Universidade Estadual de Campinas

Instituto de Computação

LUIZ APARECIDO VIRGINIO JUNIOR

Addressing Patient Safety in Healthcare: The Health Information Technology Safety Maturity Model

Abordando a Segurança do Paciente: O Modelo de Maturidade de Segurança da Tecnologia da Informação em Saúde

CAMPINAS

2024

LUIZ APARECIDO VIRGINIO JUNIOR

ADDRESSING PATIENT SAFETY IN HEALTHCARE: THE HEALTH INFORMATION TECHNOLOGY SAFETY MATURITY MODEL

ABORDANDO A SEGURANÇA DO PACIENTE: O MODELO DE MATURIDADE DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO EM SAÚDE

Tese apresentada ao Instituto de Computação da Universidade Estadual de Campinas como parte dos requisitos para a obtenção do título de Doutor em Ciência da Computação.

Thesis presented to the Institute of Computing of the University of Campinas in partial fulfillment of the requirements for the degree of doctor in Computer Science.

SUPERVISOR: PROF. DR. JÚLIO CÉSAR DOS REIS

ESTE TRABALHO CORRESPONDE À VERSÃO FINAL DA TESE DEFENDIDA PELO ALUNO LUIZ APARECIDO VIRGINIO JUNIOR, E ORIENTADO PELO PROF. DR. JÚLIO CÉSAR DOS REIS.

CAMPINAS

2024

Ficha catalográfica
Universidade Estadual de Campinas (UNICAMP)
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

V819a

Virginio Junior, Luiz Aparecido, 1990-
Addressing patient safety in healthcare : the health information technology safety maturity model / Luiz Aparecido Virginio Junior. – Campinas, SP : [s.n.], 2024.

Orientador: Julio Cesar dos Reis.
Tese (doutorado) – Universidade Estadual de Campinas (UNICAMP), Instituto de Computação.

1. Segurança do paciente. 2. Tecnologia da informação. 3. Modelo de maturidade. I. Reis, Julio Cesar dos, 1987-. II. Universidade Estadual de Campinas (UNICAMP). Instituto de Computação. III. Título.

Informações Complementares

Título em outro idioma: Abordando a segurança do paciente : o modelo de maturidade de segurança da tecnologia da informação em saúde
Palavras-chave em inglês:
Patient safety
Information technology
Maturity model
Área de concentração: Ciência da Computação
Titulação: Doutor em Ciência da Computação
Banca examinadora:
Julio Cesar dos Reis [Orientador]
Magdala de Araujo Novaes
Renato Marcos Endrizzi Sabbatini
Juliana Pereira de Souza Zinader
Ivan Luiz Marques Ricarte
Data de defesa: 27-05-2024
Programa de Pós-Graduação: Ciência da Computação

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0002-5282-7451
- Currículo Lattes do autor: http://lattes.cnpq.br/5099377750492072

University of Campinas

Institute of Computing

LUIZ APARECIDO VIRGINIO JUNIOR

Addressing Patient Safety in Healthcare: The Health Information Technology Safety Maturity Model

Abordando a Segurança do Paciente: O Modelo de Maturidade de Segurança da Tecnologia da Informação em Saúde

Banca Examinadora:

- Prof. Dr. Julio Cesar dos Reis
  Instituto de Computação / Universidade Estadual de Campinas
- Profa. Dra. Magdala de Araujo Novaes
  Núcleo de Telesaúde / Universidade Federal de Pernambuco
- Profa. Dra. Juliana Pereira de Souza Zinader
  Instituto de Informática / Universidade Federal de Goiás
- Prof. Dr. Renato Marcos Endrizzi Sabbatini
  Faculdade de Ciências Médicas / Universidade Estadual de Campinas
- Prof. Dr. Ivan Luiz Marques Ricarte
  Faculdade de Tecnologia / Universidade Estadual de Campinas

A Ata da defesa com as respectivas assinaturas dos membros encontra-se no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria do Programa da Unidade.

Campinas, 27 de maio de 2024

ACKNOWLEDGMENTS

I would like to thank my advisor for his dedication throughout the development of this Ph.D. thesis.

I would also like to thank the collaborators of the process of validating HITSMM: Dr. Claudio Giuliano Alves da Costa, Isabel Maria de Jesus Simão, Ana Carolina de Alencar Cavalcanti Sa, Paula de Brito Gonçalves, and Leandro Miranda.

I am grateful for the valuable partnership of FOLKS in this study.

I extend my sincere gratitude to the participants from the two hospitals involved in the HITSMM application. Their collaboration was instrumental in the success of this study.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001.

This study was financed in part by The Brazilian National Council for Scientific and Technological Development (CNPq), grant #142016/2019-5.

RESUMO

As Tecnologias de Informação em Saúde podem levar a consequências indesejadas para as partes interessadas quando as organizações de saúde os desenvolvem, usam ou implementam inadequadamente. Neste contexto, a literatura carece de modelos abrangentes que abordem a Tecnologia da Informação (TI) em Saúde e a segurança do paciente. Estudos existentes demonstraram que o Electronic Medical Record Adoption Model (EMRAM), Joint Commission International (JCI) accreditation program and Safety Assurance Factors for Electronic Health Records (EHR) Resilience (SAFER) Guides podem ser usados de forma complementar para ajudar as organizações de saúde a aumentarem a segurança da TI em saúde. Esta tese de doutorado desenvolve o inovador Modelo de Maturidade de Segurança de TI em Saúde (HITSMM), que é um modelo de maturidade composto por uma lista abrangente de requisitos resultantes da combinação adequada e sistemática das avaliações de EMRAM, JCI e SAFER Guides. Esta pesquisa compreendeu três fases principais: (1) Mapeamento de Requisitos, (2) Desenvolvimento do HITSMM e (3) Aplicação e Avaliação do HITSMM. Na primeira fase, desenvolvemos originalmente dois mapeamentos abrangentes: um alinhando os padrões JCI com a estrutura EMRAM e outro mapeando o EMRAM para os SAFER Guides. Esses mapeamentos foram usados para sustentar o desenvolvimento do HITSMM. Para tanto, nosso estudo realizou as seguintes atividades: análise de requisitos, remoção de duplicatas, agrupamento de requisitos, definição de categorias, definição de estágios de maturidade e avaliação por especialistas do domínio. O HITSMM é composto por 138 requisitos agrupados em doze categorias e sete estágios. Os requisitos são cumulativos ao longo dos estágios. Este estudo conduziu uma aplicação e avaliação em um estudo de caso do mundo real do HITSMM em dois hospitais brasileiros de destaque. Concluímos que a organização e os requisitos codificados pelo HITSMM abordam aspectos relevantes da segurança do paciente relacionados à TI em Saúde especificados pela JCI, EMRAM e SAFER Guides. As organizações de saúde podem usar o HITSMM como um guia para melhorar continuamente a segurança do paciente relacionada à TI em Saúde.

ABSTRACT

Health Information Technology can lead to unintended consequences for stakeholders when healthcare organizations improperly develop, use, or implement them. In this context, the literature lacks comprehensive models addressing Health Information Technology (IT) and patient safety. Existing studies have shown that the Electronic Medical Record Adoption Model (EMRAM), Joint Commission International (JCI) accreditation program, and Safety Assurance Factors for Electronic Health Records (EHR) Resilience (SAFER) Guides can be used in a complementary way to help healthcare organizations to increase Health IT safety. This Ph.D. thesis develops the novel Health IT Safety Maturity Model (HITSMM), which is a maturity model composed of a comprehensive list of requirements resulting from the proper and systematic combination of EMRAM, JCI, and SAFER Guides evaluations. This research comprised three main phases: (1) Mapping Requirements, (2) HITSMM Development, and (3) HITSMM Application and Evaluation. In the first phase, we originally developed two comprehensive mappings: one aligning the JCI standards with the EMRAM framework and another mapping EMRAM to the SAFER Guides. These mappings were used to sustain the development of HITSMM. For this purpose, our study performed the following activities: requirement analysis, duplicate removal, requirements grouping, definition of categories, definition of maturity stages, and evaluation by domain specialists. The HITSMM is composed of 138 requirements grouped into twelve categories and seven stages. The requirements are cumulative over the stages. This Ph.D. thesis conducted an application and evaluation in a real-world concept proof of HITSMM in two prominent Brazilian hospitals. We found that the organization and requirements encoded by HITSMM address relevant aspects of patient safety related to Health IT specified by JCI, EMRAM, and SAFER Guides. Healthcare organizations can use HITSMM as a guide to improve patient safety related to Health IT continuously.

LIST OF FIGURES

LIST OF TABLES

CONTENTS

Chapter 1
Introduction

1.1 Context and Motivation

Healthcare organizations face important challenges to achieve and maintain a high level of quality of their clinical, operational and financial processes. There are strong expectations that the use of Health Information Technology (Health IT), such as Electronic Health Records (EHR), can present positive impacts on healthcare quality and efficiency [1]. However, the implementation of Health IT without adequate strategic and organizational processes may not necessarily generate the expected benefits and those technologies may lead to unintended consequences when improperly developed, used or implemented [2-6]. Studies shows that Health IT has been associated with prescribing errors, wrong medication administration, tests assigned to wrong patients, and missing tests results [6-8].

Documented cases highlight the potential safety risks associated with S-RES. In 2007, a network configuration maintenance error at the Department of Veterans Affairs (VA) rendered the EHR of several facilities inaccessible for over nine hours. This critical outage forced healthcare providers to conduct consultations without access to patient records and postpone surgeries due to the unavailability of essential documentation. These incidents underscore the need for robust S-RES systems and rigorous maintenance procedures to safeguard patient safety [4].

A review of the Food and Drug Administration's (FDA) Adverse Event Reporting System (FAERS) in the United States identified serious safety concerns related to the use of EHRs. Incidents such as data loss or corruption, presentation of incorrect patient information, and system unavailability led to problems like delays in diagnosis or treatment, medication errors, and even death. These cases highlight the need for robust measures to ensure the safety and reliability of EHRs to protect patient health [2].

The growing adoption of EHR in the healthcare settings has motivated hospital accreditations bodies to include technology aspects in their requirements. The Joint Commission International (JCI), an American accreditation body of healthcare

organizations, has included a set of requirements dedicated to information management, which contains requirements specifically related to Health Information Technology (Heath IT).

The SAFER Guides is a set of guides with recommended practices related to safety and safe use of EHRs [9]. It was designed to be a self-assessment to healthcare organizations. The recommended practices are organized in three domains: Safe Health IT, Using Health IT Safely, and Monitoring Safety. HIMSS Analytics developed the Electronic Medical Record Adoption Model (EMRAM) which is composed by eight maturity stages (from zero to seven). The goal of EMRAM is to measure the adoption and utilization of EHR functions in hospitals, focusing specially on patient safety, patient satisfaction, information security and clinician support[1].

A maturity model is composed of stages that represent maturity levels of an entity (organizations, functional areas, processes, etc.) in which high stages represent high maturities. Therefore, the goal of a maturity model is to provide orientation through an evolutionary process and to serve as a roadmap to achieve a high maturity level [10].

To rationalize and manage the transition process successfully, the growing digitalization of healthcare services demands well defined rules and success reports. Numerous maturity evaluation and maturity models have been suggested and used in the sector as a solution to these difficulties [11].

1.2 Research Problem and Challenges

The growing complexity of healthcare, with its intertwined processes, people, and technology, presents challenges in managing the digital transformation effectively. To navigate this transition smoothly, clear guidelines and proven methods are crucial. While a variety of maturity models related to Health IT have been proposed, there is a need for further research, particularly regarding patient safety.

[1] https://www.himss.org/what-we-do-solutions/digital-health-transformation/maturity-models/electronic-medical-record-adoption-model-emram

Maturity models that address safe Health IT lack the comprehensiveness and detail necessary to effectively evaluate patient safety. In essence, no current model is sufficiently robust to fully assess EHR maturity in relation to patient safety [11]. Therefore, the development of approaches and methodologies that encompass and organize various aspects and requirements for evaluating patient safety within Health IT is critical.

A significant challenge lies in balancing the potential benefits of health IT for patient safety with the risks that can arise from its implementation and use. While Clinical Decision Support (CDS) alerts embedded in Computerized Provider Oder Entry (CPOE) systems can serve as safety barriers, they can also lead to alert fatigue and missed critical information if not designed and implemented thoughtfully [3].

Similarly, usability issues in EHRs can lead to medication errors, such as selecting the wrong medication due to a poorly designed interface [3]. These risks highlight the need for models and methods that not only consider how technology can enhance patient safety but also how technology should be developed, implemented, and used to avoid introducing new hazards.

The complexity of healthcare systems extends beyond the technology itself. To truly ensure patient safety, models must account for the interactions between technology and other critical components, such as people, processes, and organizational policies [5, 6].

Human factors play a significant role in the safe use of health IT. Healthcare professionals must be adequately trained and supported to effectively utilize these systems, minimizing the risk of errors. Well-defined processes and procedures are essential to guide the implementation and use of health IT, ensuring consistency and reducing the potential for deviations that could compromise patient safety.

Organizational policies, including governance structures, leadership commitment, and resource allocation, shape the overall safety culture within healthcare institutions. These policies must align with the implementation of health IT to create an environment that prioritizes patient safety and fosters continuous improvement.

Developing specific models that effectively address both the benefits and risks of health IT is crucial to ensuring the safety of patients. These models must go beyond

simply assessing the technical aspects of technology and delve into the intricate interplay of technology, people, processes, and organizational policies.

