate email address* and click **Next.**

    d. Enter *Roles* for the newly created administrator and click **Next.**

    e. Verify the setting and press **Save.**

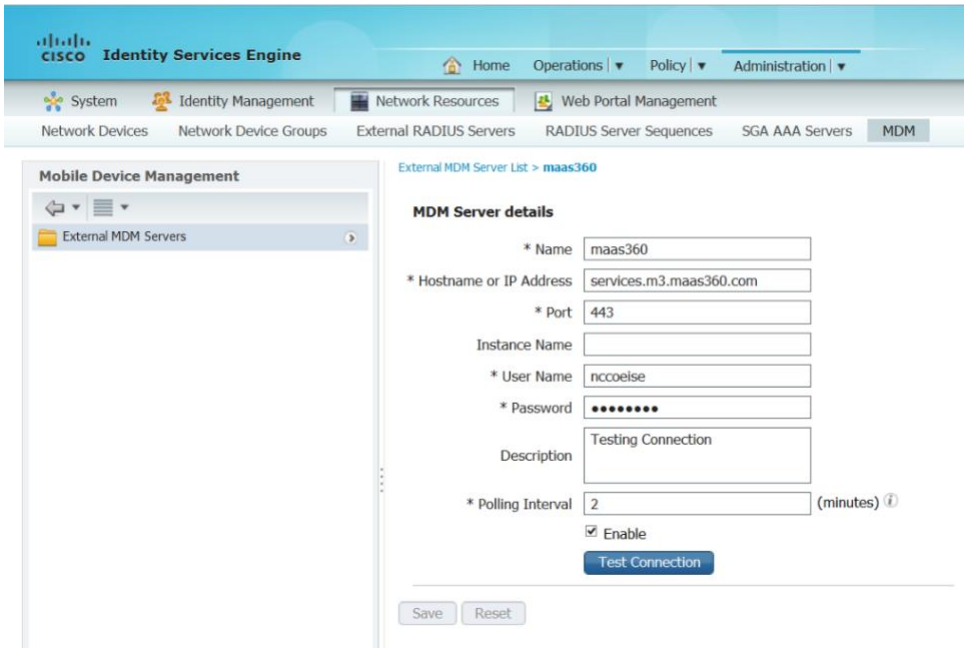
6. Add MDM server to ISE.

    a. Use the MaaS360 MDM admin account created above.

    b. Configure Cisco ISE to integrate with the MaaS360: **Administration > MDM > External MDM Server,** then click **Add.**

    c. Fill out the required information using the account created in Step 5 and the *host name* or *IP address* provided by Fiberlink. A sample result is given below:

Figure 7-5 Identity Services Engine



    d. You can use the **Test Connection** button to test the connection between the Cisco ISE and the cloud MaaS360. A successful message will be displayed if the connection succeeds.

7.3.7 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.
    a. From the **Cisco Administration Portal,** navigate to **Policy > Authorization.**
    b. 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.
    a. From the **Cisco Administration** Portal, navigate to **Policy > Authorization.**
    b. 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.
    a. From the **Cisco Administration** Portal, navigate to **Policy > Authorization.**
    b. Create a third rule as

    Name: *Default*

    Condition: *If no matches*

    Permissions: *DenyAccess*

8 Remote Office Network Configuration

8.1 Access Point: Cisco RV220W

This build uses the Cisco business class wireless APs. These business-class APs have additional functions beyond normal home-use APs. As an example, the APs allow enterprise connection security to enable certificate-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 by using the AP connection.

This section will describe how to configure the APs with IPs, media access control (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 10.2.1, MDM Setup
- Section 7.1, Cisco Identity Services Engine

8.1.1 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 wide area network (WAN) port of the RV220W.
2. Connect one end of a different Ethernet cable to one of the local area network (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 are 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.

8.1.2 Post-Setup Tasks

1. Use a PC to connect to a LAN port of the Cisco RV220W. If Dynamic Host Configuration Protocol (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 by using the default address https://<default IP address> 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 request that the user change the default password.
4. Verify that the IPv4 WAN setting is correct. It 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:

    a. 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:

        i. Download the firmware from https://software.cisco.com/download/release.html?mdfid=283118607&softwareid=282487380&release=1.0.6.6&relind=AVAILABLE&rellifecycle=&reltype=latest, and save it to a file.

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

        iii. Browse to the saved download file.

        iv. Press the Start Firmware Upgrade button and follow the instructions from the installer.

8.1.3 Cisco RV220 AP Setup for RADIUS Authentication

8.1.3.1 To configure LAN for IPv4

1. Navigate to the path from the Configuration Utility Portal: **Networking > LAN (Local Network) > IPv4 LAN (Local Network)** to set up the IPv4 LAN.
2. 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 connected 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)
3. Configure static IP addresses and MAC addresses for known computers:

    a. 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.

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

8.1.3.2 Cisco RV220 AP Wireless Setup for IPv4 LAN

1. Navigate to the path from the Configuration Utility Portal: **Wireless > Basic Setting.**
2. Enable one of the four default preset Service Set Identifiers (SSIDs) in the wireless Basic Setting table setting:

a. Assign an SSID name.

b. Disable SSID broadcast.

c. After an SSID has been selected, enable security mode.

d. Enable the MAC filter.

3. Edit Security Mode:

    a. Select a Wireless SSID to edit the security mode.

    b. Click Security Setting Mode.

    c. Select WPA2 Enterprise for Security and save, then select back.

4. Edit MAC filtering to block devices with MAC addresses that are not registered in the AP.

    a. Select a Wireless SSID to edit the security mode.

    b. Edit MAC Filtering and then select the Enable radio button. Click the radio button for Allow Only the Following MAC Addresses to Connect to the Wireless Network, then enter the MAC addresses in the boxes provided. Select SAVE. When saved, select Back. Follow the form to add the MAC addresses that you want the AP to control.

8.1.3.3 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.

1. Navigate to the path from the Configuration Utility Portal: **Security > RADIUS Server** to set up the AP to communicate with the authentication server. Select **Add** (press the button).

2. Fill out details in the RADIUS configuration pages, which normally include:

    - Authentication Server IP address – the IP address of the authenticating RADIUS server (e.g., for HealthITOrg1, it is 10.10.101.101)
    - Authentication Port – the RADIUS authentication server's port number used to send RADIUS traffic (e.g., 1812)
    - Enter a preshared secret that will be used between the AP and the RADIUS authenticator server.
    - Time-out – the time-out interval (in seconds) after which the RV220W re-authenticates with the RADIUS server
    - Retries – the number of retries for the RV220W to reauthenticate 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.

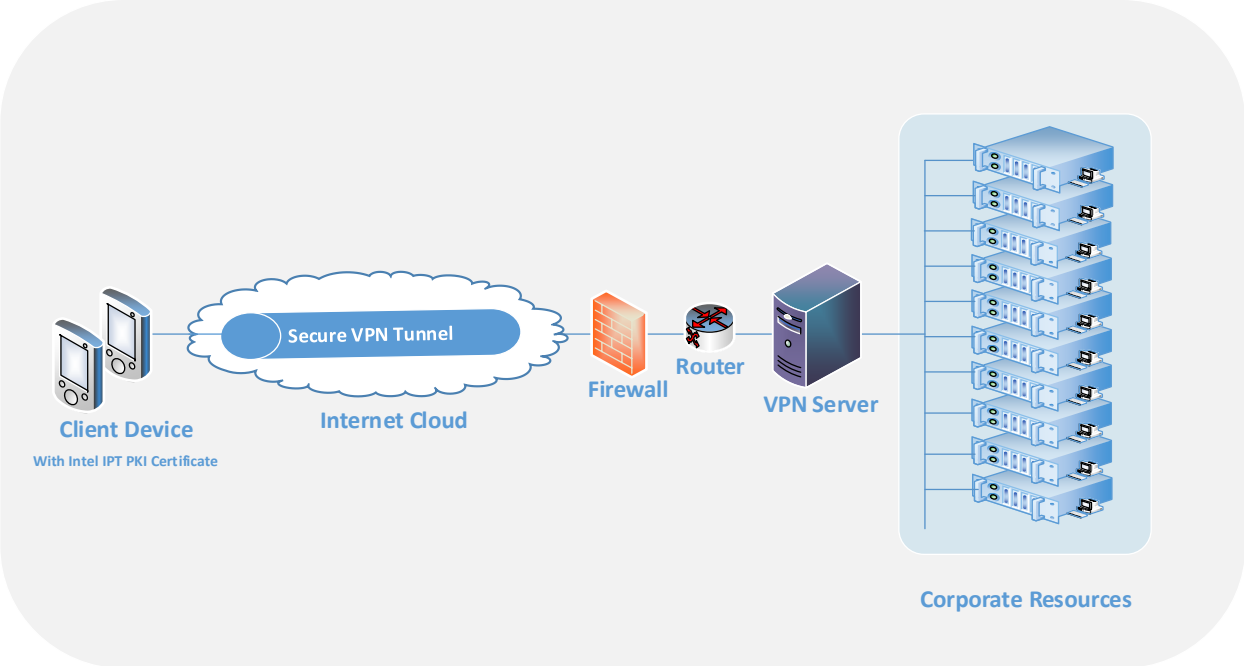
The firewall on the APs was set to the default setting for this installation. This blocked all inbound traffic except Internet Control Message Protocol traffic. All outbound traffic was allowed from internal clients. If the authentication server is installed in the cloud behind the corporate or AP firewall, you can use port

forwarding to allow the AP to communicate with the RADIUS server. In this case, use the firewall network address as the authentication server IP address.

9 Virtual Private Network Using Intel Identity Protection Technology with PKI

The Data Center is secured using a firewall as detailed in Section 3.4. One of the techniques for securing access to the Data Center when using mobile devices in unsecured networks is the VPN. This document guides you and your organization through the process of performing enhanced secure VPN access by using the Cisco ASAv and the Intel IPT to provide VPN Services. The use of Intel IPT with PKI as the VPN authentication method offers the opportunity to simplify the authentication procedure by eliminating the password authentication requirement without sacrificing the strength of the security.

Figure 9-1 Integrated VPN and IPT with PKI



Server software requirements

- Microsoft Server 2012 with .NET Framework 3.5 or 4.0
- Enterprise PKI infrastructure using Microsoft Enterprise Certificate Authority
- Intel IPT server component

Client requirements

- Fourth-generation Intel Core vPro processor-based platform with one of the following: Intel chip set Q87 or QM87 along with the Management Engine (ME) 9.X firmware
- Microsoft Windows 7 or Windows 8 OS
- Appropriate version of Intel ME component installed

Infrastructure requirements

- VH capable of housing VMs

- VM with CPU: single CPU; 2.0 GHz or faster
- 2 GB RAM
- Cisco ASAv to provide VPN services

9.1 Microsoft Enterprise CA Server Installation

Install Microsoft Enterprise CA server on the Windows 2012 server with preconfigured IP address (e.g., 192.168.200.211).

1. Install Active Directory
    a. **Start > Administrative Tools > Server Manager**
    b. Click on **Roles > Add Role** to open the Add Roles Wizard.
    c. Click **NEXT** to select the Active Directory Domain Service.
    d. Click **Add** to add the required features if listed.
    e. Follow the Add Roles Wizard to complete adding roles with the default value.
    f. The Active Directory Domain Services Configuration Wizard begins after Add Roles Wizard is finished.
    g. Leave the **Use advanced mode** unchecked and click **NEXT** to proceed with the installation.
    h. The wizard will present some information related to operating system compatibility. Click **NEXT** to continue to choose a deployment configuration.
    i. Select a new domain in a new forest and click **NEXT.**
    j. Fill in a domain name for your organization (e.g., healthit.org).
    k. Continue to follow the wizard to complete the installation by using the default value.
    l. Restart the server to complete the Active Directory and DNS server installation.
2. Install Certificate Authority Server
    a. Click **Administrative Tools > Server Manager** to add new roles.
    b. Click **Add Roles** to open the installation wizard.
    c. Check the **Active Directory Certificate Services** from the role list window; then click **NEXT** to proceed.
    d. A new window with services related to Active Directory Certificate Services is shown. The Certification Authority Web Enrollment option is needed for requesting certificates through the web. Check the **Certification Authority** and the **Certification Authority Web Enrollment** check boxes. Click **NEXT** to continue.
    e. For Setup type, choose **Enterprise** and click **NEXT.**
    f. Choose **Root CA** as the CA type.

g. For Setup Private Key, use **Create a new private key** as the option.

h. Follow the wizard and use the default values to complete the installation for the CA Server. We recommend selecting **SHA256** for hash algorithm for the Cryptography option.

3. Configure CA Web Enrollment role service

To provide a set of web pages that allow interaction with the CA role service by using web browsers, use the following instruction guide for setting up the Certificate Enrollment Web Service on the same computer where enterprise CA is installed.

a. Create a domain user account to act as the service account.

i. Sign in to the domain controller.

ii. Open Active Directory Users and Computers by using an account that has permissions to add users to the domain.

iii. In the console tree, locate the container where you want to create the user account. Right-click the container, click **New,** and then click **User.**

iv. In the New Object —User text boxes, enter appropriate names for all the fields so that it is clear that you are creating a user account, and then click **NEXT.**

v. Set a complex password for the account and confirm the password. Configure the password options to correspond to your organization's security policies regarding service accounts.

vi. Click **NEXT,** and then click **Finished.**

b. Add the service account to the local IIS_IUSERS group.

i. On the server that is hosting Certificate Enrollment Web Service, open Computer Management (**compmgmt.msc**).

ii. In the Computer Management console tree, under System Tools, expand **Local User** and **Groups,** and then click **Groups.**

iii. In the details pane, double-click **IIS_IUSRS.**

iv. On the General tab, click **Add.**

v. In the Select Users, Computers, Service Accounts, or Groups text box, type the user sign-in name for the account that you configured to be the service account.

vi. Click **Check Names,** click **OK** twice, and then close Computer Management.

c. Configure HTTPS on the Default Web Site.

i. On the server where IIS is installed, click on **Start > Administrator Tools > Internet Information Services (IIS) Manager** to open the IIS Manager.

ii. From the Server and Sites nodes, select the **Default Web Site.**

iii. On the Actions pane, click **Bindings,** and then in the **Site Bindings** click **Add.**

iv. In **Add Site Binding,** set Type to HTTPS and use the default port 443.

v. Set Secure Sockets Layer (SSL) certificate to the certificate that you issued to the server. You can confirm you have the correct certificate by clicking **View.** Click **OK.**

vi. Click **OK** to complete the site bindings and click **Close.**

9.2 Add the Intel IPT Cryptography Service Provider to Microsoft Enterprise CA Server

The Intel IPT Cryptography Service Provider (CSP) is the key to Microsoft Enterprise CA Server's ability to issue the Intel IPT PKI type of certificate to a client device with the IPT PKI client-side component installed. The following procedure describes how to install the Intel IPT component to the CA server.

1. Download the Intel IPT software

    a. An Intel Premier account is required. Log in to the Intel Premier site at https://www.intel.com/content/www/us/en/design/support/ips/training/access-and-login.html.

    b. Click downloads and select Intel PEAT SDK from the Product pull-down.

    c. Click the proper IPT component to download server-side and client-side installation files. (For example: Intel with PKI CA Components.zip for serverside and Intel IPT with PKI v2.0.0.0638.zip for client site.) The version of these components may change.

2. Add the Intel IPT CSP to the Microsoft Enterprise CA Server

    a. Locate the downloaded IPT with PKI server-side component and double-click it to start the installation.

    b. Follow the instructions and accept the license agreement to finish the installation.

    c. Check to make sure that Intel IPT with PKI Certificate Authority Components is in the list of installed programs.

3. Set Up Intel IPT Authentication Certificate Template

    a. Launch the Microsoft Management Console (**MMC**) on the Microsoft Enterprise CA Server.

    b. In the MMC window, select **File > Add/Remove Snap-in…**

    c. Select **Certificate Template** and click **Add** to add the Certificate Templates to the selected snap-ins window.

    d. Also select **Certificate Authority** to add it to the snap-ins window.

    e. Click **Finish** to complete the addition of the Certificate Authority.

    f. In the console Template Display Name list, select the **user** template and right-click it to show a drop-down list.

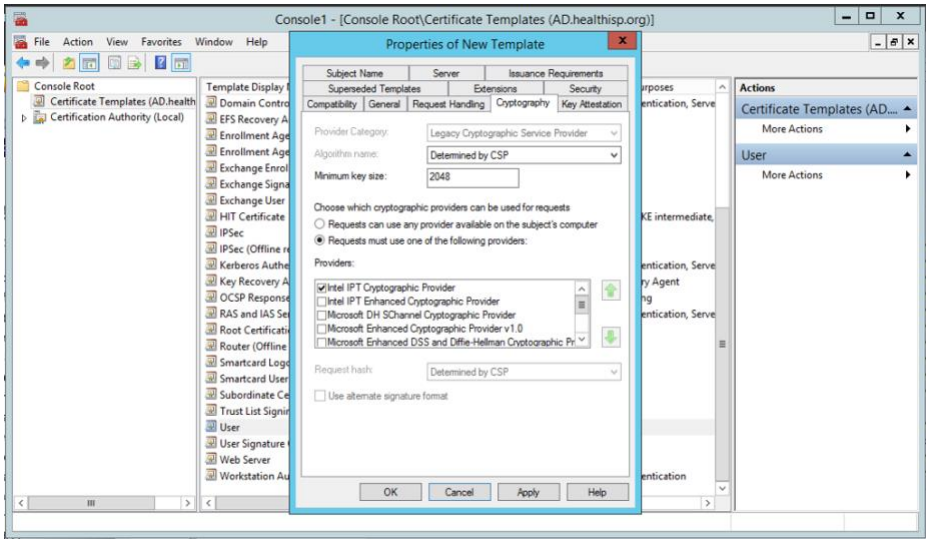
    g. Select **Duplicate Template** to open a property window for the new template.

h. Fill in the proper display name (e.g., IPT PKI User) in the General tab.

i. Uncheck the **Publish certificate in Active Directory** check box.

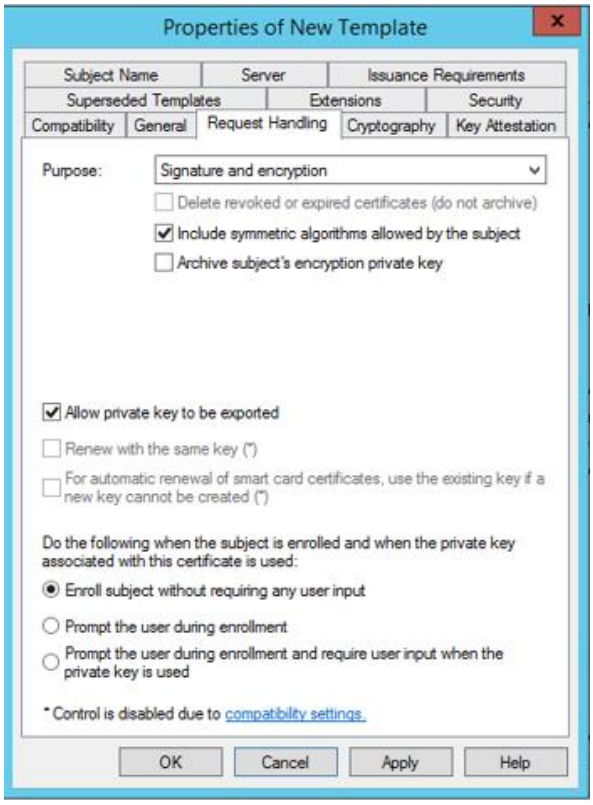
j. In the Cryptographic tab, select the **Intel IPT Cryptographic Provider** as the CSP for this certificate template as shown below.

Figure 9-2 Properties of New Template



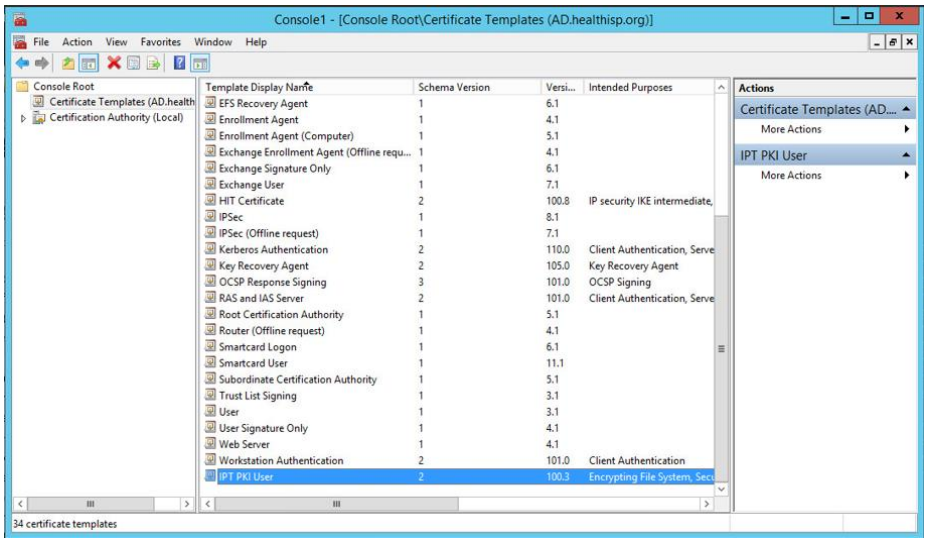
k. In Request handling, the setting is shown in the figure below.

Figure 9-3 Properties of New Template – Requesting Handling



l. Click **OK** to generate a new template as shown below.

Figure 9-4 Console 1



4. Publish the newly created template.

    a. In Administrative Tools, click **Certification Authority** to open the certificate console.

    b. In the console tree, select the **Certificate Templates** container.

    c. Right-click **Certificate Templates,** and then click **New,** then **Certificate Template to Issue.**

    d. In the Enable Certificate Templates dialogue box, select the newly created IPT certificate template, and then click **OK.**

    e. The newly selected certificate template will appear in the details pane.

9.3 Set Up Client Device for VPN by Using Intel Identity Protection Technology with PKI

In this build, the Dell Venue 10 with Intel Core i5 processor and 64-bit Windows 8 Pro OS tablet is used as the client device.

