Baseline Security Controls for HIA-Compliant EMR Systems Using a Tailored NIST RMF Approach

Ajay Patel, Pavol Zavarsky, Ron Ruhl, Dale Lindskog

Information Systems Security Department

Concordia University College of Alberta

7128 Ada Boulevard, Edmonton, AB T5B 4E4, Canada

Phone: 1.866.479.5200

Ajayp0025@gmail.com; {pavol.zavarsky, ron.ruhl, dale.lindskog}@concordia.ab.ca

***Abstract*—The proclamation of the *Health Information Act* (HIA) made the Custodian accountable for protecting the confidentiality, integrity, and availability of health information in Alberta, Canada. The health information that a Custodian creates, receives, maintains, or transmits must be protected against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures. The interpretation of the Act is often complicated and time-consuming for Custodians. The Act defines rules at a high level and most of the time, the compliance process can be lengthy and costly for Custodians. To help Custodians to comply with the Act more efficiently and to maintain industry-standard level of the information security of the electronic medical record (EMR) systems, we have developed a catalogue of baseline information security controls. The catalogue of administrative, physical and technical safeguards for the EMR system is based on a tailored Risk Management Framework (RMF) of the NIST. While the effective and efficient compliance with the HIA was the main driving force for the catalogue development, the usefulness of the catalogue is not limited to the compliance with legal regulations. The catalogue of controls is readily applicable as a guideline and a best practice for Custodians also in different jurisdictions.**

***Keywords*— Custodian, Health Information Act, NIST RMF**

I. Introduction

All information systems that deal with health information in Alberta must comply with the HIA. According to the HIA, a Custodian needs to implement reasonable administrative, technical and physical safeguards to protect health information from reasonably anticipated threats to the security or integrity of the health information, including unauthorized access, use, disclosure, modification or destruction. An Electronic Medical Records (EMR) system processes, manages, and stores sensitive information such as patient profiles including medical history, prescriptions, laboratory results, and schedule information. If reasonable security safeguards are not implemented then this could compromise the confidentiality, integrity, and availability of personal health information in an EMR system. The interpretation of the HIA is often complicated and time-consuming for the Custodian; compliance with the Act can therefore be challenging. A baseline security control catalogue will help to facilitate Custodian compliance with the Act.

According to NIST RMF, the first step of the baseline development is security categorization of an EMR system (i.e. low impact, moderate impact, and high impact). The baseline security controls have been developed to facilitate a more consistent, and repeatable approach for managing security for EMR systems. In this research, the baseline security control catalogue is derived for EMR systems which have moderate impact level. The purpose of the baseline security control catalogue is to provide guidelines to Custodians for specifying security controls for EMR systems. We briefly describe the Health Information Act and requirements for EMR systems in the background on the HIA section. In section II, baseline security control approach, we describe fundamental concepts associated with risk management framework to mange security for EMR systems. In section III, baseline security controls establishment, we describe the process of security categorization of EMR systems and developing baseline security control catalogue for EMR systems. We conclude this paper with its applicability and future work.

A. Background on the Health Information Act

Alberta's *Health Information Act* protects an individual's privacy and defines high level controls on access, collection, use, and disclosure of health information. The Act applies to "Custodians" of health information such as Alberta Health Services (AHS), the board of an approved hospital as defined in the *Hospitals Act* [3], health service providers (e.g. physicians, pharmacist, dental surgeons and pharmacists). The Act also extends to "Affiliates" of a Custodian such as employees, agents, volunteers and physicians working in hospitals, clinics or Primary Care Network(s). Health information is defined in section 1(I)(k) of the Act as "diagnostic, treatment and care information"; and "registration information" [1]. As per section 60(1)(a) of the HIA, Custodians affected by the provincially mandated *Health Information Act* regulation are required to implement and maintain administrative, physical, technical safeguards [2]. Under section 60(1)(d), Custodians must ensure that their employees and affiliates comply with the Act.

According to the Act, a Custodian must take reasonable

steps in accordance with the regulations to maintain administrative, technical and physical safeguards. This is typically inferred to mean establishing or adopting polices, processes, practices and technologies intended to protect confidentiality, integrity and availability of health information. Now the question is "what are the reasonable security controls to protect the health information in EMR that are required by the HIA?" The reasonable security controls mainly depend on the criticality of information in the system. The HIA guidelines and practice manual has stipulated administrative, physical and technical safeguard to protect confidentiality, integrity and availability of health information.