1.3 Research Goals and Overall Methodology

This Ph.D. thesis aims to develop the Health IT Safety Maturity Model (HITSMM), which is a maturity model of seven stages that provides a comprehensive list of good practices requirements to promote the safe development, implementation, and use of Health IT in hospital settings. Our solution must cope with the need of developing specific models that address patient safety regarding information technology. To the best of our knowledge, there is no maturity model in literature focused on this domain. This Ph.D. thesis investigate the following key Research Questions (RQ):

- RQ1: How existing models can be comparatively evaluated to identify strengths, weaknesses, and potential for integration?
- RQ2: Does HITSMM lead to a more specific maturity model to assess Health IT and patient safety better than using existing models individually?
- RQ3: How valid is the HITSMM in identifying and measuring the maturity level of healthcare organizations regarding Health IT safety practices?

To answer RQ1, we selected and compared three important existing models that have been used in healthcare industry worldwide to assess Health IT and patient safety. The goal was to identify their strengths and weaknesses in relation to their comprehensiveness in evaluating the safe use of Health IT and the use of information technology to improve patient safety.

This Ph.D. thesis hypothesizes the use of maturity models as the most suitable framework structure to help healthcare organizations to improve their processes in an evolutionary and less complex manner. Therefore, we also evaluated the structure of these models. For example, while EMRAM is structured as a maturity model, JCI and SAFER Guides are linear models.

Evaluating the gaps of these three models promoted the opportunity of their combination in a single and more specific maturity model to evaluate Health IT safety in hospital settings, key contribution of this Ph.D. thesis. That leads to the investigation of

RQ2, while RQ3 were investigate to the application of HITSMM in two Brazilian hospitals.

The overall methodology of our research consists of the following three phases conducted in our study:

1. **Mapping Requirements**: This phase involved creating two comprehensive mappings: one aligning the JCI standards with the EMRAM framework, and another mapping EMRAM to the SAFER Guides.
2. **HITSMM Development**: Leveraging the established mappings as a foundation, this phase centered on proposing and developing the Hospital Information Technology System Maturity Model (HITSMM) itself.
3. **HITSMM Application and Evaluation**: In this final phase, HITSMM was applied in two Brazilian hospitals to assess its real-world effectiveness and gather valuable feedback for further refinement.

Figure 1 presents the three phases of this study and their respective goals, outputs, and main contributions.

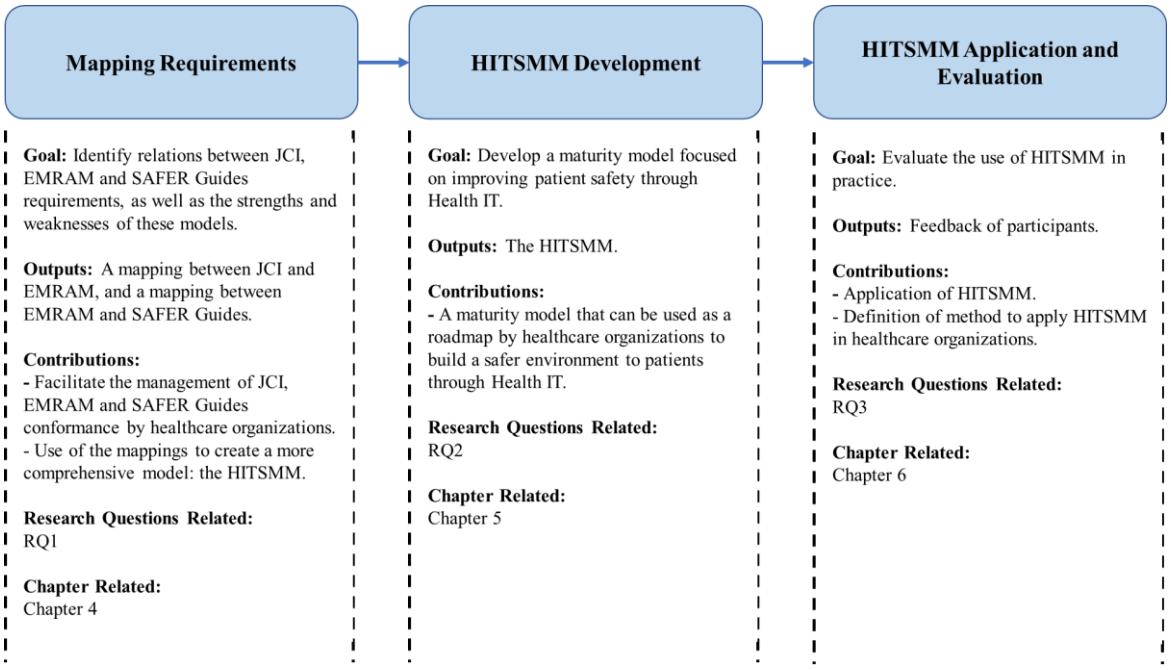


Figure 1 - Phases carried out in this this Ph.D. Thesis methodology.

1.4 Delimitations

The maturity model developed in this Ph.D. thesis focuses on evaluating the maturity of Health IT safety in hospital organizations. Therefore, aspects of our model related to inpatient care may not be applicable to outpatient settings such as ambulatory clinics, laboratories, and image diagnostic clinics.

Furthermore, our model addresses patient safety aspects related to the safe use of IT in healthcare processes. However, aspects related specifically to medical conduct, patient treatment, or hardware (e.g., medical devices) are not considered. In this Ph.D. thesis, IT is defined as software technologies.

1.5 Contributions

The main contribution of this Ph.D. investigation is the development of HITSMM. By adopting this maturity model, healthcare institutions can effectively navigate the complexities of health IT and ensure that technology serves as a powerful tool for enhancing patient safety rather than an unintended threat. This model provides a framework for adapting to new technologies and maintaining a steadfast commitment to patient well-being.

This Ph.D. thesis also presents the following secondary contributions:

- EMRAM-JCI Mapping can facilitate the management of JCI and EMRAM conformance by healthcare organizations which can use this mapping to identify technologies they can implement to ensure compliance with both validations.
- EMRAM-SAFER Guides mapping highlights requirements that are addressed by one model (EMRAM or SAFER Guides) but not the other. By identifying these gaps, HIMSS and ONC can utilize the findings to improve their respective models.
- The comparison between EMRAM, JCI and SAFER guides highlighting their strengths and weaknesses in relation to their comprehensiveness in evaluating Health IT and patient safety.

- The results of the application of HITSMM in two Brazilian hospitals can be used by these organizations to address the gaps identified and improve their process, technology and policies ensuring a safer Health IT environment.

1.6 Thesis Structure

This Ph.D. thesis is organized in six remaining Chapters. Their structure is organized as follows:

- **Chapter 2 – Background** explores the intersection of patient safety and Health IT presenting the foundations concerned to the main concepts and methods needed to understand this Ph.D thesis.
- **Chapter 3 – Related Work** presents the main related studies identified from the literature correlated to our investigation.
- **Chapter 4 - Mappings Between EMRAM, JCI and SAFER Guides Requirements** presents the methods and results of phase 1 of this study.
- **Chapter 5 - The Health IT Safety Maturity Model** presents the methods and results of phase 2 of this study.
- **Chapter 6 - HITSMM in Practice** presents the methods and results of phase 3 of this study.
- **Chapter 8 – Conclusions** presents main conclusions of this study.

Chapter 2
Background

This chapter explores the intersection of patient safety and Health IT. It begins by discussing the importance of patient safety and the role of Health IT in improving it. The chapter introduces the concept of a maturity model and discuss how maturity models can be used to assess the implementation of HIT for patient safety. Next, the chapter discusses the Joint Commission International (JCI) accreditation and SAFER Guides initiative. Finally, the chapter discusses HIMSS's Analytics Maturity Models, including EMRAM.

2.1 Patient Safety and Health Information Technology

According to the World Health Organization, patient safety is the prevention of errors and adverse events to patients associated with the healthcare process [13]. An adverse event, in turn, is any type of harm caused by healthcare [14].

However, an error in the healthcare process does not necessarily lead to an adverse event. In this context, there is the concept of a "near miss," which is an action that could have caused harm to a patient but did not [15]. An example of a "near miss" would be a nurse detecting a prescription error (e.g., overdosage) before the drug is administered to the patient.

Therefore, a "patient safety event" can be defined as an event or circumstance that did or could have resulted in harm to a patient [16]. It is important to note that these events are not only due to errors of commission (e.g., administering a medication with a higher dose than recommended), but also due to errors of omission (e.g., not performing a procedure that could benefit the patient) [15].

Despite the benefits that EHRs can bring to healthcare, several studies have shown the occurrence of patient safety events associated with the use of EHRs. These studies often use approaches such as interviews with professionals who use EHRs [17–19] and analysis of adverse event reporting [20-24].

Analyses of adverse event reporting in healthcare organizations have shown that problems such as software bugs, inadequate user interfaces, and communication failures between EHRs have contributed to the occurrence of adverse events [7,8,24]. The use of CPOE has been associated with problems such as medication dosage errors, failure to discontinue medications, duplicate prescriptions, conflicting medications, incorrect medication selection, prescribing medication to the wrong patient, among others [3]. Alert fatigue is also commonly associated with CDS mechanisms, where users fail to view CDS alerts due to the excessive and disruptive nature of these alerts [25,26].

2.2 Maturity Model Definition and Applications

A maturity model is a framework that provides a structured approach for evaluating the effectiveness of an organization's processes, practices, and systems. The model is based on a set of predefined levels of maturity, and each level represents a stage in the organization's evolution towards a higher level of capability. By using a maturity model, organizations can identify gaps in their processes, practices, and systems, and develop a roadmap for improving their capabilities. A maturity model can describe and measure the degree of maturity of a particular domain or process in an organization. The maturity of the domain is assessed based on a set of criteria or characteristics that are defined in the model [10].

Maturity models have a wide range of applications in different domain areas. In management, maturity models are used to assess the maturity of management processes, such as project and risk management. In software industry, maturity models have been used to evaluate the maturity of software development processes and practices.

As an example of a maturity model in software development industry is the Capability Maturity Model for Software (CMM). It is a framework for software process improvement that was developed by the Software Engineering Institute (SEI) at Carnegie Mellon University [27]. CMM is composed of five stages, each of which represents a different degree of maturity. The stages are Initial, Repeatable, Defined, Managed, and Optimized. Each stage is associated with specific practices grouped into several domain areas, such as project planning, requirements management, and software quality

assurance. Because the stages are progressive, a company must complete one before going on to the next [27].

Organizations that seek to enhance their performance and reach higher levels of maturity in a specific area or process might benefit greatly from using maturity models. They offer a structured framework for evaluating maturity, a roadmap for improvement, and a foundation for establishing goals and objectives. Many diverse sectors of knowledge use maturity models, which have been shown to be successful in enhancing performance and accomplishing corporate objectives [10].

The structure of a maturity model enables the assessment of the current state of the organization and presents the next steps through well-defined stages of development as a roadmap. Therefore, in this Ph.D. thesis, we propose the use of a maturity model as the most suitable framework structure to promote the evolution of healthcare organizations maturity in a more systematic and less complex way.

2.3 Joint Commission International

Joint Commission International (JCI) is a non-profit organization that provides accreditation services for healthcare organizations worldwide. Established in 1994, JCI is a subsidiary of The Joint Commission, a non-profit organization that accredits and certifies healthcare organizations in the United States. JCI's primary goal is to improve the quality and safety of patient care on a global scale [2].

JCI accreditation is widely recognized as a symbol of excellence in healthcare and involves a rigorous evaluation process that assesses healthcare organizations against international standards of performance. The accreditation process includes an on-site evaluation by a team of healthcare professionals who evaluate the organization's compliance with JCI standards related to patient safety, quality of care, patient and family rights, infection control, and leadership.

JCI's impact on global healthcare has been significant, with more than 1,000 organizations in over 100 countries accredited by JCI. Studies have shown that JCI

[2] https://www.jointcommissioninternational.org/

accreditation is associated with improved patient outcomes, including reduced mortality rates and lower rates of hospital-acquired infections [28].

The JCI Accreditation Standards for Hospitals manual, 6th edition, is organized in three sections: Patient Centered Standards, Health Organizations Management Standards, and Academic Medical Centers Hospitals Standards. The Patient Centered Standards section is related especially to the healthcare process and patient safety. The Health Organizations Management Standards section is related to management areas such as governance, data analysis, professional education, etc. The Academic Medical Centers Hospitals Standards section is composed of requirements for hospitals that perform medical education and scientific research involving human beings. The third section was not considered because the focus of this Ph.D. thesis is not medical education or clinical research.

Each section of the JCI Accreditation Standards for Hospitals is composed of chapters that represent domain areas for a set of requirements. Patient Centered Standards, Health Organizations Management Standards and Academic Medical Center Hospital Standards have eight, six and two chapters, respectively. Each domain area (chapter) specifies a set of standards that represent generic requirements, while each standard contains one or more measurement elements, which represent more specific requirements.

Table 1 presents the sections and chapters of JCI Accreditation Standards for Hospitals according to its the sixth edition (2017).