1. Add the Intel Identity Protection Technology with PKI on the client

    a. Copy the downloaded Intel IPT client component installation package to a client device.

    b. Double-click the package, and follow the instructions to install the IPT component.

    c. Check that the Intel IPT with PKI component is installed.

    d. Restart the client computer.

2. Install Intel IPT PKI certificate for client

    a. Install Root CA certificate to the client machine.

        i. From the Root CA server, click **Start,** type “MMC,” and press enter.

ii. Select **File > Add/Remove Snap-In.**

iii. Select Certificate from the available snap-ins and click **Add.**

iv. Select managed certificate for Computer account.

v. When you see Certificate (Local Computer) on the right side, click **OK.**

vi. Select **Certificates (Local Computer) > Trusted Root Certification Authorities > Certificates** to see the listed certificate.

vii. Locate the certificate issued by the Certificate Authority server generated from the previous section in the How-To guide.

viii. Right-click the certificate and select **All Tasks > Export.**

ix. Follow the Certificate Export Wizard and select **Do Not Export the Private Key** and DET encoded binary x.509 (*.CER*) for the export file format.

x. Save the export file with the extension *.cer* to a specified location.

xi. Transfer the certificate file from the server machine to the client machine by using copy, email attachment, or other methods.

xii. From the client machine, double-clicking the certificate file will open a certificate window.

xiii. Make sure this is the certificate for the root CA you want to install, and click the **Install Certificate** button.

xiv. Follow the instructions and place the certificates in the Trusted Root Certificate Authorities.

xv. Accept the warning, if there is any, and click **Finish** to complete the Root Certificate installation on the client device.

b. Request and install Intel IPT PKI user certificate for client device.

i. Create a user account for the client in the Active Directory.

ii. Connect the client device to a network that allows access to the CA certificate Web Request web page.

iii. Use Internet Explorer to request a basic certificate by connecting to https://<servername>/certsrv, where <servername> is the host name of the computer running the CA Web Enrollment role service.

iv. Accept the server certificate by clicking **Continue to this website.**

v. Log in to the web page by using the user account created for this client if requested.

vi. From the Microsoft Active Directory Certificate Services Welcome page, select the **Request a Certificate** link.

vii. Click **Advanced Certificate Request** link to submit a request.

viii. In the Advanced Certificate Request page, select the **Create and submit a certificate to this CA** link.

ix. Accept the web access confirmation. An advanced certificate request page is shown.

x. Select the template corresponding to the Intel IPT PKI template created as shown in this guide.

1) Fill in the client user information if required.

xi. Make sure the CSP is pointed to the Intel IPT Cryptographic Provider.

xii. Keep other data fields with the prefilled default values unless you would like to change them according to your needs.

xiii. Click **submit** to submit the request.

xiv. Then either:

1) If you see the Certificate Pending page, the CA administrator will have to approve the request before you can retrieve and install the certificate.

Or

2) If you see the Certificate Issued page, click Install to install this certificate. Make sure the certificate is installed successfully.

3. Install Cisco AnyConnect VPN Client for Client Device

a. Download AnyConnect VPN package from Cisco's website. The Intel IPT with PKI is expected to work with any 2.5.x or 3.0.x version.

b. Double-click the downloaded package, and follow the instructions to install AnyConnect to the client device with Intel IPT component installed.

9.4 Cisco ASAv VPN Server Configuration

1. Install ASAv into vCenter

a. Acquire the ASAv Open Virtual Appliance (OVA) file from Cisco.com.

b. Follow guidance from Cisco and your VM vendor to deploy the OVA.

2. Basic setup for Cisco ASAv VPN Post-Installation Tasks

a. Connect to the Cisco ASAv by using Adaptive Security Device Manager (ASDM) via the management interface specified during deployment.

b. Use the VPN Connection Setup Wizard. From the menu bar select **Wizards > VPN Wizards > AnyConnect VPN Wizard…,** then click the **Next** button to start the configuration.

c. Specify the Connection Profile Name, and check that the outside interface is selected in the VPN Access Interface drop-down. Click **Next** to continue to the next screen.

d. Make sure that SSL and IPsec are both selected, and the Device Certificate loaded in Section 10.1.1.3 is selected. Click **Next** to continue to the next screen.

e. For mobile access, no client images are needed. Click **Next** to continue to the next screen.

f. Specify the AAA servers that will be used to authenticate users accessing the VPN.

g. Click the **New…** button to create a new AAA Server Group. Fill out the required parameters as indicated in the form:

   i. Server IP address

   ii. RADIUS secret key

h. Click **Next** to continue to the next screen.

i. Create an Address Pool for AnyConnect clients.

j. Click the **New…** button.

k. Fill in the form with the required parameters: Specify the HealthISP's DNS server on the next screen.

l. Continue through the wizard and select **finish.**

3. VPN Server Certificate Management Configuration

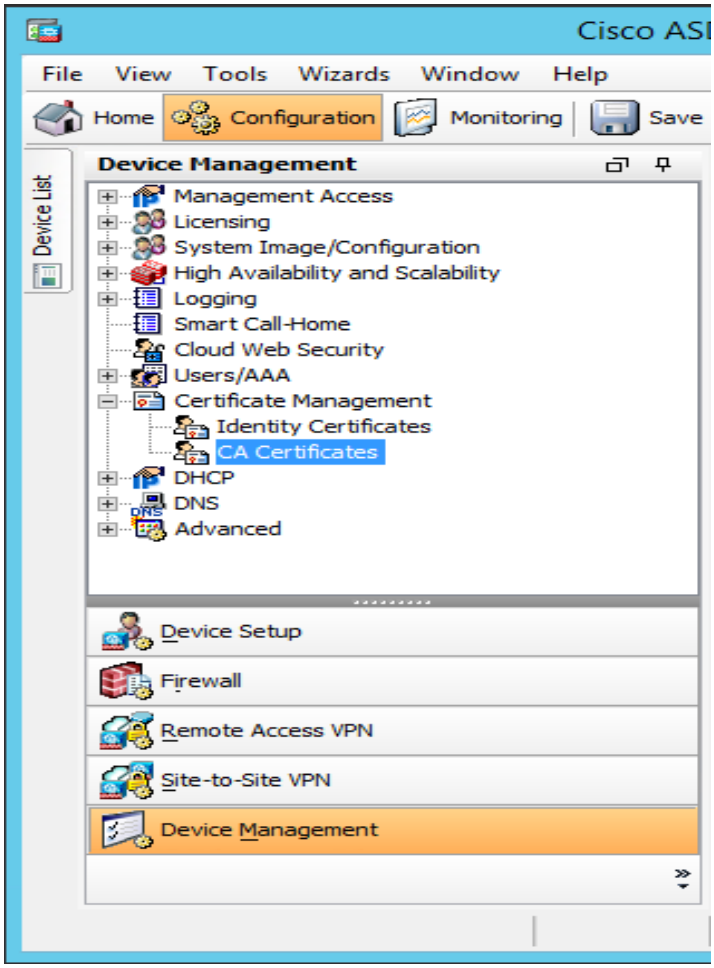
   For the VPN to function correctly, a root certificate from the CA will need to be installed.

   a. Connect to the Cisco ASAv by using ASDM via the management interface specified during installation.

   b. Click Configuration on the toolbar, and select Device Management from the lower left-hand pane.

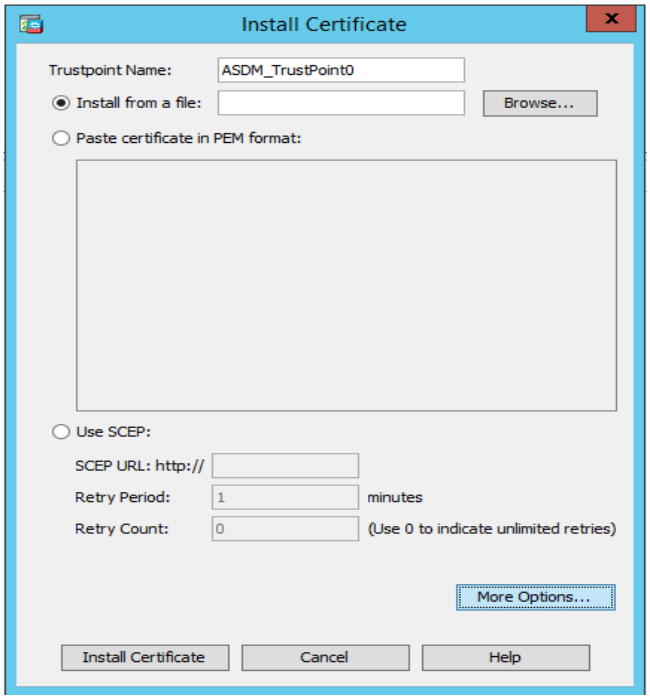
   c. In the **Device Management** pane, expand the **Certificate Management** tree element, and select the **CA Certificates** element.

Figure 9-5 Device Management



d. Click on the **Add** button to install the certificate. The Install Certificate dialogue box will appear, allowing you to install the CA's signing certificate.

Figure 9-6 Install Certificate

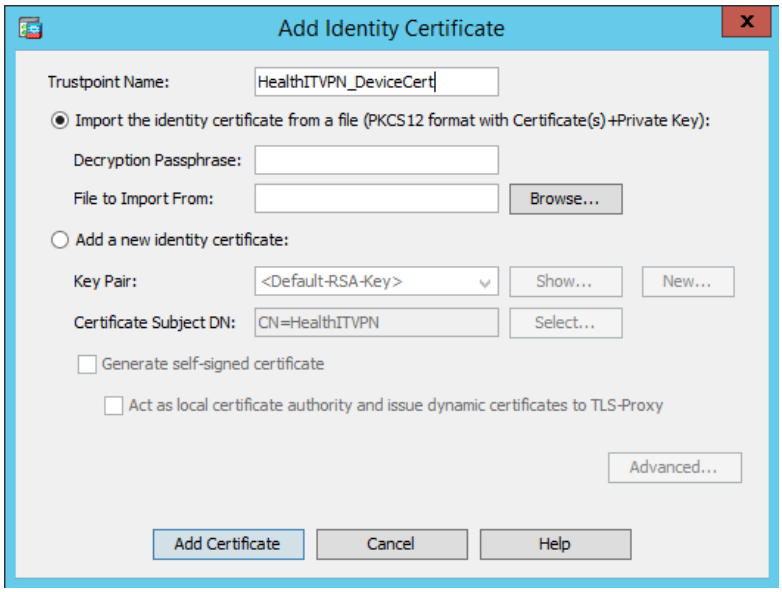


e. To secure connections with the VPN server itself, a signed certificate and private key should be installed.

   i. Generate a private/public key-pair and certificate for the VPN server. Note: If the key is larger than 2,048 bits, it will not be usable to secure the VPN connections. In this case, you should generate a second key-pair and certificate for the VPN connections, using a 2,048-bit key length.

   ii. Use the CA's signing certificate to sign the VPN server's certificate and package by using both the signed certificate and private key in a PKCS12 format file.

Figure 9-7 Add Identity Certificate



4. Configure ASAv for No-Password VPN Authentication by using Intel IPT with PKI

    a. Connect to the Cisco ASAv using ASDM via the management interface specified during installation.

    b. From the appliance's home page, select the **Configuration** tab.

    c. From the Device setup, click the **Remote Access VPN** from the left column near the bottom to access the VPN setting.

    d. Under the **Network (Client) Access** group in the left column, click the **AnyConnect Profile** to show the current VPN access configuration for the Cisco VPN AnyConnect client software.

    e. Click **Edit** to edit the profile to change the Authentication Method to **Certificate,** and click **OK.**

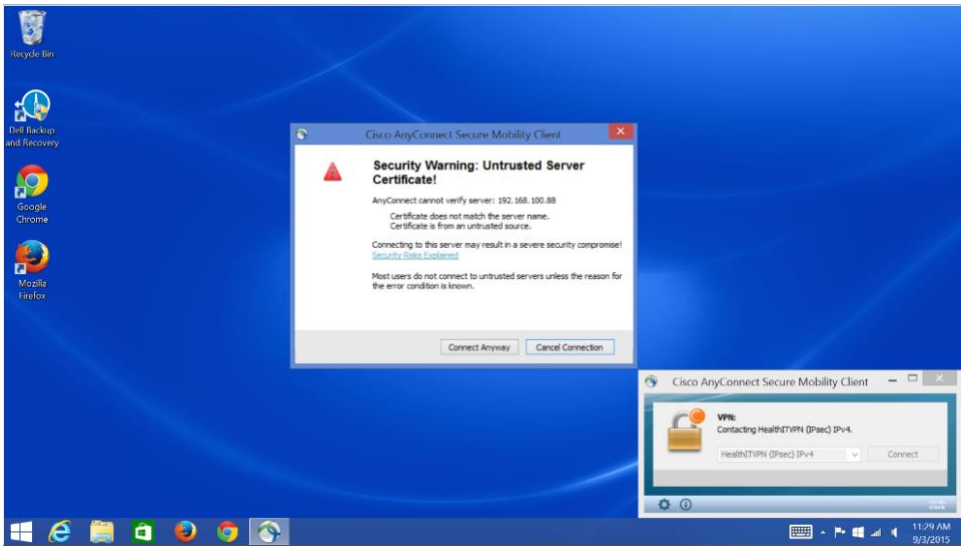
    f. Click **Apply** on the AnyConnect Connection Profiles page.

    g. Click **Save** to save the changes.

9.5 Test and Confirmation

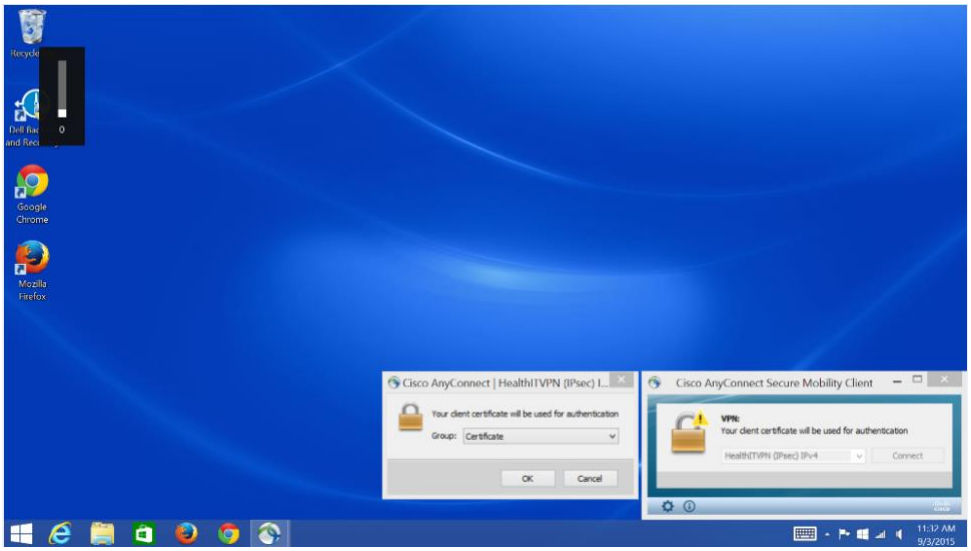
1. From the client device, launch the Cisco AnyConnect Secure VPN Client software.
2. Enter the VPN address or preconfigured VPN host name (e.g., HealthITVPN [IPsec] IPv4).
3. It may display a security warning—Untrusted Server Certificate—if a self-signed CA root certificate is used. Click Connect Anyway to accept the warning, as shown in the following screenshot.

Figure 9-8 Untrusted Server Certificate



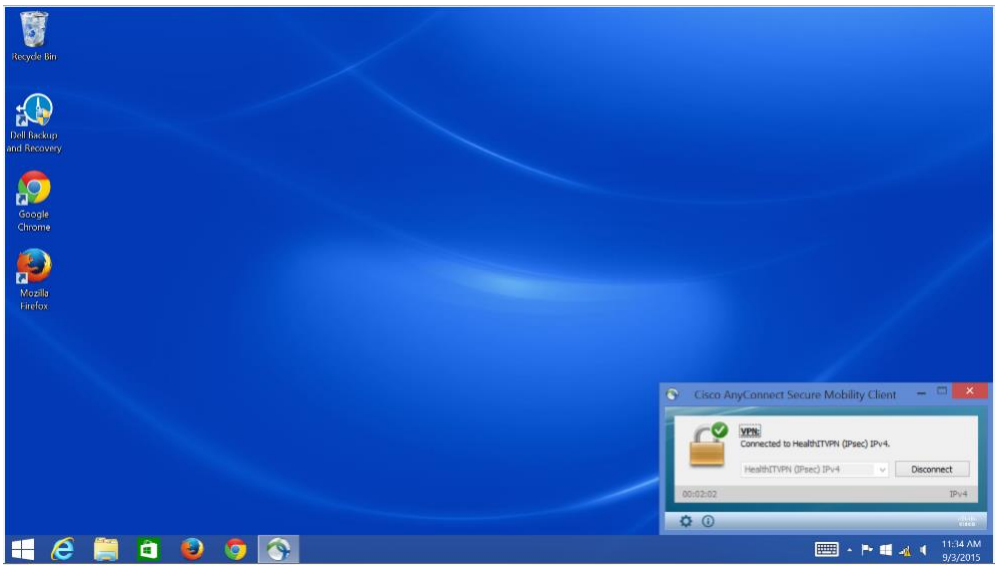
4. If there are many VPN profiles available, select the one configured for no-password Intel IPT with PKI (e.g., Certificate). Then click connect.

Figure 9-9 VPN Profile



5. The AnyConnect software should not request a password and should show connected after the successful authentication process that used the Intel IPT with PKI certificate.
6. The AnyConnect VPN window will show Connected to HealthITVPN (IPsec) IPv4 as depicted in the following screenshot.

Figure 9-10 AnyConnect VPN Window

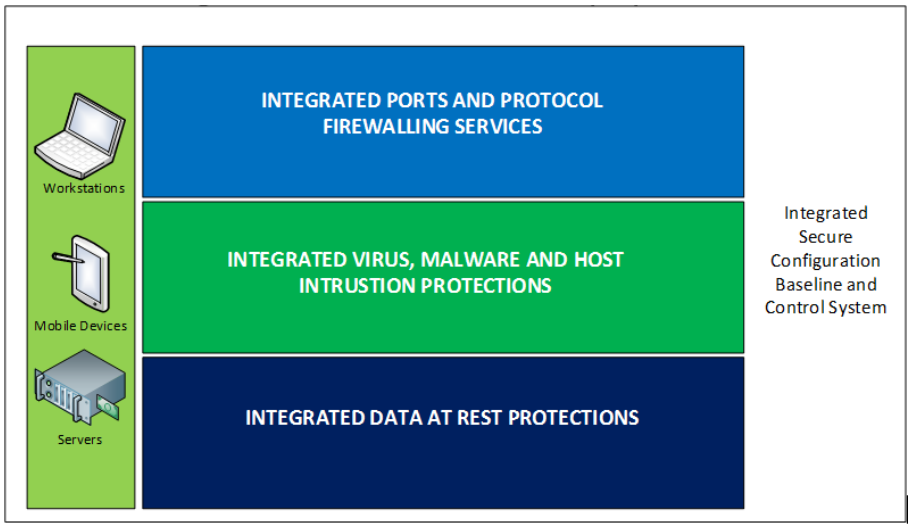


Now you can access the protected resources behind the firewall according to the access policy assigned for the client.

10 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. Authorized healthcare professionals and patients use mobile devices to add, change, read, or remove PHI.

Figure 10-1 Integrated Host-Based Security System



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

10.1 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 PHI from anywhere. These devices must be secured so that they protect both 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 connect and securely protect PHI. This section will also show you how to set up 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 device: 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 8.1, Access Point: Cisco RV220W
- Section 6.1, Fedora PKI Manager
- Section 10.2.1, MDM Setup
- Section 7.1, Cisco Identity Services Engine

10.1.1 Android Mobile Device Setup

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

10.1.1.1 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/6088915?hl=en). Follow these steps to perform the factory reset:
    a. On your mobile device, open the Settings menu.
    b. Under Personal, tap on Backup & Reset.
    c. Under Personal data, tap on Factory Data Reset.
    d. After you press 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.
    e. Start 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 in the MDM. To set the passcode, follow these steps, as described in https://support.google.com/nexus/answer/2819522?hl=en:
    a. On your mobile device, open the Settings menu.
    b. Under Personal, touch Security.
    c. Under Screen Security, navigate to Screen Lock.
    d. Select the Password option.
    e. Follow the instructions on the screen to complete the passcode setup, 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 be encrypted before enrolling it in MDM. Perform encryption using these steps, as described in https://support.google.com/nexus/answer/2844831?vid=1-635809672234145775-862949942:
    a. Plug in the device to a power cable and allow the battery to charge. Keep the power cable connected during the encryption process.
    b. On your mobile device, open the Settings menu.
    c. Under Personal, touch Security.
    d. Scroll to the Encrypt Tablet option.
    e. Press the Encrypt Tablet button.
    f. The device will reboot several times during the encryption process.
    g. 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 by using these steps:

    a. On your mobile device, open the Settings menu.

    b. Go to Wireless & Networks.

    c. If Wi-Fi is unchecked, tap the empty box.

    d. Since the SSID is not broadcast, use Add New Action to open a new Wi-Fi connection form.

    e. Type in all the details, including the SSID name; the security protocol, e.g., WPA2; and the correct password to join the Wi-Fi network.

