Secure Electronic Health Record Exchange: Achieving the Meaningful Use Objectives

Subrata Acharya
Towson University
sacharya@towson.edu

Brian Coats
Towson University
bcoats1@students.towson.edu

Arpit Saluja
Lexington Hospitalist Inc.
asaluja@altoonaregional.org

Dale Fuller
Lexington Hospitalist Inc.
dfuller@altoonaregional.org

Abstract

This research addresses the urgent need to create a comprehensive guide for healthcare providers to follow to exchange electronic health records securely and meet the associated Department of Health and Human Services’ Meaningful Use objectives. Healthcare providers have numerous legal, financial, and ethical motivations to exchange patient data securely. Unfortunately, healthcare providers are provided with minimal guidance for actually achieving this goal. To this effect the proposed research lays out a comprehensive and homogeneous approach for implementing secure electronic health record transmission. Additionally, we present a standard process of testing and validating a healthcare organization’s security and privacy practices. To solidify the effectiveness of our proposed research, the implementation plan and testing tools have been evaluated in a real-world HIMSS Stage 6 healthcare organization.

1. Introduction

Access to healthcare has been a national point of interest for most of this country’s existence. By November 1945, President Harry Truman made history with his proposal of a national health care insurance program. Twenty years later, in 1965, President Johnson signed the Medicare bill into law. In 2010, President Obama signed the Affordable Care Act which took the country yet another significant step closer to achieving the goal of national healthcare coverage. While access to healthcare isn’t a new issue, it has gained significant traction in the last few years with the federal government enacting a number of laws aimed to greatly enhance the exchange of medical information between all relevant parties: patients, providers, and payers. The ability to share and distribute health information between any and all necessary parties is a critical component to providing access to healthcare resources. The Health Insurance Portability and Accountability Act (HIPAA) established in 1996 was largely aimed at providing the guidelines and framework for how health information could be uniformly and securely shared between disparate entities throughout the healthcare community [1]. Implementing electronic health record (EHR) systems is a fundamental requirement of the HIPAA regulations, as it facilitates the accessibility and standardization of medical information nationally.

Unfortunately HIPAA compliance and likewise EHR adoption has not happened as quickly as the federal government originally hoped. Many health entities are still working towards compliance although the initial deadlines have passed some six years ago. To incentivize the healthcare providers to implement EHR systems, the federal government passed the Health Information Technology for Economic and Clinical Health Act (HITECH) in January of 2010. This legislation provided the healthcare community a “transformational opportunity to break through the barriers to progress” [2]. The ‘Meaningful Use (MU)’ program authorizes incentive payments through both Medicaid and Medicare to private practices and hospitals that use certified EHR technology to accomplish specific objectives in care delivery. A number of the Meaningful Use Stage 1 core objectives are directly relevant to EHR security, specifically regarding the exchange of that data between entities [3]. Efficient and effective data sharing of EHRs require that all parties’ information systems must meet a set of common guidelines for security, privacy, and interoperability. These challenges can be grouped into 3 key areas: storage, access, and transmission. The focus of this research is specifically on the challenges surrounding transmission security and EHR data exchanges.

To this end, this research addresses the implementation and evaluation of EHR transmission security in order to meet the requirements for Stage 1 of the Meaningful Use regulations provided the U.S. Department of Health & Human Services (HHS). The findings of this research will help healthcare providers...
identify possible EHR relevant transmission scenarios, how to perform those transmissions securely, and finally how to evaluate and test the processes to ensure that security is adequate. Specifically, the key contributions of this research to the healthcare information technology industry are:

- The creation of a comprehensive implementation guide for addressing EHR transmission security in a distributed, multi-location healthcare provider environment,
- An automated security testing process using a collection of common tools for assessment, attestation, and ongoing compliance, and
- An all-inclusive security testing plan for using the security testing tools.
- Enhanced security and privacy for a national healthcare provider that enabled qualification for Stage 1 of Meaningful Use.

The rest of the paper is as follows: Section 2 presents the significance of the research to the healthcare industry; in Section 3 the security guidelines related to transmission security for EHRs is detailed; Section 4 describes how to adequately test an organization’s security; Section 5 describes how this research is already being applied and benefiting a typical national healthcare organization; finally Section 6 summarizes the goals of this research and its importance to the landscape of information security in healthcare.