Table 1 - Sections and Chapters of JCI Accreditation Standards for Hospitals

Section	Chapter
Patient Centered Standards	• International Patient Safety Goals • Access to Care and Continuity of Care • Rights of Patients and Family Members • Assessment of Patients • Care of Patients • Anesthesia and Surgical Care • Medication Management and Use • Patient and Family Education
Health Organizations Management Standards	• Improvement of Patient Quality and Safety • Infection Prevention and Control • Governance, Leadership, and Direction • Facility Management and Safety • Education and Qualification of Professionals • Information Management
Academic Medical Centers Hospitals Standards	• Professional Medical Education • Human Research Programs

JCI has included a set of requirements dedicated to information management, which contains requirements specifically related to EHR. Therefore, JCI can be used as a source to investigate different requirements related to EHR. However, JCI is not focused on the use of Health IT. JCI requires specific policies and process to promote a better quality of patient care and governance in healthcare organizations. There are no requirements that obligates the use of Health IT along these processes. Besides, JCI requirements are not structured as a maturity model which can be challenging to healthcare organizations to improve their maturity in an evolutionary manner.

2.4 SAFER Guides

The Safety Assurance Factor for EHR Resilience (SAFER) Guides are a set of tools developed by the Office of the National Coordinator for Health Information Technology

(ONC) to help healthcare organizations improve the safety and quality of their health IT systems. SAFER Guides is composed of a set of nine guides with recommended practices, tools, and resources for healthcare organizations to use to improve the safety and effectiveness of their health IT systems. It was designed to be a self-assessment to healthcare organizations [9].

SAFER Guides are organized in three categories of guides: Clinical Process Guides, Foundational Guides, and Infrastructure Guides. Clinical Process Guides is composed of four guides: Computerized Provider Order Entry (CPOE) with Decision Support; Patient Identification; Test Results Reporting and Follow-Up; and Clinician Communication. Foundational Guides is composed of the guides High Priority Practices and Organizational Responsibilities. Infrastructure Guides is composed of three guides: Contingency Planning; System Configuration; and System Interfaces.

Table 2 - Guides of SAFER Guides summarizes the nine guides of SAFER Guides according to their guideline available in on their website[3].

[3] https://www.healthit.gov/topic/safety/safer-guides

Table 2 - Guides of SAFER Guides

Category	Guide	Description
Clinical Process Guides	Computerized Provider Order Entry (CPOE) with Decision Support	Recommendations related to CPOE and Clinical Decision Support (CDS) resources.
	Patient Identification	Recommended safety practices associated with the reliable identification of patients in the EHR.
	Test Results Reporting and Follow-Up	Recommended practices to optimize the safety electronic communication and management of diagnostic test results.
	Clinician Communication	Recommendations associated with communication between clinicians.
Foundational Guides	High Priority Practices	Identifies “high risk” and “high priority” recommended safety practices intended to optimize the safety and safe use of EHRs.
	Organizational Responsibilities	Recommendations related to individual and organizational responsibilities.
Infrastructure Guides	Contingency Planning	Recommendations associated with planned or unplanned EHR unavailability.
	System Configuration	Recommended safety practices associated with configuration of EHR hardware and software.
	System Interfaces	Recommendations to optimize the safety and safe use of system-to-system interfaces between EHR and other applications.

The recommended practices identified in the guides are organized in three phases: Safe Health IT, Using Health IT Safely, and Monitoring Safety. The phase “Safe Health IT” addresses safety concerns unique to technology (for example, providing specific EHR functionalities), whereas “Using Health IT Safely” is related to the safe use of Health IT. “Monitoring Safety” is composed by recommendations focused on monitoring the processes of design and use of health IT in order to optimize safety [9].

Since their release, the SAFER Guides have had an important impact on healthcare technology and have become a globally recognized benchmark for health IT safety. By offering a structured method for evaluating and improving health IT systems, the SAFER Guides have contributed to an improvement in patient safety and the quality of care.

A study has been conducted to evaluate SAFER Guides recommended practices across eight organizations [29]. The eight sites fully implemented only 18% SAFER Guides recommendations, which means that most organizations are not adherent to important practices to improve patient safety in relation to Health IT.

One of the key benefits of using SAFER Guides is that they help organizations identify areas for improvement that might not otherwise be obvious. For instance, an organization may discover that their EHR system does not offer adequate mechanisms to prevent medication errors. The organization can lower the risk of patient injury and raise the standard of care overall by addressing this problem [29].

We highlight that SAFER Guides requirements are not structured as a maturity model. In this Ph.D. thesis, we considered SAFER Guides linear structure as a weakness of the model, once it makes more complex to guide healthcare organizations in a improving their maturity in an evolutionary pathway.

2.5 HIMSS’s Maturity Models

The Healthcare Information and Management Systems Society (HIMSS) plays a significant role in promoting and assessing the maturity of health information technology (HIT) within healthcare organizations. HIMSS, founded in 1961, is a global non-profit organization dedicated to advancing healthcare information and it has been at the forefront of driving technological advancements in healthcare. HIMSS brings together

professionals, stakeholders, and technology vendors in the healthcare industry. HIMSS provides resources, education, and networking opportunities to support healthcare organizations in achieving their technology goals.

One of the most important HIMSS' initiatives is the development of a range of maturity models designed to evaluate and improve specific areas of technology implementation. These models enable organizations to benchmark their progress, identify gaps, and set goals for advancing their technological capabilities. HIMSS has developed the following maturities models[4]:

- **Electronic Medical Record Adoption Model (EMRAM):** EMRAM is one of HIMSS' flagship maturity models. It assesses the maturity of EHR adoption in healthcare organizations and guides them in achieving higher levels of EHR adoption, leading to improved patient care, streamlined workflows, and enhanced interoperability.

- **Community Care Outcomes Maturity Model (C-COMM):** C-COMM is focused on evaluating maturity across community care. By focusing on factors like smoother care transitions, wider adoption of secure digital tools, and data-driven performance monitoring, C-COMM aims to enhance both the delivery and outcomes of care for individuals within their communities. This includes ensuring all care documentation is readily available online for clinicians and utilizing digital tools to personalize care, increase access options, and improve patients' digital and health literacy, ultimately strengthening communication and collaboration between patients and care teams.

- **Continuity of Care Maturity Model (CCMM):** CCMM focuses on improving care coordination and information exchange among different healthcare providers. It evaluates the maturity of organizations in facilitating seamless transitions of care and ensuring effective communication across healthcare settings. CCMM provides a roadmap for achieving higher levels of interoperability, care coordination, and patient engagement, ultimately leading to improved care quality and patient outcomes.

- **Analytics Maturity Model (AMAM):** AMAM assesses an organization's maturity in utilizing data analytics to drive insights and support data-driven decision-making.

[4] https://www.himss.org/what-we-do-solutions/maturity-models

It evaluates the organization's capabilities in data governance, data management, analytics infrastructure, and analytics-driven culture. AMAM helps healthcare organizations enhance their analytics capabilities, enabling them to leverage data for population health management, quality improvement, and cost optimization.

- **Infrastructure Adoption Model (INFRAM):** INFRAM focuses on evaluating the maturity of an organization's technology infrastructure. It assesses various components such as networking, mobility, security, and disaster recovery capabilities. INFRAM provides healthcare organizations with a structured approach to improving their infrastructure, ensuring robust and secure technology systems that support the delivery of high-quality care.

- **Digital Imaging Adoption Model (DIAM):** DIAM assesses the maturity of an organization's digital imaging capabilities, particularly in radiology and medical imaging departments. It evaluates the implementation and utilization of digital imaging systems, including picture archiving and communication systems (PACS) and other imaging-related technologies. DIAM helps healthcare organizations optimize their imaging workflows, enhance image management and sharing, and improve diagnostic capabilities.

- **Clinically Integrated Supply Outcomes Model (CISOM):** CISOM is designed to evaluate a health system's capability to monitor care processes and the utilization of products by leveraging data to generate real-world evidence of their impact and outcomes for patient populations. Key objectives of CISOM include cost reduction; care process and product traceability; and personalized care and outcomes. Through the implementation of CISOM, healthcare organizations can improve supply chain efficiency and drive the delivery of personalized care based on the best available evidence.

The most adopted HIMSS' maturity model worldwide is EMRAM [5], which is focused specially on EHR adoption and patient safety. EMRAM is a maturity model that serves as a roadmap for healthcare organizations to assess and benchmark their progress

[5] https://www.himss.org/what-we-do-solutions/digital-health-transformation/maturity-models/electronic-medical-record-adoption-model-emram

in implementing electronic medical record systems. The EMRAM stages range from Stage 0 (no electronic medical record) to Stage 7 (a fully paperless environment with advanced clinical decision support and data analytics capabilities). The goals and requirements of each EMRAM stage, according to 2018 edition, are defined as follows:

- **Stage 0:** Not all key ancillary department systems (laboratory, pharmacy, and radiology) have been installed within the organization.

- **Stage 1:** All major ancillary clinical systems, including pharmacy, laboratory, and radiology, have been successfully installed. The organization utilizes comprehensive radiology and cardiology PACS systems, allowing physicians to access medical images through an intranet and eliminating the need for film-based images. Additionally, patient-centric storage of non-DICOM images is available for efficient management.

- **Stage 2:** Major ancillary clinical systems are integrated and interoperable, allowing seamless access to a unified Clinical Data Repository (CDR) or integrated data stores. Clinicians can conveniently review all orders, results, and radiology and cardiology images through a single user interface. The CDR and data stores utilize a controlled medical vocabulary, and order verification is supported by a CDS rules engine for rudimentary conflict checking. Integration of document imaging systems with the CDR is also possible at this stage. Basic security policies and capabilities are in place, addressing physical access, acceptable use, mobile security, encryption, antivirus/anti-malware measures, and data destruction.

- **Stage 3:** Nursing and allied health professional documentation, including vital signs, flowsheets, nursing notes, nursing tasks, and care plans, is integrated with the CDR at a rate of 50% (as defined by the hospital). The implementation of this capability is required in all areas except for the Emergency Department (ED), which is exempt from the 50% rule. Additionally, the organization has successfully implemented the Electronic Medication Administration Record (eMAR) application and role-based access control (RBAC) system.

- **Stage 4:** 50% of medical orders are entered electronically through CPOE by authorized clinicians. CPOE is enhanced with a CDS rules engine for basic conflict

checking, and orders are integrated into the nursing and CDR systems. The ED utilizes CPOE, but it is not included in the 50% calculation. Nursing and allied health professional documentation has achieved a rate of 90% completion, excluding the ED. Clinicians have access to regional or national patient databases for decision-making support regarding medications, images, immunizations, and lab results. During EHR downtimes, clinicians can access essential patient information such as allergies, problem/diagnosis lists, medications, and lab results. The network is secured with an intrusion detection system to detect potential network intrusions. Nurses are supported by a secondary level of CDS capabilities that align with evidence-based medicine protocols, triggering recommended nursing tasks based on risk assessment scores.

- **Stage 5:** Physician documentation, including progress notes, consult notes, discharge summaries, problem/diagnosis lists, and more, utilizes structured templates and discrete data for at least 50% of the hospital. The ED implements this capability, but it is exempt from the 50% requirement. The hospital has the ability to monitor and report on the timeliness of nurse order/task completion. An intrusion prevention system is in place to detect and prevent potential intrusions. Hospital-owned portable devices are authorized to operate on the network, and remote wiping capabilities are implemented in case of loss or theft.

- **Stage 6:** Technology plays a crucial role in achieving closed-loop processes for medication administration, blood product management, human milk administration, blood specimen collection, and tracking. These closed-loop processes are fully implemented in 50% of the hospital, excluding the ED from the 50% requirement. The eMAR and integrated technologies are connected to CPOE, pharmacy, and laboratory systems to optimize safe point-of-care practices and results. Advanced CDS systems enhance medication administration and other related processes, focusing on the "five rights" principle. Additionally, CDS provides guidance based on physician documentation, triggering variance and compliance alerts tied to protocols and outcomes (e.g., VTE risk assessment prompting appropriate VTE protocol recommendations). The hospital applies security policies and practices to user-owned mobile/portable devices. Annual security risk assessments are conducted, and reports are submitted to a governing authority for necessary action.

- **Stage 7:** The hospital has transitioned from paper charts to an EHR system, incorporating discrete data, document images, and medical images. Data warehousing is utilized for analyzing clinical data patterns, aiming to improve care quality, patient safety, and delivery efficiency. Clinical information can be easily shared through standardized electronic transactions, such as Continuity of Care Documents (CCD), with authorized entities including healthcare providers, health information exchanges, outpatient clinics, sub-acute environments, employers, payers, and patients within a data sharing environment. The hospital ensures continuity of summary data across all services, including inpatient, outpatient, and the ED, as well as any owned or managed outpatient clinics. Physician documentation and CPOE have achieved a rate of 90% (excluding the ED), while closed-loop processes have reached 95% (excluding the ED).

Although HIMSS has different models, none of them are totally focused on patient safety. EMRAM is the HIMSS's model that evaluates, among other aspects, how the EHR is used throughout the patient care process and, therefore, includes many requirements related to the use of EHR as an additional barrier for patient safety. However, it is not possible to affirm that it includes all aspects of safe use of Health IT once it is not the goal of the model.

Chapter 3

Related Work

We conducted an exploratory literature revision, in 2018, and we identified that several studies have addressed the evaluation of EHR maturity level of healthcare organizations. Ozkan *et al.* explored an assessment method called Process Based Information Systems Effectiveness (PRISE) to measure the level of process maturity of health information systems [30]. PRISE consists of 92 questions assessed on a 6-level scale (Nonexistent, Initial /Ad Hoc, Repeatable but intuitive, Defined process, Managed and measurable, and Optimized). The PRISE model consists of three main components: People, Resources, Services and Benefits, with a total of 10 process areas within those components (Table 3).