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:

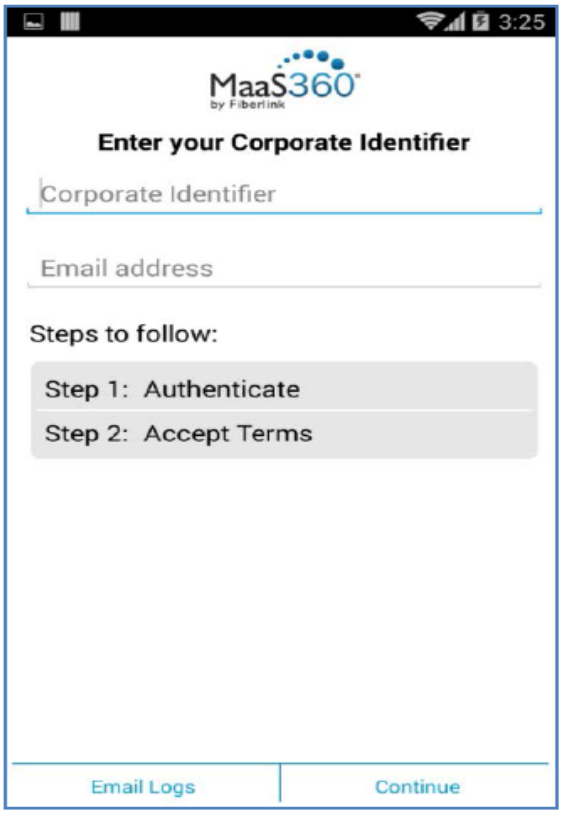
    a. Use your device to open the enrollment email as shown below:

Figure 10-2 MaaS360 Device Enrollment Request

b. Click the Device Enrollment URL to start the enrollment process, following these steps:

   i. Download and install the MaaS360 MDM for Android application to the device.

   ii. Click to open the MaaS360 MDM for Android application.



c. Fill in the Corporate Identifier and Email address as shown in the device enrollment request email.

d. Press Continue to open the agreement page, and select the check box and press to continue.

e. Press Activate to enroll the device in MDM.

f. Install all the required apps.

g. Apply policy and rule – Make sure the correct version of policy and rule is applied to the device.

h. Verify compliance – Verify that the device is compliant with all the security requirements. If not, from the Uncompliant list, click the uncompliant item to correct the problem.

10.1.1.2 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 8.1, Access Point: Cisco RV220W, for adding a device MAC address for MAC filtering service.

10.1.1.3 Install CA Trusted Certificates

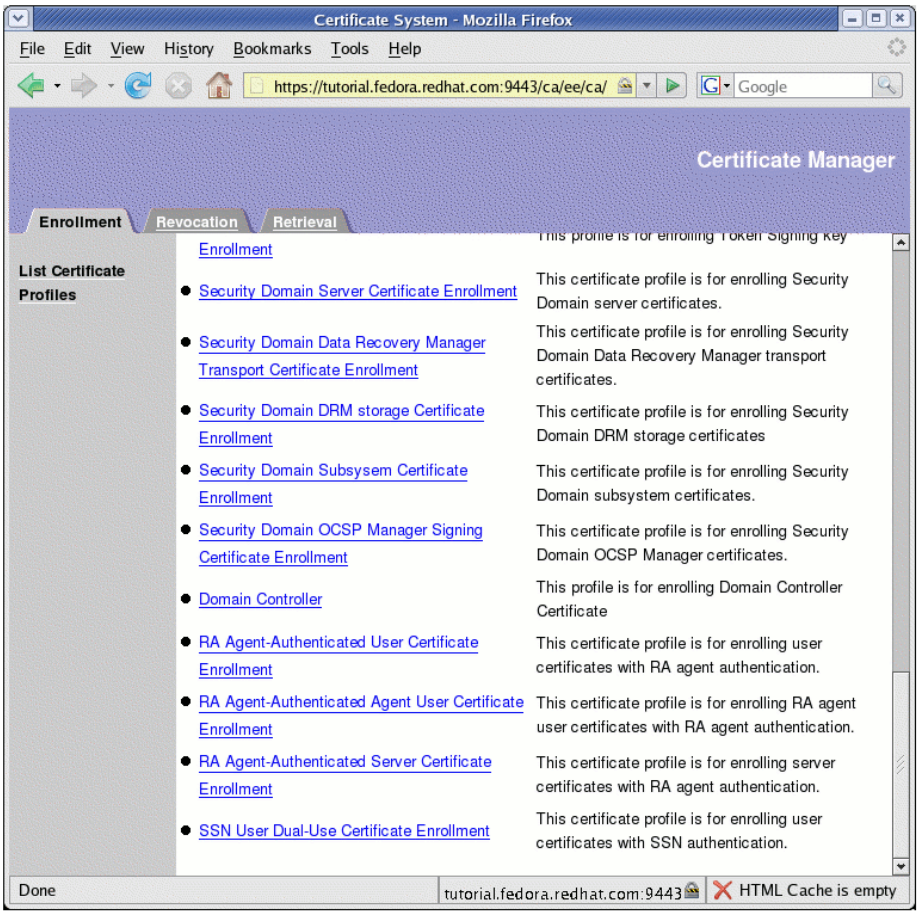
Import certificates on Android devices – Most Android devices will import certificates from an internal or external Secure Digital (SD) card. Android OS has Credential Storage under Settings/Security. Some old Android versions cannot recognize certain certificate formats, so additional steps are required to convert the certificate to the format that the device recognizes. For some newer versions of Android devices, directly importing and installing the certificate by using supported 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.

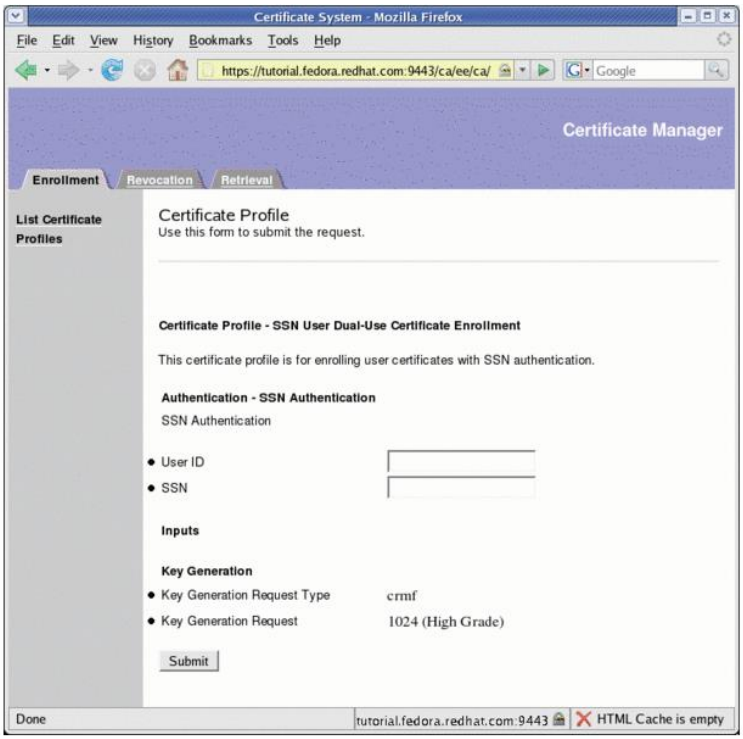
1. From your device, launch a browser.
2. Type the URL *https://<PKI hostname>:<PKI secure EE port>* into the browser to list the CA Certificate Profiles:

Figure 10-3 Certificate System – Enrollment



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

Figure 10-4 Certificate System – Certificate Profile



4. Press Submit to request the device certificate.
5. If successful, you will receive a request number. Record this number for later use.
6. The CA Authority Administrator will use the Certificate system to approve or disapprove the request. (Refer to Section 7 for details.)
7. Once approved, use the same interface as shown to select the Retrieval tab.
8. Enter the request number to retrieve the certificate. If you succeed, the certificate will be displayed on the screen with the Import button for importing the certificate to the device.
9. If you succeed, 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 to an external SD card and install the certificate from there.

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

1. Go to **Settings** on your Android device.

2. Select **Security.**

3. 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, it is possible 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 by 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 the 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. The CA admin will verify the request and approve the certificate.

11. Retrieve the approved certificate by 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.

10.1.1.4 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 set up 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 Root CA`
   - **User certificate:** `Name of your device certificate`
3. Click **Save.** You should be connected to the network by using EAP-TLS authentication.
4. In this build, we used a protected website, <https://www.examplehealthisp.com>, to verify whether or not the EAP-TLS authentication was successful.

10.1.2 Apple Mobile Devices Setup

It is assumed that the MaaS360 has been configured and that 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 and the password for the device.

10.1.2.1 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). Follow these steps to perform the factory reset:
   a. On your Apple device, open the **Settings** menu.
   b. Under **General,** tap **Reset.**
   c. Under **Reset,** tap **Erase All Content and Settings.**
   d. You will have to confirm your selection to set your device to the factory default.
   e. After you confirm your choice, the device will begin the reset process.
   f. Restart your device and follow the onscreen instructions to set up the device for a new owner.
2. Passcode protection and device encryption **–** Passcode protection is required for iOS devices to be encrypted and to enroll in the MDM. Setting a passcode in the iOS device will also enable encryption on the device. To set the passcode, follow these steps:

a. On your mobile device, open the **Settings** menu.

b. Under **Settings,** go to **Passcode Lock** and press **Turn Passcode On.**

c. Under **Screen Security,** navigate to **Screen Lock.**

d. When you turn on the passcode, you also enable encryption on your iOS device.

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 server to request and import device certificates. This Wi-Fi is protected by using the WPA2 security protocol. This Wi-Fi SSID is not broadcast. Configure the device to connect to Wi-Fi by using these steps:

    a. On your mobile device, open the **Settings** menu.

    b. Tap **Wi-Fi.**

    c. When **Wi-Fi** is on, the device will automatically search for available **Wi-Fi** networks.

    d. Join the hidden **Wi-Fi** network with no broadcast SSID: Under the **Choose a Network** section, tap **Other.**

    e. In **Name,** put the exact **Wi-Fi** network SSID you want to connect to.

    f. Tap **Security** and choose the type of network encryption used. (For the NCCoE build, WPA2 was used.)

    g. Return to the primary connection screen.

    h. Enter the Wi-Fi SSID password and tap **Join** to connect to the hidden wireless network.

MDM enrollment – We assume that your organization has already purchased a license to MaaS360 and that you have created a user account with privileges to enroll devices. We also assume that the device enrollment request has been completed and that the enrollment notification has been received via email.

1. For enrollment application

    a. Enroll your iOS device by 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.

Figure 10-5 MaaS360 Device Enrollment Request

b. Clicking the **Device Enrollment URL** will start the enrollment process.

c. The enrollment steps are to Authenticate, Accept Terms, Download & Install Profile, and Install MaaS360 for iOS App to the device.

d. Click Continue to proceed, and follow the instructions to provide necessary authentication information from the enrollment email, such as passcode and Corporation Identifier.

e. Accept terms. You must agree to the Fiberlink end user agreement to enroll your device.

f. The device will start to install the MDM Profile. Press Continue. The profile will enable the MaaS360 administrator to manage the device by using MaaS360. Click Install to install the profile, and accept any prompts for profile installation to continue with the enrollment.

g. After the profile is installed, you will be prompted to install the required MaaS360 application from the **Apple App Store.**

h. Return to the home screen and locate the **MaaS360** application. Tap the **MaaS360** icon to install the Fiberlink MDM for iOS application.

i. 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.

j. Your device is now enrolled in MaaS360.

k. Apply policy and rule – From the home screen, locate the **MaaS360** icon. Tap 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.

l. Verify compliance – Verify that the device is compliant with all the security requirements. If not, from the Uncompliant list, click the uncompliant item to correct the problem.

10.1.2.2 Register Device in AP for MAC Address Filtering

Add the 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 8.1, Access Point: Cisco RV220W for adding a device MAC address for MAC filtering service.

10.1.2.3 Install CA Trusted Certificates

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

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, it is possible 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 by 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 the process is successful, a request number will be displayed for future retrieval of the approved certificate.

10. The CA administrator will verify the request and approve the certificate.
11. Retrieve the approved certificate by 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 blob 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 iOS device by secure email.
16. Install the certificate as shown in Option 2.

10.1.2.4 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 set up 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 now be connected to the network by using EAP-TLS authentication.

10.2 MaaS360

The MDM selected for this build is based on the MaaS360 product. Maas360 is a cloud-based solution that is responsible for managing policies 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 browser installed
- Windows Phone Company Hub certificate

You will also need the following parts of this guide:

- Section 8.1, Access Point: Cisco RV220W
- Section 6.1, Fedora PKI Manager
- Section 7.1, Cisco Identity Services Engine

10.2.1 MDM Setup

10.2.1.1 Enable Mobile Device Management Service

We assume 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/). We also assume that the required Windows Phone Company Hub and the Apple Push Notification Service (APNS) certificates have been acquired. For detailed information on how to acquire these required certificates, please refer to https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/pag_source/tasks/pag_getstart_renew_apns_cert.htm for Apple MDM certificate and the document https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/winphone_enrollment_source/tasks/winphone_enrollment_mdm_enroll.htm for MaaS360 Windows Phone 8 Company Hub Certificate.

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

10.2.1.2 Enable Security Policies for Mobile Devices

1. Create a new policy for a type of device.

a. Log on to the **MaaS360** dashboard by using https://login.maas360.com.

b. Navigate to **Security > Polices,** click **Add Policy.**

c. Add a Name (e.g., Lab_Only_ISO).

d. Add Description.

e. Select a Type from the drop-down list (e.g., iOS MDM).

f. Use the **Start From** drop-down list to copy an existing policy for this new policy.

g. Click Continue to create a new policy for the type of device.

2. Edit and refine the created policies.

a. Log on to **MaaS360** dashboard by using https://login.maas360.com.

b. Navigate to **Security > Policies.**

c. From the **Policy list,** click **View** to view a selected policy.

d. Review each item in the policy to make sure it is set per your security policy and business requirements.

e. If the policy settings do not meet your security requirements, click the Edit button to enter the edit mode.

f. Change the values to your desired values.

g. Click **Save** to save the changes, or click **Save and Publish** to save and publish the new policy.

h. Enter the password and press **Continue.**

i. 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.

10.2.1.3 Enable Security Compliance Rule for Mobile Devices

1. Create a new rule set.

a. Log on to **MaaS360** dashboard by using https://login.maas360.com.

b. Navigate to **Security > Compliance Rules** and click **Add Rule Set.**

c. Add a Name (e.g., HIT-RULE).

d. Copy an existing rule set for the new rule from the Copy From drop-down list.

e. Click Continue to create a new rule.

2. Edit and refine the newly created rule.

a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

b. Navigate to **Security > Compliance Rules.**

c. Click Edit for the selected rule you want to review and edit.

d. From the **Basic Settings,** under **Select Applicable Platforms,** check the check box next to an OS's name to Enable the Real-Time Compliance for OSs.

e. In the Event Notification Recipients, fill in the emails you want to be notified in case of noncompliance.

f. Use the navigation tree to view and set other rules per your security and operational requirements.

g. Click Save to save the newly set rules.

10.2.1.4 Add Applications to Be Distributed to Mobile Devices

1. Add App to App Catalog.

    a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

    b. Navigate to **APPS > Catalog and** click **Add** to select **Apps** from different app stores.

    c. In the pop-up page, type a keyword for the application in the search box to list the available applications.

    d. Select the application you want and click Add button to add the application to the category.

2. Add Application to Bundles for Distribution.

    a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

    b. Navigate to **APPS > Bundles** and click **Add App Bundle** to open the **App Bundle** window.

    c. In the pop-up 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 applications.

    d. Click Add button to add the App Bundle.

    e. From the **App Bundle list,** click **Distribute** button to set the distribution Target.

10.2.1.5 Add Device Group to Manage Mobile Devices

1. Add Device Group.

    a. Log on to the **MaaS360** dashboard by using https://login.maas360.com/.

    b. Navigate to **USERS > Groups and** click **Add Device Group** to create a new Group.

    c. Enter search criteria and select Search.

    d. Select **Create Device Group.**

    e. Enter a group name and description.

f. From the **Device Group Details** window, specify the group Type.

g. Click **Save** to save the setting.

2. Configure Group.

   a. 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.

   b. Detailed settings for group properties can be referenced in the MDM manual: http://compliance.fiberlink.com/download/MaaS360_MDM_User_Guide.pdf.

3. Device Enrollment

   a. iOS MDM Enrollment is described in Section 10.1.2.

   b. Android MDM Enrollment is described in Section 10.1.1.

10.3 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 remote 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.

10.3.1 Symantec Endpoint Protection Suite

The Symantec Endpoint Protection server provides the following options:

- Local Host 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 manages only 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 8 GB
- Disk space Minimum 150 GB

You will also need the following parts of this guide:

- Section 2.1, 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.

11 Governance, Risk, and Compliance

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.

11.1 RSA Archer GRC

11.1.1 System Requirements

This build requires the user to install a single-host RSA Archer GRC platform node on a VMware VM 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 instructions for other options.

11.1.2 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 ran under a single server. Below are the pre-installation tasks that we performed prior to the RSA Archer installation:

- Operating System: Windows Server 2012R2 Enterprise
  - Refer to Section 2.1, 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 that database owners have sufficient privileges and correct user mappings.

Table 11-1 Configuration Settings

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

Setting	Value
Locale set	English (United States)
Database server time zone	EST
Platform language	English
Create both the instance and configuration databases within a single SQL Server instance. 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 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.

First install IIS and then install the *.NET* Framework.

Table 11-2 summarizes the required IIS components and *.NET* Framework features followed by the screenshots.

Table 11-2 IIS Components and .NET Features

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

Required Option	Value
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

Figure 11-1 Web Server (IIS) Components Selection Screenshot

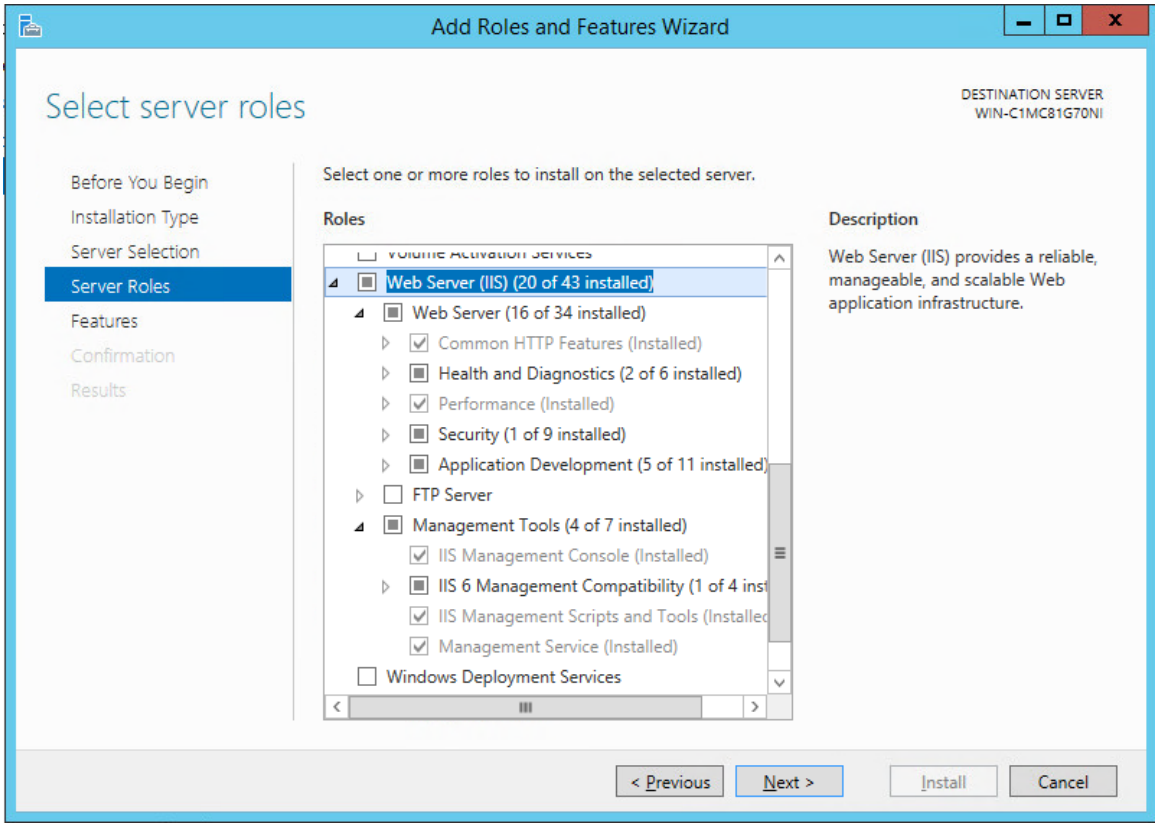
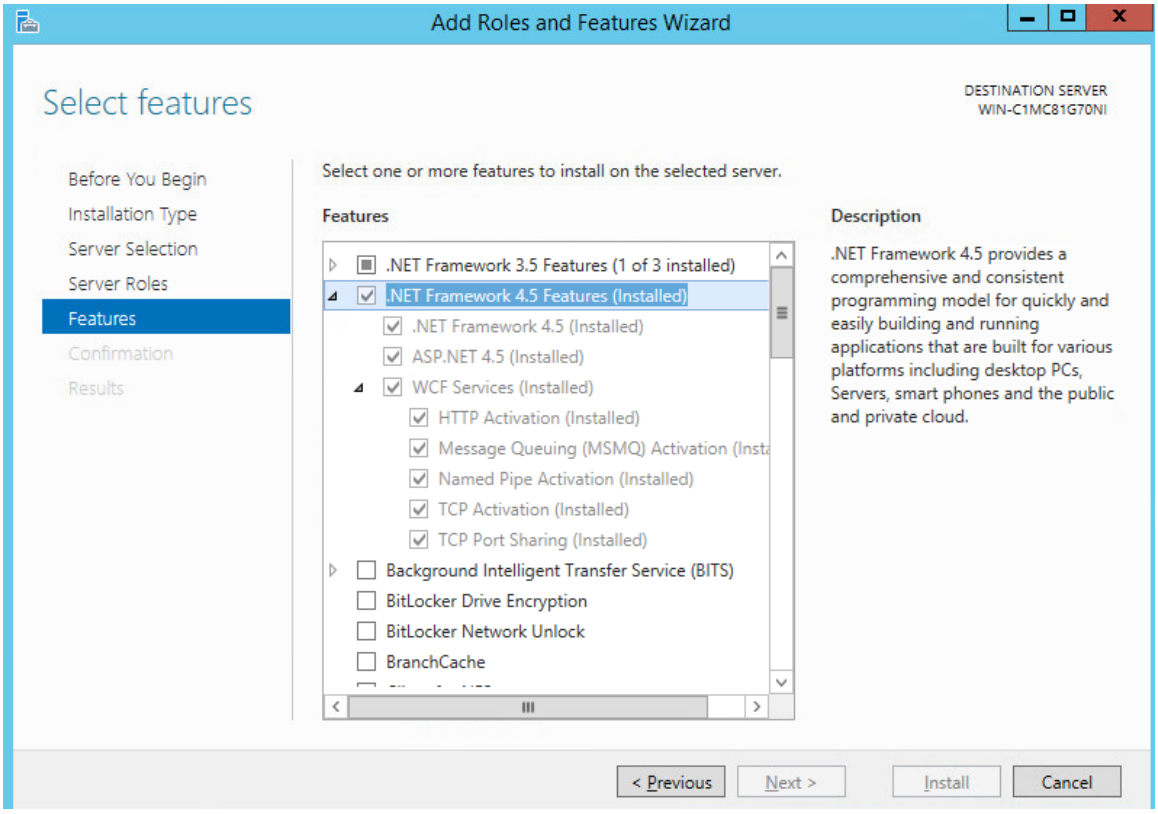


Figure 11-2 .NET Framework 4.5 Features Selection



Microsoft Office 2013 Filter Pack

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.

