Privacy and Security Vulnerabilities in Health Care Infrastructure Mobile Technology*

Sajedul Talukder
Department of Mathematics and Computer Science
Edinboro University
Edinboro, PA 16444
stalukder@edinboro.edu

Abstract

Mobile apps and technology provide a great deal of benefits for consumers, while a range of problems in terms of health, usability and risks are often known. Health care companies are gradually seeking to upgrade their aging technologies to meet these concerns by incorporating the use of mobile apps. The proliferation of mobile apps and technologies also provides the company with new challenges and dangers. We find Epic Rover as a test case, a smartphone application described as a potential alternative for the control of electronic medical devices. In this paper, we explore the information that the safety department wants to evaluate and fully analyze the vulnerable situations and risks posed by the usage of mobile apps within the medical community before this new technology is introduced, and propose risk management and mitigation strategies while ensuring compliance with regulatory requirements.

1 Introduction

The intense penetration of mobile devices into our everyday lives has fundamentally changed how we interact with each other in any sector [13, 11, 12, 10, 9, 15]. It also refers to the healthcare sector, in which technology is becoming increasingly relevant in nearly all areas of the industry. The inventing of modern

software applications and digital advances have now allowed patients to view medical records using mobile apps, check up on their main alerts, navigate and organize healthcare, and execute a large variety of activities more conveniently. We consider a safety team including CISO, the technology consultant, Technology Engineer and Chief Enforcement Officer to evaluate a suitable mobile application for a fictional health agency, as well as to assess whether or not its use is worth the risk to that organization.

This paper introduces the Epic Rover [3] mobile app, an innovative app from Epic Systems, one of the leading providers of Health Care Technology, that offers an integrated platform for nearly all areas of healthcare to a reputable collection of mobile applications. By using Epic Rover, we cover the faults and threats related to usage, future regulatory enforcement issues, quality requirements of the industry, prevention approaches and the risk assessment [14, 16], which will decide whether a decision is to implement or ban the use of the handheld medical devices in the enterprise.

Our Contributions: The following contributions are presented in this article:

- **Security Vulnerabilities and Countermeasures**. This paper identifies common security threats and vulnerabilities to EPHI, and, develop and adopt appropriate mitigation to reduce risks and maintain compliance.

- **Qualitative Risk Assessment Matrix**. This paper presents a qualitative risk assessment matrix developed by taking into account potential threats and vulnerabilities, the probability of their occurrence, the potential impact and severity if they were to occur, and the inherent risk by introducing mobile devices.

The rest of the paper is organized as follows. Section II describes the problem definition and motivation. Section III describes the proposed solution through Epic Rover. Section IV presents the vulnerabilities. Section V discusses the risk mitigation and management. Section VI discusses the risk assessment and recommendation. Finally, Section VII concludes the paper with a highlight on the scope of future work.

2 Problem Definition and Motivation

Sunshine Hospital is a hypothetical large metropolitan organization which is in immediate need to update its population of technological devices. The existing technology infrastructure is fairly old and often fails to meet the current standards of health technology, which includes an abundance of Windows Mobile-based MC75s and legacy windows workstations, most of which face end-of-life

by 2020. Moreover, the bulky MC75s and workstations are widely unpopular among the nursing and clinician staff, as most of the old devices have lost their durability and productivity due to excessive wear and tear. The unacceptably slow data transfer rate and poor connectivity have contributed to the rush to look for newer technology, and the urge to adopt mobile devices for day-to-day healthcare activities has been equally heard from the nursing staff and doctors.