Table 3 - PRISE Process Areas

Component	Processes
People	Definition of the IS organization and relationships
	Education and training of users
	Provision of assistance and advice to IS users
Resources	Information System interactions
	Configuration management
	Performance and capacity management
	Operations management
Services and Benefits	Continuous service
	Change management
	Monitoring services

Flott et al. have performed a systematic review to identify the most adequate methods and metrics for evaluating digital maturity of healthcare organizations, as well as to create a tool for evaluating digital maturity across those organizations [31]. They analyzed findings from the 28 studies identified in the literature search and grouped them into 5 themes to generate the skeleton of a new digital maturity framework: general evaluation methodology, resources and ability, usage, interoperability, and impact.

Carvalho *et al.* conducted a literature review to identify and compare the maturity models for management of information systems and technologies in healthcare [32]. The most relevant maturity models identified in the literature review were the Quintegra Maturity Model for Electronic Healthcare (eHMM), the Healthcare IT Maturity Model developed by IDC Health Industry Insights, EMRAM by HIMSS and CCMM by HIMSS.

The eHMM is a comprehensive framework that includes all healthcare providers involved in the delivery of care. This adaptable model can be applied to any healthcare organization, regardless of their current stage of development. Quintegra's eHMM Maturity Model outlines the journey of an e-health process, from its initial stages to nationwide implementation. The model's defined maturity stages serve as a roadmap for healthcare organizations, guiding them towards continuous improvement of their healthcare processes [32].

The IDC's Healthcare IT Maturity Model consists of five progressive stages, each building upon the functionalities of the previous one. IDC utilizes this model globally to assess the maturity of hospital information systems, allowing comparisons of average maturity levels across different regions and countries [32].

In a further study, Carvalho et al. proposed a six stages maturity model to measure health information systems maturity: the Hospital Information System Maturity Model [33]. This model considers both the overall maturity of a hospital information system and the maturity of its individual components. This is achieved by combining a set of key factors that influence maturity, along with their specific characteristics. The Hospital Information System Maturity Model has 6 dimensions:

- **Data analysis:** Evaluates the collection, storage, and analysis of health data.
- **Strategy:** Evaluates the ability to develop a strategic plan and effectively implement it.

- **People:** Evaluates human resources, including patients, health professionals, IT professionals and others.
- **Electronic Medical Record:** Evaluates the systems that works as main source of all information related to the patient.
- **Information Security:** Evaluates data security are confidentiality, integrity, and availability.
- **Systems and IT infrastructure:** Evaluates all systems and infrastructure needed to support Health IT.

Each dimension can be measured according to its positioning associated with the maturity stage, which can be determined by the existence or non-existence of specified characteristics [33].

Gomes and Romão discussed the use of information systems in healthcare and how they have been recognized as having crucial importance in improving the efficiency, cost-effectiveness, quality, and safety of medical care delivery [34]. The study gives an overview of several of maturity models, including the eHealth Maturity Model, the Capability Maturity Model Integration (CMMI), and EMRAM. The authors discussed the challenges and limitations associated with applying maturity models to the healthcare industry, including the necessity of continual assessment and the significance of stakeholder involvement. Overall, their research offered insightful information about the possible advantages and difficulties of applying maturity models to healthcare information systems [34].

Kolukısa Tarhan et al. performed a multivocal literature review in order to investigate the state-of-the-art on maturity models in health care [11]. The findings of this review show that maturity models are consistently provided under a variety of health care topics and are also empirically implemented. Their study explored numerous aspects on the subject and identifies maturity models' major traits and qualities, such as their emphasis on organizational development, iterative and continuous improvement strategy, and usage of maturity levels or stages to measure progress.

Kolukısa Tarhan et al. also investigate the different maturity models used in healthcare, including those developed by external organizations such as HIMSS, CMMI, and ISO, as well as those developed internally by healthcare organizations themselves. This study highlights the benefits of using maturity models in healthcare, such as helping

organizations to identify their strengths and weaknesses and prioritize areas for improvement. The authors concluded that the use of maturity models in healthcare faces difficulties and restrictions, including the risk of models becoming overly prescriptive or rigid, the need for buy-in and participation from all stakeholders, and the necessity of routinely updating and improving models to ensure their ongoing relevance [11].

Virginio and Ricarte conducted a study to identify the patient safety risks related to EHRs and investigate mitigation actions [6,35]. The study identified 38 risks patient safety. The investigation of risks was based specially on EHR life cycle defined by the authors as presented by Figure 2. For each phase of the life cycle, the risks were also categorized based on a socio-technical system of five interdependent components (technology, people, process, organization, and external environment) that interact with each other (Figure 3) [35].

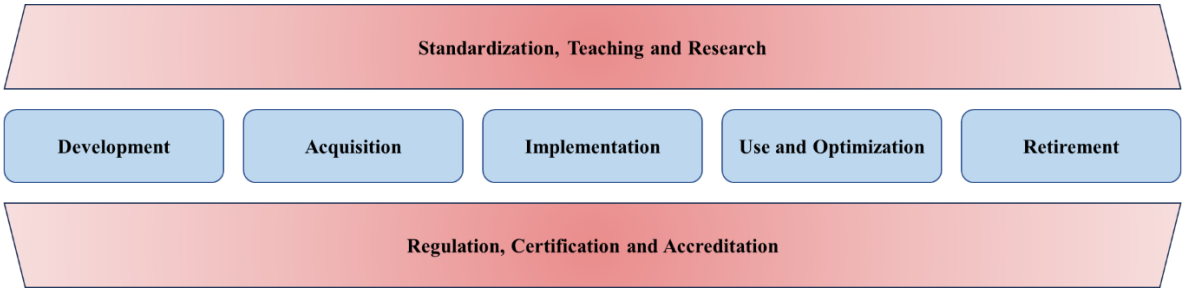


Figure 2 - EHR Life Cycle[35]

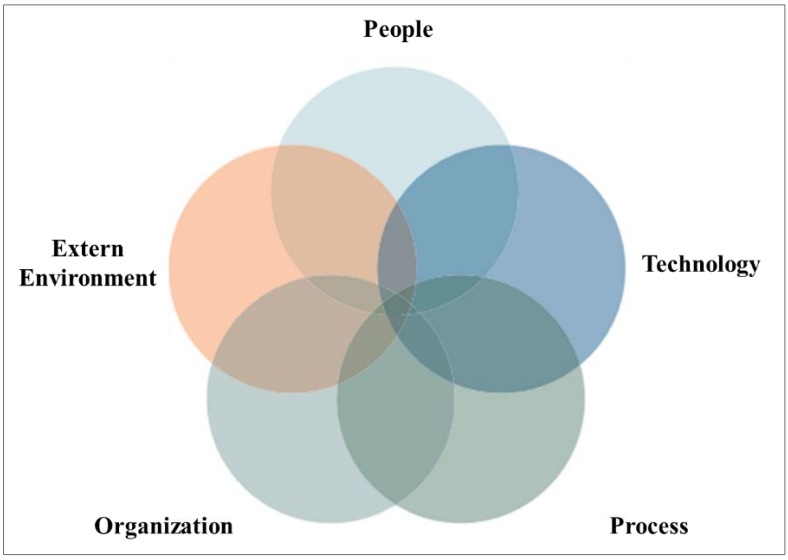


Figure 3 - Socio-technical system

Risks related to Development phase of EHR Life Cycle were associated specially with technology dimension of the social-technical system and included risks such as lack of EHR functionalities, EHR bugs and EHR usability problems. The study found Two risks were identified associated with Acquisition phase: "selection of an insecure EHR or one that is not appropriate for the needs of the healthcare organization" and "establishment of inadequate contracts [35].

The risks related to the implementation were associated to "inadequate infrastructure quality", "inadequate S-RES configuration", and "communication problems between the S-RES and other systems". The risks related to the EHR use and optimization phase were associated with the problems encountered with the use, support, maintenance, and evolution of the EHR throughout the operational process in healthcare organizations [35].

The risk associated with Retirement phase was related to the possible process of migration of data, usually need during a process of EHR changing. The EHR life cycle phase of standardization, education, and research process corresponds to the development of health informatics standards, as well as the education and research processes that support such development. The risk identified for this phase was related to the gaps existing in the standardization, education and research processes associated with EHR safety [35].

Similarly, the phase of regulation, certification, and accreditation process corresponds to the monitoring and evaluation of compliance with standards, norms, and good practices associated with the EHR. The risk identified for this phase was related to the gaps existing in the regulation, certification, and accreditation processes of the aspects associated with the S-RES [35].

Kutza et al. focused on developing criteria to assess the maturity of digital patient safety in hospitals [36]. They created a catalog of 64 criteria across 11 categories, derived from a literature review and existing maturity models. These criteria serve as a guide for hospitals to identify areas for improvement in their information systems to enhance patient safety. The study suggests that maturity in digital patient safety involves not only the adoption of advanced technologies but also their effective utilization and continuous improvement processes within healthcare organizations [36].

Sittig et al. outline nine short-term challenges across different stages of the health IT lifecycle [37]. These challenges span from the design and development phase, such as developing risk assessment models and ensuring software safety in networked environments, to the implementation and use phase, including decision support and system transition management. The study also discusses the importance of monitoring, evaluation, and optimization to develop real-time surveillance methods and improve health IT safety for consumers [37].

Taheri Moghadam et al. delves into the taxonomy of patient safety incidents related to HIT [38]. This study categorizes different types of incidents and provides a structured way to analyze and address them. They identified six classifications and found that HIT classifications generally cover more concepts and classes than medical device classifications. By classifying these incidents, the research offers valuable insights into common pitfalls and areas requiring improvement, thus aiding healthcare providers and HIT developers in designing safer systems [38].

McInerney et al. explored the patient safety challenges associated with emerging digital health technologies [39]. They identified six key challenges, including conceptualizing digital threats, building trust in complex systems, integrating and interpreting data sources, addressing reactive regulations and standards, managing emergent patient safety consequences, and avoiding the pitfalls of solutionism (oversimplifying complex problems). The authors proposed recommendations to mitigate these challenges, emphasizing a proactive and systems-based approach that considers the social, technical, and regulatory aspects of patient safety informatics [39].

Chapter 4

Mappins Between EMRAM, JCI and SAFER Guides Requirements

In this phase of our investigation, we aimed to compare different models that could be used as sources to develop a new and more specific model to better evaluate and promote the increasing of Health IT safety maturity in healthcare organizations. Therefore, we conducted exploratory research to identify frameworks on healthcare industry that have been used in healthcare organizations around the world to assess the use of Health IT to improve patient safety.

While JCI is not focused on Health IT does not focus on Health IT, it is a globally recognized model for ensuring patient care quality. Notably, it includes a dedicated chapter for evaluating information technology aspects. JCI has been implemented across various countries.

EMRAM is the leading HIMSS's maturity model, and it is focused on the adoption of information technology in hospitals. It guides and assesses these organizations through well-defined stages to improve their digital health maturity. EMRAM has been adopted in many countries around the world.

Although SAFER Guides is primarily used in the United States, it stands out as the only model referenced in this Ph.D. thesis that entirely concentrates on Health IT and patient safety. However, it is important to note that SAFER Guides is not structured as a maturity model.

Therefore, the use of these three models (EMRAM, JCI, and SAFER Guides) is proposed in this Ph.D. thesis as a strategy to develop a new maturity model that is more specific in evaluating and guiding healthcare organizations in improving patient safety through Health IT.

To answer RQ1 ("how existing models can be comparatively evaluated to identify strengths, weaknesses, and potential for integration?"), we defined a method to compare JCI, EMRAM and SAFER Guides. As a first step, we performed an evaluation to identify

relations between JCI, EMRAM and SAFER Guides requirements [40,41]. This phase involved creating two comprehensive mappings: one aligning the JCI standards with the EMRAM framework, and another mapping EMRAM to the SAFER Guides.

Both mappings followed similar methodology with two main activities: requirement extraction and identification of relations between EMRAM and JCI requirements or between EMRAM and SAFER Guides requirements. The first activity focused on the extraction and documentation of all EMRAM, JCI and SAFER Guides. The second activity focused on identifying relations between their requirements.

4.1 Mapping Between EMRAM and JCI

In the first mapping carried out, we performed an evaluation to identify relations between JCI and EMRAM requirements. This evaluation creates a mapping between their requirements, which can guide hospitals to achieve both validations. Additionally, this evaluation enables to identify JCI requirements associated to Health IT that are not currently required by EMRAM, which can be used to promote the evolution of this maturity model.

4.1.1 Requirements Extraction

The process of EMRAM requirements extraction was performed based on the material provided by HIMSS Analytics Latin America, represented by the Brazilian company FOLKS, in partnership with this Ph.D. thesis. Such material corresponds to a sheet of EMRAM requirements based on the current version of EMRAM and it is more detailed than the original material provided by HIMSS Analytics on their website[6]. Once the EMRAM stages are cumulative (each stage includes the criteria of all previous stages), we only considered stage 7 requirements.

All EMRAM requirements presented in the available material was atomic, which was one of the criteria for our investigation. We consider a requirement as atomic when it cannot be divided into two or more other requirements. For example, the requirement *"the hospital shall use clinical decision support alerts on Computerized Provider Order*

[6] https://www.himssanalytics.org/emram

Entry (CPOE) for allergy and drugs interactions" is not atomic because it could be divided into two requirements (one for allergy and another for drugs interaction).

Each EMRAM requirement has the following attributes:

- Identification number: uniquely identifies each requirement;
- Category: domain area of the requirement, such as "information security" and "clinical documentation"; and
- Requirement text: describes the criteria specified by the requirement.