2. Background & Related Work

The Healthcare Information and Management Systems Society (HIMSS) define an EHR as the cumulative electronic record of patient health information created from each interaction with a healthcare provider. A patient EHR can contain demographic data, medical history, medications, immunizations, laboratory data, radiology reports, and any other relevant health care information [4]. Having a patient’s complete medical record in an electronic format both automates and streamlines healthcare provider’s workflow across the board. In addition to traditional care delivery, EHRs enable activities such as quality management, statistical reporting, outcomes reporting, and evidence-based decision support.

The federal government is enticing healthcare providers to start taking advantage of EHR usage with a fairly lucrative ‘carrot’. HHS has laid out the incentive programs such that meeting Stage 1 requirements of Meaningful Use in 2011 or 2012 can earn private practices over $100,000 and hospitals over $2 million between Medicaid and Medicare [5]. While HHS is offering incentives for early adoption, they are also levying penalties if these same requirements aren’t satisfied by 2015. Stage 1 is just the first of an anticipated 3 stages to ensure full EHR adoption nationally. Stage 2 is slated for implementation in 2014 and Stage 3 is tentatively scheduled for 2015.

The Stage 1 requirements established by HHS list 15 core objectives for Eligible Professionals (EP), such as private physician practices, and 14 core objectives for Hospitals (H) [3]. Of these core objectives, those that are directly relevant to EHR transmission security include:

- Provide patients with an electronic copy of their health information, upon request (EP/H)
- Provide patients with an electronic copy of their discharge instructions at time of discharge, upon request (H)
- Provide clinical summaries for patients for each office visit (EP)
- Capability to exchange key clinical information among providers of care and patient-authorized entities electronically (EP/H)
- Protect electronic health information (EP/H)

Another closely related core objective of Stage 1 is the ability to report ambulatory/hospital clinical quality measures to the Centers for Medicare & Medicaid Services (CMS) or similar State agencies. All of these objectives require electronic protected health information (ePHI), captured in EHR systems, to be transmitted from or received by the healthcare provider. Further, in order to satisfy the MU Stage 1 requirements, organizations must attest they have met all the core objectives for a continual 90-day period.

HIPAA lays out an extensive set of regulations to ensure both privacy and security of ePHI data both at rest and in transit. Specifically, the regulations address transmission security in §164.312(e) (1) by the following statute, “implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network” [1]. The regulation goes on to state that there are 2 key components of ensuring the security of ePHI during transit: integrity controls and encryption. The primary purpose of integrity controls is to ensure the ePHI data isn’t modified in any way during transmission. Encryption serves to disguise the true content of data such that it is not easily readable or decrypted without proper authorization. These 2 security measures are the basic foundation of providing secure transmissions. If an unauthorized entity can’t read the contents of a transmission or alter or delete any portion of it, the authenticity and confidentiality of the transmission is ensured. While the concepts are straightforward, the regulations don’t offer detailed
guidelines for implementation. Therefore with no clear direction, successfully achieving the requirements can be quite challenging.

While healthcare providers are undoubtedly attracted to participate in the HHS’ Meaningful Use programs for the financial benefits, many providers have not been able to capitalize on the opportunity. The Centers for Medicare & Medicaid Services (CMS) released a number of reports in June 2012 that detailed how the incentive programs have performed through May 2012 [6]. Based on the CMS reports, nationally only slightly better than a 35% of all healthcare providers that have registered for the incentive programs are actually receiving the benefits of the Medicare program. Further, just over 50% are receiving benefits for the Medicaid program. With such a variance between the number of providers that have registered for the programs and those that have met the requirements, it is clear that EHR adoption and its related security are considerable challenges. HealthLeaders Media rated EHR adoption, specifically meeting MU requirements, the #8 issue for healthcare providers in the United States in 2011 [7]. Similarly, PricewaterhouseCoopers predicts that privacy and security, particularly as it relates to the sharing of medical data for coordination of service, is the #6 top issue faced by the healthcare community in 2012 [8]. This research aims to lessen those challenges by providing a comprehensive implementation guide for healthcare providers to follow to enable the secure, electronic exchange of EHR data. All aspects of security are addressed including both strategic and operational aspects of the transmission process and how to test its effectiveness in order to complete the required Meaningful Use attestation.