II. Baseline Security Controls Approach

The HIA safeguards are all about implementing an effective risk management framework to adequately and effectively protect health information. A significant challenge for Custodians is to determine an appropriate set of effective security controls that adequately mitigate risk and comply with all security requirements defined in the HIA. The selection of security controls can be accomplished as part of an organization-wide information security program that involves the management of organization risk i.e. the risk to information [4]. The management of risk is a crucial point in the organization's security program and provides an effective framework for managing the appropriate security controls for EMR systems.

NIST RMF [7] has been widely utilized by health-related organizations in United States to comply with the Health Insurance Portability and Accountability Act (HIPAA). We used a tailored NIST RMF approach to create a catalogue of security controls for HIA compliant EMR systems. The biggest advantage of the NIST RMF is that every step in the RMF is supported by well defined NIST 800 series standards. The flexible nature of the NIST RMF allows the framework with NIST security guidelines to apply right security controls for the EMR system to adequately protect the confidentiality, integrity and availability of health information [5].

A tailored NIST RMF described in Figure 1, represents an information security life cycle that facilitates continuous monitoring and improvement in the security state of the EMR systems within the organization. In this research, we categorized the EMR system (Step 1 in Fig 1) and developed baseline security controls catalogue (Step 2 in Fig 1) using several NIST 800 special publication guidelines (i.e., NIST 800 60, NIST 800 53). It is expected that the baseline security catalogue will allow Custodians to implement proper security controls more easily and to successfully comply with the Act.

III. Baseline Security Controls Establishment

This section includes the first two steps from a tailored NIST RMF: (i) categorizing the health information in the EMR system and determining the EMR system impact; (ii) developing baseline security catalogue for EMR systems. The creation process is based on potential impact of loss of confidentiality, integrity and availability of health information in EMR systems.

A. Security Categorization of the EMR System

The first step of RMF requires an organization to categorize EMR systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability. The following steps are outlined to determine the overall impact of EMR systems:

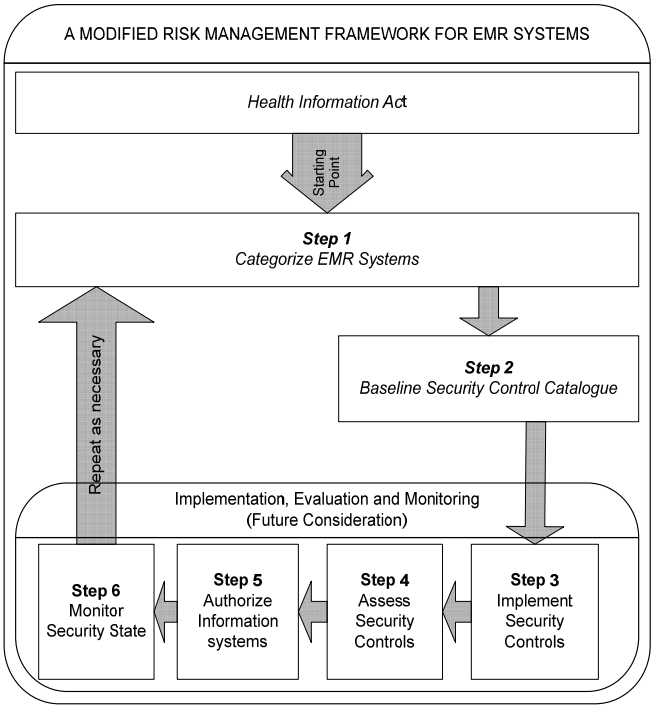

Figure1. A tailored NIST RMF for HIA compliant EMR systems

Step-1A: Determine different types of health information that are collected, processed, and transmitted by EMR systems. According to the HIA section 1(1)(K) health information means one or both of the following: 1) Diagnostic, treatment and care information; 2) Registration information.

1) Diagnostic, treatment and care information means information about any of the following

- The physical and mental health of an individual (HIA section 1(1)(i)(i))
- A health service provided to an individual, including the information respecting a health service provider (i.e., name, business title, profession, license number, etc.) who provides a health service to that individual (HIA section 1(1)(i)(ii))
- The donation by an individual of a body part or bodily substance. Including information derived from the testing or examination of a body part or bodily

substance (HIA section 1(1)(i)(iii))
- A drug provided to an individual (HIA section 1(1)(i)(iv))

2) Registration information means information about any of the following

- Demographic information, including the individual's personal health information (HIA section 1(1)(u)(i))
- Location information (HIA section 1(1)(u)(ii))
- Telecommunication information (HIA section 1(1)(u)(iii))
- Residency information (HIA section 1(1)(u)(iv))
- Health service eligibility information (HIA section 1(1)(u)(v))
- Billing information (HIA section 1(1)(u)(vi))