11.1.3 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.
    a. Open installation folder, right-click on *ArcherInstall.exe.*
    b. Select **Run as Administrator.**
    c. Click **OK** to Run the Installer.

d. Follow the prompts from the installer for each step, set the value, and click Next.

e. Select all components **(Web Application, Services, Instance Database)** for installation, then click **Next**.

f. Specify the X.509 Certification by selecting it from the checklist (create new cert or use existing cert). We created a new cert.

g. 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)

h. 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.

i. Set the Configuration of the Service Credentials.

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

j. 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*.

k. Set the Log File Path to *C:\ArcherFiles\Logging.*

l. Perform the installation by clicking **Install,** wait for the installer to complete installing all components, then click **Finish.** The **RSA Archer Control Panel** opens.

11.1.4 Post-Installation

11.1.4.1 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.
    a. Start the RSA Archer Queuing Service by doing the following steps:
        i. Go to **Start.**
        ii. Open **Server Manager.**
        iii. Locate **RSA Archer Queuing** in the list under the SERVICES section.
        iv. Right-click **RSA Archer Queuing** and click **Start.**
    b. Add a new instance by doing the following steps:
        i. Open the **RSA Archer Control** Panel.
        ii. In **Instance Management,** double-click **Add New Instance.**
        iii. Enter EHR1 as the Instance Name, then click **Go.**
        iv. Complete the properties as needed.
    c. Configure the Database Connection Properties by doing the following steps:
        i. Open the **RSA Archer Control** Panel.
        ii. In the **Database** tab, go to the **Connection Properties** section.
        iii. In **Instance Management,** double-click the EHR1 instance.
        iv. In the **Database** tab, set up the following:
            1) SQL Server: (local)
            2) Login name: *xxxxxx*
            3) Password: *xxxxxx*
            4) Database: *grc-config*
4. Click on the **Test Connection** link to make sure the **Success** message appears.
5. Configure the General Properties by doing the following steps:
    a. Open **RSA Archer Control** Panel.
    b. Go to **Instance Management.**
    c. Under All Instances, click on EHR1.

d. In the **General** tab, set up the following:

i. File Repository section – Path *C:\ArcherFiles\Indexes*

ii. Search Index section – Content Indexing: Check on Index design language only; Path: *C:\ArcherFiles\Indexes\EHR1*

6. Configure the Web Properties by doing the following steps:

a. Open the **RSA Archer Control** Panel.

b. Go to **Instance Management.**

c. Under **All Instances,** click on EHR1.

d. In the **Web** tab, set up the following:

i. Base URL: http://localhost/RSAArcher/

ii. Authentication URL: *default.aspx*

7. Change SysAdmin and Service Account passwords by doing the following steps:

a. Open the **RSA Archer Control** Panel.

b. Go to **Instance Management.**

c. Under **All Instances,** click on EHR1.

d. Select the **Accounts** tab.

e. Change the password on the page by using a strong password.

f. Complete the Default GRC Platform Instance Creation by clicking **Save** on the toolbar.

8. Register the Instance by doing the following steps:

a. Open the **RSA Archer Control** Panel.

b. Go to **Instance Management.**

c. Under **All Instances,** right-click on EHR1.

d. Select Update Licensing, enter the following information, then click on Active:

i. Serial Number (obtained from RSA)

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

iii. Activation Method (select Automated)

9. Activate the Archer Instance by doing the following steps:

a. Start the **RSA Archer Services.**

b. On **Server Manager,** go to **Local Services or All Services.**

c. Locate the following services, right-click on each service, and click **Start.**

   i. RSA Archer Configuration

   ii. RSA Archer Job Engine

   iii. RSA Archer LDAP Synchronization

d. Restart the RSA Archer Queuing Service.

   i. Open **Server Manager.**

   ii. Go to **Local Services** or All Services.

   iii. Locate the RSA Archer Queuing.

   iv. Right-click on **RSA Archer Queuing** and click **Restart.**

e. Rebuild the Archer Search Index.

   i. Open **RSA Archer Control** Panel.

   ii. Go to **Instance Management.**

   iii. Under **All Instances,** right-click on EHR1, then click on **Rebuild Search Index.**

10. Configure and activate the Web Role (IIS).

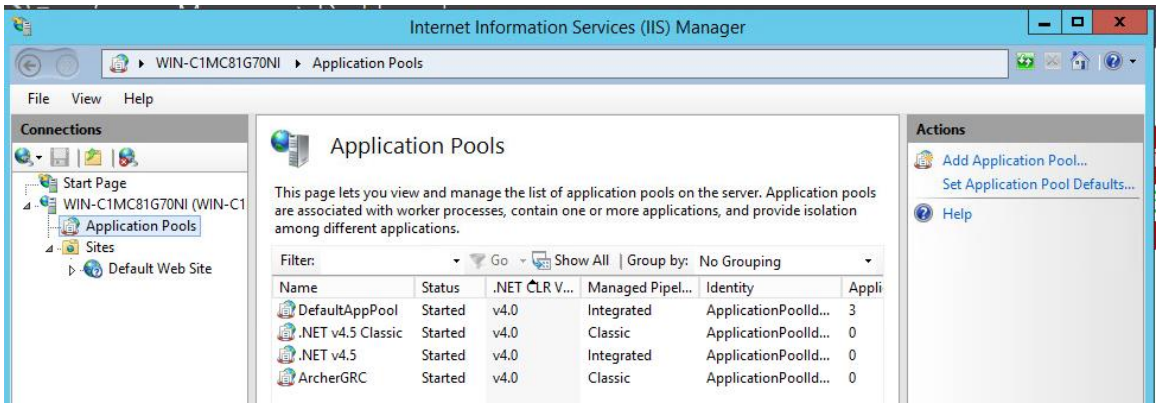
    a. Set up Application Pools as shown in the screenshot.

       i. Open **Server Manager.**

       ii. Navigate to **Tools > IIS Manager > Application Pools** (in the left side bar).

       iii. Right-click to add applications (.NET, Archer GRC, etc.), example screenshot below.

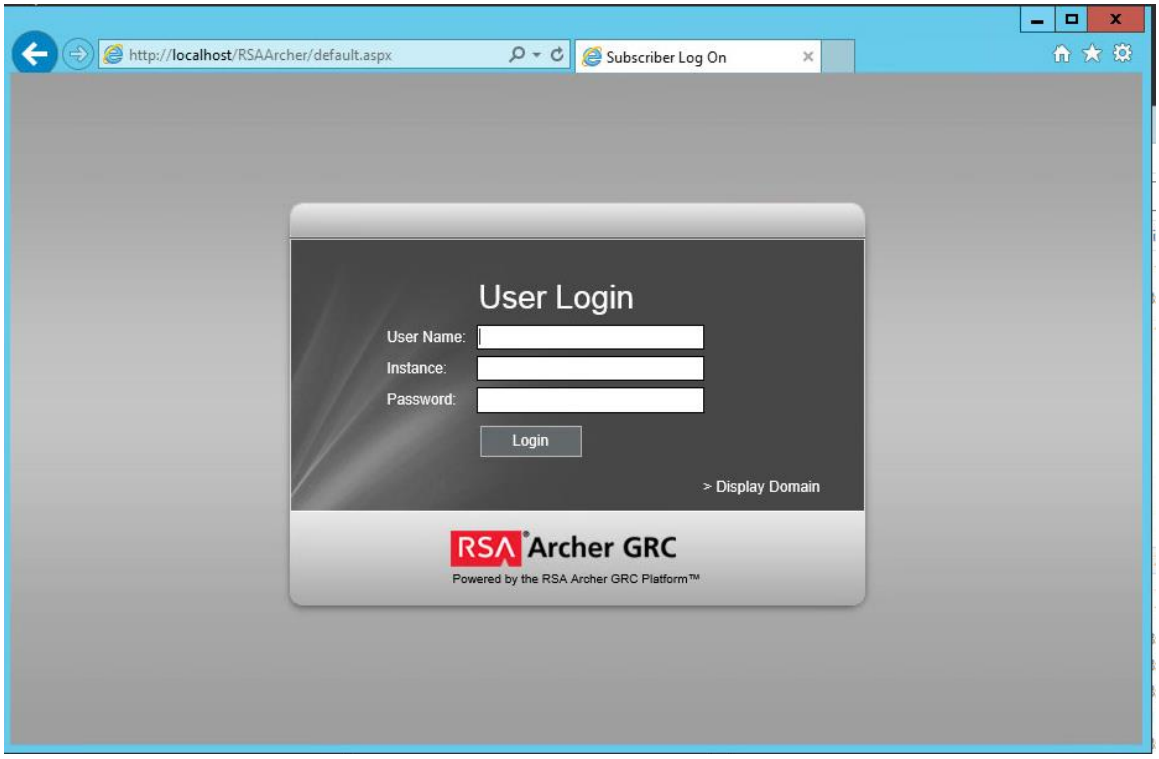
Figure 11-3 Internet Information Services (IIS) Manager



b. Restart IIS.

11. Verify that RSA Archer GRC is accessible by opening a browser and inserting the Base and Authentication URL from the web tab of the RSA Archer Control Panel. The RSA Archer GRC Login screen appears as shown below.

Figure 11-4 RSA Archer GRC User Login



12. Log in to EHR1 Instance.

Figure 11-5 Welcome to the Archer Policy Center

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

11.1.5 Content Setup for Establishing GRC Process

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 11-3 Content Sources for GRC Tool

Source	Description
NIST Framework for Improving Critical Infrastructure Cybersecurity	• 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, and control standards and selecting the relevant control procedures
NIST SP 800-66 rev1	• Used 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)
Department of Health and Human Services (HHS) — Office of the National Coordinator for Health Information Technology (ONC) Security Risk Assessment (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

Figure 11-6 High-Level Structure and Process Steps for NCCoE HIT Mobile Device Use Case GRC Program

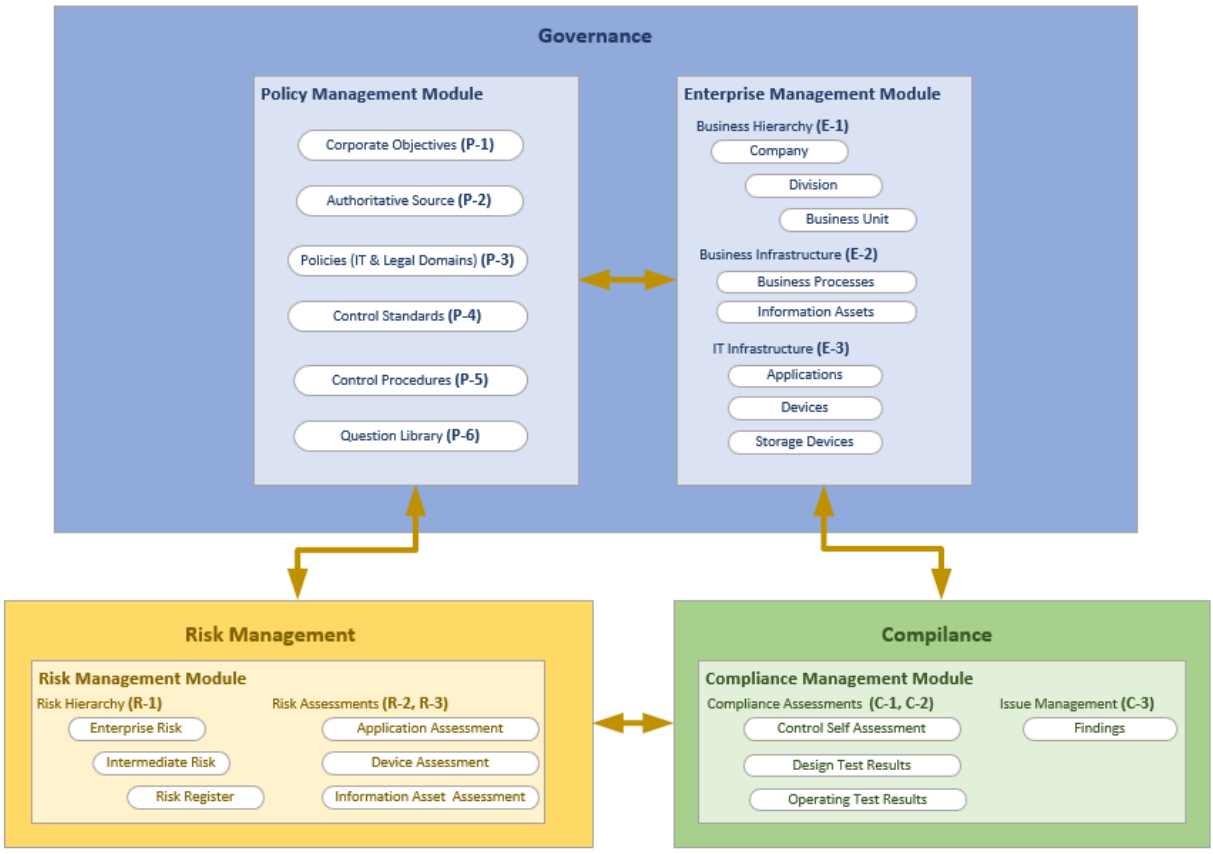


Table 11-4 summarizes the tasks that are conducted for this use case via GRG program. For most of the tasks, the sequential order is not necessary. The task step is used as the content correlator within this guide. The techniques and relevant content sources are outlined as references. The column "RM Tool Required?" indicates that the organization, 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 11-4 High-Level Process Steps for GRC Program

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, and reporting and compliance. The objectives can be related to the defined policies and risks. Through those associations, Archer supports an organization to track policies and monitor related risks and key performance indicators. For demonstration purposes, this use case selected 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 user interface (UI) to create/update the Corporate Objectives and associate the objective to necessary existing policies, organizations, and risks. *To create a Corporate Objective:* **Policy Management (tab) > Corporate Objectives (side menu) > New Record >> Complete desired fields > Save** *To update a Corporate Objective:* **Policy Management (tab) > Corporate Objectives (side menu) > Record >> Select the desired record >> Edit >> Update desired fields > Save**	No
P-2	Select/Define Authoritative Source	To scope down the set of relevant controls, NCCoE takes advantage of Archer's content library for	*Archer Module:* Policy Management *Archer App:* Authoritative Sources	Yes

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
P-3	Select/Define related policies	HIPAA Security as the authoritative source, but remaps it to the set of control standards that are specifically created for HIPAA Security (P-4 and P-5). **Primary Source:** HIPAA/Archer content library, NCCoE	*Actions:* Created new report for Authoritative Sources for the target subset of the authoritative source *To create the new report:* **Policy Management (tab) > Authoritative Source (side menu) > Reports > New > Fields to Display > Select desired reporting fields > Enter filters (for HIPAA security technical safeguards) > Enter sort option > Enter display option > Save report** *To access the new report:* **Policy Management (tab) > Authoritative Source (side menu) > Records (side menu) > Reports (icon) > HIPAA Security Technical Safeguard Compliance (Select Report pop-up)**	
P-4	Create relevant Control Standards	NIST SP 800-66 is used as guidance for NCCoE to create a set of Control Standards that are directly mapped to the HIPAA	*Archer Module:* Policy Management *Archer App:* Control Standards	No

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
P-5	Select SP 800-53 control procedures	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 800-66, and NIST SP 800-53r4	*Actions:* Use the Archer UI to create/update the control standards that correspond 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:* **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	

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
P-6	Create questionnaires by importing questions	The SRA Tool from the HHS 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 to present the organizations that are 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 it to necessary existing policies, objectives, risks, etc. *To create new company/division/business unit:* **Enterprise Management (tab) > Business Hierarchy (side menu) > Company/Division/Business Unit > New Record**	No

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
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, etc. *To create new business processes/information assets:* **Enterprise Management (tab) > Business Infrastructure (side menu) > Business Processes/Information Assets > New Record**	No

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
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, 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, select format option, perform data mapping, and import data	No

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
R-1	Identify and rate risks and define Risk Hierarchy	Three-level Risk Hierarchy enables an organization to roll up its 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 Risk Assessment Methodology section in Volume E of this guide for details on the risk identification procedures. **Primary Source:** Identified risks from the risk assessment sections	*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, etc. *To create a new risk hierarchy/risk register:* **Risk Management (tab) > Risk Hierarchy/Risk Register (side menu) > New Record**	No

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
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 from 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) > Application Builder > 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

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
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 application that has risk management tab to be associated or reports that are on the dashboard *Actions:* various – see sample screenshots in Figure 11-16	Yes
C-1	Compliance Assessment	Various assessments can be used for checking the compliance with HIPAA, control standards, and control procedures. **Primary Source:** HIPAA, HHS ONC SRA tool, Archer Content Library	*Archer Module:* Compliance Management *Archer App:* Compliance Assessments *Actions:* Use the Archer UI to conduct assessments *To conduct compliance assessment:* **Compliance Management (tab) > Compliance Assessments (side menu) > Select type of assessment (side submenu) > select record > conduct assessment > Save**	Yes
C-2	Compliance Assessment result/impact analysis and decision-making	Create new customized reports by using existing reports and charts to view the assessment results, and conduct 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 are on the dashboard *Actions:* various – see sample screenshots in section 11.1.5.1	Yes

Task Step #	Task	Description & Primary Source	Techniques / Steps in Using Archer	RM Tool Required?
C-3	Issue Management	The Issue Management module is embedded in other modules, such as Risk Management and Compliance Management. 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 in section 11.1.5.1 *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 for other actions)	Yes
Final	Integrate with external data sources and customize reports and dashboards	Utilize the Data Feed feature to set up the dashboards		Yes

11.1.5.1 Sample Screenshots of Content Setup for Establishing GRC Process

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

Figure 11-7 P-1: Define Corporate Objectives

Objective	Category ▲	Description	Key Performance Indicators	Status
Ensure the confidentiality, integrity, and availability of EPHI	Strategic	"Ensure the confidentiality, 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

Figure 11-8 P-2: and P-3: Select/Define Authoritative Source (HIPAA Security) and Related Policies

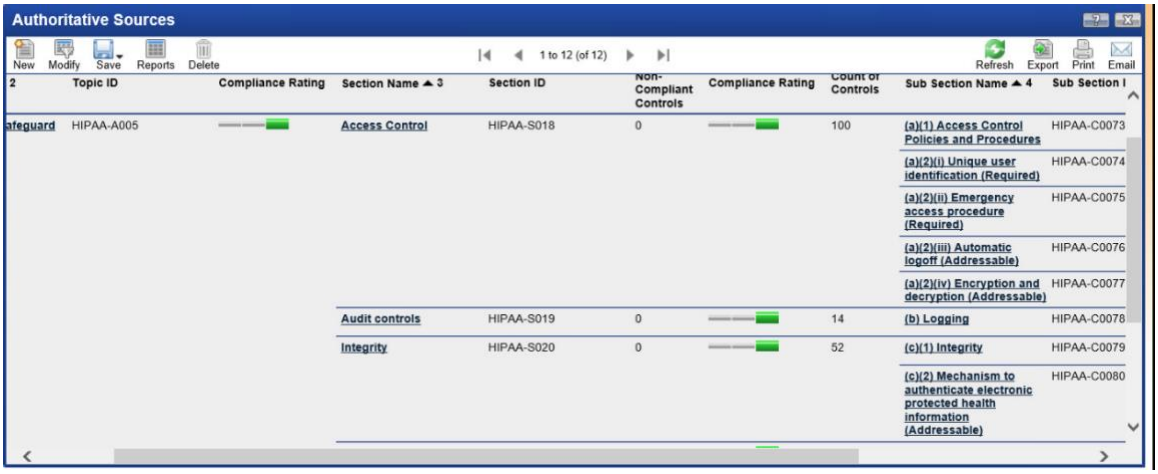
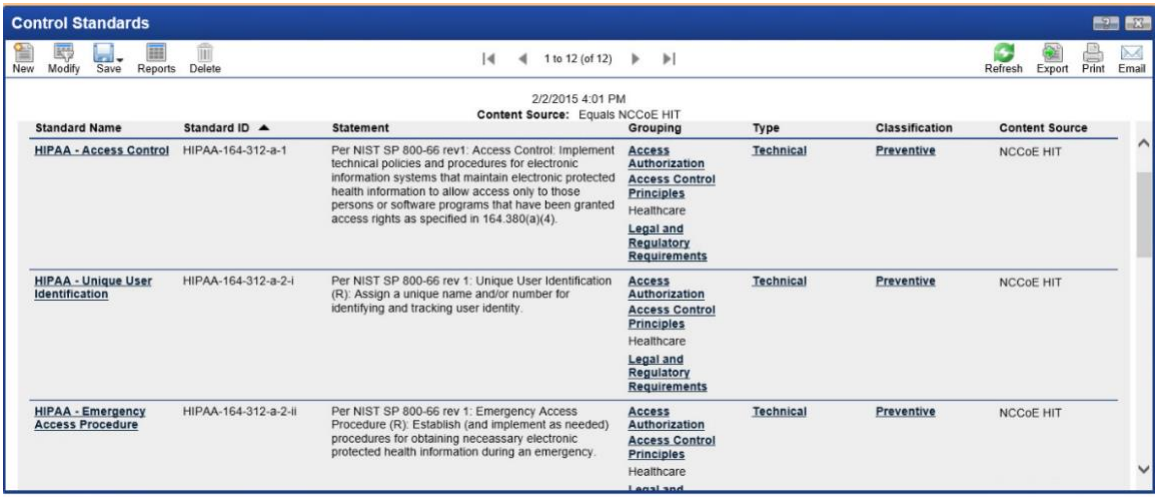