3. EHR Security Implementation

Although all 3 EHR security areas have a certain amount of overlapping considerations, the actual transmission of ePHI is the primary focus of this research and storage and access will be considered out of scope.

3.1. Network Segregation

How transmissions are secured depends on what network area they are originating from and to which network area they are destined. The path the transmission takes will vary the exposure that transmission has to interception and misdirection. This research addresses 4 primary network types:
- Green – Internal LAN
- Orange – Demilitarized Zone (DMZ)
- Blue – Wireless LAN
- Red – External LAN

![EHR Transmission scenarios](2557)

Figure 1: EHR Transmission scenarios
LAN segmentation is typically configured using network firewalls. Firewalls can be either hardware or software solutions that control the flow of network traffic between different network segments. They can leverage a number of technologies to filter, restrict, and segregate the network traffic they manage. Some of the more common of these technologies include packet filtering, stateful inspection, virtual private networking (VPN), and network access control (NAC). Both VPN and NAC are specifically related to gaining access to the internal network, either from a remote location or directly to the internal network using an unregistered device. Packet filtering and stateful inspection are the components that are typically associated with firewalls. These technologies allow traffic to be examined to include source, destination, ports, protocol, interface, and state. Firewalls can be used to allow connections to very specific ports on specific destinations from specific sources. This type of control over the network traffic affords considerable transmission security for both ingress and egress. Many times security is focused on external threats to internal resources but it is critical to recognize potential internal risks. All network segments, internal and external, should be initially set to ‘Deny All’ by default and then access granted as necessary [11].

3.2. Wireless Connections

The nature of wireless connections creates an unparalleled flexibility for connectivity with regard to physical location and power sources. Unfortunately the same transmission medium that grants these benefits is inherently insecure due to the inability to restrict where the transmission travels and therefore who can receive or intercept it. While measures are available to minimize wireless vulnerabilities, it should be regarded as an insecure medium and only used for such applications and services that are tolerant to the intrinsic risk. For those wireless access points (WAP) deemed necessary, a process should be established for documenting the location, range, and use of each access point. All wireless communications should be utilizing the 802.11i standard as it is the only wireless encryption method approved by the Federal Information Processing Standards (FIPS) agency [12]. Only known, registered wireless hosts should have direct connectivity to internal network segments. The wireless access points should be on segregated networks similar to a DMZ. The location and placement of wireless access points should minimize the broadcast range of the SSID beyond the physical perimeter of the building and any other unnecessary locations to minimize potential exposure [12].

3.3. Transmission Techniques

Firewalls, network segregation, VPN, NAC, and wireless access all deal with securing access to the transmission medium. The next category of security measures deal with how the data is actually transmitted. Unquestionably the first basic strategy to securing sensitive data during transit is to use encryption. Cryptographic mechanisms are one of the most effective ways of providing security to sensitive data whether at rest or in transit. Many of the security measures recommended by this research employ encryption as a means of providing ePHI data protection. The appropriate encryption algorithm and corresponding strength or level must be evaluated per scenario. In order to ensure HIPAA compliance, the encryption level and type selected should conform to the FIPS and NIST recommendations [13].

Once an encryption algorithm has been selected, a determination must be made about the actual transmission protocol that will be used to send the data. Commercial applications as a rule address many of the transmission security concerns for the application itself and should require little, if any, modification. Typically vulnerabilities related to how ePHI is transmitted arise when data is being sent with a
peripheral application, like Email, or the application being used is a home-grown application [14]. Internally developed applications and processes usually cannot scrutinize security implications to comparable levels of commercial software development companies. As such, it is highly recommended to use commercial applications for all activities involving ePHI transmissions. Hypertext Transfer Protocol (HTTP), Simple Mail Transfer Protocol (SMTP), and File Transfer Protocol (FTP) are the common protocols used to send ePHI data. All of these protocols have the capacity to use both unencrypted and encrypted connections. The HIPAA technical safeguards specifically require all ePHI data to be transmitted using encryption, regardless of the protocol.