Step-1B: Categorise the confidentiality, integrity, and availability of each information type as low-impact, moderate-impact, or high-impact. The definitions and examples of high, moderate and low impact are defined in Table 1. The security categorization of health information as follows:

- *Diagnostic, treatment and care information:* Health care organizations provide and support the delivery of health care to individuals. This includes assessing health status; planning health services; ensuring quality of services and continuity of care; and managing clinical information and documentation. The recommended provisional security categorization for health care diagnostic, treatment and care information is as follows:
  Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)} (Please see Appendix B for detail description)
- *Registration information:* Registration information includes that information necessary to ensure that all persons who are potentially entitled to receive any health care/benefit are enumerated and identified so that organizations can have reasonable assurance that they are treat or communicating with the right individuals. The recommended security categorization for the registration information type is as follows:
  Security Category = {(confidentiality, Moderate), (integrity, Moderate), (availability, Low)} (Please see Appendix B for detail description)

Step-1C: To determine overall impact for EMR systems we selected the maximum potential impact values for each security category from registration information, and diagnostic, treatment, and care information. EMR systems categorization is as follow:

Security Category (EMR System) = {(confidentiality, Moderate), (integrity, Moderate), (availability, Moderate)}

Step-1D: The overall impact level of the EMR system is moderate, which is the highest impact level among three security objectives in the above EMR systems security categorization.

TABLE 1
DEFINITION OF LOW, MODERATE, AND HIGH IMPACT [6], [11]

High Impact	
	Definition: Could reasonably be expected to cause a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. **Confidentiality** examples include: 1) information on a police informant or witness protection subject; 2) cabinet confidence. **Integrity** examples include: 1) law enforcement information; 2) extremely large financial transaction transfers. **Availability** examples include: 1) crisis communications during emergencies; 2) essential police communications information.
Moderate Impact	
	Definition: Could reasonably be expected to cause a serious adverse effect on organizational operations, organizational assets, or individuals. **Confidentiality** examples include: 1) compromise of personal medical or health information; 2) information describing personal health issue. **Integrity** examples include: 1) financial transactions and payments for patients; 2) information that could be used for criminal purposes (e.g., false identity or impersonation.). **Availability** examples include: 1) payments of benefits to patients; 2) financial and management information systems.
Low Impact	
	Definition: Could reasonably be expected to cause a limited adverse effect on organizational operations, organizational assets, or individuals. **Confidentiality** examples include: 1) status of a government evaluation of treatment; 2) unauthorized release of the patients' schedule. **Integrity** examples include: 1) information assets relating to administrative information such as volume and type of drug orders; 2) operational procedure assets relating to patients' contact information. **Availability** example include: 1) denial of service resulting in status of schedule not being available.

B. Baseline Security Controls Catalogue

The most significant challenges for the organization are to determine an appropriate set of security controls for the EMR system and to comply with the HIA. The baseline security control catalogue is created to assist organization in making the appropriate selection of security controls for moderate impact EMR systems. If a Custodian categorizes the EMR system as High impact system then some of the controls from the catalogue need to be enhanced. Controls in the baseline security catalogue are a starting point for the appropriate security control selection process. Appendix C summarizes the security controls for moderate impact EMR systems.

Baseline security controls are already tailored for EMR systems. However, an organization can further evaluate using nine NIST 800 53 factors such as common control, scalability, technology, security factor, etc. In most cases, EMR systems are affected by common control and technology

considerations.

These considerations are discussed below:

- *Common control consideration:* Common controls are security controls that are implemented centrally and managed organization wide rather than system specific. When evaluating the security controls for an EMR system, organizations can inherit the control from another existing information system or organization control, thus reducing the cost of re-implementing it for each system. For example, policies and procedures are mostly implemented organization-wide.
- *Technology consideration:* Some baseline security controls are technology dependent. If an EMR system is not utilizing a particular technology, then the security would not apply. For example, T 1.8 in technology controls (refer to Appendix C) defines a security control for wireless access. EMR systems that do not require wireless technology can remove the control.

Due to the specific nature of EMR systems or its environment of operation in organizations, the control in the baseline is not a cost-effective solution to mitigate the identified risk. In that case, organizations may find it necessary to employ compensating controls. A compensating security control is a physical, administrative or technical control employed by an organization instead of a recommended security controls in baseline security catalogue, which provides an equivalent or comparable level of protection for the EMR system.

After all baseline security controls are tailored and un-achievable controls are compensated, organizations may wish to supplement the baseline security controls requirements to achieve additional security for mission specific requirements. Organizations may decide to add more security controls for a number of reasons such as mission, political, or risk tolerance. In most cases, organizations do not require more security controls.

