2020

Systemic Risk Management Plan for Electronic Medical Records (EMR): Why and How?

Ziniya Zahedi

Faisal Mahmud

Cesar Pinto
Old Dominion University

Original Publication Citation

Zahedi, Z., Mahmud, F., & Pinto, C. (2020). Systemic risk management plan for electronic medical records (EMR): Why and how? In *HTI Open Access Collection 2020* (19 pp.). IOS Press https://doi.org/10.3233/SHTI200016

doi:10.3233/SHTI200016

Systemic Risk Management Plan for Electronic Medical Records (EMR): Why and How?

Ms. Ziniya ZAHEDI[a,1,2], Dr. Faisal MAHMUD[b] and Dr. Cesar PINTO[c]
[a]*Business Operations Analyst, Georgetown University Law Center, Washington, DC, USA*
[b]*Senior Instructional Technology Systems Specialist and Assistant Professor, Center for Learning and Teaching, Old Dominion University, Norfolk, Virginia, USA*
[c]*Associate Professor, Engineering Management and Systems Engineering Department, Old Dominion University, Norfolk, Virginia, USA*

Abstract. Electronic patient data use and handling are critical issues in terms of privacy, confidentiality, security, and the Health Insurance Portability and Accountability Act (HIPAA) regulations. The risks associated with electronic patient data are not limited to identity theft but rather include a person's social, economic, and psychological well-being. However, there have not been many studies that have focused on the associated risk factors that could lead to these situations. This paper identifies those risks related to electronic patient data breaches by means of a grounded theory approach and develops a systemic risk management plan that enables engineering managers and risk managers to more effectively and efficiently overcome risks associated with electronic patient data.

Purpose: The purpose of this paper is to identify the risks associated with electronic patient data breach using a grounded theory approach and also to recommend a set of guidelines to support a better, effective, and efficient system and thereby overcome these risks.

Patients and methods: No patients were involved either to participate in this study or any of their opinions are reflected with this research.

Keywords. Electronic medical records (EMR), protected health information (PHI), health insurance portability and accountability act (HIPAA), risks, and systems

Background

The use of electronic medical records (EMRs) has increased significantly over the past few years. An EMR is a health information systems application that provides healthcare providers with patients' medical records, billing information, prescription history, and diagnostic results in a digital rather than paper format [10]. In the health industry and in medical research, EMRs have proven to be a critical source of information for pharmaceutical, diagnostic research, insurance purposes, coding enhancement for medical billing, and understanding overall patient encounter and

[1]Corresponding Author: Ziniya Zahedi, MEM, 600 New Jersey Avenue, N.W., McDonough Hall 583, Washington, D.C. 20001, USA. Tel: (202) 662-9829, Email: ziniya.zahedi@georgetown.edu.

history. Studies have revealed that the EMRs may also contain important information relevant to outcomes, concomitant diseases, procedures, interventions, or test results in observational studies [5]. Public demand for flexible access to health information and services is growing as well, encouraged by internet trends and policies promoting patient rights and empowerment [7]. With the EMR implementation started in the United States around 1990, it was not until 1996 when Health Insurance Portability and Accountability Act (HIPAA) came to fruition to provide data privacy and security provisions for safeguarding medical information. Later, the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, a part of the American Recovery and Reinvestment Act (ARRA) (aka "stimulus package"), was signed into law with an explicit purpose of incentivizing providers (e.g., hospitals and physicians) to adopt EMR (Electronic Medical Record) systems [15].

Despite the policy and associated benefits with EMR, there are still existing risk factors that could lead to data breach resulting in severe consequences for patients' privacy. Some of the widely known recent EMR data breaches from 2018 include North-Carolina based Catawba Valley Medical Center (20,000 data hacked [6]), Gold Coast Health Plan (37,000 data hacked [19]), and Minnesota Department of Human Services (21,000 data hacked [20]). The trend is growing despite various security measures, policies, and regulations. Either in the form of phishing attacks, spam emails, or just by mishandling of electronic records, data breaches nearly always have negative impacts upon patients.

This paper will discuss the current situation of data breaches, then it will propose a systemic risk management plan to deal with the situation and finally, it will demonstrate a sample application of the plan.

Data Breaches

Data breaches in the healthcare industry are outlined by some of the following research questions [2]:

1. What are the common risk factors among healthcare organizations where there have been data breaches?
2. What can be done to mitigate the identified risk factors?
3. What are some common characteristics of those healthcare organizations that have not experienced a data breach?

Certain industries are more susceptible to data breaches [2]. The three industries that are identified as most at risk are financial, healthcare, and technology. Cyber criminals and criminals in general pursue the most lucrative monetary gain. A meta-analysis [2] to formulate the general themes in the case studies identified two key factors- carelessness and negligence. The article concluded that cyber risk was not valued to the healthcare industry as much as it should have been.

The healthcare industry, in general, is more at risk than other industries. Some risk factors are more significant to the healthcare industry. Among those risk factors are [2]: (1) lack of information security awareness training programs for non-IT employees, (2) the absence of access control for server rooms, (3) lack of password standards, (4) lack of data back-up systems, and (5) meager IT/InfoSec budgets. Exhibit 1 [2] below summarizes the causes of data breaches in four different health organizations.

Exhibit 1. Causes for Data Breaches [2].