Electronic mail (Email) is a very common peripheral applications used by organizational users to transmit ePHI data. While Email was never directly designed to be a transmission vehicle for ePHI, its functionality lends itself to be an easy and convenient option for many users. Sending ePHI data via Email can be secure but it introduces considerable complexity into an organization’s security policies and practices. In order to ensure transmission security using Email, there are 2 basic tactics: policy and technology. Organizations should have policies about how ePHI transmissions should be performed. Data Loss Prevention (DLP) systems can be used to review all email transmissions and proactively take action, regardless of what users do, based on rules set up within the application. Ideally, the solution for most organizations should be a hybrid of both approaches. Users should be trained how to securely send ePHI and when it is appropriate to do so. The DLP system should serve as an oversight and enforcement system to satisfy compliance, liability, and legality concerns. When ePHI is transmitted via Email, digital signatures and encryption should be employed as a data integrity control measure. The DLP system can once again be used to verify encryption and digital signatures are being used as appropriate by the users.

3.4. Intrusion Detection and Prevention Systems (IDPS)

Once the transmission medium has been secured and the method and protocols determined for how to safely move the data, the remaining aspect to address is the actual monitoring of the network for suspicious activities. IDPS’s provide many tools and techniques to monitor and react to intrusion events, detect and mitigate attacks, and provide notification of unauthorized system use. An effective IDPS strategy utilizes both the delivered capabilities of the network devices as well as a stand-alone IDPS application. Monitoring and logging the network traffic and events is a requirement of providing adequate transmission security of ePHI. The monitoring should be able to respond automatically to detected events as appropriate. Logs should be maintained for the appropriate length of time for non-repudiation and protected from alteration and deletion. Knowing what is happening on the network as well as having the ability to research what has happened is a critical component to providing a high degree of transmission security.

3.5. Usability Considerations

There are fundamental approaches to providing security that are effective across almost all environments. However, it is important to acknowledge that before making architectural decisions related to the technical aspects of transmission security, it is imperative that operational needs, functional and financial, be considered. It is easy for the technical staff tasked with the implementation of the HIPAA technical safeguards to lose sight of how the technology will actually be used in practice. If the chosen measures provide the appropriate levels of security but are impractical to utilize, the overall solution is ineffective. Further, in such cases the likelihood of both intentional and accidental misuse as well as circumvention of the organization’s security mechanisms entirely, will increase dramatically.

4. EHR Security Testing

There are considerable challenges to achieving adequate security for all ePHI transmissions in and out of a healthcare organization. Even after an organization feels an acceptable security level has been reached, it is paramount to verify the security measures are functioning as expected. The very first step of any information security test is to define the actual security objectives for the systems to establish an expected performance baseline. This stage can be very beneficial to review documentation, examine policies and procedures, and address any deficiencies. Once the security objectives have been defined, the next step is actually creating a test plan or methodology. An effective information security testing plan is easily repeatable. Repetition often allows many issues to be identified through comparative analysis of prior test results. Having a well documented and repeatable testing plan will also speed up the testing process, yield more consistent results, minimize the testing resources.
needed, and present less risk to the normal business operations of the organization [14].

There are two main testing techniques that this research has focused on with regard to EHR security: target identification and analysis; and target vulnerability validation. The first type of testing focuses on network discovery, port and service identification, and vulnerability scanning. The other group of testing methods includes penetration testing, password cracking, and application security testing. Unfortunately there is no single, comprehensive test that can be used to validate all systems and services. This research has focused on consolidating the collection of necessary testing tools to create a comprehensive set of tests with the minimal amount of overlap. Further, the tests are preconfigured and automated to run consecutively and recursively so the effort to conduct the testing is minimized.