IV. Conclusion and Future Work

This research is expected to provide the clear baseline security controls that can be utilized by Custodians to implement security controls in an EMR system thereby protecting health information adequately and also helping Custodians to achieve compliance with the HIA. These baselines are not presented as a standard but as guidelines for the Custodian to utilize when implementing security controls for EMR systems. It is also anticipated that Custodians in different jurisdictions can also use these baselines and tailor it, as required.

The baseline security controls can be implemented as security requirements for new EMR systems. For new EMR systems, baseline security controls are expected to be incorporated into the system during the development and implementation phase of the System Development Life Cycle (SDLC). In contrast, for existing EMR systems, the baseline security control can be implemented from a gap analysis perspective when the organization is anticipating significant changes to the EMR system such as major upgrades, modification or outsourcing. According to the HIA regulation section 8(3), a Custodian must periodically assess its implemented controls. For future work, implementation, monitoring, and assessment plan (Steps 3, 4, 5, and 6 in Fig 1) can be developed for the organization using various NIST 800 special publication guidelines.

Acknowledgment

This research would not have been possible without the contribution of my research advisors, Dr. Pavol Zavarsky, Dr. Dale Lindskog and Ron Ruhl, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject. I owe my deepest gratitude to Purvi and my family members to support during this process. Lastly, I offer my regards and blessings to all of those who supported me in any respect during the completion of this research.

References

[1] Alberta Queen's Printer, *"Health Information Act (HIA)"*, Nov 2010. [Online]. Available: http://www.qp.alberta.ca/570.cfm?frm_isbn=9780779752607&search_by=link [Accessed Mar. 10, 2011]

[2] Alberta Queen's Printer, "The HIA Guidelines Practices Manual", Feb 2007, pp.6-8. [Online]. Available: http://www.qp.alberta.ca/570.cfm?frm_isbn=9780779721320&search_by=link [Accessed Nov. 1, 2010]

[3] Alberta Queen's Printer, "Hospitals Act", Nov 2010. [Online]. Available: http://www.qp.alberta.ca/574.cfm?page=H12.cfm&leg_type=Acts&isbncln=9780779753604 [Accessed Nov. 25, 2010]

[4] NIST Special Publication 800-66, "an Introductory Resource Guide for Implementing the HIPPA Security Rule", Oct 2008, pp. 6-33. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf [Accessed Oct. 1, 2010]

[5] NIST Special Publication 800-53, revision 3, "Recommended Security Controls for Federal Information Systems and Organizations", Aug 2009. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf [Accessed March. 1, 2011]

[6] The Public Sector CIO Council (PSCIOC), "Public Sector Security Classification Guideline", Sept 2004, pp. 4-6. [Online]. Available: http://www.iccs-isac.org/en/practice/security.htm [Accessed Feb. 1, 2011]

[7] National Institute of Standards and Technology (NIST), "Risk Management Framework", June 2010. [Online]. Available: http://csrc.nist.gov/groups/SMA/fisma/framework.html#footnote4 [Accessed Feb. 1, 2011]

[8] D. Garets and M. Davis, Healthcare Informatics "Electronic Patient Records EMRs and EHRs", October 2005, pp. 1-2. [Online]. Available:

http://www.providersedge.com/ehdocs/ehr_articles/Electronic_Patient_Records-EMRs_and_EHRs.pdf [Accessed Feb. 1, 2010]

[9] NIST Special Publication 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)", April 2010, pp. 4.1-4.7. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf [Accessed Feb. 1, 2010]

[10] NIST Special Publication 800-60, rev 1, Volume 1&2, "Guide for Mapping Types of Information and Information Systems to Security Categories" Aug 2008, pp. 6-33. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf [Accessed April. 1, 2010]

[11] Federal Information Processing Standard (FIPS), 199, "Standards for Security Categorization of Federal Information and Information Systems" Feb 2004. [Online]. Available: http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf [Accessed April. 1, 2010]

APPENDIX A GLOSSARY

Custodian: A "Custodian" is an organization or individual in the health system that receives and uses health information and is responsible for ensuring that it is protected, used and disclosed appropriately. It is defined in HIA section 1(1) (f) [2].

Affiliate: An Affiliate (section 1(1) (1)) is; an individual employed by a Custodian, a person who performs a service for the Custodian as an appointee, volunteer or student or under a contract or agent relationship with the Custodian, and a health services provider who has the right to admit and treat patients at a hospital as defined in the hospital act [2].

EMR: An electronic medical record is usually a computerized legal medical record created in an organization that delivers care, such as a clinic [8].