We require an app that would allow hospital staff and administrators to provide a more efficient healthcare experience. The app should be able to minimize errors, paper work, and improve efficiency and quality in healthcare management in general. There should be a positive outcome and feedback from the patients as well, as they are the main drivers in our business. Keeping all these factors in mind, our team has worked with the nurses and doctors to find out their expectations and problems with the current technology, allowing us to identify several issues and challenges as we generalized the feedback into a common goal. Furthermore, an equal amount of staff requested a mobile application that was either compatible with an iOS device, or an Android device, depending on their familiarity or level of comfort with the operating system on their own personal devices.
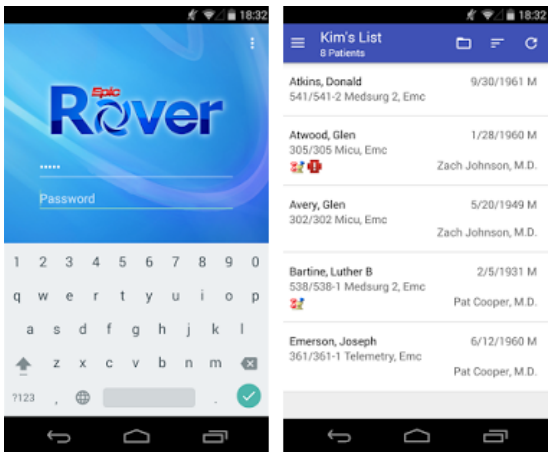

Figure 1: Epic Rover App

3   Proposed Solution – Epic Rover

Considering the requirements mentioned in the previous section, we have identified Epic Rover as the proposed solution to fulfill our company's needs. Epic

Rover is a mobile application developed by Epic Systems that facilitates the validation, monitoring, and documentation tasks for doctors and nursing staff. Because of its availability on both iOS and Android, it can satisfy the demand for both groups of staff. Furthermore, it has already been adopted by several large hospitals, including Texas Children's, Cleveland Clinic, University of Colorado, and Ochsner, making it a more trustworthy solution.

3.1 Basic Design

In order to use Epic Rover, an organization must possess a license to Epic Systems 2014 or later. With Rover, hospital staff can use a device mounted barcode scanner to utilize barcoded medication administration (BCMA) features, which allows nurses to positively identify patients, and give them the proper medication by sending alerts if the wrong medication is attempted to be produced [4]. Furthermore, through the Rover app [2], users have access to Epic's central data repository, which allows them to collect and review a variety of patient data such as charts, clinical summary of lab reports, allergies, medications, immunizations, medical history, and current condition such as vitals, all in real-time, and by simply tapping the patient's name on the device. In addition, through Rover, hospital staff can document and update all patient information directly, and send them directly to the central repository. Clinicians collecting patient specimens can use Rover to update collection workflows, print labels, and document the collection, while nurses can update patients' dosage and medications, and record vitals. Moreover, Rover can find and contact other care providers related to a patient's condition by generating a Care Team Report through secure messaging. These features provide more organization, proficiency, and heightened communication between nurses and other healthcare providers, ultimately improving patient safety.

3.2 Basic security mechanisms

The Epic Rover mobile application implements several basic mechanisms to ensure that electronic health records are securely accessed only by authorized users, and protect the confidentiality, integrity, and availability of patients' personal information. Table 1 depicts Epic Rover's security controls, along with the threats and vulnerabilities that they mitigate:

3.3 Regulatory Compliance

While the adoption of mobile devices for health care applications and management systems could offer a more convenient experience for our staff, it is important to be aware that it also introduces a new set of risks and challenges,

Threats	Vulnerabilities	Security Control
Man-in-the-middle attack	Unencrypted data	TLS/SSL: Supports Transport Layer Security (TLS)/Secure Sockets Layer (SSL) and encryption for communications to ensure that all data is transmitted securely over HTTPS.
Unauthorized access	Lack of proper access controls	Two-factor authentication: Two-factor authentication is embedded into the app, providing stronger access controls. Additionally, it is not possible to access the app from someone else's device, as Epic Rover is assigned to specific devices only. This ensures that, even if someone's credentials are stolen, their account will still be secured as long as they still possess the actual device.
Malicious application sharing data with Epic Rover	Improper implementation of application verification	Signature-based permissions: Ensures that the apps accessing the data among themselves are signed using the same signing key, thus offering a more streamlined and secure user experience.
Code injection attack	Improper input validation	No dynamic code loading: Epic Rover completely runs over native code, meaning it does not load code from outside of the application environment.
Violation of patient's private or confidential information	Inadequate review of privacy policies	Data privacy: Epic Rover states that it does not sell or license any information that it may collect from the user or provider, nor does it store any personal information on the device, or send directly to Epic.