The process of JCI requirements extraction was performed based on the 6th Edition of the JCI Accreditation Standards for Hospitals available for purchase on the JCI website[7]. The requirements for achieving JCI accreditation are organized in three sections: Patient Centered Standards; Health Organizations Management Standards; and Academic Medical Centers Hospitals Standards. This third section was not considered in our investigation because it focuses on medical education and clinical research.

Each section of the JCI Accreditation Standards for Hospitals is composed of chapters that represent domain areas for a set of requirements. Patient Centered Standards and Health Organizations Management Standards sections have eight and six chapters, respectively. Each domain area (chapter) specifies a set of standards that represent generic requirements, while each standard contains one or more measurement elements, which represent requirements that are more specific. Because the measurement elements are more specific and atomic, we only considered them as requirements.

4.1.2 Types of Relations Investigated

The goal of this mapping was to identify relations between JCI and EMRAM requirements, as well as JCI requirements that could be supported by Health IT. Therefore, we divided the JCI requirements in IT-related and IT-not-related. We considered a JCI requirement as IT-related if it is associated specifically to Information Technology (IT), for example, the requirement has a premise that a technology is being used by the hospital (for example, requirements related to copy and paste functionalities that are conditional to hospitals that has implemented an EHR).

[7] https://www.jointcommissioninternational.org/jci-accreditation-standards-for-hospitals-6th-edition/

We aimed to identify three types of relations: (1) relation between IT-related JCI requirements and EMRAM requirements; (2) relation between IT-not-related JCI requirements and EMRAM requirements; and (3) relation between IT-not-related JCI requirements and Health IT.

For each JCI requirement, we analyzed the existence of one of the three types of relations described above. For this purpose, it was necessary to evaluate whether a JCI requirement had any kind of relation to IT direct or indirectly, as well as whether it presents some relation with EMRAM requirements. Once we already had EMRAM requirements, the identification of relations between JCI e EMRAM requirements was facilitated and was performed by comparing each JCI requirement with each EMRAM requirement. However, the identification of JCI requirements that could be supported by Health IT was quite challenging because it was based especially on the authors' experience, with further validation by specialists.

We considered that a JCI requirement was related to Health IT if it could be supported by Health IT. This support should be a differential to ensure compliance to the requirement. For example, when a JCI requirement only specified that an information should be recorded on the patient's chart, we did not consider the record on EHR as a Health IT support, once the EHR just replaces the paper in this case. However, when the JCI requirement specified that a summary of patient's health data should be registered, we considered that it could be supported by Health IT, here the EHR can generate this summary automatically based on the data already recorded.

4.1.3 Validation Process

As mentioned previously, the process of identifying the three relations described above was performed by the authors with further validation by specialists. The validation process aimed to verify whether the relations identified were adequate. In this sense, the results concerning the JCI requirements and respective relations were submitted to a validation process. To this end, we invited eight professionals with experience in digital health consulting who had led or participated in digital health initiatives in Brazilian healthcare organizations. .

Each specialist received a different subset of JCI requirements with their respective relations identified. The subsets included not only the JCI requirements with a relation to EMRAM and/or Health IT, but also the JCI requirements we did not find a

relation, because we wanted to check whether the specialists could identify some relation we could not.

We submitted 40% of the JCI requirements to validation. We excluded from validation the JCI domain areas we found less than three requirements related to EMRAM and/or Health IT (Patient and Family Rights, Care of Patients, Anesthesia and Surgical Care, Patient and Family Education, Prevention and Control of Infections, Governance, Leadership and Direction, Facilities Management and Security, and Staff Qualification and Education).

The task of each specialist was to verify each JCI requirement in the subset and indicate if he/she agrees with the relation established by the authors. Even if no relation was established, the specialist could indicate his/her agreement. The specialist also could indicate a justification for his/her opinion, suggesting modifying or removing a relation or creating a new relation. Afterwards, for each disagreement or partial disagreement, the authors evaluated whether the suggestion would be considered.

4.1.4 Results of EMRAM and JCI Mapping

We extracted 1.199 JCI requirements and identified 113 specifically related to IT (IT-related) and/or with some relation with EMRAM and/or Health IT. As mentioned previously, 40% of the JCI requirements and respective relations were submitted to validation. Out of 489 JCI requirements/relations validated, 463 were agreed and 26 were disagreed by the specialists. The specialists' suggestions resulted in two relation removals, eight relation modifications, and 16 relation creations.

After validation process, we obtained 127 JCI requirements specifically related to IT (IT-related) and/or with some relation with EMRAM and/or Health IT. Table 4 presents the number of relations with EMRAM and/or Health IT identified for each JCI standard category. The list of Stage 7 EMRAM requirements provided by HIMSS Analytics Latin America is composed of 116 requirements organized in 15 categories. Table 5 presents these categories and the number of JCI requirements with which we identified relations.

Table 4 – Number of relations with EMRAM identified for each JCI standard category

Standard Category	**Number of JCI Requirements**	**Number of JCI Requirements with some relation**
International Patient Safety Goals	34	17
Access to Care and Continuity of Care	119	34
Patient and Family Rights	77	1
Assessment of Patients	169	14
Care of Patients	108	1
Anesthesia and Surgical Care	55	0
Medication Management and Use	83	17
Patient and Family Education	18	0
Quality Improvement and Patient Safety	43	12
Prevention and Control of Infections	75	3
Governance, Leadership and Direction	142	1
Facilities Management and Security	96	0
Staff Qualifications and Education	98	0
Management of Information	72	27

Table 5 – Number of JCI requirements related to EMRAM for each EMRAM category

EMRAM Category	Number of JCI requirements with relation to EMRAM
Analytics	10
Clinical Documentation	7
CPOE	0
Disaster Recovery and Business Continuity	5
Document Management	0
Governance	1
Health Information Exchange	0
Information Security	7
Laboratory	1
Medical Device Integration	0
Medical Documentation	2
Medical Imaging	1
Pharmacy	4
System Overview and Pervasiveness of Use	0
Technology-Enabled Bedside Product Administration	15

JCI Accreditation Standards contains a standard category for information management with 72 requirements. This is the only category we have found requirements specifically related to information technology with 11 IT-related requirements (Table 6), which six are not related to EMRAM. In other words, JCI has six requirements specifically related to Health IT that are not required by EMRAM.

All JCI requirements related to EHR downtime are also covered by EMRAM. However, there are two topics not addressed by EMRAM: copy and paste and evaluation of Health IT systems. The functionalities of copying and pasting health records can facilitate professional documentation, but when used improperly, can result in issues such as propagation of incorrect information and registration of outdated information. In addition, performing tests before and after Health IT implementation is essential to ensure its proper performance. Such tests are required by JCI, but not by EMRAM.

Table 6 – IT-related JCI requirements and their relation to EMRAM

JCI Requirement	**Relation to EMRAM-HIMSS**
The hospital develops a process to regulate the proper use of copy and paste when electronic medical records of patients are used.	-
The hospital provides education and training on the proper use of copy and paste to all professionals who keep records in the patient's electronic medical record.	-
The hospital monitors compliance with the use of copy and paste guidelines and implements corrective actions as needed.	-
The hospital develops a process to ensure that the accuracy of records in patient electronic records is monitored.	-
Information technology systems in health are evaluated and tested before implementation.	-
Information technology systems in health are evaluated after implementation to usability, effectiveness and patient safety.	-
The hospital develops and maintains, and tests at least annually, a program for response to planned and unplanned data systems outages.	EMRAM-HIMSS requires that the hospital has a contingency plan for possible system unavailability and perform periodic simulations of system shutdown response.
The hospital identifies the likely impact that planned and unplanned downtime of data systems will have on all aspects of care and services.	EMRAM-HIMSS requires that the hospital has a contingency plan for long term system unavailability.

The program includes continuity strategies for the continued provision of safe, high-quality care and services during planned and unplanned downtimes of data systems.	EMRAM-HIMSS requires that the hospital have a plan for continuity of clinical documentation during unavailability of the information system. EMRAM-HIMMS also requires the hospital to have a contingency computer with a backup of patient data so that it can access clinical documentation even when the information system is unavailable.
The hospital identifies and implements inactivity recovery tactics and data backup processes in place to restore and maintain data and ensure data integrity.	EMRAM-HIMSS requires a backup of the latest patient data are made periodically and made available on a contingency machine, so that such data can be accessed even in case of network outage or electricity.
The professionals are trained in the strategies and tactics used for planned downtime and unplanned, data systems.	EMRAM-HIMSS requires the hospital to perform training for contingency.

Out of 1.199 JCI requirements extracted, we found 48 requirements not specifically related to Health IT that are related to EMRAM. Most of these requirements are related to EMRAM because they do not specify the implementation method, whereas EMRAM makes the same requirement specifying that a technology should be used (technology-enabled bedside product administration, for example).

We identified two main themes addressed by the relations between IT-not-related JCI requirements and EMRAM requirements: technology-enabled bedside product administration and data analytics. We found 17 relations associated to the process of technology-enabled bedside product administration required by EMRAM. That process specifies that the hospital must use some technology (barcode, QR code, etc.) to identify patients and products to be administrated at the bedside (at least medication, human milk, and blood products). Through scanning of patient wristband and product, the EHR shall verify whether the patient and product identification are correct. If some mistake is detected (for example, professional scanned a drug not prescribed to the patient), the EHR shall alert the professional, preventing a potential product administration mistake. For medication, EMRAM also requires the EHR to alert about correct time, dose, and administration route. JCI requires the safe product administration and safe samples

collection through many requirements, but it does not require the use of the scanning process. Table 7 presents some examples of these requirements and their relation to EMRAM.

We identified 10 relations between JCI and EMRAM requirements regarding data analytics. All JCI requirements that address data analytics are specified in the chapter "Quality Improvement and Patient Safety". This chapter requires the hospital to have a quality and patient safety program, which demands the use of data analysis to measure the proper functioning of processes, as well as to implement and sustain changes that result in improvements. Table 7 and Table 8 presents examples of these requirements and their relation to EMRAM.

Table 7 – Examples of relations between JCI and EMRAM requirements associated to technology-enabled bedside product administration

JCI Requirement	**Relation to EMRAM-HIMSS**
Patients are identified using two identifiers (patient's name, ID number, date of birth, wristband with bar codes, etc.), not including the use of the patient's room number or the patient's location in the hospital.	EMRAM-HIMSS requires the use of wristband with barcode, RFID or QR code for safe patient identification.
Patients are identified before undergoing diagnostic procedures, treatments, and other procedures.	EMRAM-HIMSS requires bar code to be scanned at the bedside for drugs, blood products, breast milk, parenteral nutrition and collecting blood samples.
The hospital has a process that prevents the inadvertent administration of concentrated electrolytes.	EMRAM-HIMSS requires that all drugs to be labeled dispensed by the pharmacy by demand of a prescription and scanned at the bedside checking potential errors.
Procedures are established and implemented to collect and identify [laboratory blood] samples.	EMRAM-HIMSS requires laboratory blood samples to have barcode and to be scanned at the bedside to ensure correct patient identification.

Clinical guidelines and procedures are established and implemented for handling, use and administration of blood and blood components.	EMRAM-HIMSS requires blood products to be scanned at the bedside. It also requires that there is a safe process to bind the blood bag with the patient / prescription so that the information system can alert if an incompatible bag is being bound. In addition, there must be a dispensing process where the blood bag is scanned in order to ensure that the correct bag is being dispensed.
Medications and chemicals used in drugs preparation are precisely labeled with content, expiration date and alerts.	EMRAM-HIMSS requires drugs to be scanned during medication preparation in order to check potential mistakes.
The hospital establishes and implements a process that includes the items from a) to e) the purpose for nutritional products. a) Receipt; b) Identification; c) Labeling; d) Storage; and e) The control and distribution.	EMRAM-HIMSS requires human milk and parenteral nutrition to be labeled and scanned at the bedside.
The medication doses conferred with the prescription or requisition.	EMRAM-HIMSS requires drugs to be scanned at the bedside so that the system checks whether the medication dose is correct and alerts if a fractionation is required.
Data is aggregated, analyzed and transformed into useful information to identify opportunities for improvement.	EMRAM-HIMSS requires data analysis in the Business Intelligence system to involve technological interventions that deliver positive results for assistance, operation, and finance.

Table 8 – Examples of relations between JCI and EMRAM requirements associated to data analysis

JCI Requirement	**Relation to EMRAM-HIMSS**
The quality and patient safety program has a process to aggregate data.	EMRAM-HIMSS requires the use of a Business Intelligence system for storage and analysis of data from different sources, enabling the creation of dashboards that aggregate data.
There is a process to contribute and learn from external databases for comparison purposes.	EMRAM-HIMSS requires the hospital to import external data from other institutions onto the Business Intelligence system in order to compare their indicators.
Data is aggregated, analyzed, and transformed into useful information to identify opportunities for improvement.	EMRAM-HIMSS requires that the data analysis on the Business Intelligence system shall encourage the implementation of technological interventions that result in assistance, operational, and financial benefits.
Professionals with experience, knowledge and appropriate clinical or managerial skills are involved in the process.	EMRAM-HIMSS requires the hospital to have a formal strategy for data governance, including the definition of responsible and procedures for quality assurance, accuracy, completeness and updating of data used for analytics.
Data analysis supports internal comparisons over time, including comparisons with databases of similar organizations, best practices and with objective professional scientific sources	EMRAM-HIMSS requires the hospital to import external data from other institutions onto the Business Intelligence system in order to compare indicators.
Data on the amount and type of resources used to use at least an existing process, is collected and evaluated and reviewed to this process, after the implemented improvement.	EMRAM-HIMSS requires that the hospital has projects in which data analysis enabled the identification of a problem and / or opportunity for improvement. It also requires that the assistance, operational and / or financial data to be evaluated again after the implementation of improvement.