Healthcare Organization	Cause
Community Health System	Heartbleed Bug, unprotected test server mistakenly connected to the Internet
Advocate Medical Group	Stolen laptops that contained unencrypted PHI
Cogent Health	Transcription service uploaded PHI to an unsecured Google server
Carolinas Medical Center	Undetected email interception

To help with the situation, the healthcare industry is turning towards encryption. The Ponemon Institute's 2016 Global Encryption Trends Study [21] found that using encryption have become more prevalent in healthcare and pharmaceuticals than any other sector with the exception of financial services. Based on a survey of 5,009 individuals across multiple industries in 11 countries, the study determined that, on average, 14 different encryption technologies are used by 49 percent of all health and pharma organizations. Around 50 percent of US healthcare IT pros said their organizations are investing in healthcare data encryption to protect sensitive data, according to a recent survey by network management and security company Infoblox [27].

The risk of medical identity theft to support whether encrypting devices actually reduce the risk of patient data breach has been investigated [17]. There were four sources of data for this empirical analysis: (1) data on security breaches, (2) data on hospitals, (3) data on hospitals' IT systems, and (4) data on state regulation. Studies [17] show that empirical evidence that the use of encryption software does not reduce overall instances of publicized data loss. Instead, its installation is associated with an increase in the likelihood of publicized data loss due to fraud or loss of computer equipment.

If the encryption makes any lost or stolen data useless anyway, then why does it matter if an encrypted software/device is lost? The analysis [17] of the paper showed that losing encrypted data may still harm firms in three ways:

1. First, the loss of encrypted data may not be harmless. When data are encrypted, users generally access the data either via a separate key on a USB drive or a password. Studies support that keys can easily be lost or compromised [9]. This study [9] found that eight percent of organizations (including those who have not had a security breach) have experienced problems with a lost encryption key over the last two years.
2. The adoption of encryption software is associated with an increase in instances of fraud. This emphasizes that encryption software is not always effective at preventing insiders from accessing readable data and using it in a harmful way.
3. There are many instances where firms encrypt some data, but leave other data unencrypted, and also instances where employees de-encrypt data and download it to laptops or other unsecured portable devices.

The empirical findings of this study also suggested that digitization of patient records may increase the likelihood of data breaches. This supports the fact that federal policy encouraging the digitization of patient data, such as the 2009 HITECH Act, also addresses issues of data breaches and patient protection. The authors concluded that

health data security policy may want to focus on ensuring that these kinds of organizational master keys have appropriate protections and safeguards built into the hospital's system. The results suggested that prior to adopting EMRs, hospitals must both address the insider threat and ensure that encryption policies are both systemic and universally applied in reality.

The speculation of the result is that the adoption of encryption software is positively associated with more instances of publicized data losses because it encourages people to be careless, or makes internal data breaches in the form of fraud easier to conduct because of the false sense of security given by the encryption software.

Risk factors for data breach that have been identified from above discussions [2,17] are:

- Carelessness
- Negligence
- Malware attack
- Third party
- Lack of IT knowledge
- Lack of password protection
- Lack of data backup systems

These factors are risky because these make EMR systems vulnerable and hackers can easily access the data. Cyber risk is way different than any other risks out there so the mitigation needs to be very thorough.

History of Data Breaches

Exhibit 2 [29] shows the number of breaches and number of records exposed since 2009. According to HIPAA Journal Statistics (2019), between 2009 and 2018, there have been 2,546 healthcare data breaches involving more than 500 records that have been uploaded to the OCR breach portal. Those breaches have resulted in the theft/exposure of 189,945,874 healthcare records. That equates to more than 59 percent

Exhibit 2. 2018 Healthcare Data Breaches of 500 or More Records [28].

Year	Number of Breaches (500+)	Number of Records Exposed
2018	365	13,236,569
2017	359	5,138,179
2016	327	16,471,765
2015	269	113,267,174
2014	314	12,737,973
2013	278	6,950,118
2012	217	2,808,042
2011	200	13,150,298
2010	199	5,534,276
2009	18	134,773
Total	**2546**	**189,945,874**

of the population of the United States. Healthcare data breaches are now being reported at a rate of more than one per day.

There has been a general upward trend in the number of records exposed each year, with a massive increase in 2015. This was the worst year in history for breached healthcare records with more than 113.27 million records exposed. It should be noted that the three big entities- Anthem Inc., Premera Blue Cross, and Excellus Health Plan – contributed to 88.11% of hacked records in 2015. The best year was 2012 with just 2,808,042 healthcare records exposed. The situation has improved since 2015 with successive falls in the number of exposed records. Although that trend did not continue in 2018. The number of exposed records more than doubled year over year, from 5,138,179 records in 2017 to 13,236,569 records in 2018. (HIPAA Journal, 2019 [28])

The HIPAA Journal (2019) also reports the main Causes of Healthcare Data Breaches in 2018 and the data source for the numbers is the Department of Health and Human Services' Office for Civil Rights (2019). Exhibit 3 below indicates that hacking and insider breaches are the root causes in the healthcare industry.

Exhibit 3. Main Causes of Data Breach.

Main Causes of Breach	2018	2017	2016
Unauthorized Access/Disclosure	143	128	130
Hacking/IT Incident	158	147	113
Theft/Loss	55	73	78
Improper Disposal	11	9	7

Note: One cause of breach in 2016 was not reported.

HIPAA Regulations for Risk Mitigations

According to the study [29] performed by the Ponemon Institute on behalf of IBM Security, the average cost of a data breach is now $3.86 million. The annual rate of increase between 2017 and 2018 was 6.4 percent. The per capita cost of a data breach has risen by 4.8 percent, from $141 per record in 2017 to $148 per record in 2018. Ponemon/IBM analyzed the costs of mega data breaches as well. The average cost of a mega data breach involving one million records is $40 million. That figure rises to an average of $350 million for a breach involving the exposure/theft of 50 million records. The biggest cost of these mega data breaches is loss of customers, typically costing $118 million for a 50-million record breach (HIPAA Journal, 2018).