Table 1: Basic security mechanisms

particularly in regards to adhering to Federal Government regulations. As professionals in the Health Care Industry, we are listed as covered entities under the U.S. Department of Health & Human Services' Health Insurance Portability and Accountability Act of 1996 (HIPAA) [5]. By electing to use mobile technologies, we would be required to comply with HIPAA's Security Rule, which mandates a set of standards for covered entities to follow in order to secure the confidentiality, integrity, and availability of Electronic Protected Health Information (EPHI).The standards developed in HIPAA's Security Rule are divided into three sections: Administrative Safeguards, Physical Safeguards, and Technical Safeguards. While the implementations for some standards are required for compliance, others are merely addressable, leaving it up to the organization to determine whether or not it is appropriate to adopt based on their needs. Therefore, it is crucial to have a general understanding and familiarity with the Security Rule standards, so that our organization not only remains compliant, but can also use the standards as a baseline to keep our clients' invaluable information protected, and maintain our reputation as a trustworthy and security-conscious company.

Administrative Safeguards (164.308) The Administrative Safeguards for the HIPAA Security Rule sets forth a list of security measures related to administrative actions, policies, and procedures, to ensure protection of EPHI.

There are a total of nine standards that include security management process, assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency plan, evaluation, business associate contracts and other arrangement.

Physical Safeguards (164.310) The Physical Safeguards for the HIPAA Security Rule sets forth a list of applicable policies and physical measures to protect EPHI from threats such as unauthorized access, and natural disasters. There are a total of four standards that include facility access controls, workstation use, workstation security, device and media controls.

Technical Safeguards (164.312) The Technical Safeguards for the HIPAA Security Rule sets forth a list of security measures related to the use of technology to protect EPHI, and such policies and procedures implemented for access control. There are a total of five standards that include access control, audit controls, integrity, person or entity authentication and transmission security.

Although there are numerous standards to comply with in HIPAA, they provide a straightforward

and effective guideline to helping ensure the confidentiality, integrity, and availability of EPHI, and should be taken seriously. Failure to comply with HIPAA may result in criminal penalties, as specified in the HIPAA Enforcement Rule.

3.4   Industry Standards – NIST

Safeguarding the confidentiality, integrity, and availability of EPHI, while also making sure to comply with HIPAA's Security Rule can be challenging, especially with the inherited risks that the use of mobile technology introduces. Fortunately, there are industry standards available that can be used to facilitate HIPAA compliance, and improve the overall security measures that we have already developed and implemented. While there are a number of standards formulated by different organizations to choose from, the standard we have selected as a guideline to fit our organizations' needs is from the National Institute of Standards and Technology (NIST) [7], which is under the U.S. Department of Commerce. In response to President Obama's Executive Order for Improving Critical Infrastructure Cybersecurity, NIST developed a Cybersecurity Framework [1] that outlines a set of standards, guidelines, and best practices to assist organizations in managing and controlling the risks and threats to cybersecurity. Identified as valuable guidance to improve security programs and aid in HIPAA compliance, the Office of Civil Rights (OCR), which is responsible for auditing and enforcing HIPAA compliance, developed a crosswalk that creates a mapping between the standards listed in the NIST Cybersecurity Framework, and those found in the HIPAA Security Rule. This makes it easier to identify how the Cybersecurity Framework compliments the