Information management systems support the program to prevent and control infections. Functions of the management information system support the analysis and interpretation of data and presentation of results. In addition, the data and information on the prevention and infection control program are managed with the management and improvement of hospital quality program.	EMRAM-HIMSS requires the hospital to perform the analysis of welfare indicators, including those related to hospital infection control.
Monitoring data are collected and analyzed for activities to prevent and control infection and include major infections from an epidemiological point of view.	EMRAM-HIMSS requires the hospital to perform the analysis of Key Performance Indicators, including those related to hospital infection control.

In addition, we aimed to identify IT-not-related JCI requirements that could be supported by Health IT. We identified 106 of these requirements and, as expected, many of them (41) were related to EMRAM. However, 65 IT-not-related JCI requirements does not have a relation to EMRAM. Table 9 presents some examples of these requirements.

Some requirements can be supported by Health IT simply by using the EHR. For example, issues regarding illegibility of medical prescriptions are mitigated through the use of the electronic prescription. Other aspects are related to the automation that Health IT can bring to the process. For example, JCI requires, for each clinical record, the identification of responsible professional, date, and time. The EHR can automatically record those data as soon as the professional concludes the record. The most interesting Health IT support to JCI requirements is associated to functionalities that Health IT can offer. For example, JCI requires the hospital to use sources of information about drugs available for professionals. To that purpose, the EHR can be integrated to the Health Level 7 (HL7) Context Aware Knowledge Retrieval Application ("Infobutton"), which provides the communication between the EHR and knowledge resources[8].

[8] http://www.openinfobutton.org/hl7-infobutton-standard

Table 9 – Examples of IT-not-related JCI requirements without relation to EMRAM and how they can be supported by Health IT

JCI Requirement	Health IT Support
Appropriate sources of information about drugs are readily available for professionals involved in medication use.	Information system can use the engine that clinical decision support, such as Infobutton, which provide access to information sources.
The discharge summary contains the reasons for admission, diagnosis, and comorbidities.	The discharge summary can be generated automatically by the information system based on the information already recorded in the electronic medical record and then reviewed by a qualified professional.
The hospital establishes and implements a process for managing prescriptions and illegible requests, including measures to prevent the continued occurrence.	The use of an information system avoids illegibility problems.
The author can be identified for each record in the patient's chart.	System can automatically record the responsible user and date / time for each record in the chart.

4.1.5 EMRAM-JCI Mapping Limitations

The process of EMRAM-JCI Mapping has some limitations associated to the validation process. Due to the limited number of available specialists, we submitted to validation 40% of JCI requirements and their relations to EMRAM and/or Health IT. Eight JCI standard categories were not reviewed by any specialist and, therefore, it is possible there are other potential relations beyond those presented here. Additionally, each JCI requirement and respective relation were validated by only one specialist and, therefore, we did not make an agreement evaluation between validation participants.

Another limitation of this mapping is related to the EMRAM requirements extraction. As mentioned previously, the EMRAM requirements were extracted based on a material provided by a company that represents HIMSS Analytics in Latin America, which is a copyright of the company. Therefore, we did not use a material provided officially by HIMSS Analytics once they do not provide a detailed source with EMRAM requirements.

4.2 Mapping Between EMRAM and SAFER Guides

As a second step to develop HITSMM, we performed an evaluation to identify relations between SAFER Guides and EMRAM requirements. This evaluation creates a mapping between their requirements which helped to identify opportunities to improve both EMRAM and SAFER Guides.

4.2.1 Requirements Extraction

The EMRAM requirements extraction were conducted as previously described. The process of SAFER Guides requirements extraction was performed based on the guidelines available on the The Office of the National Coordinator for Health Information Technology (ONC) website. SAFER Guides are organized in three categories: Clinical Process Guides, Foundational Guides, and Infrastructure Guides. Clinical Process Guides is composed of four guides: Computerized Provider Order Entry (CPOE) with decision Support, Patient Identification, Test Results Reporting and Follow-Up, and Clinician Communication. Foundational Guides is composed of the guides High Priority Practices and Organizational Responsibilities. Infrastructure Guides is composed of Contingency Planning, System Configuration, and System Interfaces.

Each guide consists of a set of good practices organized in three phases: Safe Health IT, Using Health IT Safely, and Monitoring Safety. The first phase addresses safety concerns unique to technology (for example, providing specific EHR functionalities), whereas the second phase is related to the safe use of Health IT. The third phase addresses capabilities to monitor and improve patient safety.

Each guide contains a set of recommended practices in three domains. Each recommended practice is complemented by “examples of potentially useful practices/scenarios”, which goal is to give a rationale and examples of how to implement each recommended practice. In this study, we considered the recommended practices as a general requirement and the examples as specific requirements.

Each SAFER Guides requirement has the following attributes: identification number, guide category, domain, phase, indication for generic or specific, and requirement text. In this Ph.D. thesis, we did not consider the requirements of High Priority Practices Guide because it is composed of a set of the main recommended practices, which means that its requirements are already included in the other guides.

4.2.2 Types of Relations Investigated

During the process of relation establishment between EMRAM and SAFER Guides requirements, we investigated three types of relations: (1) direct; (2) indirect; and (3) partial. Therefore, the relations identified in this study were manually classified by the authors using these three types of relations. The direct relation indicates a perfect match, that is, both requirements are equivalents. The indirect relation indicates that one of the requirements indirectly requires the same criteria as the other. For example, SAFER Guides requires that allergy shall be coded. Despite EMRAM does not have this requirement, it requires drug-allergy alerts which indirectly implicates that the allergy should be coded. The partial relation indicates that one requirement partially requires the same criteria as the other.

For each SAFER Guides requirement, we identified one of these three relations to EMRAM requirements. We included a rational when the relation was “indirect” or “partial”.

4.2.3 Results of EMRAM and SAFER Guides Mapping

We extracted 775 SAFER Guides requirements which 696 was considered after the removal of the duplicate requirements from High Priority Practices guide. We identified 108 SAFER Guides requirements with some relation to EMRAM requirements. On the other hand, we found 38 EMRAM requirements with some relation to SAFER Guides requirements, which means that the relations were not one-to-one. For example, the SAFER Guides requirement “Orders for diagnostic tests are placed using CPOE and electronically transmitted to the diagnostic service provider (e.g., laboratory, radiology)” is related directly to two EMRAM requirements: “Lab orders shall be sent electronically

from the CPOE to the Laboratory Information System (LIS)" and "Radiology orders shall be sent electronically from the CPOE to the Radiology Information System (RIS)". The many-to-many relations are inherent to the SAFER Guides structure and EMRAM requirements extraction.

Out of 696 SAFER Guides requirements, we identified 108 relations to EMRAM requirements (15,5%) which indicates that EMRAM does not include most of SAFER Guides requirements. Most of these relations is associated to Contingency Planning (39,7%) and Computerized Provider Order Entry (CPOE) with Decision Support (26,9%).

The following results are presented considering relations on direction from SAFER Guides to EMRAM requirements. Table 10 presents the number of relations with EMRAM identified for each SAFER Guides requirement.

Table 10 – Number of relations with EMRAM identified for each guide

Guide Category	**Domain Guide**	**No. SAFER Guides Requirements**	**No. Direct Relations**	**No. Indirect Relations**	**No. Partial Relations**	**Total of SAFER Guides Requirements with some relation to EMRAM**
Clinical Process	Computerized Provider Order Entry (CPOE) with Decision Support	130	9	21	5	35
Clinical Process	Patient Identification	60	0	0	1	1
Clinical Process	Test Results Reporting and Follow-Up	90	5	1	3	9
Clinical Process	Clinician Communication	66	0	0	0	0
Foundational Guides	Organizational Responsibilities	123	1	13	1	15
Infrastructure	Contingency Planning	73	11	13	5	29
Infrastructure	System Configuration	80	6	10	0	16
Infrastructure	System Interfaces	81	0	2	1	3

We identified 32 SAFER Guides requirements with a direct relation to EMRAM requirements, which 14 are from Clinical Process Guides (9 from CPOE with Decision Support Guide and 5 from Test Results Reporting and Follow-Up Guide), 17 from Infrastructure Guides (11 from Contingency Planning and 6 from System Configuration), and one from Foundational Guides (all of them from Organization Responsibilities Guide).

Table 11 presents some examples of direct relations between SAFER Guides and EMRAM requirements.

Most of the direct relations identified is related to contingency planning, which goal is to prevent and mitigate EHR downtime. Nine requirements from CPOE with Decision Support Guide are directly related to EMRAM, specially because of the requirement of alerts in CPOE. It is important to note that there are other types of CPOE alerts required by SAFER Guides, but not required by EMRAM, such as drug-patient age alerts. Besides, SAFER Guides require other kinds of functionalities related to clinical decision support on CPOE that are not required by EMRAM, such as the external knowledge bases access. To that purpose, the EHR can be integrated to the Health Level 7 (HL7) Context Aware Knowledge Retrieval Application ("Infobutton"), which provides the communication between the EHR and knowledge resources[9].

[9] http://www.openinfobutton.org/hl7-infobutton-standard

Table 11- Examples of direct relations between SAFER Guides and EMRAM requirements

SAFER Guides Requirement	EMRAM Requirement Related
Drug-allergy interaction checking occurs during the entry of new medication orders.	CPOE shall provide drug-allergy alerts.
Drug-drug interaction checking occurs before medication orders are submitted for dispensing.	CPOE shall provide drug-drug interaction alerts.
Dose range checking for single dose occurs before medication orders are submitted for dispensing.	CPOE shall provide dose range alerts.
Results outside normal reference ranges, or otherwise determined to be abnormal, are flagged (i.e., presented in a visually distinct way).	Laboratory testes results outside normal reference ranges shall be flagged (i.e., presented in a visually distinct way).
Hardware that runs applications critical to the organization's operation is duplicated.	The hospital shall have an IT redundancy plan (data redundancy, support hardware, and network).
Users are trained on how to proceed during system unavailability (i.e., downtimes).	The care team of the hospital shall be aware of the IT resources available during systems unavailability.

We identified 60 indirect relations between SAFER Guides and EMRAM requirements, which 22 are from Clinical Process Guide (21 from CPOE with Decision Support Guide and 1 from Test Results Reporting and Follow-Up Guide), 25 from Infrastructure Guides (13 from Contingency Planning, 2 from System Interfaces, and 10 from System Configuration), and 13 from Foundational Guides (all of them from Organization Responsibilities Guide). Table 12 presents some examples of indirect relations between SAFER Guides and EMRAM requirements.

Most of indirect relations is due to EMRAM requirements that are not so specific as SAFER Guides. For example, EMRAM requires the hospital to have one or more committees to discuss Clinical Decision Support (CDS) governance and functionalities, but it does not specify what exactly should be discussed, while SAFER Guides requires specific aspects that should be addressed, such as order-sets updating and alert fatigue.

Table 12 – Examples of indirect relations between SAFER Guides and EMRAM requirements

SAFER Guides Requirement	EMRAM Requirement Related	Relation Rationale
Coded allergen and reaction information (or "no known allergies" [NKA]) are entered and updated in the EHR prior to any order entry.	CPOE shall provide drug-allergy alerts.	EMRAM requires drug-allergy alerts, which requires coded entry of allergies in the EHR.
Backup media are rendered unreadable (i.e., use software to scramble media contents or physically destroy/shred media) before disposal.	The hospital shall have data destruction policy (devices, backup media, paper documents, servers, computers, etc.).	EMRAM requires that the hospital has data destruction policies, which includes access to backup media destruction.
The server hosting the interface hardware and software is maintained in a physically secure (i.e., locked room) location.	The hospital shall have physical access policy to IT system / datacenters.	EMRAM requires physical access policy, which includes interface hardware.
The EHR is hosted safely in a physically and electronically secure manner.	The hospital shall have physical access policy to IT system / datacenters.	EMRAM requires physical access policies, which includes the EHR.

We identified 16 partial relations between SAFER Guides and EMRAM requirements, which 9 are from Clinical Process Guide (5 from CPOE with Decision Support Guide, 3 from Test Results Reporting and Follow-Up Guide, and 1 from Patient Identification Guide), 6 from Infrastructure Guides (5 from Contingency Planning and 1 from System Interfaces), and 1 from Foundational Guides (from Organization Responsibilities Guide). Table 13 presents some examples of partial relations between SAFER Guides and EMRAM requirements.

The main reason for partial relations is because of SAFER Guides structure that usually requires more than one criterion in the same requirement, while EMRAM requirement extraction considered only atomic requirements. For example, SAFER Guides require the hospital to use and maintain updated operating systems, virus and malware protection software, application software, and interface protocols. On the other hand, EMRAM only addresses the use and maintenance of anti-virus and anti-malware.

Another important partial relation is due to an important requirement from EMRAM that is not required in SAFER Guides, the Technology-Enabled Bedside Product Administration. That process specifies that the hospital must use some technology (barcode, QR code, etc.) to identify patients and products to be administrated at the bedside (at least medication, human milk, and blood products). Through scanning of patient wristband and product, the Electronic Medical Record (EHR) shall verify whether the patient and product identification are correct. If some mistake is detected (for example, professional scanned a drug not prescribed to the patient), the EHR shall alert the professional, preventing a potential product administration mistake. For medication, EMRAM also requires the EHR to alert about correct time, dose, and administration route.