Figure 11-9 P-4: and P-5: Create Relevant Control Standards and Select SP 800-53 Control Procedures (Focus on HIPAA Security, Technical Safeguards)



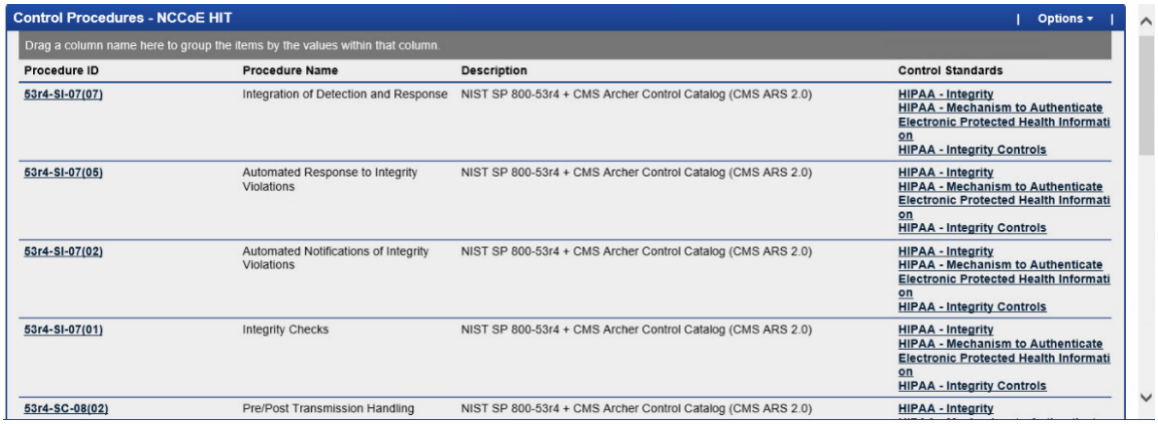


Figure 11-10 P-6: Create Questionnaires by Importing Questions from HHS ONC SRA Tool

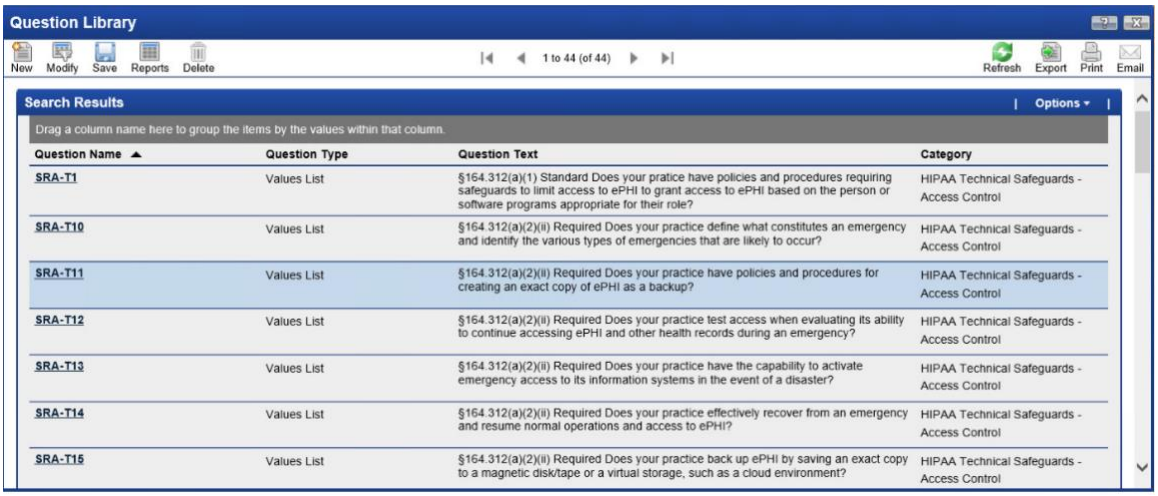
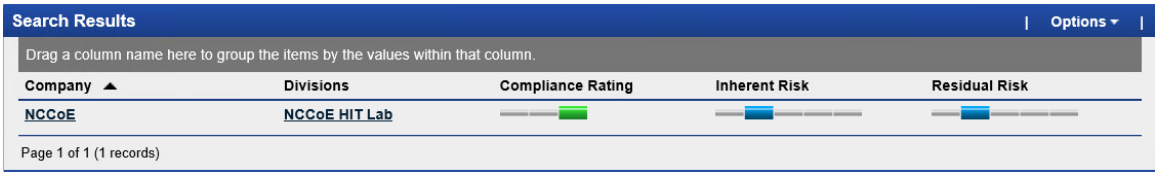
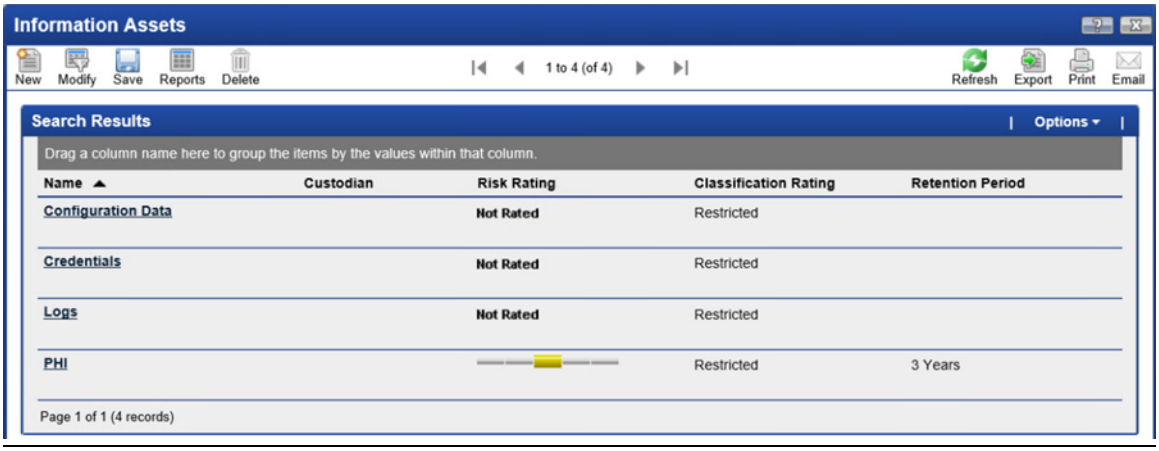


Figure 11-11 E-1: Define/Import Business Hierarchy





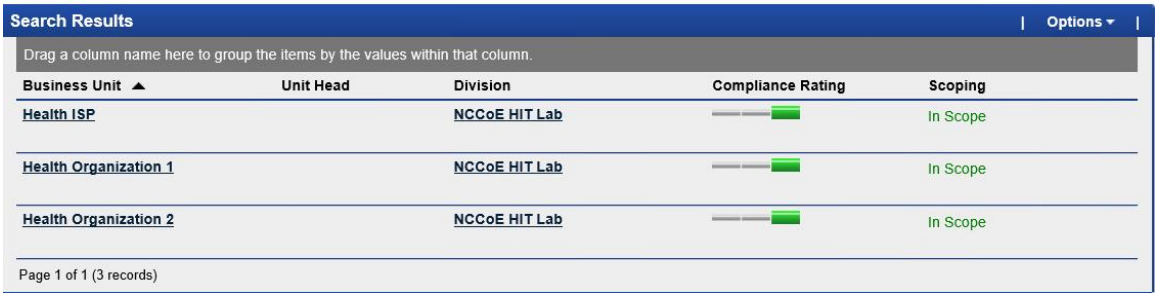


Figure 11-12 E-2: Define/Import Business Infrastructure

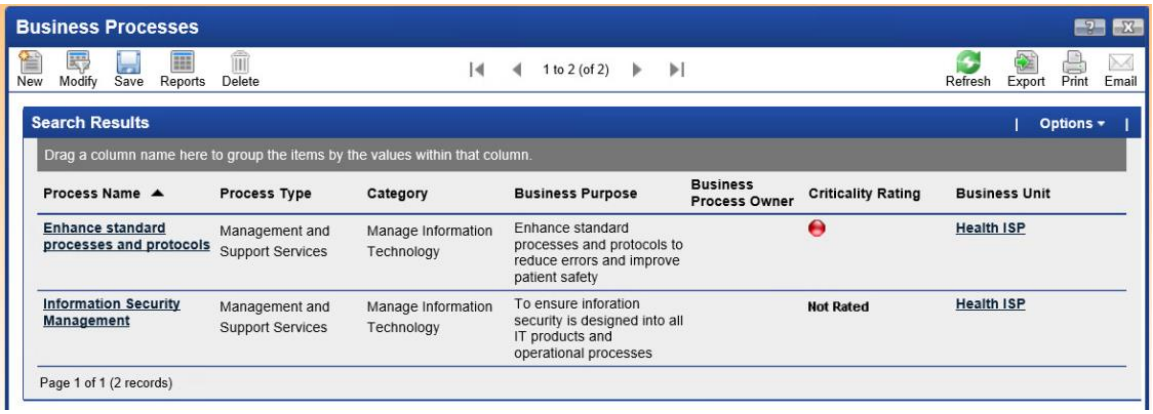
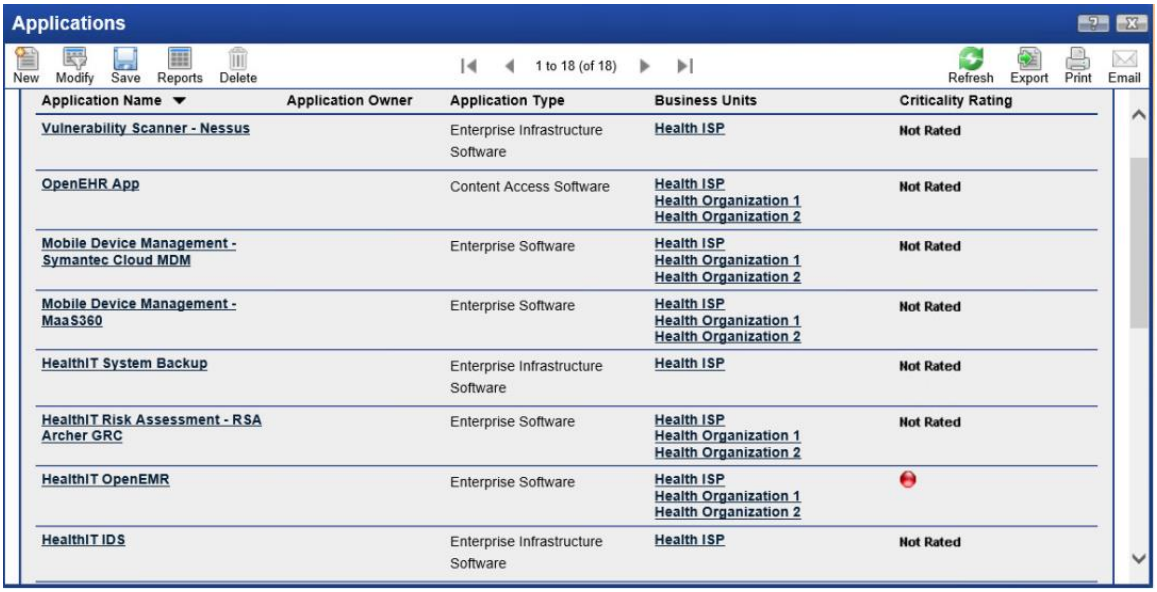


Figure 11-13 E-3: Define/Import IT Infrastructure



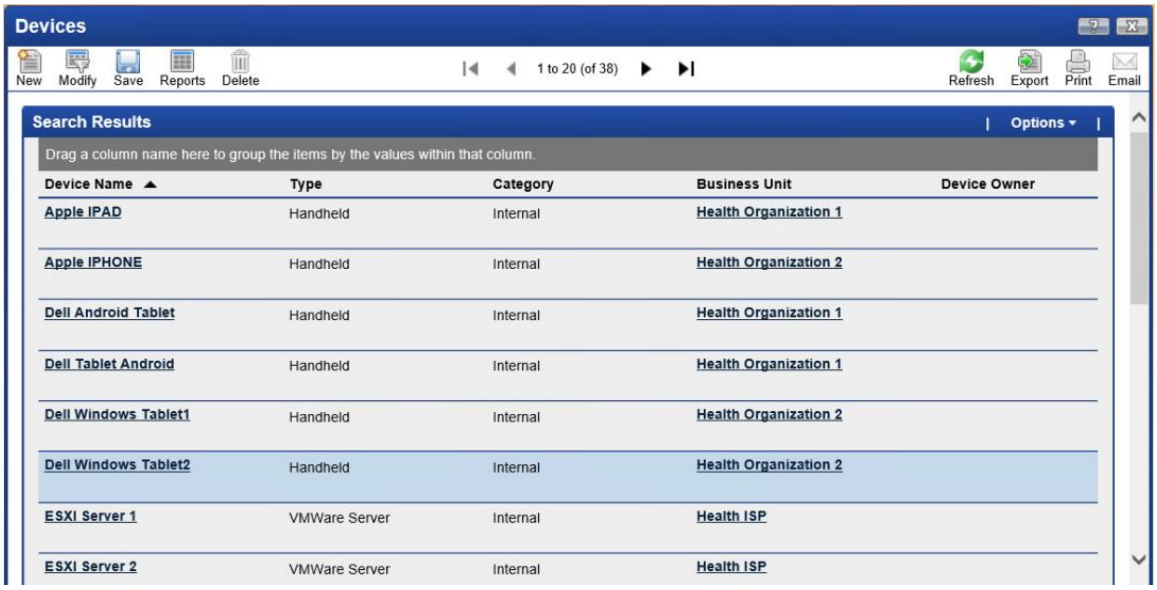


Figure 11-14 R-1: Identity and Rating Risks and Define Risk Hierarchy

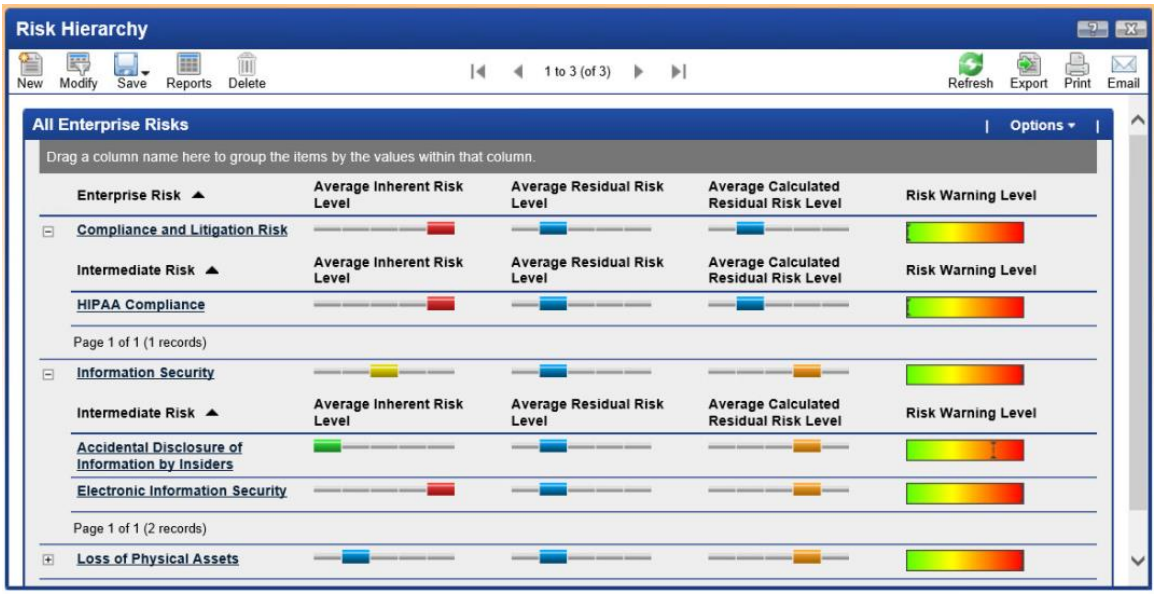


Figure 11-15 Risk Register

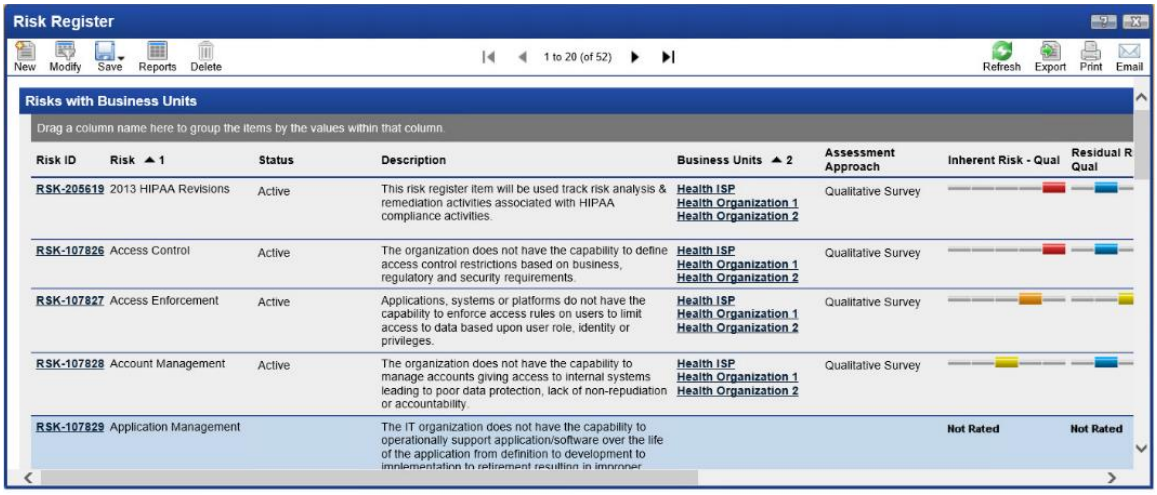


Figure 11-16 R-2: and R-3: Perform Risk Assessment, Result/Impact Analysis, and Decision-Making for Applications, Devices, and Information Asset

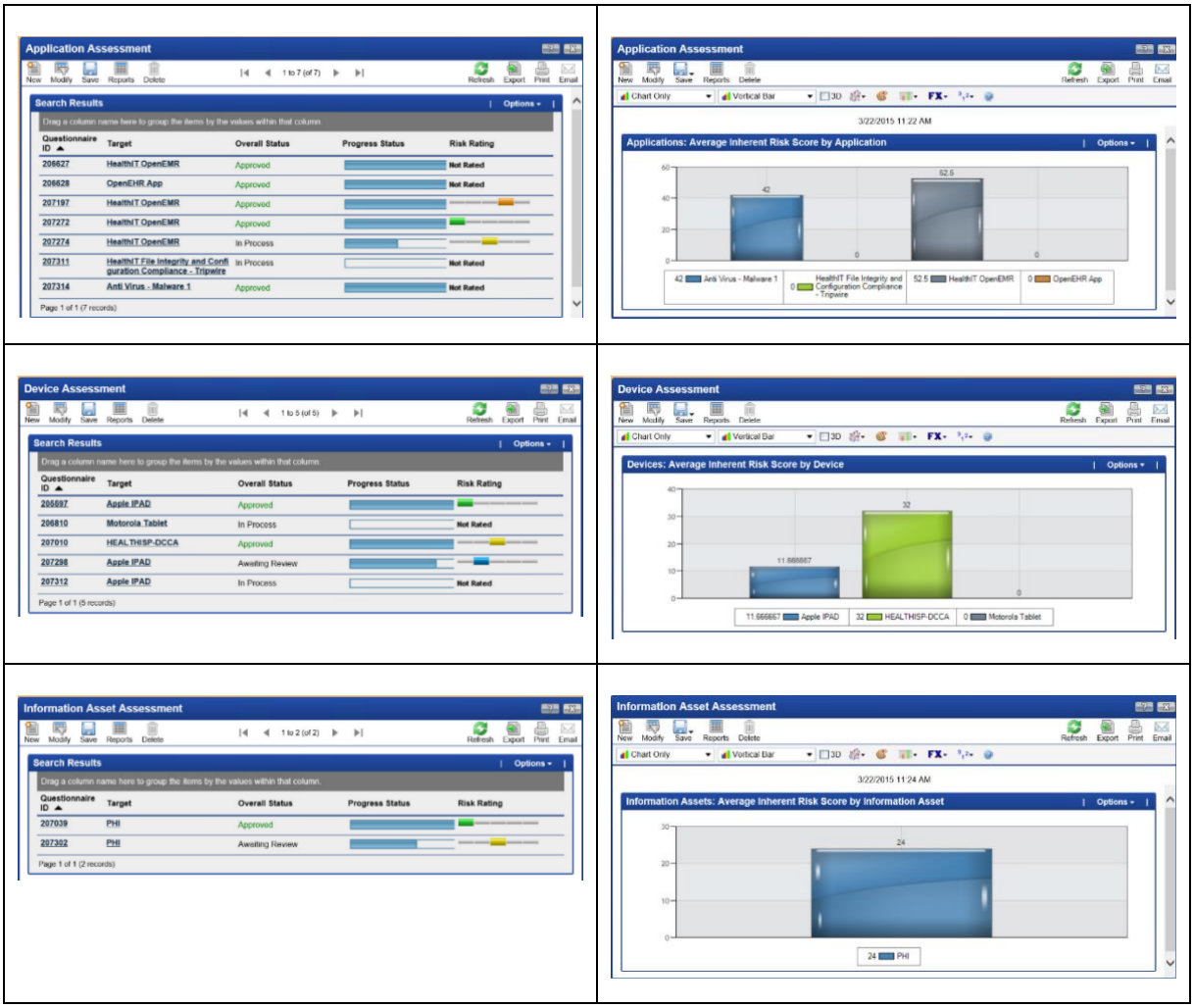


Figure 11-17 C-1: and C-2: Perform Compliance Assessment, Result/Impact Analysis, and Decision-Making