What exactly is a patient data breach? According to The Health Information Technology for Economic and Clinical Health (HITECH), it is the acquisition, access, use, or disclosure of protected health information (PHI) [19] in a manner not permitted and compromises the security or privacy of the protected health information.

Are there any strict rules regarding privacy and security breach notices? Unfortunately, there are none. A number of states have enacted their own laws requiring business entities to notify the consumers for any such breaches.

The U.S. Department of Health and Human Services rolled out HIPAA Omnibus Final Rule in 2013 to implement major changes in the HITECH Act. The four major risk factors that were pointed out in the HIPAA omnibus rule by the Institute for Health Technology Transformation are:

1. **Evaluate the nature and extent of the PHI involved, including types of identifiers and likelihood of re-identification of the PHI.**
   There are different types of identifiers that need to be evaluated. On the financial side, things like credit card and Social Security numbers and other information may increase risk for identity or credit fraud. On the clinical side, the risk factor requires the covered entity to investigate the information included in the disclosure, such as illness or diagnosis.
2. **Consider the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made.**
   There's an important scenario in terms of if there was an impermissible use or disclosure to another healthcare provider or employee of a covered entity versus a scenario where it was just a random person that didn't have the responsibility to protect PHI.
3. **Consider whether the PHI was actually acquired or viewed, or if only the opportunity existed for the information to be acquired or viewed.**
   If data is lost or stolen or falls into the wrong hands, the unauthorized user must not be able to access the data because it was encrypted and password protected.
4. **Consider the extent to which the risk to the PHI has been mitigated.**
   Was there something that could have been done to mitigate the impermissible use or disclosure?

Systemic Risk Management (SRM) Plan- What to Consider?

Cybersecurity is about more than implementing a checklist of requirements—cybersecurity is managing cyber risks to an ongoing and acceptable level. A systemic cybersecurity program leverages industry standards and best practices to protect systems and detect potential problems. It informs processes of new threats and enables timely response and recovery. Exhibit 4 is an example of a Risk Management (RM) plan that has been customized after thoroughly researching the risks of EMR implementation by analyzing the articles and the HIPAA mitigation plan. The EMR risk management plan could be used by any healthcare organization. The plan explains the steps of how to mitigate the risks of patient data breach by educating the employees and securing the servers.

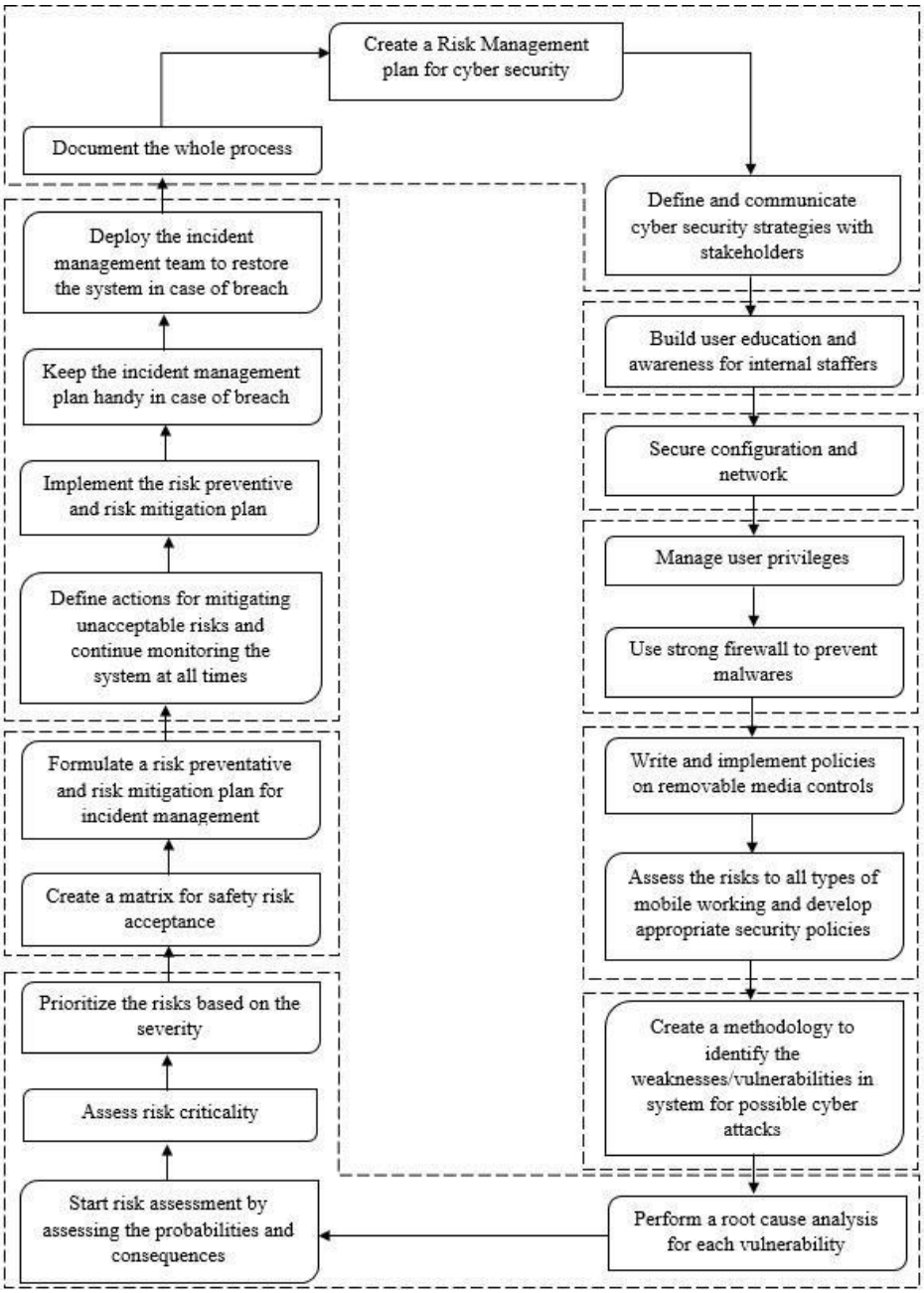
There is a large volume of guidance from organizations such as the National Institute of Standards (NIST), HIPAA Regulations**,** North American Electric Reliability Corporation (NERC), and the Pinto-Garvey framework [20].