It is recommended that all organizations establish an information security testing environment to become acquainted with the testing tools by running simulations. The testing demonstration environment created during this research is shown in Figure 2. The diagram illustrates the type of servers used, the network configuration, and the placement of the Tester VMs on the various LAN segments. The configuration of each tester VM as it relates to EHR transmission security is listed in Table 1. In order to truly validate adequate security exists for each of the transmission scenarios illustrated in Figure 1, it is crucial the test configurations be equivalent to the actual configurations. After running the tests, the results can be analyzed to determine potential issues and formulate corrective actions based on the guidelines laid out in Section 3. Any systems or processes discovered that are unnecessary or inappropriate can be removed or disabled.

4.1. Target Identification and Analysis

First, the systems on the relevant network segment will be cataloged including information about each system’s operating system (OS), open ports, active services, and patching status. The network discovery can be accomplished using an active scanning tool or passively using a network sniffer. It should be noted that discovery scanning can be fairly intensive and therefore significantly impact the systems it is scanning. Network discovery can also be used to detect unauthorized systems on the scanned network segment. Many IDPS have a form of discovery tool built-in for this very functionality. Scanning should not be limited just to the wired network. There are a number of very effective wireless scanners that collect relevant pieces of information to the wireless network that wouldn’t apply to a traditional wired network. The wireless scanning should include all 802.11
channels, Bluetooth, and a general radio frequency (RF) spectrum analyzer [14]. Some sophisticated wireless scanners having mapping utilities and support Global Positioning System (GPS) mapping. Identified hosts are further examined using a port scanner to see which ports appear open, what services are running on those ports, and what OS the hosts are running. The next step is to perform vulnerability scanning. Vulnerability scanners can identify out of date software, missing patches, misconfigurations, and mitigation suggestions for issues found. The vulnerability scanning effort does have a number of limitations and weaknesses that are important to recognize. First, vulnerability scanning is similar to virus scanning in the sense that it relies on a repository of signatures therefore it can only detect documented issues and requires frequent updating of the repository. Secondly, it tends to have a high false positive error rate and requires a fairly experienced networking and OS security individual to effectively interpret the results. These conditions limit the scanning process since there are significant portions that cannot be automated and are labor intensive. At the conclusion of vulnerability scanning, the first phase of testing will have generated a comprehensive report of all connected systems and pertinent information including OS, active services, and vulnerabilities they possess.

### 4.2. Target Vulnerability Validation

The next stage will continue to search for additional vulnerabilities and demonstrate the risks created when they are exploited. The first type of testing performed is penetration testing. This testing simulates real-world attacks by showing how the system, application, or network will respond to an actual attack. Penetration testing can also help provide information about how to detect an attack, how to appropriately respond, and create effective countermeasures. Unfortunately, penetration testing is very labor intensive, similar to vulnerability scanning. Likewise, it requires someone with considerable skill to perform the testing successfully without damaging the targeted systems. Following penetration testing, a series of password cracking tests should be performed. Password attacks have a couple general approaches: dictionary attacks, brute force, and rainbow table attacks. In most cases, password cracking is performed by obtaining the hash of the actual password then using a variety of approaches to generate a matching hash, thus discovering the actual password. Unlike penetration testing, password cracking can usually be performed offline with little to no impact on the target system, network, or application. The purpose of password cracking is to identify how susceptible password policies are to being compromised. If passwords are determined to be too weak, their entropy can be increased accordingly.

<table>
<thead>
<tr>
<th>VM1 – Ubuntu 11.10</th>
<th><a href="http://www.ubuntu.com/">http://www.ubuntu.com/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Nessus 5.0 – Vulnerability Scanning</td>
<td><a href="http://www.tenable.com/products/nessus">http://www.tenable.com/products/nessus</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VM2 – BackTrack 5 R2</th>
<th><a href="http://www.BackTrack-linux.org/">http://www.BackTrack-linux.org/</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>THC-Hydra – Password Cracking</td>
<td><a href="http://www.thc.org/thc-hydra">http://www.thc.org/thc-hydra</a></td>
</tr>
<tr>
<td>w3af – Web Application Testing (White box, Black box)</td>
<td><a href="http://w3af.sourceforge.net/">http://w3af.sourceforge.net/</a></td>
</tr>
<tr>
<td>NMAP – Network Enumeration and Port Scanning</td>
<td><a href="http://nmap.org">http://nmap.org</a></td>
</tr>
<tr>
<td>Enum4Linux – Windows Enumeration</td>
<td><a href="http://labs.portcullis.co.uk/application/enum4linux/">http://labs.portcullis.co.uk/application/enum4linux/</a></td>
</tr>
<tr>
<td>OneSixtyOne – SNMP Scanning</td>
<td><a href="http://www.phreedom.org/software/onesixtyone/">http://www.phreedom.org/software/onesixtyone/</a></td>
</tr>
<tr>
<td>Bluediving – Bluetooth Penetration Testing</td>
<td><a href="http://bluediving.sourceforge.net/">http://bluediving.sourceforge.net/</a></td>
</tr>
<tr>
<td>SSLScan – Encryption Testing</td>
<td><a href="http://sourceforge.net/">http://sourceforge.net/</a> projects/sslscan/</td>
</tr>
</tbody>
</table>