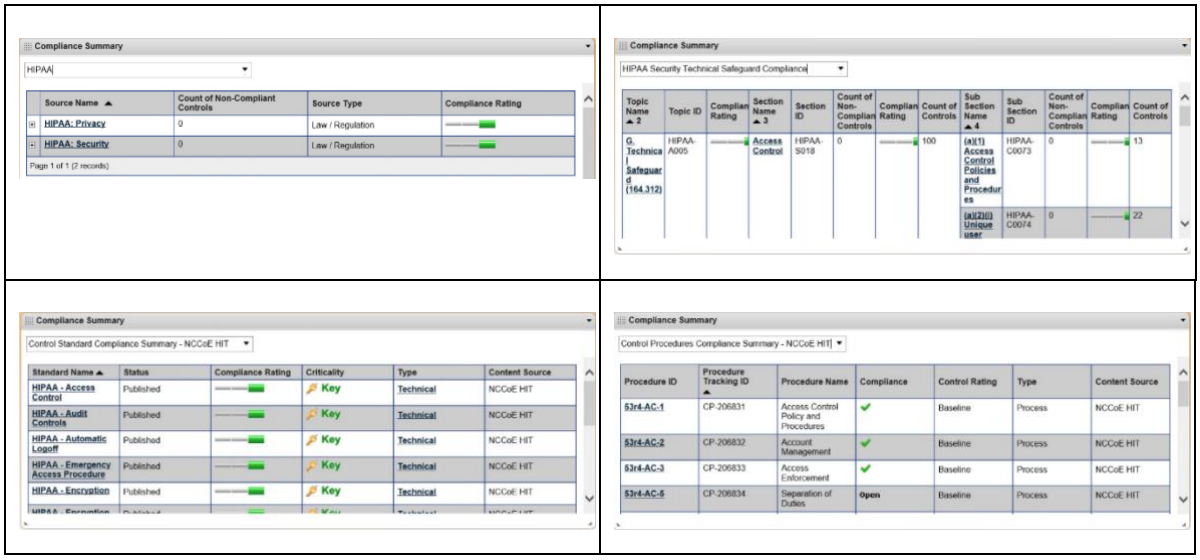


Figure 11-18 C-3: Manage Issues (Findings)

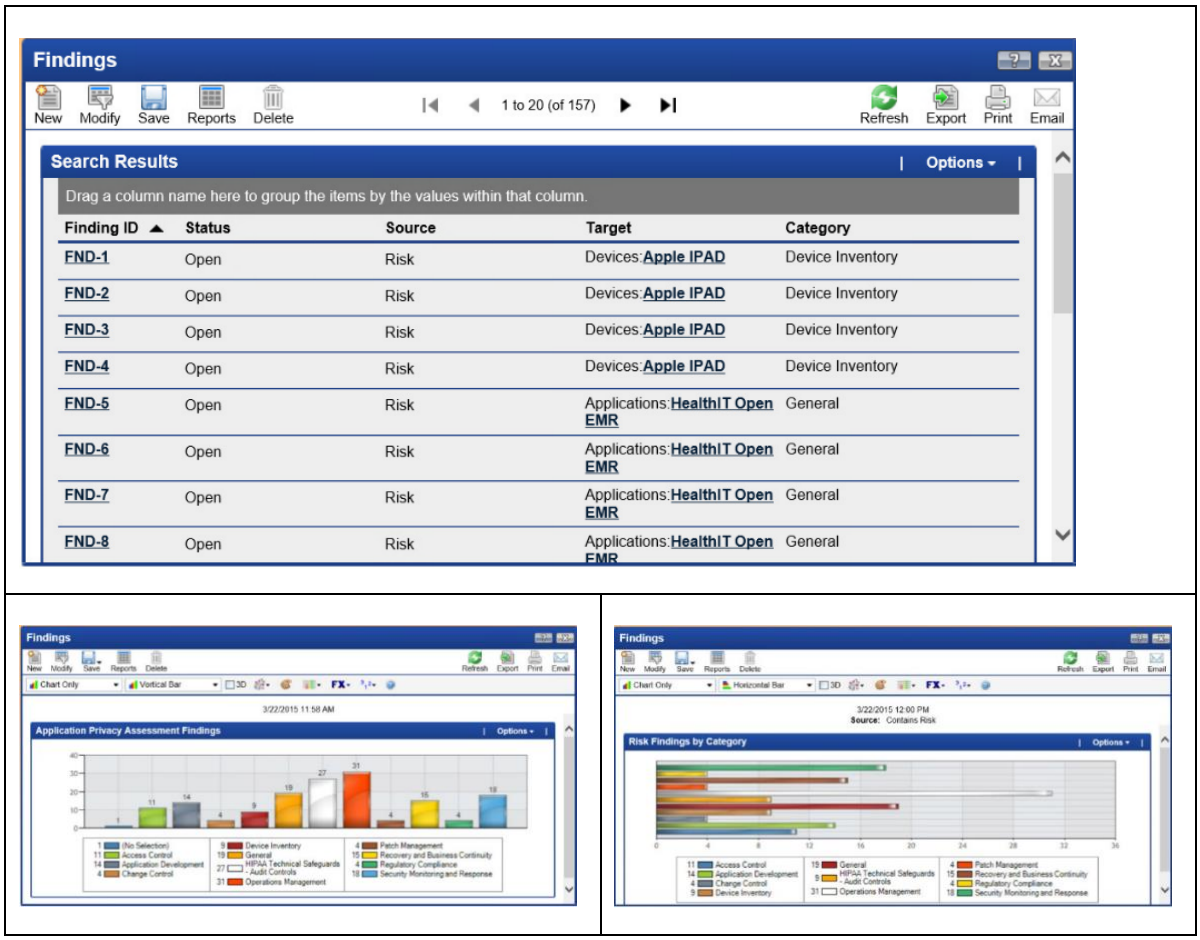


Figure 11-19 Executive Dashboard

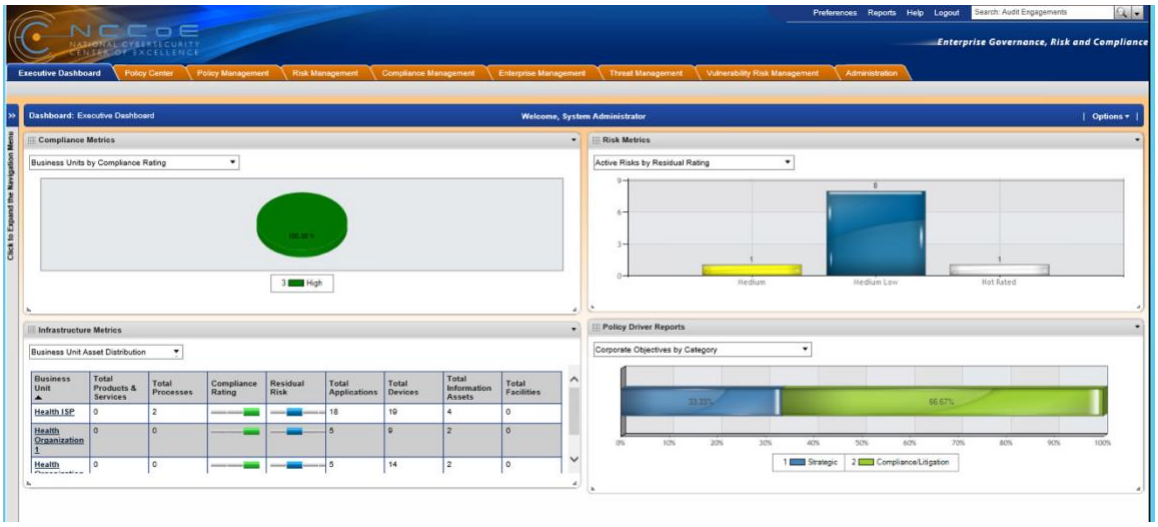


Figure 11-20 Enterprise Management Dashboard

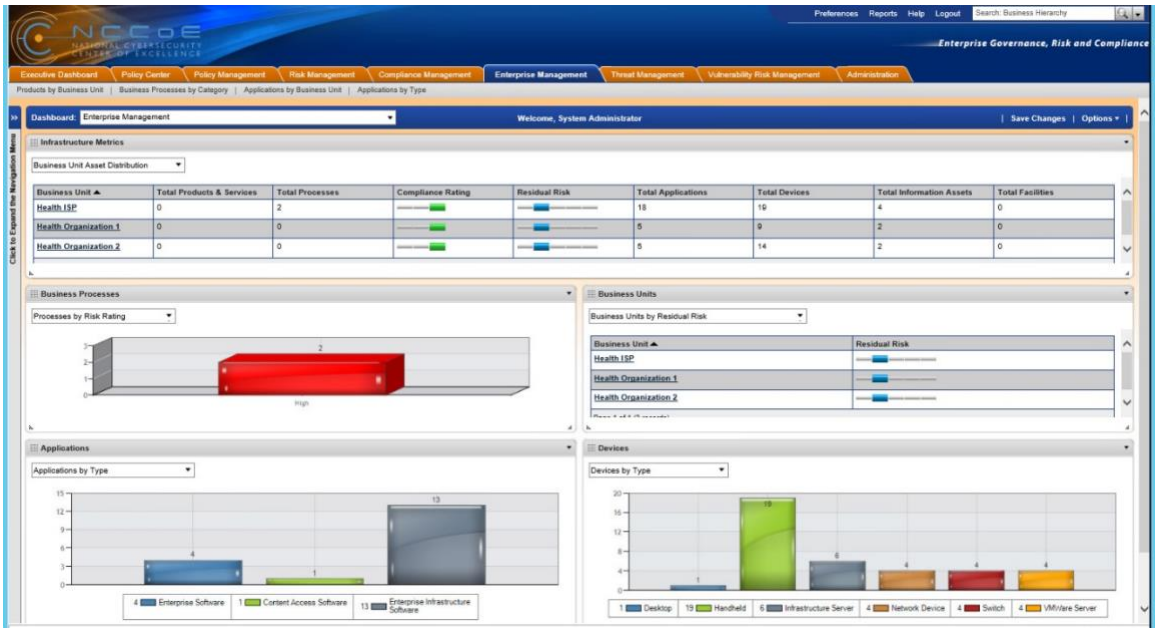


Figure 11-21 Enterprise Risk Management Dashboard

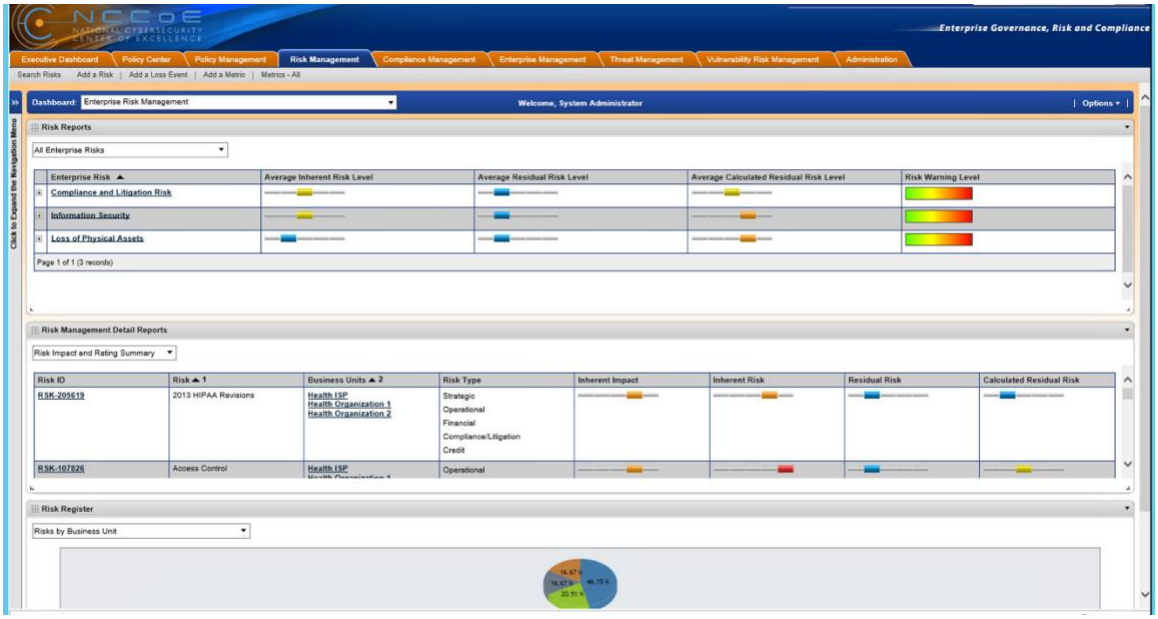
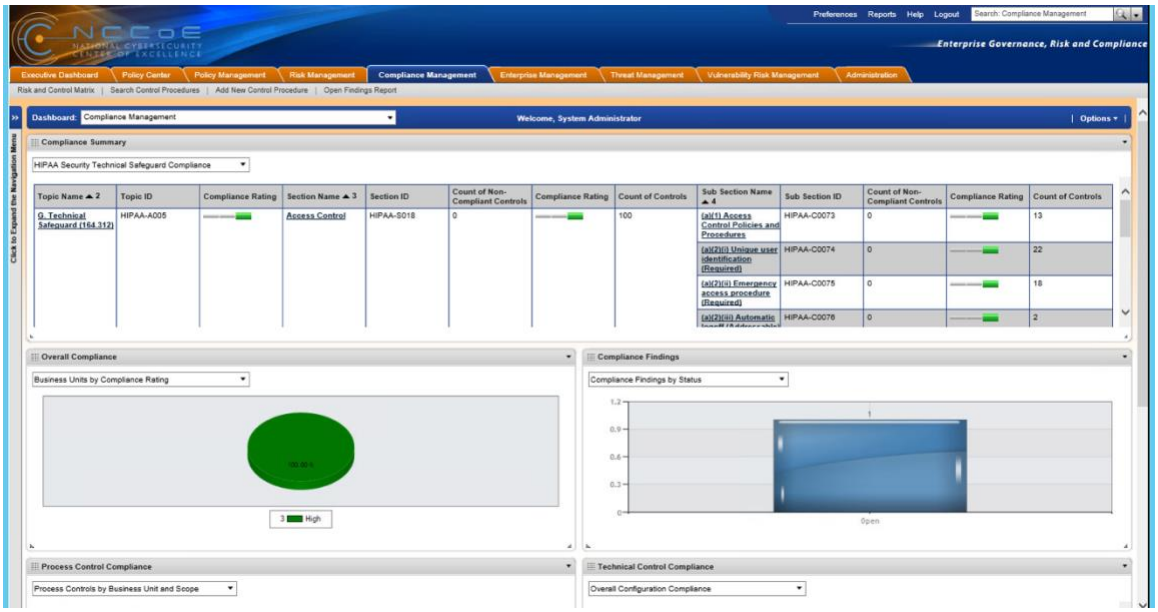


Figure 11-22 Compliance Management Dashboard



Appendix A References

[1] K. Marchesini, *Mobile Devices Roundtable: Safeguarding Health Information: Real World Usages and Real World Privacy & Security Practices*, March 16, 2012, The Office of the National Coordinator for Health Information Technology, Department of Health & Human Services, https://www.healthit.gov/sites/default/files/onc_ocpo_mobile_device_roundtable_slides_3_16_12.pdf [accessed April 30, 2018].

[2] *Windows Server Installation Options*, Microsoft TechNet, August 31, 2016, [website], https://technet.microsoft.com/en-us/library/hh831786.aspx [accessed April 30, 2018].

NIST SPECIAL PUBLICATION 1800-1D

Securing Electronic Health Records on Mobile Devices

Volume D:
Standards and Controls Mapping

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

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

DISCLAIMER

Certain commercial entities, equipment, products, 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, equipment, products, or materials 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, 32 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://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 align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Healthcare 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 healthcare providers, mobile devices can introduce vulnerabilities in a healthcare organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that many providers are using mobile devices for healthcare delivery before they have implemented safeguards for privacy and security [1].

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

KEYWORDS

EHR; electronic health records; HIPAA; mobile device security; patient health information; PHI; risk management; standards-based cybersecurity; stolen health records

ACKNOWLEDGMENTS

We would like to highlight and express our gratitude to Leah Kauffman, with NIST, who served as editor-in-chief of this guide.

We are grateful to the following individuals for their generous contributions of expertise and time.

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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. We worked with:

Technology Partner/Collaborator	Build Involvement
Cisco	Identity Services Engine (ISE), Adaptive Security Virtual Appliance (ASAv), and RV220W
IBM	MaaS360
Intel	Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI)
MedTech Enginuity	OpenEHR software
Ramparts	Risk assessment and security testing
RSA	Archer Governance, Risk & Compliance (GRC)
Symantec	Endpoint Protection

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 Controls 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 3.5, 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) and relevant security controls

3 Security Standards

In addition to using the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Risk Management Framework [2], it is important to consider industry-specific security standards and best practices where possible. Table 3-1 is a list of security standards used to create this architecture.

Table 3-1 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	https://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.pdf
	ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls	https://www.iso.org/iso/catalogue_detail?csnumber=54533
	20 Critical Security Controls	http://www.sans.org/critical-security-controls/
Healthcare Related	Health Insurance Portability and Accountability Act (HIPAA) Security Rule	https://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	https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
	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 Content	https://www.healthit.gov/sites/default/files/20140320_sratool_content_-_technical_volume_v1.docx

Related Technology	Relevant Standards	URL
	US Department of Health & Human Services (DHHS) Office for Civil Rights (OCR) HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework	http://www.hhs.gov/sites/default/files/NIST CSF to HIPAA Security Rule Crosswalk 02-22-2016 Final.pdf
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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-97.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 Security (Remote Access)	NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf
	NIST SP 800-46 rev2, Guide to Enterprise Telework and Remote Access Security	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.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

Related Technology	Relevant Standards	URL
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 Modifications 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) Extensible Authentication Protocol (EAP)	https://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, The TLS Protocol Version 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

Related Technology	Relevant Standards	URL
	RFC 5216, The EAP-TLS Authentication Protocol	http://tools.ietf.org/html/rfc5216
Key Management	NIST SP 800-57 Part 1 – rev4, Recommendation for Key Management, Part 1: General (Revision 4)	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf
	NIST SP 800-57 Recommendation for Key Management — Part 2: Best Practices for Key Management Organization	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p2.pdf
	NIST SP 800-57 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://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf
Risk Management	NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
	NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-39.pdf
	NIST SP 800-37 Rev. 1, 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 NIST Cybersecurity Framework, 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;* in the ISO and IEC Information Technology – Security techniques – Code of practice for information security management (ISO/IEC 27002) [3]; in the Center for Internet Security (CIS) Critical Security Controls [4]; and in the Health Insurance Portability and Accountability Act of 1996 [5].

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. In our example implementation, we also used some relevant technologies and products with the security characteristics that mapped to the Respond or Recover functions of the NIST Cybersecurity Framework. See details in NIST SP 1800-1B, Section 3.6, Technologies.

Table 4-1 Security Characteristics Mapped to Cybersecurity Standards and Best Practices, and HIPAA

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
Access control	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-2, IA Family	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-9	45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
			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	45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24	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	45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.308(a)(8), 164.312(b), 164.312(e)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(3)(ii)(A), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(b), 164.312(d), 164.312(e)
			DE.CM-4: Malicious code is detected	SI-3, SI-8	10.4.1	CSC-7	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. § 164.308(a)(1)(ii)(D)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)
			DE.CM-8: Vulnerability scans are performed	RA-5	12.6.1, 15.2.2	CSC-7, CSC-10	45 C.F.R. §§ 164.308(a)(1)(i), 164.308(a)(8)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
Device integrity	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15	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	45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)
		Data Security (PR.DS)	PR.DS-1: Data-at-rest is protected	MP-8, SC-12, SC-28	None	CSC-15	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(b)(1), 164.310(d), 164.312(a)(1), 164.312(a)(2)(iii), 164.312(a)(2)(iv), 164.312(b), 164.312(c), 164.314(b)(2)(i), 164.312(d)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1), 164.310(d)(2)
			PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SC-16, SI-7	10.4.1, 12.2.2, 12.2.3	CSC-3	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(b), 164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
		Information Protection Processes and Procedures (PR.IP)	PR.IP-1: A baseline configuration of information technology/ industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	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	45 C.F.R. §§ 164.308(a)(8), 164.308(a)(7)(i), 164.308(a)(7)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
		Protective Technology (PR.PT)	PR.PT-2: Removable media is protected and its use restricted according to policy	MP-2, MP-3, MP-4, MP-5, MP-7, MP-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	45 C.F.R. §§ 164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.310(d)(1), 164.310(d)(2), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b)
	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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(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	6.1.5, 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	45 C.F.R. § 164.308(a)(1)(ii)(D)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			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	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B), 164.308(a)(5)(ii)(C), 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(b), 164.310(c), 164.310(d)(1), 164.310(d)(2)(iii), 164.312(b), 164.314(b)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
Person or entity authentication	Protect (PR)	Identity Management, Authentication and Access Control (PR.AC)	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	8.3.3, 11.2.1, 11.2.2, 11.2.4, 15.2.1, 11.4.3	CSC-5, CSC-9, CSC-11	45 C.F.R. §§ 164.308(a)(3)(ii)(B), 164.308(a)(3)(ii)(C), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iii), 164.312(d)
			PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15	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		45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-1, 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	45 C.F.R. §§ 164.308(a)(3), 164.308(a)(4), 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii)
Transmission security	Protect (PR)	Access Control (PR.AC)	PR.AC-3: Remote access is managed	AC-1, AC-17, AC-19, AC-20, SC-15	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	45 C.F.R. §§ 164.308(a)(4)(i), 164.308(b)(1), 164.308(b)(3), 164.310(b), 164.312(e)(1), 164.312(e)(2)(ii)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
			PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4, AC-10, 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	45 C.F.R. §§ 164.308(a)(4)(ii)(B), 164.310(a)(1), 164.310(b), 164.312(a)(1), 164.312(b), 164.312(c), 164.312(e)
		Data Security (PR.DS)	PR.DS-2: Data-in-transit is protected	SC-8, SC-11, SC-12	10.4.2, 10.6.1, 10.6.2, 10.9.1, 10.9.2, 12.2.3, 12.3.1		45 C.F.R. §§ 164.308(b)(1), 164.308(b)(2), 164.312(e)(1), 164.312(e)(2)(i), 164.312(e)(2)(ii), 164.314(b)(2)(i)

Security Characteristics	NIST Cybersecurity Framework v1.1				Sector-Specific Standards & Best Practices		
	Function	Category	Subcategory	NIST SP800-53 Rev 4	IEC/ISO27002	20 Critical Security Controls	HIPAA Security Rule [2]
		Technology (PR.PT)	PR.PT-4: Communications and control networks are protected	AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	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		45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(b), 164.312(e)

5 Technologies

To build an example solution (reference design), we needed to use multiple commercially available and open-source technologies. Table 5-1 shows how the products used to create the reference design are mapped to security controls and architectural components listed in Figure 5-1.