Steps:

1. Define and communicate cybersecurity strategies with stakeholders:

Without active sponsorship by executive/top management and a specific role dedicated to ensuring the fulfillment of security goals, instituting security controls is next to impossible. This includes a business framework for setting security objectives and

Exhibit 4. Risk Management Plan for Data Breach.



aligning strategic risk management with business needs, as well as, external statutory and regulatory compliance drivers. Active and visible support from executive management is very necessary at each stage of planning, deploying, and monitoring security efforts.

2. Build user education and awareness for internal staffers:

Produce user security policies that describe acceptable and secure use of the organization's systems. All users should receive regular training on the cyber risks they face as employees and individuals. Security-related roles (such as system administrators, incident management team members, and forensic investigators) will require specialized training. Insufficiently trained personnel and staffers may provide the visibility, knowledge, and opportunity to execute a successful attack without even knowing they are helping. An inadequately trained workforce will not be aware of the policies and procedures necessary to secure organizational information and equipment, resulting in the potential for weaknesses to be exploited. Some of the things they should know about:

- Inserting malicious USB sticks found in the parking lot into machines with access to control systems, which provides attackers with control over the control systems.
- Holding the door for potential attackers carrying a big box entering a "secured premise," allowing them unauthorized access and physical proximity to critical/control systems.
- Surfing restricted sites, which often compromise workstations with bots or worms.
- Failing to respond to someone capturing wireless network traffic on the front lawn or parked in the guest parking lot.
- Being careless with ID badges and credentials that can be leveraged to gain access to critical machines.

This step is ensuring that the security training and awareness program is adequate to address the risks resulting from insecure behavior of employees. Organizations should ensure that all employees undergo security training when hired and at least once a year thereafter. Because of their unawareness and lack of policies, vulnerabilities can also be introduced. Insufficient privacy policies can also lead to unwanted exposure of employee or customer/client personal information, leading to both business risk and security risk. Organizations must ensure that security policies adequately cover all aspects of maintaining a secure environment.

3. Secure configuration and network:

A secure configuration must be adopted, adjusted, and fine-tuned to an organization's particular circumstances and the type of data being protected. Organizations should establish and maintain secure baseline configurations and inventories of IT systems (including hardware, software, firmware, and documentation) and enforce security configuration settings. Introduce corporate policies and processes to develop secure baseline builds and manage the configuration and use of the systems.

Remove or disable unnecessary functionality from network systems and keep them patched against known vulnerabilities. Follow recognized network design principles when configuring perimeter and internal network segments and ensure all network devices are configured to the secure baseline build. Effective testing and ongoing monitoring and evaluation can provide a level of confidence that security controls adequately mitigate perceived risks.

4. Manage user privileges:

Organizations must limit information system access to authorized users. All users of the systems should only be provided with the user privileges that they need to do their job. Control the number of privileged accounts for roles such as system or database administrators and ensure this type of account is not used for high risk or day-to-day user activities. Ensure that employees have access to resources and systems only for the duration that this need exists. Failure to ensure that employee access is revoked when no longer needed may result in unauthorized access.

Classifying data and resources as public, restricted, confidential, or private will help dictate the security control and managing the privileges. Public information is in the public domain and does not require any special protection (e.g.an organization's address or number). Restricted information is generally restricted to all or only some employees. Confidential information protects the privacy of the clients and disclosure of it will have huge negative consequences.

5. Use strong firewall to prevent malwares:

Use technologies like firewalls and virtual local area networks (VLANs) to properly segment the network system in order to increase compartmentalization (e.g., machines with access to business services like electronic mail should not be on the same network segment as your server machines). Routinely review and test your firewall rules to confirm.

6. Write and implement policies on removable media controls:

Produce removable media policies that control the use of removable media for the import and export of information. Organizations must protect itself from the fraud of removable media like USBs or external hard drives. Restrict the media uses completely unless needed. All drives need to be encrypted that have sensitive information. Scan all media for malware using a standalone media scanner before any data is imported into your organization's system.

7. Assess the risks to all types of mobile working and develop appropriate security policies:

Limit remote access to networks to an absolute minimum. When required, use technologies like Virtual Private Networks (VPNs, IPSec) to create a secure tunnel after properly authenticating the connecting party using their individual credentials.

Train mobile users on the secure use of their mobile devices for locations they will be working from. Apply the secure baseline build to all types of mobile device used. Protect data-at-rest using encryption (if the device supports it) and protect data-in-transit using an appropriately configured Virtual Private Network (VPN).

8. Create a methodology to identify the weaknesses/holes/vulnerabilities in system for possible cyber-attacks:

Weaknesses like planning failure, stakeholders' hesitation, privacy and security breach, network breach, financial exposure and delayed ROI and such. Perhaps the most

important is to identify all critical vulnerabilities in physical and cyber components, as well as, in their interdependencies. However, the process will also provide the opportunity to identify and rank key assets, to develop the business case for cybersecurity investment, and to enhance the awareness of all cybersecurity stakeholders.