Administrative safeguard: The formal practice to manage the selection, development, implementation, and maintenance of security controls to protect health information, and to manage the conduct of personnel in relation to protection of information.

Physical Safeguard: The physical protection of Information Technology systems, and related buildings and equipment from fire and other natural hazards, as well as from intrusion.

Technical Safeguard: The protection of information in Information Technology system by technological controls.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and propriety information. A loss of confidentiality is the unauthorized disclosure of information [6].

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system [6].

Integrity: Guarding against improper modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information [6].

APPENDIX B THE SECURITY CATEGORIZATION OF HEALTH INFORMATION

This appendix provides a detail description for security categorization of health information includes: 1) diagnostic, treatment and care information; 2) registration information. We have derived the following recommended impact level based on NIST [11] and PSCIOC [6] guidelines.

1) Diagnostic, treatment and care information

Confidentiality: The confidentiality impact level is the effect of unauthorized disclosure of diagnostic, treatment and care information as it impacts the ability of organizations to support the delivery of health care to individuals. This will have a limited adverse effect on organization operations, assets, or individuals. Information associated with health care involves confidential patient information subject to the HIA. In some cases, unauthorized disclosure of this information such as highly sensitive medical records can have serious consequences for organization operations and individuals.

Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for disclosure of health care delivery services information is moderate.

Integrity: The integrity impact level is based on the specific mission and the data supporting that mission, not on the time required detecting the modification or destruction of information. Many activities associated with health care delivery services are not time critical and the adverse effects of unauthorized modification or destruction of health care information on organization mission functions and/or public confidence in the organization will be limited. However, the consequences of unauthorized modification or destruction of health care information may result in incorrect, inappropriate, or excessively delayed treatment of patients. In these cases, serious adverse effects can include legal actions and danger to human life. However, an EMR contains only a small amount of delivery information which reduces the impact from high to moderate.

Recommended Integrity Impact Level: From EMR perspective, the provisional integrity impact level recommended for health care delivery services information is moderate.

Availability: The availability impact level is based on the specific mission and the data supporting that mission, not on the time required to re-establish diagnostic, treatment, and care information. Except for cases of emergency actions necessary to correct urgent threats to patient health, health care processes are usually tolerant of reasonable delays. Some health care delivery services information is time-critical (e.g.,

Electronic Health Record) information in hospital emergency care unit but not EMR information in small clinic) and is dependent on the severity of the health threat(s) and the rapidity with which the threat is spreading/growing. Delays in the communication of specific situations may be life threatening. This can result in assignment of a high impact level to such information.

Recommended Availability Impact Level: The provisional availability impact level recommended for health care diagnostic, treatment, and care information is moderate.

2) Registration information

Confidentiality: The confidentiality impact level is based on the effects of unauthorized disclosure of registration information and the ability of organizations to determine if communications with individuals are being made to the correct individuals, and to protect individuals against identity theft and against fraud. There are many cases in which unauthorized disclosure of registration information will have only a limited adverse effect on organizations operations, assets, or individuals. However, the potential for use of such information by criminals to perpetrate identity theft and related fraud can do serious harm to individuals.
Recommended Confidentiality Impact Level: The provisional confidentiality impact level recommended for registration information is moderate.

Integrity: The integrity impact level is based on the time required to detect the modification or destruction of information. Unauthorized modification or destruction of registration information can result in inappropriate allocation or deployment of health care services to an individual.
Recommended Integrity Impact Level: The provisional integrity impact level recommended for registration information is moderate.

Availability: The availability impact level is based on the specific mission and the data supporting that mission. It is not based on the time required to re-establish registration information. With the exception of emergency actions which are necessary to correct urgent threats to patient health, health care processes are usually tolerant of reasonable delays. This information can also be received from different entities in emergency.

Recommended Availability Impact Level: From EMR perspective, the provisional availability impact level recommended for registration information is low.