Figure 5-1 Architecture for the Secure Exchange of Electronic Health Records on Mobile Devices in a Healthcare Organization

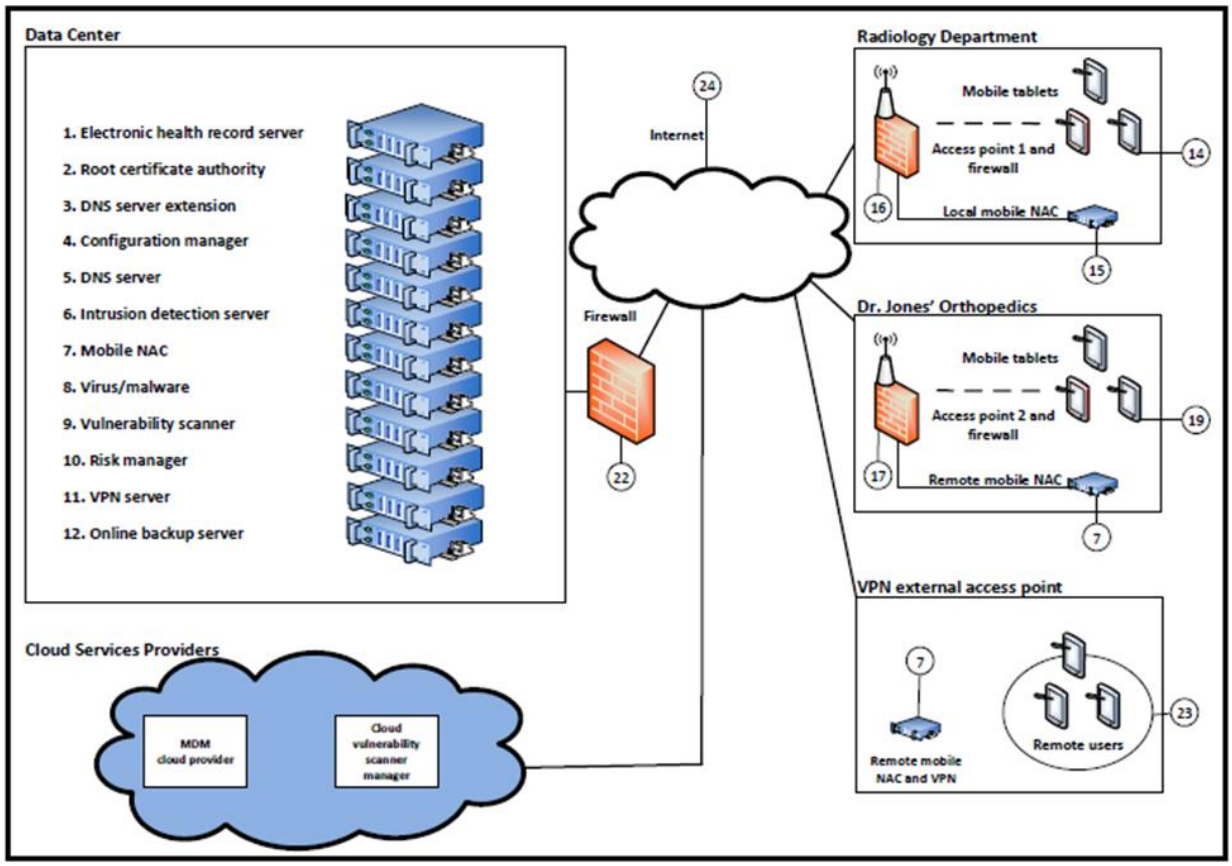


Table 5-1 Products and Technologies Used in the Secure Exchange of Electronic Health Records on Mobile Devices Reference Design

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	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	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	Current	20	Cloud-based Mobile Device Management (MDM)
		Open source	Iptables firewall	1.4	1, 2, 3, 4, 5, 22	Stateful inspection firewall

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	Use
		Open source	Fedora PKI Manager	9	2	Root CA cryptographically signs identity certificates to prove authenticity of users and devices
		Open source	BIND	9.9.4	3, 5	Domain name system (DNS) server performs host or fully qualified domain resolution to Internet Protocol (IP) addresses
		Open source	Puppet Enterprise	3.7	5	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
		Cisco	Identity Services Engine	1.2	7, 15	Local and remote mobile network access control (NAC), RADIUSbased authentication, authorization, and accounting management server
		Cisco	ASAv	9.4		Enterprise-class VPN server based on both TLS and IPsec
		Open source	UrBackup	1.4.8	12	Online remote backup system used to provide disaster recovery
		Cisco	RV220W	6.0.4	16, 17	Wi-Fi access point

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	Use
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	Puppet Enterprise	3.7	5	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts
		Open source	Security Onion IDS	12.04	6	Intrusion detection server (IDS) monitors network for threats via mirrored switch ports
		Open source	Host-based security manager (freeware)		8	Host-based virus and malware scanner
		Open source	Vulnerability scanner (freeware)	Current	9	Cloud-based proactive network and system vulnerability scanning tool
Respond (RS)	AU-6, CA-2, CA-7, CP-2, PE-6, IR-4, IR-5, IR-8, SI-4	Open source	Iptables firewall	1.4	1, 2, 3, 4, 5, 22	Stateful inspection firewall
		Open source	Puppet Enterprise	3.7	5	Secure configuration manager for creation, continuous monitoring, and maintenance of secure server and user hosts

NIST Cybersecurity Framework Function	Reference to NIST 800-53 Rev 4 Controls	Company	Product	V.	Architecture Element*	Use
		RSA	Archer GRC	5.5	10	Centralized enterprise, risk and compliance management tool
Recover (RC)	CP-2, CP-10, IR-4, IR-8	Open source	UrBackup	1.4.8	12	Online remote backup system used to provide disaster recovery
		RSA	Archer GRC	5.5	10	Centralized enterprise, risk and compliance management tool

**See Figure* 5-1.

Appendix A References

[1] *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST Special Publication 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, June 2014. http://doi.org/10.6028/NIST.SP.800-37r1 [accessed 5/1/18].

[2] U.S. Department of Health and Human Services, *HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework*, February 2016. https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf [accessed 5/1/18].

[3] International Organization for Standardization/International Electrotechnical Commission, *Information technology — Security techniques — Code of practice for information security controls*, ISO/IEC 27002:2013, 2013. https://www.iso.org/standard/54533.html [accessed 5/1/18].

[4] *CIS Critical Security Controls*, SANS CAG20 [Website], https://www.sans.org/critical-security-controls/ [accessed 5/1/18].

[5] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. 104–191, 110 Stat 1936. https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf [accessed 5/1/18].

NIST SPECIAL PUBLICATION 1800-1E

Securing Electronic Health Records on Mobile Devices

Volume E:
Risk Assessment and Outcomes

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

July 2018

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.1800-1

The first draft of this publication is available free of charge from:
https://www.nccoe.nist.gov/sites/default/files/library/sp1800/hit-ehr-nist-sp1800-1-draft.pdf

DISCLAIMER

Certain commercial entities, equipment, products, 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, equipment, products, or materials 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, 80 pages, (July 2018), CODEN: NSPUE2

FEEDBACK

As a private-public partnership, we are always seeking feedback on our Practice Guides. We are particularly interested in seeing how businesses apply NCCoE reference designs in the real world. If you have implemented the reference design, or have questions about applying it in your environment, please email us at hit_nccoe@nist.gov.

All comments are subject to release under the Freedom of Information Act (FOIA).

National Cybersecurity Center of Excellence
National Institute of Standards and Technology
100 Bureau Drive
Mailstop 2002
Gaithersburg, MD 20899
Email: nccoe@nist.gov

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity issues. This public-private partnership enables the creation of practical cybersecurity solutions for specific industries, as well as for broad, cross-sector technology challenges. Through consortia under Cooperative Research and Development Agreements (CRADAs), including technology partners—from Fortune 50 market leaders to smaller companies specializing in IT security—the NCCoE applies standards and best practices to develop modular, easily adaptable example cybersecurity solutions using commercially available technology. The NCCoE documents these example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution. The NCCoE was established in 2012 by NIST in partnership with the State of Maryland and Montgomery County, Md.

To learn more about the NCCoE, visit https://www.nccoe.nist.gov. To learn more about NIST, visit https://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 align more easily with relevant standards and best practices and provide users with the materials lists, configuration files, and other information they need to implement a similar approach.

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

ABSTRACT

Healthcare 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 healthcare providers, mobile devices can introduce vulnerabilities in a healthcare organization's networks. At the 2012 Health and Human Services Mobile Devices Roundtable, participants stressed that many providers are using mobile devices for healthcare delivery before they have implemented safeguards for privacy and security [1].

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

KEYWORDS

EHR; electronic health records; HIPAA; mobile device security; patient health information; PHI; risk management; standards-based cybersecurity; stolen health records

ACKNOWLEDGMENTS

We would like to highlight and express our gratitude to Leah Kauffman, with NIST, who served as editor-in-chief of this guide.

We are grateful to the following individuals for their generous contributions of expertise and time.

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

The Technology Partners/Collaborators who participated in this build submitted their capabilities in response to a notice in the Federal Register. Respondents with relevant capabilities or product components 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. We worked with:

Technology Partner/Collaborator	Build Involvement
Cisco	Identity Services Engine (ISE), Adaptive Security Virtual Appliance (ASAv), and RV220W
IBM	MaaS360
Intel	Intel® Identity Protection Technology (Intel® IPT) with Public Key Infrastructure (PKI)
MedTech Enginuity	OpenEHR software
Ramparts	Risk assessment and security testing
RSA	Archer Governance, Risk & Compliance (GRC)
Symantec	Endpoint Protection

Contents

List of Figures

List of Tables

1 Practice Guide Structure

This National Institute of Standards and Technology (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 creating this Practice Guide
- NIST SP 1800-1E: *Risk Assessment and Outcomes* – risk assessment methodology, results, tests, 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 4)
- Risk Questionnaire for healthcare organizations selecting a cloud-based electronic health record (EHR) provider (Section 8)

3 Results

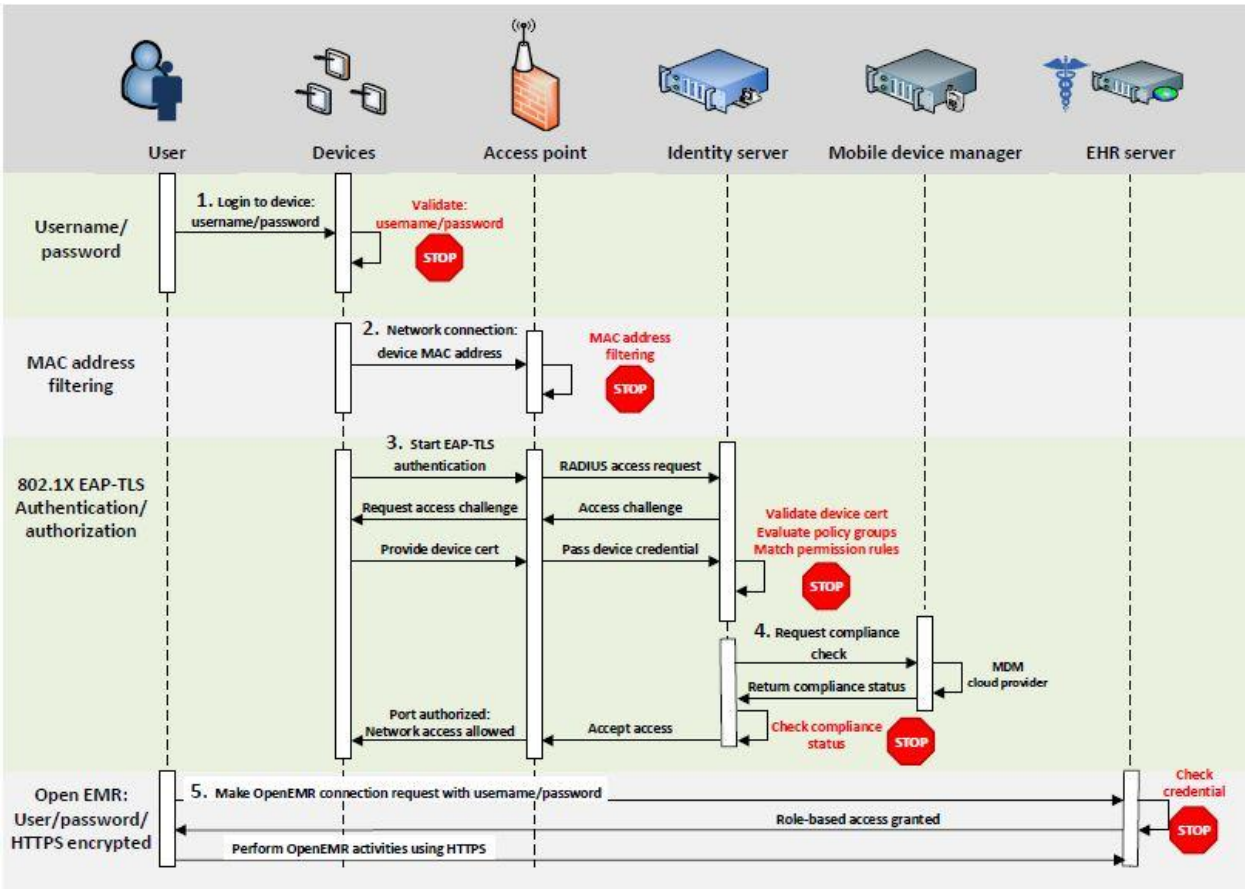
The features in this reference design and our process of continued risk assessment increase the difficulty for an adversary to gain unauthorized access to patient health information. Here the term “patient health information” refers to any information pertaining to a patient’s clinical care. “Protected health information” has a specific definition according to Health Insurance Portability and Accountability Act (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.

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 3-1.

Figure 3-1 The Steps Necessary for a User and Device to Gain Access to the Electronic Health Record Server



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 access points (APs) to facilitate communication to the EHR 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. A user who does not have this certificate on his or her device 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 (CA) 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 insiders or attackers who have gained access to a lost or stolen device. They may get access to the AP, but not to the OpenEMR.

Step 4. The mobile device manager (MDM) performs a compliance check on the device based on the policy that was assigned. The MDM used in this build has the ability to track the specific location of a device, which can be used to restrict use of the device to a specific medical facility. Devices that are not in compliance will not be admitted to the network.

Step 5. OpenEMR is configured to use mutual authentication when establishing the encrypted connection. This prevents access from any device that does not have a valid certificate. When a device is reported lost or stolen, its certificate is revoked, preventing access from that device.

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 login attempts.

It is important to note that all access to the OpenEMR system uses two different forms of authentication device and user. The certificate needed for mutual authentication is bound to the device, turning the device into a second form of authentication.

In this last step, a user with the right login credentials ultimately logs in to 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 EHRs 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 resource intensive. 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. These scenarios were chosen to bypass specific security controls in order to accelerate the testing of different parts of the defense-in-depth strategy. 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 healthcare 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 virtual private network (VPN) access or the attacker's initial foothold. The test procedure assumed the attacker was able to compromise an internal Windows desktop computer.

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 EHR 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 EHR 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 did not 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 internet service provider (ISP) network. At a time coordinated with us, the defenders implemented a block. Blocking the device can be accomplished in several ways, depending in the policy within the MDM. Some examples of what blocking does are revoking the digital certificate or wiping specific contents from the mobile device. Wiping can be further defined within your policy to wipe the whole contents or specific contents on the mobile device.

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 that 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 by 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. In the process of obtaining this network diagram, as well as in several other attacks, the intrusion detection system flagged the attacker's actions.

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

4.1.3 OpenEMR Access Scenario

In this scenario, an attacker accessed the OpenEMR web application with limited privileges (e.g., technician). The attacker was either a malicious insider with limited access to the system or an outsider who captured the user's credentials.

Once the attacker had access to the OpenEMR web application, they attempted to access information for which they were not authorized. This attempt to breach the security of patient health information was thwarted by security characteristics and controls, such as entity authorization and application firewalling, and reduced 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 a wireless access point used by clinicians to access the OpenEMR web application. We assumed the attacker had unsupervised access to this device for an extended period. The attacker was able to bring in electronics and tools. The attacker connected to the access point, performed packet captures, 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 EHR 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 EHR solution to electronically create and transmit a referral to another physician. In this scenario, the receiving physician was able to access the same EHR 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 EHR 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 EHR solution's prescription-sending capability. The test simulated a physician using a mobile device and EHR application to send a prescription

- to a pharmacy directly through the EHR application
- outside the application via email or fax

These actions were successfully completed.

4.3 Security Assessment

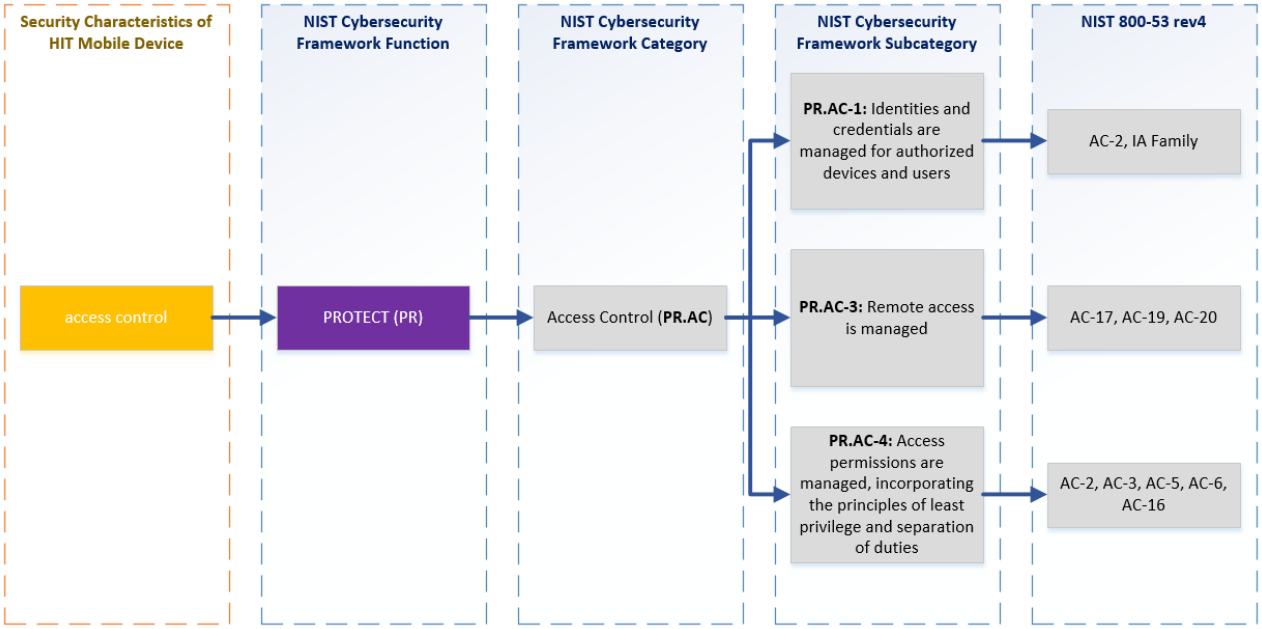
A security assessment evaluated the security characteristics that we thought were satisfied by the architecture. To determine what tests to include, we consulted Table 1, Relevant Standards and Controls, in NIST SP 1800-1D: Standards and Controls Mapping. Five security characteristic requirements are 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 NIST Cybersecurity Framework categories and subcategories to which it maps. The NIST 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 4-1.

Figure 4-1 An Example of the Process for Determining Which Tests to Include in the Security Assessment



The security standards that are mapped to the NIST Cybersecurity Framework Subcategories provided additional validation points. By systematically developing tests based on the NIST Cybersecurity Framework Subcategories, we generated a set of reasonably comprehensive tests for the security characteristic requirements we identified when we first identified this challenge [2].

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

In our solution, we used NIST SP 800-30 as our risk assessment methodology. You may want to consider a methodology that best fits your organization's needs.

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.
- Determine risk.

We offer two methods for conducting a risk assessment:

1. Table-driven method: by following the task list and exemplary tables outlined in NIST SP 800-30: Section 3.2, Conducting the Risk Assessment; and Appendixes D–I. 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 as referenced in NIST 800-30 [3]. The attack/fault-tree methodology was customized for this use case. This was done by decomposing the architecture of the use case. (Note: 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 Cybersecurity 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 – Eighth Annual Canadian Computer Security Symposium, and Intelligence-Driven Computer Network Defense informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.)

Both methods performed a risk assessment and an analysis against this use case for all risk factors, and then determined 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 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 to a focused subset.

The risk assessments identify a list of the risks and their levels of severity. We used the identified risks as the foundation to validate the security characteristics. The mapping to the NIST Cybersecurity Framework 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. The complete assessment results can be found in Section 6 of this volume.

5.1 Table-Driven Risk Assessment Example

This section provides a walk-through for assessing and identifying the following:

- an example of adversarial risk
- an example of non-adversarial risk

During the risk assessment process, we followed the tasks outlined in NIST SP 800-30, Section 3.2, Conducting the Risk Assessment, and used the reference tables, templates, and assessment scale tables outlined in Appendixes D–I.

To recap, we performed the following tasks [4]:

- 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 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 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 walk-throughs are presented. For each step, the column Example Walk-Through/Explanations provides the details on how the sample risk assessment was conducted.