To locate vulnerabilities, the following steps should be considered:

- Analyzing network architecture
- Assessing threat environment
- Conducting penetration testing
- Assessing physical security
- Conducting physical asset analysis
- Assessing operations security
- Examining policies and procedures
- Conducting impact analysis
- Assessing infrastructure dependencies
- Conducting risk characterization

9. Perform a root cause analysis for each vulnerability:

Electronic security perimeter (ESP) should be defined and protected properly. The access points to each perimeter may include: servers, VPNs, firewalls, routers, and modems. Perform an EMR vulnerability assessment of the access points to each electronic security perimeter at least once a year. The vulnerability assessment should examine ways in which the security perimeter can be breached, and existing security controls bypassed to compromise confidentiality, integrity, or availability of critical cyber assets.

10. Start risk assessment by assessing the probabilities and consequences:

Organizations must periodically assess the risk:

- People and policy security risks
- Operational security risks
- Insecure software development life cycle (SDLC) risks
- Physical security risks
- Third-party relationship risks
- Network security risks
- Platform security risks
- Application security risks

Careful system definitions are essential to the accuracy of vulnerability and risk assessments and to the selection of controls that will provide adequate assurances of cybersecurity. It is important to understand the information that may need to be protected along with their classification (e.g., confidential information, private information, etc.). That way an informed decision can be made.

Realistic assessments of (a) weaknesses in existing security controls and (b) threats and their capabilities create the basis for estimating the likelihood of successful attacks. They also help to prioritize remedial actions.

The risk assessment combines the likelihood of a successful attack with its assessed potential impact on the organization's mission and goals. It helps ensure that mitigation efforts target the highest security risks and that the controls selected are appropriate and cost-effective for the organization. Perform a cyber-vulnerability assessment of the access points to each ESP at least once a year. The vulnerability assessment should examine ways in which the security perimeter can be breached, and existing security controls bypassed to compromise confidentiality, integrity, or availability of critical cyber assets.

11. Assess risk criticality:

An important part of the risk management process is to determine the severity of each risk as a function of its impact and likelihood. Each risk factor needs to be assigned a rating for severity and probability. One risk item will impact several aspects of the project, including cost, time, scope, and quality, which are the key criteria to assess the implementation success.

Therefore, it is more complicated than calculating one single risk score. Although a risk management strategy strives for risk prevention where practical, it also must balance the costs and benefits of security controls. The goal is cost-effective controls that ensure acceptable risk levels.

12. Prioritize the risks based on the severity:

The priority step involves the development of a risk response plan for each of the risk items. Each risk item has its critical date, such as with EMR implementation, where some risk items are approaching, while others are not urgent. The risk team needs to assess all risk items and input them into the risk register.

The risk level, or its severity, is a combination of assessed likelihood and assessed impact. The systems with high impact ratings and those with significant threats and vulnerabilities might currently carry the highest risk to the organization and receive high priority for remediation.

The nature of an impact affects the level of risk the organization is willing to assume. Not all high impact ratings are equal. Impacts could be ranked as follows:

- *Safety*: Causing risk to life and limb.
- *Outage*: Leading to improper operation of a power system device, possibly resulting in a consumer outage.
- *Privacy*: Disclosing private data, such as social security or credit card numbers.
- *Monetary*: Leading to increased tangible costs to the utility.

Once the organization identifies and prioritizes risks and the gaps that exist in current security controls, it is possible to build a prioritized remediation plan that focuses on improving existing security controls or adding security controls to mitigate high-priority risks first, then medium priority, and then low priority (as appropriate).

13. Create a matrix for safety risk acceptance:

Understanding an event's impact allows the organization to make informed decisions about mitigating the risk by some combination of the following:

- Reducing the likelihood of its occurrence
- Detecting an occurrence
- Improving the ability to recover from an occurrence
- Transferring the risk to another entity (e.g., buying insurance)

It is important to apply risk mitigation strategies at each stage in the life cycles of system components and protocols. Questions such as the following can help guide strategy choices:

- Is the risk a compliance issue, a privacy issue, a technical issue, or some other issue?
- Does the mitigation deal primarily with people, process, or technology?
- Is the assessed risk acceptable to the organization?
- Is the cost of fully remediating the risk reasonable?

14. Formulate a risk preventative and risk mitigation plan for incident management:

Establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur. All incident management plans (including disaster recovery and business continuity) should be regularly tested. Some of the steps could be:

- *Developing the recovery planning policy statement.* A formal policy provides the authority and guidance necessary to develop an effective recovery plan.
- *Conducting business impact analysis (BIA).* The BIA helps identify and prioritize information systems and components critical to supporting the organization's business functions.
- *Identifying preventive controls.* Measures taken to reduce the effects of system disruptions can increase system availability and reduce recovery life-cycle costs.
- *Creating recovery strategies.* Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption.
- *Developing an information system recovery plan.* The recovery plan should contain detailed guidance and procedures for restoring a damaged system unique to the system's security impact level and recovery requirements.
- *Ensuring plan testing, training, and exercises.* Testing validates recovery capabilities, training prepares recovery personnel for plan activation, and exercising the plan identifies planning gaps. Combined, the activities improve plan effectiveness and overall organization preparedness.
- *Ensuring plan maintenance.* The plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

15. Define actions for mitigating unacceptable risks and continue monitoring the system at all times:

The organization must develop, implement, and maintain cybersecurity test procedures and tools. Multiple types of testing may be required:

- Conducting compatibility test of personnel awareness and capability.
- Testing the security features and software logic by using manual penetration testing.
- Scanning all media for malware using a standalone media scanner before any data is imported into your organization's system.
- Testing of software security requires static analysis tools.
- All information supplied to or from your organization should be scanned for malicious content.
- Testing of Web applications requires dynamic testing tools.
- Monitoring all ICT systems using Network and Host Intrusion Detection Systems (NIDS/HIDS) and Prevention Systems (NIPS/HIDS).
- Filtering all traffic at the network perimeter so that only traffic required to support your business is allowed and monitor traffic for unusual or malicious incoming and outgoing activity that could indicate an attack (or attempted attack).