Despite SAFER Guides does not require Technology-Enabled Bedside Product Administration, it demands a comprehensive set of practices related to safe patient identification. Most of them are not addressed to EMRAM because only one relation in Patient Identification Guide was identified.

Table 13 – Examples of partial relations between SAFER Guides and EMRAM requirements

SAFER Guides Requirement	EMRAM Requirement Related	Relation Rationale
Order entry information is electronically communicated (e.g., through the computer or mobile messaging) to the people responsible for carrying out the order.	All medications and other materials must be automatically sent from the CPOE to the pharmacy worklist (PHIS).	SAFER Guides requirement is more comprehensive.
The EHR facilitates the tracking of "send-out" tests at the point of ordering and provides a mechanism to allow clinicians or organizations to incorporate these results into the EHR and assign them to the correct patient.	Results of laboratory tests are electronically sent in a structured form and stored on the EHR, so that the data can be used for analysis and for clinical decision support mechanisms.	EMRAM requires that tests result to be incorporated into the EHR automatically.

Patient identity is verified at key points or transitions in the care process (e.g., prior to procedures and surgeries, rooming patient, vital sign recording, order entry, medication administration, check out).	The patient shall be identified using a technology that allows unique identification, such as a bar code on a wristband.	EMRAM requires Technology-Enabled Bedside Product Administration
Organizational policy facilitates reporting of EHR-related hazards and errors and ensures that reports are promptly investigated and addressed.	The hospital shall report “overrides” and “near miss” to track potential mistakes during bedside product administration. For example, scanning an incorrect drug.	EMRAM requires EHR-related hazards reporting only for bedside product administration.
The EHR downtime policy describes when the warm-site backup process should be activated (ideally, before the system has been down for 2 hours).	The hospital shall have a formal procedure for EHR reactivation after downtime describing all steps to activate the redundant datacenter and subsequent return to the main datacenter.	EMRAM requirement has less specifications.
Established and up-to-date versions of operating systems, virus and malware protection software, application software, and interface protocols are used.	Hospital shall use and maintain anti-virus and anti-malware tools on their devices.	This EMRAM requirement requires only virus and malware protection.

4.2.4 EMRAM-SAFER Guides Mapping Limitations

The identification of relations of EMRAM and SAFER Guides requirements performed in this study was not submitted to a validation process by other specialists, which is a limitation of the study. Such validation was not possible because of the limited number of specialists in EMRAM in Brazil. In addition, as previously mentioned, HIMSS Analytics do not provide a publicly detailed source with EMRAM requirements.

4.3 Discussion

This phase of our investigation focused on comparing EMRAM, JCI, and SAFER Guides. The analysis revealed key results that highlights strengths and weaknesses, offering valuable insights into the effectiveness of each model for improving Health IT safety.

Our analysis of JCI requirements identified 11 IT-related aspects. Notably, five of these are not directly addressed by EMRAM. Most of them are related to copy and paste policies. On the other hand, JCI is not focused on Health IT and, therefore, EMRAM is a more targeted framework for assessing and improving Health IT safety. For instance, JCI mandates a safe medication administration process, but it doesn't require technology-enabled bedside product administration, which EMRAM enforces. This highlights EMRAM's focus on leveraging technology to enhance safety.

A comparison with SAFER Guides reveals a wider gap in EMRAM. Only 108 out of 696 SAFER Guides requirements are directly addressed by EMRAM. However, a key finding emerged during the mapping process: none of EMRAM's technology-enabled bedside product administration requirements are addressed by SAFER Guides. This suggests a potential blind spot in SAFER Guides, as these functionalities can significantly improve patient safety. Furthermore, SAFER Guides lack the structure of a maturity model. This makes it less user-friendly for healthcare organizations seeking a roadmap for incremental improvements in their Health IT safety maturity.

The types of relationships investigated in each mapping (EMRAM x JCI and EMRAM x SAFER Guides) differ due to the distinct structures of the JCI and SAFER Guides models. JCI does not primarily focus on IT, so identifying requirements directly related to IT was crucial. Conversely, the SAFER Guides specifically address IT and patient safety, allowing us to concentrate on identifying relationships with EMRAM requirements.

Our comparison of EMRAM, JCI, and SAFER Guides revealed limitations in each model's ability to comprehensively address health IT and patient safety. This underscores the need for a new, more holistic maturity model. Table 14 presents a summary of each model, highlighting their goals, and relation to Health IT and patient safety. We also present their strengths and weaknesses in comparison to each other.

Table 14 - Comparison between EMRAM, JCI and SAFER Guides

Model	Highlights
EMRAM	**Goal** To offer a roadmap to promote the use of information technology to improve efficiency and patient outcomes. **Relation to Health IT and Patient Safety** All requirements are related to Health IT, but not necessarily related to patient safety. **Strengths** - It is structured as a maturity model. - It includes technology-enabled bedside product administration requirements, which are not required by JCI and SAFER Guides. **Weaknesses** - It is not totally focused on patient safety. - It does not address 5 IT-related JCI requirements. - It does not address 588 SAFER Guides requirements.
JCI	**Goal** To specify policies and process to promote a better quality of patient care and governance in healthcare organizations. **Relation to Health IT and Patient Safety** Accreditation focused on patient safety, but not on Health IT. **Strengths** - Includes 5 Health IT safety requirements that are not addressed by EMRAM. **Weaknesses** - It is not structured as a maturity model. - It is not focused on Health IT. There are only 11 requirements directly related to Health IT.

SAFER Guides	**Goal** To offer a set of guidelines focused on enabling healthcare organizations to address information technology safety. **Relation to Health IT and Patient Safety** Totally focused on Health IT and patient Safety. **Strengths** - Totally focused on Health IT safety. **Weaknesses** - It is not structured as a maturity model. - It does not address technology-enabled bedside product administration requirements.

4.4 Final Remarks

In this phase of our investigation, we develop two mappings: EMRAM-JCI requirements and EMRAM-SAFER Guides requirements. One of the main goals of this investigation was to identify relations between these three models so we could find gaps and opportunities to integration of them, obtaining a more specific model to evaluate health IT safety. Therefore, the mappings and comparisons between EMRAM, JCI and SAFER Guides were used in a complementary manner to develop HITSMM during the second phase of this Ph.D. thesis, presented on Chapter 5.

Chapter 5

The Health IT Safety Maturity Model

To develop the HITSMM, we used the mappings resulted from the previous phase of this Ph.D. thesis. The mappings were used to identify requirements related to patient safety in these three evaluation methods. This was the basis in our methodology as a starting point to group them in a unique maturity model.

The maturity model was developed through the following tasks: requirement analysis, duplicate removal, requirements grouping, definition of categories, definition of maturity stages, and evaluation by domain specialists (Figure 4).

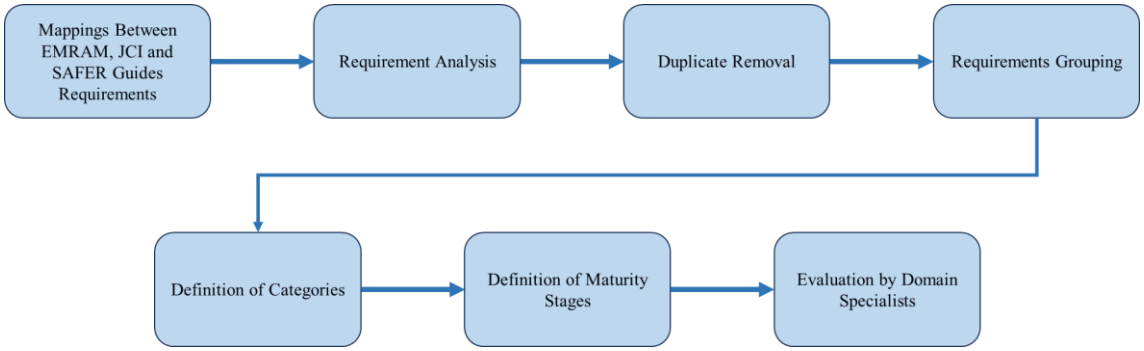


Figure 4 - Summarization of the process of HITSMM Development

5.1 Requirement Analysis

To develop the maturity model, it was necessary to identify requirements that address patient safety related to Health IT in the three evaluation methods (JCI, EMRAM and SAFER Guides). We analyzed each requirement to verify whether it is related to information technology and has a positive impact on patient safety.

For JCI analysis, we selected the 11 IT-related requirements identified in the previous study because all of them can have an impact on patient safety. The functionalities of copying and pasting health records can facilitate professional documentation, but when misused, can result in issues such as propagation of incorrect

information and registration of outdated information. EHR downtime without a contingency planning can affect patient care because professionals may have no access to the patient's medical record. In addition, performing tests before and after Health IT implementation is essential to ensure its proper performance.

Once SAFER Guides is related specifically to Health IT and patient safety, all its 147 generic requirements were considered. EMRAM is composed of 116 requirements analysis, which we considered only the ones related to patient safety. Therefore, we removed a set of 29 requirements related to data analytics and patient safety, obtaining 87 requirements.

5.2 Duplicate Removal and Requirements Grouping

After analyzing requirements, we obtained a list with 245 requirements related to Health IT and patient safety. The mapping developed previously was able to identify requirements that are specified by both EMRAM, JCI and SAFER Guides. Therefore, we used these mappings to identify and remove duplicates between requirements. All of 11 IT-related JCI requirements are also addressed by EMRAM and/or SAFER Guides and, therefore, had considered them as duplicate. Out of 116 EMRAM requirements, we removed 38 that are also included in SAFER Guides. Therefore, we removed 49 duplicate and obtained a list of unique 196 requirements.

To simplify and better organize the maturity model, many of these requirements, especially in SAFER Guides, were grouped in only one requirement once were related to similar aspects. For example, SAFER Guides has four requirements related to Clinical Decision Support (CDS) presentation adequacy, which were unified in only one requirement in the maturity model. Table 15 presents these four requirements (first column) that were grouped in only one requirement (second column). With this grouping task, we grouped 69 requirements in only 11. Figure 5 summarizes the process of obtaining the requirements list.

Table 15 - Grouping of Requirements

Safer Guides Requirement	Maturity Model Requirement
CDS alerts are displayed in the relevant clinical context.	The hospital shall have policies to evaluate CDS presentation adequacy that include, but is not limited to: - Evaluation if CDS alerts are displayed in the relevant clinical context. - Evaluation of interruptive alerts (e.g., pop-ups at the time of ordering). These kinds of alerts shall be used with discretion and only for high risk and/or priority conditions. - Review interactions so that only the most significant interaction-related alerts, as determined by the organization, are presented to clinicians. - Evaluation of clarity of questions posed to users.
Interruptive alerts (e.g., pop-ups at the time of ordering) are used with discretion and only for high risk, high priority conditions.	
A process is in place to review interactions so that only the most significant interaction-related alerts, as determined by the organization, are presented to clinicians.	
Questions presented to the user by CPOE or CDS are unambiguous.	

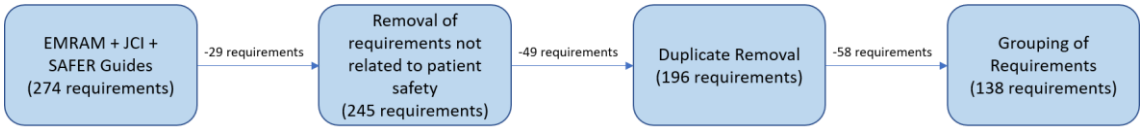


Figure 5 - Summarization of the process of obtaining the requirement list

5.3 Definition of Categories and Maturity Stages

After specifications of requirements, the maturity model was organized through two tasks: definition of categories and definition of requirements maturity stage. In the first task, we identified thematic groups of requirements based specially on SAFER Guides requirements categories.

In the second task, we defined the requirements maturity stages. Once the adoption of EMRAM is being disseminated around the world, we developed a maturity model with a similar structure to HIMSS Analytics maturity models. Therefore, the

maturity stages of HITSMM ranges from one to seven, where the higher the stage, the greater the maturity.

To define the maturity stage of a requirement, we considered three aspects: (1) importance of the requirement to patient safety; (2) complexity for development by information technology; and (3) complexity for implementation by the healthcare institution. For each aspect, we assigned a score from 1 to 7. For the first aspect, the higher the score, the greater the importance of the requirement to patient safety. For the second and third aspects, the higher the score, the greater the complexity to development and implementation, respectively.

To determine the maturity stage, we calculated the weighted average of the three aspects. Once we embraced the concept of an evolution model where the healthcare institution can progress in maturity across stages, aspects two and three were assigned a weight of two, while aspect one was given a weight of one. Additionally, to perform the calculation of the maturity stage, it was also necessary to apply an inversion of the score assigned to the first aspect. This is because the higher the score, the greater the importance of the requirement for patient safety, and consequently, the lower the maturity stage at which it should be mandated. For instance, a requirement with a score of 7 for aspect one was inverted to a score of 1, whereas a requirement with a score of 5 was inverted to a score of 3. Therefore, the formula used for determining the maturity stage of a requirement based on its scores was:

$$\textit{Maturity Stage} = \textit{Round Up } (((\textit{Score Aspect 1}) + (2 \times \textit{Score Aspect 2}) + (2 \times \textit{Score Aspect 3})) \div 5)$$

That analysis considered that complex requirements demand the need for formalization of organizational policies and team trainings; human process changes; acquisition of different tools; and/or acquisition of high-cost infrastructure.