Function	Category	Subcategory	HIPAA Control Mapping
Identify	Risk Management: The organization's priorities, constraints, risk tolerance, and assumptions are established and used to support operational risk decisions.	Risk management processes are established, managed, and agreed to by organization stakeholders	164.308(a)(1)(ii)(B) – Risk Management
		Organizational risk tolerance is determined and clearly expressed	164.308(a)(1)(ii)(B) – Risk Management
		The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	164.308(a)(1)(ii)(B) – Risk Management, 164.308(a)(6) (ii) – Response and Reporting, 164.310(a)(2)(i) – Contingency operations
Protect	Protective Technology: Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements	Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	164.308(a)(1)(ii)(D) –Information system activity review, 164.308(a)(5)(ii)(C) – Log-in monitoring, 164.310(a)(2)(iv) – Maintenance records, 164.310(d)(2)(iii) - Accountability, 164.312(b) – Audit controls
		Removable media is protected and its use restricted according to policy	164.308(a)(3)(i) – Workforce security, 164.308(a)(3)(ii)(A) – Authorization/-Supervision, 164.310(d)(1) – Device and media controls, 164.312(a)(1) – Access control, 164.312(a)(2)(iv) – Encryption/Decryption, 164.312(b) – Audit controls
		Access to systems and assets is controlled, incorporating the principle of least functionality	164.308(a)(3) – Assigned security responsibility, 164.308(a)(4) – Information access management, 164.310(a)(2)(iii) – Access control and validation procedures, 164.310(b) – Workstation use, 164.310(c) – Workstation security,
		Communications and control networks are protected	164.308(a)(1)(ii)(D) – Information system activity review, 164.312(a)(1) – Access control, 164.312(b) – Audit controls, 164.312(e) – Transmission security
Detect	Anomalies and Events: Anomalous activity is detected in a timely manner and the potential impact is understood	A baseline of network operations and expected data flows for users and systems is established and managed	164.308(a)(1)(ii)(D) – Information system activity review, 164.312(b) – Audit controls
		Detected events are analyzed to understand attack targets and methods	164.308(6)(i) – Security incident procedures
		Impact of events is determined	164.308(a)(6)(ii) – Response and Reporting
Respond	Mitigation: Activities are promptly performed to prevent further expansion of the event, mitigate the effects caused by the incident, and eradicate it.	Incidents are contained	164.308(a)(6)(ii) – Response and Reporting
		Incidents are mitigated	164.308(a)(6)(ii) – Response and Reporting
		Newly identified vulnerabilities are mitigated or documented as accepted risks	164.308(a)(1)(ii)(A) – Risk analysis 164.308(a)(1)(ii)(B) – Risk management ,
Recover	Communications: Restoration activities are coordinated with internal and external parties	Public relations are managed	164.308(a)(6) (i) – Security Incident Procedures
		Reputation after an event is repaired	164.308(a)(6) (i) – Security Incident Procedures
		Recovery activities are communicated to internal stakeholders and executive and management teams	164.308(a)(6)(ii) – Response and reporting, 164.308(a)(7)(ii)(B) – Disaster Recovery Plan,

Table 2: Correlation of administrative, physical, and technical safeguard in the HIPAA Security Rule to a function from the NIST Cybersecurity Framework.

Security Rule, and also identify gaps in security measures that may not have been met following either standard alone, allowing a more comprehensive and enhanced safeguarding for our organization's EPHI.

One of the key components of the NIST Cybersecurity Framework is the Framework Core, which are comprised of five functions that are essential to cybersecurity management. Each function is divided into categories, which are the desired outcomes of security measures associated with the function. The categories can be further divided into subcategories, which further detail and specify the outcomes related to the security control function. Lastly, each function has an informative reference, which map to sections of existing standards to "illustrate" ways that the outcomes of each function can be implemented. The five functions are listed below:

- **Identify:** Understanding risks and threats to cybersecurity in order to implement appropriate policies and procedures to mitigate them.

- **Protect:** Providing safeguards to prevent systems and assets from being compromised.

- **Detect:** Implementing methods to positively identify when a security event has taken place.

- **Respond:** Executing actions as part of a plan to respond effectively to an identified security event.