16. Implement the risk preventive and risk mitigation plan:

Put all the plans and measurements in place. Make sure all personnel/staffers follow them regularly. To provide assurance that risk mitigation plans are current and would operate as intended during a disruption, they should do regular testing of their business continuity arrangements.

17. Keep the incident management plan handy in case of breach:

Always assume the worst-case scenario and keep the plan handy. The incident response team may need specialist training across a range of technical and non-technical areas. Regularly review, update, and test the plan.

18. Deploy the incident management team to restore the system in case of breach:

Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

19. Document the whole process:

Companies should build detailed incident scenarios and incorporate into the annual development plan the opportunity for key decision makers to use. Steps may include:

- Documenting incident details and response actions
- Collecting lessons learned from incident response
- Updating plan to improve future response.

NIST and Pinto-Garvey Framework

The EMR risk management plan described in Exhibit 4 has a major influence on the NIST and Pinto-Garvey framework [20], yet still have some differences. The EMR risk management plan started from the Pinto-Garvey's basic risk management process that includes risk identification, risk impact assessment, risk prioritization analysis, risk tracking, and risk mitigation. Later it was customized specific for the EMR with many more additional steps that should be followed to manage and mitigate the risks of the EMR field. This specific framework might not work for other fields while the Pinto-Garvey framework could be used in any kinds of field because it does not have a specific association with any areas or fields and works as a skeleton for any fields.

NIST's basic framework also serves as a great starting point that includes the basic steps of identify, protect, detect, respond, and recover. While the main goal and the goal of most of the steps are the same, the core functions are still different from an EMR plan. The EMR framework is not categorized based on the core functions of NIST even though it includes most of the categorical steps. It also did follow some of the IT specific guide from NIST, but NIST's IT RM plan is for cyber risks, which is a broader segment than the EMR field. The cyber field has unlimited users from all over the world while the EMR field has limited end users and only covers the risks at the back end.

The main similarity in all three frameworks is that all frameworks intend to achieve the same goals through management, analysis, mitigation, improvements, and communications. The EMR plan basically started from the Pinto-Garvey framework and captured NIST's guide for IT to become specific.

Sample Application: MedJack25

Based on the proposed risk management plan for data breach, a sample application area is outlined in this section. A medical device hijack, also known as MedJack, is a type of cyber-attack where they target the medical devices of a hospital. Such hijacks may endanger patients by the remote control of critical devices or the theft of sensitive data.

Anatomy of a generic medical device hijack attack (TrapX report [23]):

Stage 1: Attacker researches target, chooses one or more approaches, then targets and executes attacks, penetrating at least once.

Stage 2: Attacker gains foothold in a medical device and cautiously seeks general information and escalation of privileges. Attacker then begins lateral movement.

Stage 3: Attacker continues reconnaissance and identifies targets, moves laterally within networks.

Stage 4: Attacker engages with chosen targets, exfiltrates confidential patient healthcare data and financial records, cleans up the artifacts of attack as best as possible can and leaves.

Stage 5: Attacker leaves a ransomware tool to run in the network to extort funds directly from the healthcare institution.

Based on the above listed anatomy of a generic medical device hijack attack, various steps of the proposed management plan are mapped in Exhibit 5.

Exhibit 5. MedJack stages with mapped steps of the proposed management plan.

Anatomy of a generic MedJack Stages	Mapped steps of the proposed risk management plan for data breach	Description
Stage 1: Attacker researches target, chooses one or more approaches, then targets and executes attacks, penetrating at least once.	Steps 5, 8, 14, and 18.	Strong firewall to prevent malwares would be beneficial so as to identify the vulnerabilities in the system. A risk management plan is handy in case it needs to deploy for a system's breach.
Stage 2: Attacker gains foothold in a medical device and cautiously seeks general information and escalation of privileges. Attacker then begins lateral movement.	Steps 2, 4, 5, 7, 8, 16, and 18.	An awareness and a good management of user privileges is essential. Organizations must limit information system access to authorized users. Strong firewall, limit remote access to networks, identifying all critical vulnerabilities in physical and cyber components are also important. A risk mitigation plan and incident management plan should be handy.
Stage 3: Attacker continues reconnaissance and identifies targets, moves laterally within networks.	Steps 2, 3, 4, 5, 7, 8, 16, and 18.	All users should receive regular training on the cyber risks. A secure configuration must be adopted, adjusted, and fine-tuned to an organization's particular circumstances and information system access to authorized users should be limited. In access to these, a strong firewall implementation, risk mitigation, and incident management plan must be ready at all times.
Stage 4: Attacker engages with chosen targets, exfiltrates confidential patient healthcare data and financial records, cleans up the artifacts of attack as best as possible and leaves.	Steps 11, 16, and 18.	Each risk factor needs to be assigned a rating for severity and probability. Put all the plans and measurements in place to deploy incident management.
Stage 5: Attacker leaves a ransomware tool to run in the network to extort funds directly from the healthcare institution.	Steps 16 and 18.	Implement the risk preventive and risk mitigation plan and deploy incident management plan to ensure the availability of critical information resources and continuity of operations in emergency situations.

On top of the different stages of a generic medical device hijack attack, TrapX recommendation to prevent MedJack incidents are:

1. Isolate and remediate groups of medical devices on the same network. If one medical device gets impacted by cyber attacker activity, it is likely more medical devices are impacted.

2. Make sure your maintenance contracts include responsibility for the remediation of medical devices impacted by cyber threats. The cost for this can be really expensive for small hospitals and health institutions (unless it is explicitly defined in your medical devices' maintenance agreements.)