Table 5-1 Adversarial Risk Template [5]

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, Personal Digital Assistants (PDAs), smart phones)	Adversarial/Hacker	Moderate	High	Low	Possible	Moderate	Malware — TECHNICAL/ Architectural and Functional	Moderate	Moderate	Moderate	Low	Moderate

Table 5-2 Adversarial Risk Sample Walk-Through [6]

Column	Heading	Content	Example Walk-Through / 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, smartphones)"
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"

Column	Heading	Content	Example Walk-Through / Explanations
5	Targeting	Assess threat source targeting	The threat source targeting is low, as attackers can use only 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 threat event, so "Moderate" is used here
8	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities that could be exploited by threat sources initiating the threat event and the predisposing conditions that 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"

Column	Heading	Content	Example Walk-Through / Explanations
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 Guide for Conducting Risk Assessments, Table G-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	This threat event is potentially harmful 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 lose 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 (Column 12, Moderate). By checking Guide for Conducting Risk Assessments, Table G-5: Assessment Scale — Overall Likelihood, the Level of Risk is Moderate

Table 5-3 Non-adversarial Risk Template [7]

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	Moderate

Table 5-4 Non-adversarial Risk Sample Walk-Through [8]

Column	Heading	Content	Example Walk-Through / 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
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 "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"

Column	Heading	Content	Example Walk-Through / Explanations
5	Likelihood of Threat Event Occurring	Determine the likelihood that the threat event will occur	Accident is somewhat likely to occur, so "Moderate" is used here
6	Vulnerabilities and Predisposing Conditions	Identify vulnerabilities that could be exploited by threat sources initiating the threat event and the predisposing conditions that 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 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 threat 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 Guide for Conducting Risk Assessments, Table G-5: Assessment Scale – Overall Likelihood the Overall Likelihood is Moderate.

Column	Heading	Content	Example Walk-Through / Explanations
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	This threat event is potentially harmful 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 lose 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 5-6, Assessment Scale — Level of Risk (Combination of Likelihood and Impact), the Level of Risk is Moderate.

Table 5-5 Assessment Scale – Overall Likelihood [9]

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

Table 5-6 Assessment Scale – Level of Risk (Combination of Likelihood and Impact) [10]

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

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

NCCoE worked with Ramparts, LLC to perform a risk assessment by using attack/fault trees. The methodology allowed us to identify and prioritize the impacts of the attack events. Prioritizing the impacts of the attack events 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:

1. threat sources and threat events
2. threat events and vulnerabilities
3. threat events and impacts/assets

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

1. Scope the Risk Assessment (define the Potential Harm, Security Characteristics, Critical Data Assets, and map to NIST Cybersecurity 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. Analyze 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: Scope the Risk Assessment.

The NIST Cybersecurity Framework 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 NIST Cybersecurity Framework and other standards.

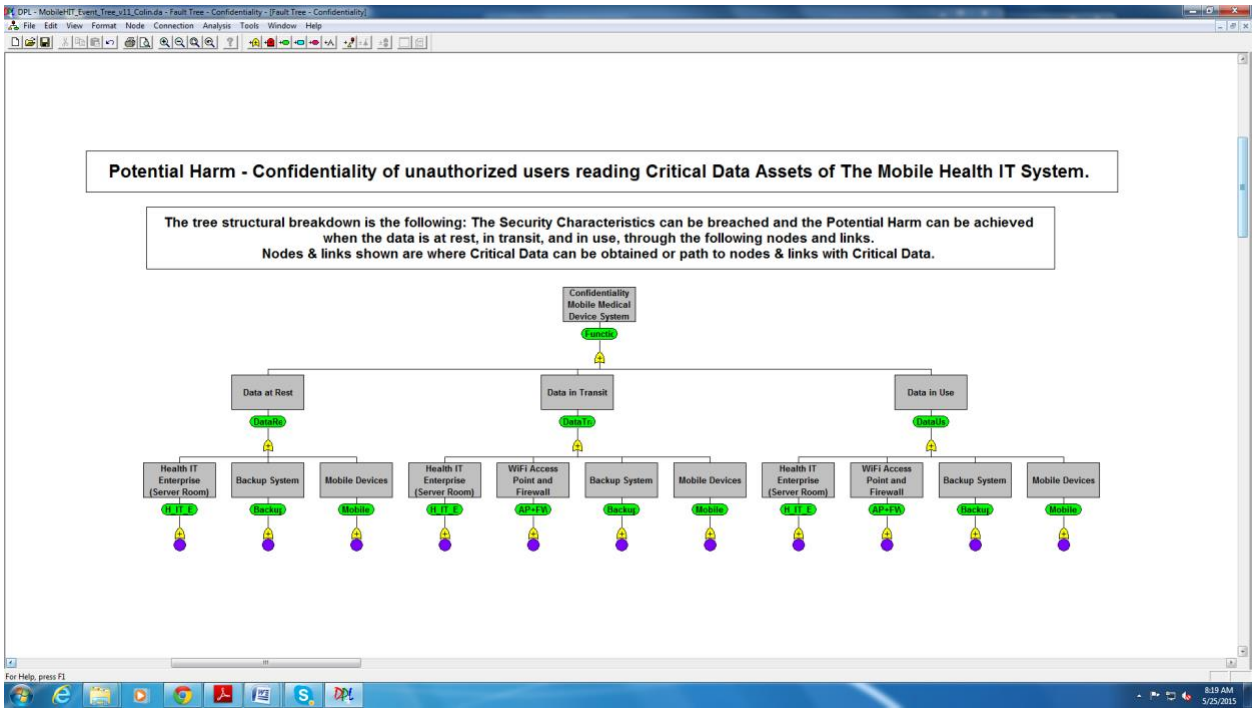
Step 2: Create Attack Event Trees (Attack Scenarios) that target the Security Characteristics and Critical Data Assets.

The potential attack events are developed by 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 review and contribute to the assessment more easily. The event nodes were decomposed to a level where a likelihood of occurrence could be assigned. An attack scenario is considered successful when all parallel events are AND'ed together. Which means, for an attack on a parent event to be considered successful, all parallel child events would need to be compromised. If the attack occurred to any one child event, then the parent event was potentially attacked; therefore, the paralleled events are considered OR'ed together.

The logical structure 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. The third layer modeled the devices and data nodes of the system. Reference the confidentiality attack tree below.

Figure 5-1 Confidentiality Attack Tree



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 anti-virus 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 of 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, or 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:

Table 5-7 Scale of Likelihood of Occurrences

Value	Qualitative Numeric Value
Low	.01
Medium Low	.1
Medium	.5
Medium High	.75
High	.9

The qualitative numeric values are used in the event trees to calculate probabilities at the higher levels of the trees. This was done 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 access 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 are given a qualitative value for the event. Borrowing from MORDA, the following scale was used:

   Table 5-8 Value/Range Scales

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 an adversary's Low likelihood of success, it is still important to consider the adversary's likelihood of not being detected. A detection countermeasure(s) can help 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 gives equal weight to the adversary's likelihood of success and of not being detected. One goal of any organization providing good security is to make the resources that an adversary would need to accomplish its objective to be cost prohibitive. For this assessment, we have assumed those same low-level resources for all attack scenarios.

   Table 5-9 shows how the three types of Adversary Likelihoods can be combined to come up with a single value for the Assigned Likelihood of Occurrence.

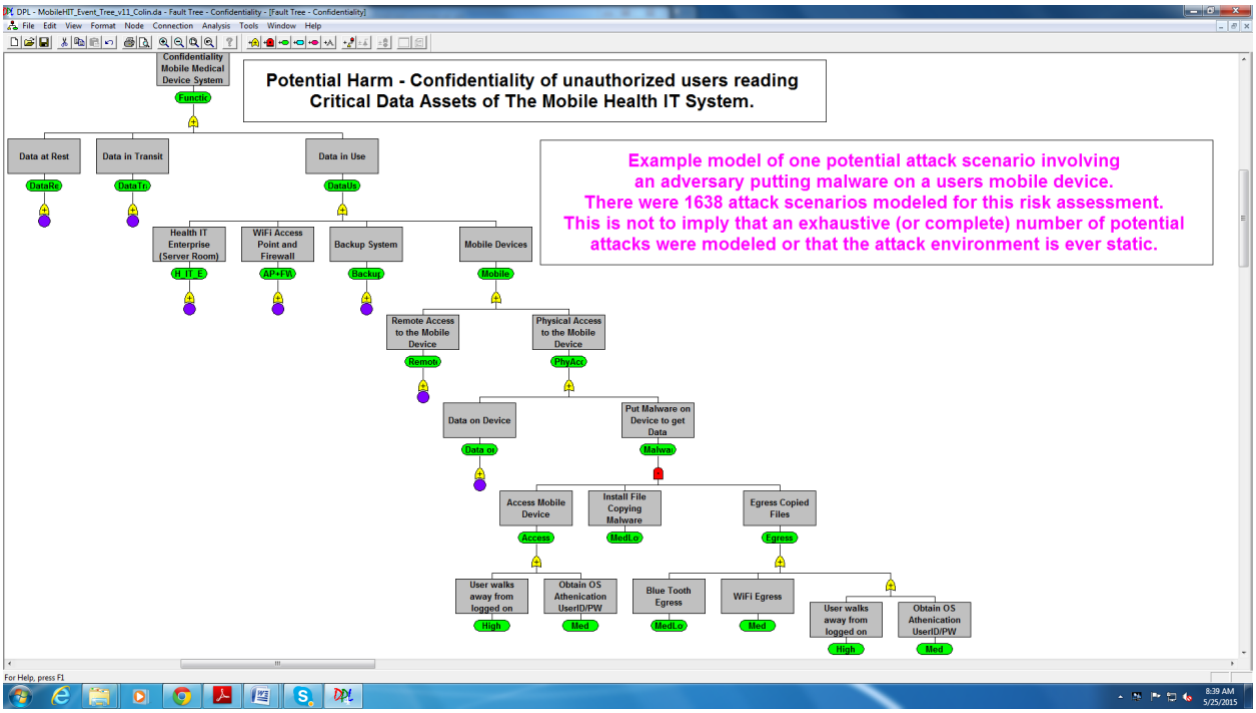
Table 5-9 Assigned Likelihood of Occurrence

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

Event	Adversary's Likelihood of Success	Adversary's Likelihood of Not Being Detected	Adversary's Resources Required	Assigned Likelihood of Occurrence Value
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.

Figure 5-2 Attack Branch Scenario



Step 5: Analyze and Present Results.

Using established reliability probability theory, 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 event 2 and event 3 have been accomplished by an adversary. Events AND'ed together (those that are sequential) can be represented as P = p4*p5, which is the probability that neither event 4 nor event 5 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) – Eighth Annual Canadian Computer Security Symposium.

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

6 Risk Assessment Results

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 a logged-on mobile device
  - downloads viruses or other malware
  - uses an insecure Wi-Fi network
- inadequate
  - access control and/or enforcement
  - change management
  - configuration management
  - data retention, backup, and recovery

The detailed risk assessment results for table-driven and fault-tree methods are captured in Appendix A and Appendix B, respectively.

7 Tests Performed in Security Controls Assessment

Table 7-1 summarizes the security controls assessment. We used NIST 800-53 controls for our methodology. You can use security and privacy controls that best fit your organization's needs.

Table 7-1 Security Controls Assessment

Test ID	NIST Cybersecurity Framework Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
1	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-2	Architecture accounts for multiple user roles and 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 users to perform their job function	The solution can allow multiple privilege and role levels
2	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	AC-2	Only currently authorized users are able to access the EHR data	Test that 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 devices 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: Attempt to access OpenEMR by using a device that does not have a valid certificate	The EHR system recognizes the device as an unknown and either denies access completely or demands additional authentication before establishing connectivity.

Test ID	NIST Cybersecurity Framework Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
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 a) via FTP, port 21; b) via HTTP port 80	The EHR system allows connections but does not allow access via insecure connections. Only secured and appropriate connection protocols are used
5	PR.AC-4: Access permissions and authorizations 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 access control lists, firewall rules, operating system (OS) permissions, application settings) to verify that mechanisms exist to limit access to only authorized users and services. a)Verify that those restricted settings are in place b)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 and authorizations are managed, incorporating the principles of least privilege and separation of duties	AC-6	The system will not allow users greater access than their assigned role permits	Test that the system applies access controls: a) Log in as a privileged user; log out b) Log in as a user with no special privileges, attempt to gain privileged access	The nonprivileged user does not gain additional privileges
7	PR.AC-4: Access permissions and authorizations are	IA-5	Application and system components contain a mechanism to allow the	Within the application, examine settings to identify whether the components used in the solution provide an audit capability	An audit capability exists and can be employed

Test ID	NIST Cybersecurity Framework Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
	managed, incorporating the principles of least privilege and separation of duties		auditing of privileged functions	that will indicate when privileged use has been employed	when implemented in a production environment
8	DE.CM-4: Malicious code is detected	SI-3	Malicious code protection (anti-virus software) is installed on mobile devices	a) Examine mobile devices to verify that malicious code protection is installed b) 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	a) Inspect the OS to ensure that malicious code protection is installed b) 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 c) Attempt to upload an EICAR test file that has been compressed d) 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: a) Log in to the OpenEMR application b) Identify fields within the application requiring user input c) Attempt to upload multiple file types, including those containing Hypertext Markup Language 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)

Test ID	NIST Cybersecurity Framework Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
11	PR.DS-1: Data-at-rest is protected	SC-28	Data within EHR is accessible only to authorized users and services	Inspect: a) 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 b) Indicate the encryption type in use and whether it is embedded in the EHR product or a separate mechanism c) Identify any noncryptographic 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: a) Have user A log in via the Internet; log out b) Have user A try to log in via dial-up. This should fail c) Have user B try to log in via the Internet. This should fail d) Have user B log in via dial-up from the authorized source location; log out e) Have user B try to log in via dial-up from an unauthorized source location. This should fail f) Have users A and C log in via Internet. Both users attempt to perform a privileged function. Only user C should be successful g) Have users B and C log in via dial-up from authorized source locations. Both users attempt to perform a privileged function. Only user C should be successful	Attempted logins and use of privileged functions succeed or fail 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

Test ID	NIST Cybersecurity Framework Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
				h) 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	
13	PR.AC-3: Remote access is managed	AC-17	Only devices with authorized MAC addresses will be granted access to the network	a) Use an authorized mobile device to log an authorized user in to the EHR b) Configure that otherwise legitimate mobile device to have a MAC address that is not authorized to access the network, and attempt to log on c) Verify that the login attempt fails	MAC address checking is performed
14	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	AC-4	Information flow control policy is enforced to control the flow of info between the designated mobile devices and the EHR server	Test: a) Attempt to send EHR information from one mobile device directly to the other via the EHR application b) Attempt to perform Internet Protocol 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) by using a cryptographic mechanism	Examine transmission settings. Verify that the encryption mechanism is in place when transmitting data. Test: a) 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)	FIPS 140-2-compliant mechanism is used to secure data-in-transit

Test ID	NIST Cybersecurity Framework Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
				b) Send EHR info from mobile device to EHR server c) Turn off packet capture d) Examine packet capture to verify that a digital signature was sent with the EHR info transmitted e) Calculate what the digital signature should be for this EHR and verify that it is the same as the value that was transmitted f) Verify that the packets containing health information are encrypted exactly as they should be given the encryption algorithm used	
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 Wi-Fi 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 a) WPA2™ (Wi-Fi Protected Access®, b) 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, anti-virus software, and an intrusion detection system [IDS], and all patching is up-to-date)	Inspect wired network to verify presence of a firewall, anti-virus 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	SC-7	Mobile device (wireless client) is hardened in general	Mobile device has a firewall, anti-virus software, and an IDS installed; its patching is up-to-date; 802.11 ad hoc mode is	Mobile device has listed security components installed

Test ID	NIST Cybersecurity Framework Subcategory	Related NIST 800-53 Control	Evaluation Objective	Evaluation Steps	Evidence of Conformance
	networks are protected			disabled; and Bluetooth is turned off by default	
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	a) Use a mobile device to log in to OpenEMR. Log out b) Turn on Bluetooth on that mobile device and attempt to log in to the EHR c) Verify that the mobile device can no longer log in to the EHR server	Noncompliant 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	a) Use a mobile device to log in to OpenEMR b) While logged in to OpenEMR, turn on Bluetooth for that mobile device c) Verify that the mobile device is not visible to other devices	Mobile devices outside the EHR application are unable to connect to a mobile device accessing OpenEMR

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

8.1 Introduction

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

The functionalities provided, the 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 Civil Rights (OCR) for Health Information Technology provides a questionnaire [11] to help healthcare organizations perform the security risk assessment. On top of utilizing the risk assessment results, an organization can also tailor the OCR's questionnaire to shop for a cloud vendor that provides security for health 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 recommend that each organization performs a thorough risk assessment before moving to cloud-based healthcare IT services, and makes a strategic decision based on the organization's financial, business operation, and legal and regulatory requirements. We also recommend regular reassessments 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 healthcare organization need to integrate the cloud-based EHR system with other in-house products, such as practice management software, billing systems, and email systems?
    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 policies 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 prevent 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 life cycle 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 protected 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 that 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 EHR system vendor provide a written copy of its security and privacy policies and procedures (including disaster recovery)?

    c. How often are new features released? How are they deployed?

Appendix A Table-Driven Risk Assessment Results

Table A-1 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

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	High	High	8
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smartphones)	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 A-2 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, smartphones)	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	Moderate	Moderate	Moderate	High	Moderate	5

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									
							complexity control						
Conduct communication 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 A-3 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

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
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 insecure 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 A-4 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

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
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 insecure 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 A-5 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

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
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 insecure 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

Appendix B Fault-Tree Risk Assessment Results

Table B-1 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_Authentication443
7.71E-05	0.5	3.85E-05	Obtain_OS_Authentication555
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_Physical_Transfer_Obtain_Copy54

Partial Derivative	Probability	Maximum Impact	Event
7.19E-05	0.5	3.59E-05	During_Physical_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_Authentication442
3.37E-05	0.5	1.69E-05	Obtain_OS_Authentication55
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

Partial Derivative	Probability	Maximum Impact	Event
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	Physical_Access_to_the_MDM1
0.000674	0.01	6.74E-06	Remote_Access_to_the_MDM54
0.000674	0.01	6.74E-06	Physical_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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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_Authentication1
1.43E-06	0.5	7.13E-07	Obtain_OS_Authentication54
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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_

Partial Derivative	Probability	Maximum Impact	Event
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 B-2 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_Authentication4433
0.0009	0.5	0.00045	Obtain_OS_Authentication443
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_Critical_Data4122
0.0033	0.01	3.30E-05	Changing_Critical_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_Modifying_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

Partial Derivative	Probability	Maximum Impact	Event
0.000204	0.01	2.04E-06	Decrypt_the_Back_up4
4.07E-06	0.5	2.04E-06	During_Physical_Transfer_Obtain_Copy1
4.07E-06	0.5	2.04E-06	During_Physical_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_Critical_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_Critical_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_Critical_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_Critical_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_Critical_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_Critical_Data6
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data35

Partial Derivative	Probability	Maximum Impact	Event
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_Critical_Data323
1.29E-06	0.01	1.29E-08	Changing_Critical_Data233
1.29E-06	0.01	1.29E-08	Changing_Critical_Data333
1.29E-06	0.01	1.29E-08	Decrypt_Critical_Data7
1.29E-06	0.01	1.29E-08	Changing_Critical_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_Critical_Data32
1.29E-06	0.01	1.29E-08	Changing_Critical_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_Critical_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_Critical_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

Partial Derivative	Probability	Maximum Impact	Event
7.33E-07	0.01	7.33E-09	Re_Encrypt_Modified_Critical_Data2623
7.33E-07	0.01	7.33E-09	Changing_Critical_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_Critical_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_Critical_Data223
7.11E-07	0.01	7.11E-09	Changing_Critical_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_Critical_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

Partial Derivative	Probability	Maximum Impact	Event
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_Critical_Data1
1.29E-07	0.01	1.29E-09	Changing_Critical_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_Critical_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_Critical_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_Critical_Data263
4.07E-08	0.01	4.07E-10	Re_Encrypt_Modified_Critical_Data263
4.07E-08	0.01	4.07E-10	Breach_Firewall

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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_Critical_Data284
8.15E-10	0.1	8.15E-11	Backup_data_Captured54

Partial Derivative	Probability	Maximum Impact	Event
8.15E-09	0.01	8.15E-11	Decrypt_Data20
8.15E-09	0.01	8.15E-11	Changing_Critical_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_Critical_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_Critical_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

Partial Derivative	Probability	Maximum Impact	Event
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 B-3 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_Physical_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

Partial Derivative	Probability	Maximum Impact	Event
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_Authentication4433
9.66E-14	0.5	4.83E-14	Obtain_OS_Authentication4431
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Partial Derivative	Probability	Maximum Impact	Event
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

Appendix C References

[1] K. Marchesini, *Mobile Devices Roundtable: Safeguarding Health Information: Real World Usages and Real World Privacy & Security Practices*, The Office of the National Coordinator for Health Information Technology, U.S. Department of Health & Human Services, March 16, 2012. https://www.healthit.gov/sites/default/files/onc_ocpo_mobile_device_roundtable_slides_3_16_12.pdf [accessed 5/3/18].

[2] *Mobile Devices – Secure Exchange of Electronic Health Information*, Final draft, National Cybersecurity Center of Excellence, National Institute of Standards and Technology, Gaithersburg, Maryland. http://nccoe.nist.gov/sites/default/files/nccoe/NCCoE_HIT_MobileDevices_UseCase.pdf [accessed 5/3/18].

[3] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 15 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[4] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, 29 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[5] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, Table I-5: Template – Adversarial Risk, I-3 – I-4 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[6] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, Table I-4: Column Descriptions for Adversarial Risk Table, I–3 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[7] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, Table I-7: Template – Non-adversarial Risk, I–4 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[8] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, Table I-6: Column Descriptions for Non-adversarial Risk Table, I–4 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[9] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, Table G-5: Assessment Scale – Overall Likelihood, G–2 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[10] *Guide for Conducting Risk Assessments*, NIST Special Publication 800-30 Revision 1, National Institute of Standards and Technology, Gaithersburg, Maryland, September 2012, Table I-2: Assessment Scale – Level of Risk (Combination of Likelihood and Impact), I-1 pp. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [accessed 5/3/18].

[11] *Security Risk Assessment Tool,* Office of the National Coordinator for Health Information Technology, HealthIT.gov [Website]. http://www.healthit.gov/providers-professionals/security-risk-assessment [accessed 5/3/18].