- **Recover:** Executing actions as part of a plan to resume normal business operations following a security event.

Table 2 shows OCR's mapping that demonstrates how each administrative, physical, and technical safeguard in the HIPAA Security Rule correlates to a function from the NIST Cybersecurity Framework.

Following the standards, guidelines, and best practices introduced in the NIST Cybersecurity Framework should have a positive impact on our overall security program, and help us to ensure we remain HIPAA compliant as we take into consideration the adoption of mobile devices and technology, and the additional risks that doing so may bring.

3.5 Threats and Attacks

As the use of mobile devices in the healthcare environment is on a continuous rise, so too are the threats against them. There are four categories of malicious attacks to security, which includes interruptions, interceptions, modifications, and fabrications [8, 6]. Below are some of the top identified threats from each category of attack, and how they can negatively affect the security of EPHI.

Vulnerability	Description	Countermeasure
Outdated Software Version and Delay in Patching:	Not patching the OS or software on a regular basis leaves the system in a vulnerable state, and could allow new and identified threats to exploit the system's lack of updates. This increases the system's susceptibility to malware, and can result in the data being compromised.	Automatic updates, policies requiring patching when made available
Insufficient Authorization	Authorization procedures should be specifically defined for users in respect to their role in the organization, their status, and their department, to avoid users who aren't authorized to view personal data gaining access to it.	Two-factor authentication, access control lists, IDS/IPS
Improper use of Device	If a user carries out unacceptable behavior on a device containing EPHI, such as accessing untrustworthy sites, downloading media, or emailing personal information, they may not only put EPHI at risk, but also the network.	Acceptable Use Policy, system logs, training
Connection to Unsecure or Untrusted Network	If there is an incoming and outgoing of data over a network which has not been secured or verified using a trusted certificate, the data is exposed to invalid access and modification, especially without the use of cryptography.	Restrict devices to intranet connection, VPN, firewall, encryption
Jailbreaking	Rooting or jailbreaking a mobile device may leave it open to malicious attacks, as the encryption protection gets bypassed if the app is running on a rooted device.	Acceptable Use Policy, perform regular system test/analysis
Unattended Device	If a device containing EPHI is not properly monitored, it may be accessed or stolen by unauthorized users, exposing personal and confidential data.	Remote wiping, lock inactive devices, monitoring (cameras and logs)

Table 3: Vulnerabilities and Countermeasures

Mobile Ransomware (Interruption): Mobile Ransomware can 'lock out' patient information contained in the device, and then demand a ransom in exchange for restoring access to the data and its availability, usually in the form of Bitcoin to avoid tracking, which affects the availability of systems.

Mobile Spyware (Interception): Mobile spyware is a program that unknowingly gets loaded onto a mobile device and records critical user information, and affects the confidentiality. Having a healthcare app on the same infected device can result in the spyware picking up the login credentials for the app and as a result, unauthorized access to EPHI.

Compromised Servers (Modification): As a host to Epic's central data repository, servers can be a prime target for attackers, who may not only seek to access confidential information, but also modify or delete information contained in the database, affecting the integrity of the EPHI.

Social Engineering (Fabrication): With personal and valuable information contained in a single location, mobile devices containing EPHI would be an attractive target for attackers such as social engineers, who may manipulate unknowing individuals into willingly providing them with access to EPHI, and giving them the opportunity to steal the device itself, making it a serious threat to the assurance of CIA. Examples include phishing, or vishing.

4 Vulnerabilities

Although we have identified common threats, it is only through vulnerabilities that these threats are able to be exploited. According to a security report from Maryland based IT security provider, Arxan Technologies, at least two of the top 10 OWASP (Open Web Application Security Project) vulnerabilities were present in the majority of the mobile health apps that they tested, despite nearly 80 percent of these applications having been approved by the FDA. Thus, we have identified important vulnerabilities that the use of mobile devices in a healthcare environment exposes our organization to, as well as appropriate countermeasures to mitigate them, as depicted in the table 3:

5 Risk Mitigation and Management

After evaluating the threats and vulnerabilities to EPHI, it is imperative to develop and adopt appropriate mitigations to reduce risks and maintain compliance. The following are appropriate mitigations to manage risks, which were recommended by the Department of Health and Human Services for guidance, and involve managing the risks associated with storing, accessing, and transmitting EPHI.