**Table 1: Security testing VM configurations**

The final type of testing performed is directed specifically at the applications that collect, interact with, or transmit ePHI data. Application testing should involve both **white box** and **black box** approaches. White box testing uses an insider approach with attacks and tests performed assuming a working understanding of how the application works. Black box testing takes the opposite approach as it assumes the attack is external and has no knowledge of the application. Both types of tests and attacks should include injection attacks, data corruption attempts, or attempted misuse of the application outside of published policies and procedures. The vulnerability validation testing phase is used to evaluate systems during actual use. The more realistic the conditions in which the tests are performed, the more beneficial the results of the tests will be to identifying potential risks.

### 5. Research Validation

In order to verify the effectiveness of this research, it was vital that both the EHR transmission security guide and security testing tools be employed in an actual healthcare environment. Using the fully functional testing environment shown in Figure 2, a partnering HIMSS Stage 6 [15] hospital served as the subject for conducting validation of the proposed research. The tester VMs were replicated and
integrated into the hospital’s environment. A battery of tests that simulated ePHI data transmissions were then conducted in the hospital’s test environment. Numerous high and medium level vulnerabilities were identified. The tests involved standalone scans using each tool as well business process testing. While examining each component of an IT environment should be tested individually, it is also important to examine entire processes. Process testing verifies each individual technology component is being used appropriately during normal business practices. It is possible that not all security capabilities of each component are actually employed in practice. Additionally, exceptions may have been ‘built-in’ to processes that circumvent the safeguards the components could normally exert. There were 2 specific business processes that received extra scrutiny during the security testing: authentication into an EHR from a remote physician practice; and entering ePHI into the EHR system from a remote physician practice. The partnering hospital has many physicians that have offsite private practice locations in addition their facilities at the hospital campus. As such, the hospital wants their physicians’ access and functionality to be ubiquitous but uniformly secure.

In the first test case, authenticating into the EHR system remotely, the fundamental control was the credentials required by the EHR system itself. However by modeling the information flow, Figure 3, there were in fact a significant number of other controls present in the transaction that required testing. This scenario simulated a physician connecting to the EHR system using their laptop in their private practice location. The transmission encryption used by the wireless access points (WAP) was the first control mechanism. Using AirCrack, it was quickly determined that many of the WAPs within the physician practice offices were using the WPA encryption scheme. WPA encryption has been repeatedly proven vulnerable to attacks and there are tools readily available to compromise its encryption. The recommendation was to use a FIPS-approved wireless encryption 802.11i standard, such as WPA2. The hospital and remote locations were able to quickly respond to this finding and change all WAPs to use WPA2 encryption, thereby mitigating this risk. The testing then followed the transmission path from the WAP to the main hospital’s network and the next control mechanism - the network firewall. The firewall routed the transmission to the EHR system’s web server, which was located in the hospital’s demilitarized zone (DMZ). Using NMAP and AMAP, it was determined that the firewall was properly segmenting the internal network, which holds the EHR database, from external networks. Further, the firewall was properly routing transmissions to the web server located in the DMZ. This series of tests also verified that the EHR system was properly configured with a 2-tier architecture in which the web server and database server reside on separate physical servers, on segregated network segments. The next control point was the HTTP encryption used by the web servers. The presence and type of SSL ciphers used by the web servers was examined using SSLScan. The tests concluded that
only SSL connections were allowed for HTTP traffic and 1024 bit SSL certificates were being utilized, which is an acceptable level. The transmission of the credentials was then forwarded by the web server to the EHR database for validation. This control point was tested by examining the EHR application, eClinicalWorks, to verify it was indeed accepting valid credentials and rejecting invalid credentials. As part of the credential validation, not only was the username and password pair examined for accuracy, but also integrity checks such as password expiration, prior invalid authentication attempts by the same user, and data/application authorization were performed. Additionally, this control point was tested using THC-Hydra, a password cracking tool, to verify the configured password entropy was acceptable. After running extended tests using THC-Hydra, a number of passwords were compromised thus demonstrating passwords with a weak complexity were present. The organization was able to quickly respond to the finding and implement complexity controls that met the NIST guidelines for password entropy. Another issue discovered that raised special concern was that the EHR system did not differentiate how authentication was managed – directly to the database or within the application. Direct database access should be extremely restricted for administrative activities only. The organization was able to quickly remedy this issue. At this point all controls were satisfied in the information flow and access was granted to the EHR system. Subsequently the HTTP rendering of the EHR application was transmitted back to the user from the web server, following the same transmission path as the inbound request.