APPENDIX C BASELINE SECURITY CONTROLS CATALOGUE

This appendix provides a summary of the baseline security control catalogue for moderate impact EMR systems. The baseline security controls are categorized in three main sections: i) administrative safeguard; ii) technical safeguard; iii) physical safeguard (NIST moderate baseline controls are grouped by administrative, technical and physical safeguards as per Table 3). However, some of the controls may represent more than one safeguard (e.g., access control represents administrative and technical safeguards). Each safeguard contains several security control families (i.e., policies and procedures, risk assessment, access control). In addition, each security control family contains sub security controls related to the security functionality of the family. A numeric identifier is provided to each security control to identify each security control family. For example, A1- Policy and Procedure is the first control family of Administrative Safeguards and T2- Audit and Accountability is the second control family of Technical Safeguards. Detail description of each control, in security control families, can be found in appendix F (Security Control Catalogue) in NIST SP 800 53 [5] (Recommended Security Controls for Federal Information Systems and Organizations). However, we have described one control from each safeguard to help Custodian to interpret appendix F in NIST 800 53 [5] for detail description of security controls. In this catalogue, each security control has the recommended priority code (i.e. a Priority Code P1 has first priority then a Priory Code P2, shown in Table 2), HIA and its regulation reference, and NIST 800 53 baseline reference for a moderate baseline control. The recommended priority sequence helps organizations to ensure that fundamental controls are implemented first. The priority codes should only be used for implementation sequencing.

Table 2
Priority Sequence for Security Controls [5]

Priority Code	**Sequencing**	**Action**
P1	FIRST	Implement P1 security controls first.
P2	SECOND	Implement P2 security controls after implementation of P1 controls
P3	THIRD	Implement P3 security controls after implementation of P1 and P2 controls.

A. Administrative Safeguards

Administrative safeguards contain ten security control families i.e., policies and procedures, risk assessment, planning, security assessment and authorization, incident response, personnel security, system and service acquisition, awareness and training, contingency planning and configuration management. An example of one control will be used to illustrate interpretation of the control from NIST 800 53 [5] is provided:

Example: A1.1 Policies and Procedures (NIST moderate baseline reference: we consolidate the first control of all control families under A1.1 (The first control of all control families in NIST 800 53 refers to polices and procedures))

Control: The organization develops, disseminates, and reviews/updates [Assignment: organization defined frequency]:

a) A formal, documented security policies that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

b) Formal, documented procedures to facilitate the implementation of the policy and associated security controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the each control family from administrative, technical and physical safeguards. The policy and procedures are consistent with the HIA. Existing organizational policies and procedures make the need for additional specific policies and procedures unnecessary. The security control policy can be included as part of the general information security policy for the organization. Security control procedures can be developed for the security program in general and for a particular EMR system, when required. The organizational risk management strategy is a key factor in the development of the security policy.

B. Technical Safeguards

Technical safeguards contain six security control families i.e., access control, audit and accountability, identification and authentication, system and communication protection, maintenance, and system and information integrity. An example of one control will be used to illustrate interpretation of the control from NIST 800 53 [5] is provided:

Example: T2.1 Auditable Events (NIST moderate baseline reference: AU-2 (3) (4), this control requires additional control enhancements (3) and (4))

Control: The organization:

a) Determines, based on a risk assessment and mission/business needs, that the EMR system must be capable of auditing the following events: [Assignment: organization defined list of auditable events];
b) Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;
c) Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and
d) Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the EMR system: [Assignment: organization defined subset of the auditable events defined in AU-2 a. to be audited along with the frequency of (or situation requiring) auditing for each identified event].

Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the EMR system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the EMR system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems.

Control Enhancements:

(1) Withdrawn
(2) Withdrawn
(3) The organization reviews and updates the list of auditable events [Assignment: organization defined frequency].

Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.

(4) The organization includes execution of privileged functions in the list of events to be audited by the EMR system.

C. Physical Safeguards

Physical safeguards contain two security control families: 1) physical and environmental protection, and 2) media protection. An example of one control will be used to illustrate interpretation of the control from NIST 800 53 [5] is provided:

Example: T1.1 Physical Access Authorizations (NIST moderate baseline reference: PE-2, there is no control enhancement requirement assigned but control enhancement is provided if the organization needs to enhance the control

Control: The organization:

a) Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);
b) Issues authorization credentials;
c) Reviews and approves the access list and authorization credentials [Assignment: organization defined frequency], removing from the access list personnel no longer requiring access.

Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards.

Control Enhancements:

(1) The organization authorizes physical access to the facility where the information system resides based on position or role.
(2) The organization requires two forms of identification to gain access to the facility where the information system resides.

Enhancement Supplemental Guidance: Examples of forms of identification are identification badge, key card, cipher PIN, and biometrics.
(3) The organization restricts physical access to the facility containing an information system that processes classified information to authorized personnel with appropriate clearances and access authorizations.