5.1 User Training and Awareness:

Users are identified as the weakest link in security, which increases the risk of a situation leading to compromised EPHI. Therefore, it is essential that the workforce be trained and given clear and concise instructions on the steps that need to be taken in order to follow best practices to avoid any risk to EPHI. This includes:

- Implementing policies to hold regular information and training sessions regarding acceptable use of mobile devices, careful monitoring of devices, and having it enforced.

- Developing password management procedures for changing and safeguarding passwords.

- Maintaining system logs for accountability, and deterring improper use.

				Mitigating Controls				
Potential Threats and Vulnerabilities	Probability of Occurrence (H, M, L)	Potential Impact/Severity (H, M, L)	Inherent Risk Rating (H, M, L)	Administrative	Technical	Physical Security	Residual Risk	Comments
Mobile Malware: Trojans and Viruses	H	H	H	Implement policies requiring anti-virus on all mobile devices containing EPHI	Install a firewall and antivirus software on all devices on network	Monitor devices	M (antivirus must be kept up to date)	Regularly update anti-malware software
Zero-day Vulnerabilities	L	H	M	Implement policies and procedures for regularly testing application	Stay up to date on applying patches	IDS/IPS	M (New risks will always come)	N/A
Log on credentials lost or stolen	M	H	M	Implement policies and procedures for strong passwords, and two-factor authentication	Implement access controls for credentials to expire after a certain amount of time, and requiring long characters with special characters	Lock out device when not in use, use biometrics for authentication and access	M (social engineering can bypass security measures)	Immediately reset passwords that are stolen, or remove permission for users who log-on info is compromised
Brute force attacks	M	H	H	Implement policies to change password every 30 days, and two-factor authentication	Lock at accounts after a certain number of failed login attempts	Lock unattended devices and store in secure location	L (biometrics should decrease risk)	Use logs to monitor log-in attempts
Data modified during transmission	M	H	M	Implement policies to allow devices containing EPHI to only connect to the intranet, and prohibit access to public networks	Transmission through secure channels such as SSL/TSL over HTTPS	Secure wireless access points	M	Set up VPN if remote access is necessary, or allowed
Lost or stolen device	M	H	H	Implement policies requiring encryption for all devices containing EPHI	Allow remote wiping of data for lost or stolen devices	Store devices in secure location, and never leave unattended	M (hospital staff may be careless)	Hold regular training for user awareness
Operating System or Application on Mobile device is outdated	H	H	H	Implement policies requiring updates within 24 hours after notification	Enable automatic updates	Leave notification and reminders	M (The application must be updated)	Train users, and enforce compliance

Table 4: Qualitative Risk Assessment Matrix

- Keeping firmware and apps updated, and applying patches when immediately available.

- Restricting apps on mobile devices that relate to transmission of EPHI over a secure and private network. For example, emails should be sent only over the organization's private email server, and use of apps like Dropbox and Google drive should be discouraged.

5.2 Risk Management for Accessing EPHI

- Implement Two-factor authentication to restrict unauthorized access.

- Implement access controls to categorize users on the basis of their job function in order to restrict access to EPHI to only authorized users.

- Install and update antivirus protection regularly in order to create a secure environment for accessing the data.

- Install firewalls to filter traffic on the network.

5.3 Risk Management for Storing EPHI

- Utilize encryption on mobile devices containing EPHI to protect the confidentiality and integrity.

- Implement locking methods for unattended or inactive devices.

- Maintain backups of EPHI contained on devices.

- Have methods to log activity for accountability.