3. Make sure you review all of your medical devices and understand their vulnerabilities and system life expectations in terms of cyber-defense. It may be simpler to replace some devices than to upgrade their software. Medical devices often have system lives of five to ten years. The cybersecurity industry, however, moves at a much faster pace in response to escalating cyberattacks.

4. Cybersecurity expenses will most likely increase in your security operations budgets. These cyber threats may not have been anticipated five to ten years ago, but here they are. Your budget for cybersecurity will most likely be higher than it was ten years ago.

5. Hire an external contractor to do regular, periodic Red Team reviews of your network security and to independently evaluate your medical devices, servers, and endpoints for active compromises. This also supports your risk assessment for your HIPAA compliance.

6. MSSPs that specialize in healthcare can be a good supplement to your inside team. They can also do the regular and necessary audits.

7. Isolate medical devices to the greatest practical extent, ideally behind their own firewalls in a separate network.

8. Network micro-segmentation can help to restrict lateral movement which emanate from within the medical devices.

9. Identify and utilize a technology designed to provide visibility to attackers that have evaded your firewalls and endpoint security, but have gained residency and access within your network and sit within your medical devices.

Now these recommendations can also be integrated with the proposed risk management plan (Exhibit 6):

Exhibit 6. Prevention of the MedJack incidents with the mapped steps of the proposed management plan.

TrapX recommendation to prevent MedJack incidents	**Mapped steps of the proposed risk management plan for data breach**	**Description**
Isolate and remediate groups of medical devices on the same network	Steps 11, 12, 13 and 18	Each risk factor needs to be assigned a rating for severity and probability. Also, prioritize the risks based on the severity, creating a safety risk acceptance matrix, and deployment of the incident management plan are necessary.
Make sure maintenance contracts include responsibility for the remediation of medical devices impacted by cyber threats	Steps 1 and 19	Active and visible support from executive management is important at each stage of planning, deploying, and monitoring security efforts. Proper documentation of the contracts are essential as well.
Review all of your medical devices and understand their vulnerabilities and system life expectations in terms of cyber-defense	Steps 1 and 2	Stakeholders must be informed in a timely manner for the fulfillment of security goals. User education and awareness for internal staffers are necessary.
Cybersecurity expenses will most likely increase in your security operations budgets	Step 1	A business framework for setting security objectives and aligning strategic risk management is essential for the fulfillment of security goals.

TrapX recommendation to prevent MedJack incidents	Mapped steps of the proposed risk management plan for data breach	Description
Hire an external contractor to do regular, periodic Red Team reviews	Steps 14,15, and 19	Create a risk preventative and risk mitigation plan for incident management by defining actions for mitigating unacceptable risks for the entire risk management plan.
MSSPs that specialize in healthcare can be a good supplement to your inside team	Steps 1 and 2	Stakeholders must be informed in a timely manner for the fulfillment of security goals. User education and awareness for internal staffers are necessary.
Isolate medical devices to the greatest practical extent	Steps 4,11,12,13, and 18	Ensure that employees have access to resources and systems only for the duration that the need exists. Assessing risk criticality, prioritize the severity, creating a safety matrix, and deployment during the breach are necessary.
Network micro-segmentation	Steps 4 and 6	Ensure restrictive access to resources and systems only for the duration that this need exists. Organizations must protect itself from the fraud of removable media like USBs or external hard drives.
Identify and utilize a technology designed to provide visibility to attackers	Steps 13 and 14	Understanding an event's impact allows the organization to make informed decisions. Thus, a risk preventative and risk mitigation plan for incident management are required.

Conclusion

Healthcare organizations are facing the challenge to maintain, update, and safeguard healthcare customers' healthcare records while trying to move paper-based records to EMR. The use of EMRs will better position organizations and providers in a competitive landscape as changes to healthcare continue to evolve. It benefits providers, patients, and the overall economy. But it comes with a fair share of challenges. Maintaining the patient data and safeguarding them in parallel is a huge challenge. Therefore, a risk management plan can save organizations from a massive roadblock and offer a certain level of risk mitigation.

The EMR RM plan has been customized by thoroughly researching any existing plans and simultaneously considering the risks of EMR implementation. It is a sound foundation for any organization thinking to implement EMR. However, it could be improved over time by learning from various situations but at present, it includes the risk mitigation plan for the risks that have been identified over the years by medical researchers and HIPAA. Thus, it can be assumed that if organizations take certain measures to manage risks, then they will be able to achieve all the benefits that are offered by EMR.

Disclosure

The authors report no conflicts of interest in this work.

References

[1] Bates, D.W., Teich, J.M., Lee, J., Seger, D., Kuperman, G.J., Ma'Luf, N., Leape, L. (1999). The Impact of Computerized Physician Order Entry on Medication Error Prevention. *Journal of the American Medical Informatics Association: JAMIA, 6*(4), 313–321.

[2] Barilovich, N. (2016). Data Breach Risk Factors in the Healthcare Industry, Davenport University. Retrieved from https://www.davenport.edu/node/15443.

[3] Bureau of Justice Statistics (2011). Identity Theft Reported by Households, 2005–2010. U.S. Department of Justice, Bureau of Justice Statistics.

[4] Balas, E.A., Weingarten, S., Garb, C.T., Blumenthal, D., Boren, S.A., and Brown, G.D. (2000). Improving Preventive Care by Prompting Physicians. *Archives of Internal Medicine: 160*(3), 301–308.

[5] Call, B. (2013). Indexing electronic medical records using a taxonomy. Proceedings of the 2013 international workshop on Data management & analytics for healthcare – DARE'13. doi:10.1145/2512410.2512423.