Table 3: Baseline Security Controls Catalogue

Controls	Priority	HIA and its Regualtion Reference	NIST 800-53 MODERATE Baseline Refrence
Administrative Safeguards			
A1 Policies and Procedures			
A1.1 Policies and Procedures	P1	HIA 63(1), HIA Reg 8(1)	ALL
A2 Risk Assessment			
A2.1 Risk Assessment	P1	HIA 60(2), HIA Reg 8(3)	RA-3
A2.2 Vulnerability Scanning	P1	HIA Reg 8(3)	RA-5 (1)
A3 Planning			
A3.1 System Security Plan	P1	HIA Reg 8(1)	PL-2
A3.2 Rules of Behavior	P1	HIA 107, 62	PL-4
A3.3 Privacy Impact Assessment	P1	HIA 64	PL-5
A4 Security Assessment and Authorization			
A4.1 Security Assessments	P2	HIA 60(1)(d),HIA Reg 8(3)	CA-2 (1)
A4.2 Information System Connections	P1		CA-3
A4.3 Security Authorization	P3	HIA Reg 8(2)	CA-6
A4.4 Continuous Monitoring	P3	HIA Reg 8(2)	CA-7
A5 Incident Response			
A5.1 Incident Response Training	P2	HIA Reg 8(6)	IR-2
A5.2 Incident Handling, Monitoring, Reporting	P1		IR-4 (1), IR-5, IR-6 (1)
A5.3 Incident Response Plan	P1		IR-8
A6 Personnel Security			
A6.1 Position Categorization	P1		PS-2
A6.2 Personnel Screening, Termination, Transfer, and Sanctons	P1	HIA 62(1), HIA Reg 8(7)	PS-3, PS-4, PS-5, PS-8
A6.3 Access Agreements	P3	HIA 62(1)	PS-6
A6.4 Third-Party Personnel Security	P1		PS-7
A7 System and Services Acquisition			
A7.1 Life Cycle Support	P1		SA-3
A7.2 Acquisitions	P1		SA-4 (1) (4)
A7.3 Information System Documentation	P2		SA-5 (1) (3)
A7.4 Software Usage Restrictions	P1		SA-6
A7.5 User-Installed Software	P1		SA-7
A7.6 External Information System Services	P1		SA-9
A7.7 Developer Configuration Management	P1		SA-10
A7.8 Developer Security Testing	P2		SA-11
A8 Awareness and Training			
A8.1 Secuirty Awareness and Training	P1	HIA Reg 8(6)	AT-2 AT-3
A8.2 Security Training Records	P3		AT-4
A9 Contingency Planning			
A9.1 Contigency Plan	P1		CP-2 (1)
A9.2 Contigency Training	P2	HIA Reg 8(6)	CP-3
A9.3 Contingency Plan Testing and Exercises	P2	HIA Reg 8(3)	CP-4 (1)
A9.4 Alternate Storage Site	P1		CP-6 (1) (3)
A9.5 Information System Backup, Recovery and Reconstitution	P1		CP-9 (1), CP-10 (2) (3)
A10 Configuration Management			
A10.1 Baseline Configuration	P1	HIA 60(1)(c)	CM-2 (1) (3) (4)
A10.2 Configuration Change Control	P1		CM-3 (2)
A10.3 Security Impact Analysis	P2		CM-4
A10.4 Access Restrictions for Change	P1		CM-5
A10.5 Least Functionality	P1		CM-7 (1)
A10.6 Information System Component Inventory	P1		CM-8 (1) (5)
A10.7 Configuration Management Plan	P1		CM-9

Table 3: Baseline Security Controls Catalogue (Continued)