- Implement procedures to remotely wipe data contained on lost or stolen devices.

5.4 Risk Management for Transmitting EPHI

- Mobile devices containing EPHI should only connect to the organization's intranet, and never connect to public access points.

- Use of non-secure transmission modes such as non-organizational email systems should be prohibited.

- Only the use of secure connections for transmission such as SSL, and the use of message-level standards such as S/MIME, SET, PEM, PGP, should be allowed.

Identifying the risk and applying the appropriate countermeasures and mitigations is an important step in determining how the use of mobile of devices affects our organization's security, and a crucial factor for the final demonstration in our report: the risk assessment.

6   Risk Assessment and Recommendation

Table 4 shows the qualitative risk assessment matrix developed by taking into account potential threats and vulnerabilities, the probability of their occurrence, the potential impact and severity if they were to occur, and the inherent risk by introducing mobile devices. The results of each are rated either (H)igh, (M)edium, or (L)ow. Additionally, administrative, technical, and physical mitigating controls for the risk are also identified, along with the residual risk after applying the controls.

When considering the initial risks and the residual risk levels after implementing security management measures, it is expected that the mitigation controls should reduce the risks to appropriate levels. Thus, after properly identifying and qualifying the potential vulnerabilities and threats, and thoroughly examining the proper countermeasures and safeguards as well, it is our recommendation that our organization adopt the use of mobile devices, as our security team is prepared to address the challenges that the use of mobile devices would bring, and believe that the benefits derived from using the Epic Rover mobile app, along with its security mechanisms already set in place, outweigh the risks.

7   Conclusions

Given certain safety limitations, Amazing Rover implementation with effective counter steps will ease day-to-day activities of healthcare administration and healthcare personnel, while ensuring that the mobile device's EPHI is secure, essential and accessible. According to the NIST Cyber Security Framework, steps to ensure compliance will promote the process of integration of mobile devices into our system and advise us to establish and enforce the appropriate policies and procedures to better secure the EPHI we make, store, view and distribute.

References

[1] Cybersecurity framework.

[2] Epic privacy policies.

[3] Epic rover app.

[4] Epic systems modules.

[5] Hipaa security guidance.

[6] Mobile devices and health information privacy and security.

[7] Nist-security-hipaa-crosswalk.

[8] Y. Cifuentes, L. Beltrán, and L. Ramírez. Analysis of security vulnerabilities for mobile health applications. *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, 9(9):33 – 38, 2015.

[9] S. K. Talukder, M. I. Islam Sakib, and M. M. Rahman. Model for e-government in bangladesh: A unique id based approach. In *2014 International Conference on Informatics, Electronics Vision (ICIEV)*, pages 1–6, May 2014.

[10] Sajedul Talukder. Abusniff: An automated social network abuse detection system. *J. Comput. Sci. Coll.*, 35(3):209–210, October 2019.

[11] Sajedul Talukder. Tools and techniques for malware detection and analysis. *arXiv preprint arXiv:2002.06819*, 2020.

[12] Sajedul Talukder and Bogdan Carbunar. Abusniff: Automatic detection and defenses against abusive facebook friends. In *Twelfth International AAAI Conference on Web and Social Media*, 2018.

[13] Sajedul Talukder and Bogdan Carbunar. A study of friend abuse perception in facebook. *Transactions on Social Computing*, 1(1), 2020.

[14] Sajedul Talukder, Iftekharul Islam Sakib, Faruk Hossen, Zahidur Rahim Talukder, and Shohrab Hossain. Attacks and defenses in mobile ip: Modeling with stochastic game petri net. In *2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC)*, pages 18–23, 2017.

[15] Sajedul Talukder and Zahidur Talukder. A survey on malware detection and analysis tools. *International Journal of Network Security & Its Applications*, 12(2), 2020.

[16] Sajedul Karim Talukder. Detection and prevention of abuse in online social networks. *FIU Electronic Theses and Dissertations. 4026*, 2019.