[6] Catawba Valley Medical Center Phishing Attack Impacts 20,000 Patients (2018, October 25). Retrieved from https://www.hipaajournal.com/catawba-valley-medical-center-phishing-attack-impacts-20000-patients/.

[7] Cayton, H. (2004). Introduction. In: Better information, better choices, better health London: Department of Health. www.dh.gov.uk/PolicyAndGuidance/PatientChoice/Choice/BetterInformationChoicesHealth/BetterChoicesArticle/fs/en?Content_ID=4123252&chk=/BMoN%2B ClearData. (n.d.). Preventing and Curing Data Breaches in Healthcare: Three Case Studies. Health Data Management. Retrieved from www.healthdatamanagement.com.

[8] Essex, D. (1999). Skip the Song & Dance. *Healthcare Informatics: 16*(7), 49–52, 54–56.

[9] Getgen, K. (2009). 2009 Encryption and Key Management Benchmark Survey. Technical Report. Weston, FL: Thales Group.

[10] HealthIT (2019, March 21). What is an electronic health record (EHR)? Retrieved from https://www.healthit.gov/faq/what-electronic-health-record-ehr.

[11] Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., and Taylor, R. (2005). Can Electronic Medical Record Systems Transform Health Care? Potential Health Benefits, Savings, and Costs. *Health Affairs (Project Hope). 24*(5). 1103–17.

[12] HIMSS Analytics SM Database (formerly the Dorenfest IHDS+TM Database), second release (2004.) http://healthitsecurity.com/news/reviewing-the-hipaa-omnibus-four-data-breach-risk-factors.

[13] Hunt D.L., Haynes R.B., Hanna S.E., and Smith K. (1998). Effects of Computer-based Clinical Decision Support Systems on Physician Performance and Patient Outcomes: A Systematic Review. *The JAMA Network: 280*(15), 1339–46.

[14] Khey, D.N., and Sainato, V.A. (2013). Examining the Correlates and Spatial Distribution of Organizational Data Breaches in the United States. *Security Journal: 26*(4), 367–382. doi: http://dx.doi.org.proxy.davenport.edu/10.1057/sj.2013.24.

[15] Menachemi, N., and Collum, T.H. (2011). Benefits and drawbacks of electronic health record systems. *Risk Management and Healthcare Policy: 4*, 47–55. http://doi.org/10.2147/RMHP.S12985.

[16] McDonald C.J., Hui S.L., Smith D.M., Tierney W.M., Cohen S.J., Weinberger M., and McCabe G.P. (1984). Reminders to physicians from an introspective computer medical record. A two-year randomized trial. *Annals of Internal Medicine: 100*(1), 130–138.

[17] Miller, A.R., and Tucker, C.E. (2011), Encryption and the loss of patient data. J. Pol. Anal. Manage, 30: 534–556. doi:10.1002/pam.20590 (n.d.). Retrieved from https://www.healthit.gov/providers-professionals/electronic-medical-records-emr.

[18] Minnesota DHS Notifies 21,000 Patients That Their PHI Has Potentially Been Compromised (2018, October 15). Retrieved from https://www.hipaajournal.com/minnesota-dhs-21000-patients-phishing-attack/.

[19] PHI of 37,000 Gold Coast Health Plan Members Potentially Compromised (2018, October 09). Retrieved from https://www.hipaajournal.com/phi-of-37000-gold-coast-health-plan-members-potentially-compromised/.

[20] Pinto, C., and Garvey, P.R. (2012). Advanced Risk Analysis in Engineering Enterprise Systems (electronic resource). (Statistics: A Series of Textbooks and Monographs). Hoboken: CRC Press.

[21] Ponemon Institute (2016, March 02). 2016 Global Encryption Trends Study. Retrieved from https://www.ponemon.org/library/2016-global-encryption-trends-study.

[22] Shea, S., DuMouchel, W., and Bahamonde, L. (1996). A Meta-Analysis of 16 Randomized Controlled Trials to Evaluate Computer-Based Clinical Reminder Systems for Preventive Care in the Ambulatory Setting. *Journal of the American Medical Informatics Association: 3*(6), 399–409.

[23] TrapX Research Labs (2018). Retrieved from https://www.trustdimension.com/wp-content/uploads/2015/02/MedJack.4-ilovepdf-compressed.pdf.

[24] Snyder-Halpern, R., Thompson, C.B., and Schaffer, J. (2000). Comparison of mailed vs. Internet applications of the Delphi technique in clinical informatics research. *Proceedings of the AMIA Symposium*, 809–813.
[25] United States Joint Task Force Transformation Initiative (2012). Guide for Conducting Risk Assessments. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology.
[26] Wang, S.J., Middleton, B., Prosser, L.A., Bardon, C.G., Spurr, C.D., Carchidi, P.J., Kittler, A.F., Goldszer, R.C., Fairchild, D.G., Sussman, A.J., Kuperman, G.J., and Bates, D.W. (2003). A Cost-Benefit Analysis of Electronic Medical Record.
[27] Donovan, F. (2018, May 15). Healthcare Data Encryption Used by Half of US Organizations. Retrieved June 12, 2019, from https://healthitsecurity.com/news/healthcare-data-encryption-used-by-half-of-us-organizations.
[28] Retrieved from https://www.infoblox.com/wp-content/uploads/infoblox-report-what-is-lurking-on-your-network.pdf.
[29] HIPAA Journal (2019). Healthcare Data Breach Statistics. Retrieved June 12, 2019, from https://www.hipaajournal.com/healthcare-data-breach-statistics/.
[30] HIPAA Journal (2018, July 12). Healthcare Data Breach Costs Highest of Any Industry at $408 Per Record. Retrieved June 12, 2019, from https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/.