Controls		Priority	HIA and its Regualtion Reference	NIST 800-53 MODERATE Baseline Refrence
Technical Safeguards				
T1 Access Control				
T1.1	Account Management	P1	HIA 60(1)(a), HIA 60(1)(c)(ii),HIA Reg 8(3)(c)	AC-2 (1) (2) (3)(4)
T1.2	Access Enforcement	P1	HIA 45, HIA Reg 8(3)(c)	AC-3
T1.3	Separation of Duties	P1		AC-5
T1.4	Least Privilege	P1		AC-6 (1) (2)
T1.5	Unsuccessful Login Attempts	P2		AC-7
T1.6	System Use Notification	P1		AC-8
T1.7	Remote Access	P1	HIA 60(1)(a),HIA 60(1)(c)(ii)	AC-17 (1) (2) (3) (4) (5) (7) (8)
T1.8	Wireless Access	P1	HIA 60(1)(a),HIA 60(1)(c)(ii)	AC-18 (1)
T1.9	Access Control For Mobile Devices	P1	HIA 60(1)(a),HIA 60(1)(c)(ii)	AC-19 (1) (2) (3)
T2 Audit and Accountability				
T2.1	Auditable Events	P1	HIA 62(4)	AU-2 (3) (4)
T2.2	Content of Audit Records	P1		AU-3 (1)
T2.3	Audit Storage Capacity	P1		AU-4
T2.4	Response to Audit Processing Failures	P1		AU-5
T2.5	Audit Review, Analysis, and Reporting	P1	HIA 62(4)	AU-6
T2.6	Time Stamps	P1		AU-8 (1)
T2.7	Protection of Audit Information	P1	HIA 61	AU-9
T2.8	Audit Record Retention	P3	HIA 56.6(1)	AU-11
T2.9	Audit Generation	P1		AU-12
T3 Identification and Authentication				
T3.1	Identification and Authentication	P1	HIA 45	IA-2 (1) (2) (3) (8)
T3.2	Device Identification and Authentication	P1		IA-3
T3.3	Identifier Management	P1		IA-4
T3.4	Authenticator Management	P1		IA-5 (1) (2) (3)
T3.5	Authenticator Feedback	P1		IA-6
T3.6	Cryptographic Module Authentication	P1		IA-7
T4 System and Communications Protection				
T4.1	Application Partitioning	P1		SC-2
T4.2	Denial of Service Protection	P1		SC-5
T4.3	Boundary Protection	P1		SC-7 (1) (2) (3) (4) (5) (7)
T4.4	Transmission Integrity	P1	HIA 61	SC-8 (1)
T4.5	Transmission Confidentiality	P1		SC-9 (1)
T4.6	Network Disconnect	P2		SC-10
T4.7	Cryptographic Key Establishment and Management	P1	HIA 61	SC-12
T4.8	Use of Cryptography	P1	HIA 61	SC-13
T4.9	Public Key Infrastrcuture Certificates	P1		SC-17
T4.10	Mobile Code	P1		SC-18
T4.11	Secure Name /Address Resolution Service (Authoritative Source	P1		SC-20 (1)
T4.12	Architecture and Provisioning for Name/Address Resolution Ser	P1		SC-22
T4.13	Session Authenticity	P1		SC-23
T4.14	Protection of Information at Rest	P1	HIA 61	SC-28
T5 Maintenance				
T5.1	Controlled Maintenance	P2		MA-2 (1)
T5.2	Maintenance Tools	P2		MA-3 (1) (2)
T5.3	Non-Local Maintenance	P1		MA-4 (1) (2)
T5.4	Maintenance Personnel	P1		MA-5
T6 System and Information Integrity				
T6.1	Flaw Remediation	P1		SI-2 (2)
T6.2	Malicious Code Protection	P1	HIA 60(1)(c),HIA 61	SI-3 (1) (2) (3)
T6.3	Information System Monitoring	P1	HIA Reg 8(3)	SI-4 (2) (4) (5) (6)
T6.4	Security Alerts, Advisories, and Directives	P1		SI-5
T6.5	Software and Information Integrity	P1	HIA 60(1)(c), HIA 61	SI-7 (1)
T6.6	Spam Protection	P1	HIA 60(1)(c), HIA 61	SI-8
T6.7	Information Input Restrictions	P2		SI-9
T6.8	Information Input Validation	P1		SI-10
T6.9	Error Handling	P2		SI-11
T6.10	Information Output Handling and Retention	P2		SI-12

Table 3: Baseline Security Controls Catalogue (Continued)

Controls		Priority	HIA and its Regualtion Reference	NIST 800-53 MODERATE Baseline Refrence
Physical safeguards				
P1 Physical and Environmental Protection				
P1.1	Physical Access Authorizations	P1		PE-2
P1.2	Physical Access Control	P1	HIA 63(1)(c)	PE-3
P1.3	Access Control for Transmission Medium	P1		PE-4
P1.4	Access Control for Output Devices	P1		PE-5
P1.5	Monitoring Physical Access	P1	HIA Reg 8(3)	PE-6 (1)
P1.6	Visitor Control	P1		PE-7 (1)
P1.7	Access Records	P3		PE-8
P1.8	Power Equipment and Power Cabling	P1		PE-9
P1.9	Emergency Shutoff, Power, and Lighting	P1		PE-10, PE-11, PE-12
P1.10	Fire Protection	P1		PE-13 (1) (2) (3)
P1.11	Temperature and Humidity Controls	P1		PE-14
P1.12	Water Damage Protection	P1		PE-15
P1.13	Delivery and Removal	P1		PE-16
P1.14	Location of Information System Components	P2		PE-18
P2 Media Protection				
P2.1	Media Access	P1	HIA 63(1)(c)	MP-2 (1)
P2.2	Media Marking	P1		MP-3
P2.3	Media Storage	P1	HIA 63(1)(c)	MP-4
P2.4	Media Transport	P1		MP-5 (2) (4)
P2.5	Media Sanitization	P1		MP-6