![Diagram](image)

Figure 4: Information flow diagram for remote physician editing ePHI

The second test case, Figure 4, was focused specifically on the action of adding, editing, or deleting ePHI from a remote location. This scenario assumed the authentication event had already occurred and the physician has already been granted access to the EHR application. The significant difference between the first and second case is that the data flow in this scenario was inbound instead of outbound. The objectives of the NMAP, AMAP, and SSLScan tests were identical to the first test case, as were the findings and mitigating actions. Different than the first case, this scenario included a series white box and black box tests using w3af. These tests of the web server control point were aimed at discovering flaws in the application’s design that allowed a user to gain unauthorized access to functionality or data within the application. Being a certified EHR application, eClinicalWorks did not have any evident exploits or vulnerabilities. The next control mechanism was the security framework of the application where permissions and authorizations are defined about what data each individual could access and what activities they could perform. These tests consisted of making sure that the actual permissions set up for users and groups matched what was intended. There was also an examination of whether data and functionality access was minimized as much as operationally possible. This analysis discovered numerous cases were users had privileges to view/add/edit/delete data, run reports, and alter application parameters although these abilities were not needed to perform their routine job duties. With these findings, the organization was able to quickly restructure certain security groups within the EHR application to ensure privileges were only granted as necessary for staff to perform their jobs. After the application authorizations were verified, the last control point was within the EHR database. The
database control point verifies the data to be entered is properly formatted and the proper data type. Using the sqlmap tool, the database was tested for unauthorized access, privilege escalation, and data integrity. Once again, being a certified EHR application, eClinicalWorks did not have any evident exploits or vulnerabilities with its database. With the data integrity verified, all controls were satisfied and the data was committed to the EHR database. Some other, less complex business processes were similarly tested. Following these process tests and the individual tool scans, a comprehensive mitigation strategy and implementation plan was submitted to the organization. This plan assisted the partner hospital in implementing the necessary security safeguards required by HIPAA and the Meaningful Use objectives. Ultimately the evaluation and corrective actions allowed the organization to meet the Meaningful Use Stage 1 attestation requirements and become eligible for the program’s incentive payments.

6. Conclusions

The exchange of electronic health records promises the potential for immense benefits for healthcare providers and the individual alike. This ability offers vast possibilities for collaborative and integrated partnerships between healthcare providers and patients. The challenge of ensuring security and privacy is critical to the success of this collaboration. Further, securely transmitting ePHI to patients, other providers, payers, and/or government bodies is required for healthcare providers to meet compliance regulations such as HIPAA and the Meaningful Use objectives. This research provides a comprehensive roadmap for healthcare providers to satisfy these requirements. Additionally the suite of tools and security testing plan facilitates the evaluation and basis for attestation of an organization’s systems. The contributions of this research have been demonstrated at a national healthcare provider. The organization’s security and privacy have been dramatically improved and was ultimately awarded the Meaningful Use Stage 1 certification.

7. References