For example, the implementation of technology-enabled bedside administration requires the acquisition of laptops, scanners devices, full Wi-Fi coverage, changes in process, trainings, and organizational policies to formalize the process. Therefore, requirements related to technology-enabled bedside administration were included in higher stages.

For illustration purposes, Table 16 outlines three requirements associated with the implementation of technology-enabled bedside medication administration. The initial requirement specifies that the healthcare organization implements this process in at least

25% of the medication administration volume. Subsequently, for the second and third requirements, this percentage escalates to 50% and 95%, respectively. This progression adds complexity to the implementation for the healthcare organization and, consequently, elevates the maturity stage.

Table 16 - Examples requirements associated with the implementation of technology-enabled bedside medication administration

Requirement	Importance to Patient Safety (inverted)	Development Complexity	Implementation Complexity	Maturity Stage
The organization shall implement a process for Technology-Enabled Bedside Product Administration using the patient's wristband identification code and the medications to be administered. The system of bedside administration shall automatically check the 5 rights of medication administration: patient, medication, data/hour, route and dose. This process should be implemented for a minimum of 25% of the total administration volume.	3	7	4	5

The hospital shall implement a process for Technology-Enabled Bedside Product Administration using the patient's wristband identification code and the medications to be administered. The system of bedside administration shall automatically check the 5 rights of medication administration: patient, medication, data/hour, route and dose. This process should be implemented for a minimum of 50% of the total administration volume.	3	7	6	6
The hospital shall implement a process for Technology-Enabled Bedside Product Administration using the patient's wristband identification code and the medications to be administered. The system of bedside administration shall automatically check the 5 rights of medication administration: patient, medication, data/hour, route and dose. This process should be implemented for a minimum of 95% of the total administration volume.	3	7	7	7

5.4 Evaluation by Domain Specialists

The maturity model was submitted to an evaluation process by five digital health specialists with extensive experience as consultants in improving healthcare processes through information technology. The validation process was concentrated on eliciting

the opinions of each specialist regarding the requirement specifications and their respective maturity stages. We conducted a meeting with the specialists to elucidate the objectives and structure of HITSMM, and to guide them on how to effectively carry out the validation process.

The specialists analyzed all HITSMM requirements to indicate whether he/she agrees with the requirement text and the stage assigned to the requirement. After the evaluation process, the specialists' suggestions were evaluated to verify if it would be necessary to adjust any requirements and/or stages. This evaluation considered the consistence of the specialists' comments related to their opinion about the degree of development complexity, degree of implementation complexity and importance to patient safety.

The validation process resulted in 15 maturity stages changes. Most of these changes is related to the requirements about Contingency Planning (10 requirements). Three specialists noted that such requirements are of great importance to patient safety and, therefore, should be in a lower maturity stage. As a result, we increased the score of importance to patient safety of these requirements from 6 to 7, and consequently, the maturity stage decreased from 6 to 5. The low number of changes requested by specialists during the validation process suggests that the original decision on the maturity stage of the requirements specified in HITSMM was consistent. Table 17 presents examples of specialists' comments and respective changes applied.

Table 17 - Examples of specialists' comments and respective changes applied

Requirement	Specialist Comments	Changes Applied
The hospital shall have policies and procedures on EHR downtimes and recovery processes to ensure continuity of operations regarding safe patient care and critical business operations. The policies shall include at least: - When a downtime should be called.	The requirements related to contingency plans are crucial for patient safety. Therefore, they should be in a lower stage.	Importance to Patient Safety (inverted): from 2 to 1 Stage: from 6 to 5

- Who will be in charge during the downtime (both on the clinical and technical side). - How everyone will be notified. - What are the procedures to recovery. The EHR downtime policy is reviewed at least every 2 years.		
"TALLman lettering" shall be used to prevent from order entry errors due to orthographically similar medication names (sound alike, look alike).	It is not a complex task for EHRs. Therefore, it should be on a lower stage.	Development Complexity: from 6 to 4 Stage: from 6 to 5
All medications (including the anesthetic record) administered to the patient during medical procedures, must be recorded in the administration module at the time the patient is in the next level of care (for example, after the patient leaves the Surgical Center).	Although it is not complex to develop in the system, this requirement is complex to implement in the care process. Therefore, it should be in a higher stage.	Implementation complexity: from 2 to 4 Stage: from 2 to 3
The hospital shall develop a process to regulate the proper use of copy and paste.	It is not a complex task for the system. Therefore, this requirement should be in a lower stage.	Development complexity: from 6 to 5 Stage: from 7 to 6

5.5 Results of HITSMM Development

The HITSMM comprises 138 requirements organized into seven stages and 12 categories. The stage structure draws inspiration from EMRAM, while the categories are primarily based on the SAFER Guides. In addition to the SAFER Guides categories, we incorporated four additional categories to better classify requirements addressed by EMRAM but not directly covered by the SAFER Guides (Clinical Documentation, Pharmacy, Product Administration, Laboratory and Blood Bank, Medical Imaging).

To enhance the integration of EMRAM and SAFER Guides requirements, we renamed the SAFER Guides "System Interfaces" category as "Interoperability" and merged the "Organizational Responsibilities" and "System Configuration" categories into a single category called "System Configuration and Governance.

5.5.1 HITSMM Categories

HITSMM is composed by the categories:

- Patient Identification,
- Clinical Documentation;
- Computerized Provider Order Entry (CPOE);
- Pharmacy;
- Product Administration;
- Tests Results Reporting and Follow-up;
- Laboratory and Blood Bank;
- Medical Imaging;
- Clinical Communication;
- Contingency Planning;
- Interoperability;
- System Configuration and Governance.

The category Patient Identification is focused on recommended practices to safe identification of patients. Clinical Documentation category specifies requirements related to the electronic documentation of health information.

The category CPOE includes requirements related to safe design and use of the electronic prescription, as well as Clinical Decision Support (CDS) resources such as drug-drug interaction alerts. The Pharmacy category is focused on Health IT best practices related to pharmacy that can impact on patient safety, such as pharmaceutical evaluation of prescriptions and medication dispensation.

In Product Administration category, we evaluate the proper use of technology to safe administration of medication and other products (blood, milk, etc.). This category addresses specially the technology-enabled bedside administration, which requires the

use of barcode, QR code, etc. to identify patients and products to be administrated at the bedside.

The category of Tests Results Reporting and Follow-up addresses requirements related to the use of technology to support the process of communication and follow-up of tests results. Laboratory and Blood Bank category is composed by requirements related to the use of technology in the process of samples collection and correct association of blood products to patients. The Medical Imaging category includes requirements related to availability of clinical documentation, reports, and medical images to health professionals.

Clinical Communication is composed by requirements related to the use of technology to ensure proper electronic communication between professionals to avoid communication breakdowns. The Contingency Planning category addresses the best practices to avoid and deal with information system downtime.

Interoperability category addresses requirements related to health data exchange for continuity of care, as well as best practices to ensure safe system interfaces. The System Configuration and Governance category is composed by requirements related to the configuration of the Health IT hardware and software and best practices related to the management of Health IT in the organization.

5.5.2 HITSMM Stages

To determine the amount of maturity stages of HITSMM, we used HIMSS' maturity models as references to the structure of our model. Therefore, the HITSMM requirements were distributed in seven stages according to their importance to patient safety, development complexity and implementation complexity. Since the requirements of the maturity model are cumulative over the stages, a stage includes all requirements of the previous stages.

Additionally, to continuously increase maturity, some requirements follow the same criteria, but with greater rigor throughout the stages. For example, the technology-enabled bedside administration is required first in stage 5. However, the percentage of administrations using this technology must be at least 25% in stage 5, while it must be greater than 50% in stage 6 and 100% in stage 7.

Another strategy to increase maturity in each subsequent stage was to distribute different requirements throughout the stages according to their importance and complexity. For example, the CPOE category includes many requirements related to safety alerts during prescription. Alerts such as drug-allergy, drug-drug interaction and duplicate order were included in stage 3. The stage 4 adds the alerts for drug-condition, drug-patient age, dose range, and daily dose. The stage 5 includes drug-diet and drug-lab results checking. The stage 6 adds safety alerts for tests and procedures, while the stage 7 adds alerts when recording allergies, medical conditions and test results.

Table 18 presents the number of requirements for each stage and category and

Table 19 presents the main aspects evaluated in each HITSMM maturity stages. System Configuration and Governance is the category with more requirements especially due to recommendations related to governance in Health IT. The second category with more requirements is CPOE. This category is composed specially by best practices related to clinical decision support, such as safety alerts during prescription. Appendix A presents the table with HITSMM requirements.

Table 18 - Number of Requirements in Each Stage and Each Category

Category	Number of Requirements							
	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**	**Total**
Clinical Communication	0	0	0	0	4	0	0	**4**
Clinical Documentation	4	4	3	1	1	1	2	**16**
Contingency Planning	0	0	0	0	10	0	0	**10**
CPOE	1	2	3	6	3	2	1	**18**
Interoperability	0	0	3	4	2	0	2	**11**
Laboratory and Blood Bank	0	0	0	0	3	1	1	**5**
Medical Imaging	0	2	0	0	0	0	0	**2**
Patient Identification	0	1	6	0	0	0	0	**7**
Pharmacy	0	1	0	2	12	1	1	**17**
Product Administration	0	2	1	0	4	3	3	**13**
System Configuration and Governance	0	0	2	0	9	4	8	**23**
Tests Results Reporting and Follow-up	0	4	1	6	0	1	0	**12**
Total Geral	**5**	**16**	**19**	**19**	**48**	**13**	**18**	**138**

Table 19 - HITSMM Maturity Stages

Stage 1
Electronic clinical documentation. Structured CPOE and diagnostic recording.
Stage 2
Structured clinical documentation. All clinical systems integrated.
Stage 3
Clinical Decision Support (three types of alerts on CPOE and order sets). Safe patient identification. All clinical documentation available in the information system. Safe system interfaces.
Stage 4
Clinical Decision Support (seven types of alerts on CPOE and order sets). Safe drug unitarization, storing and dispensing. Safe tests results reporting and follow-up. Safe system interfaces.
Stage 5
Clinical Decision Support (nine types of alerts on CPOE, order sets and one clinical protocol). Technology-enabled bedside administration (25% of administrations). Clinical Pharmacy (evaluation of 25% of orders). Safe communication. Safe system interfaces. IT support and systems tests. Contingency Planning.
Stage 6
Clinical Decision Support (11 types of alerts on CPOE, order sets and two clinical protocols). Technology-enabled bedside administration (50% of administrations). Clinical Pharmacy (evaluation of 50% of orders).
Stage 7
Clinical Decision Support (11 types of alerts on CPOE, order sets, five clinical protocols and alerts when recording allergies, medical conditions, and test results). Technology-enabled bedside administration (100% of administrations). Clinical Pharmacy (evaluation of 100% of orders). Interoperability for continuity of care. Governance committees. Safety events management.

5.6 Discussion

In this phase of our investigation, we used EMRAM, JCI and SAFER Guides in a complementary manner to develop HITSMM, a maturity model to evaluate and guide healthcare organizations to improve patient safety through IT. The requirements included in the HITSMM address all aspects of patient safety related to Health IT specified by JCI, EMRAM and SAFER Guides.

The HITSMM can be used by healthcare organizations to evaluate what is its current maturity stage regarding Health IT and patient safety, as well as to identify recommendations to improve its maturity by implementing HITSMM requirements. Therefore, the model guides healthcare organizations in progressively optimizing IT for enhanced patient safety.

In this Ph.D thesis, we only considered three models as references (EMRAM, SAFER Guides, and JCI) to develop HITSMM. The use of these specific models was based on our exploratory study, which focused on widely adopted references, and the author's experience. Consequently, other models such as the Brazilian Accreditation National Organization (ONA), standards from the International Organization for Standardization (ISO), and other HIMSS' maturity models (e.g., CCMM) were not considered. This limitation means our maturity model does not address aspects not covered by the reference models, such as the use of artificial intelligence in healthcare, telemedicine, and patient-facing IT applications.

5.7 Final Remarks

In the second phase of this Ph.D. thesis, we conducted the development of HITSMM using as inputs the mappings developed in the first phase. Our resulting model was than applied in practice in the third phase which employed a concept proof approach to assess the practical application of the HITSMM in two hospitals. The results of this concept proof are presented in Chapter 6.

Chapter 6

HITSMM in Practice

After HITSMM development, we applied the model in two Brazilian private hospitals. To protect the confidentiality of the two participating hospitals, we have not identified them in this document. We refer to them as Hospital A and Hospital B. We selected hospitals that have already been validated on EMRAM Stage 6 because we aimed to investigate whether the participants perceive HITSMM can evaluate a more comprehensive set of requirements related to patient safety than EMRAM.

6.1 HITSMM Application Method

To assess hospital adherence to HITSMM requirements, we conducted two separate virtual meetings and interviews with key personnel at each institution. Participants included IT professionals and managers directly involved in healthcare IT operations and that were responsible to lead EMRAM certification project. For each hospital, only one virtual meeting of approximately three hours were caried out with all professionals invited.

During the interviews, we systematically evaluated each HITSMM requirement, asking questions to investigate the conformance of the hospital to the respective requirement being evaluated. We documented the participant responses and registered conformances and gaps on a dedicated spreadsheet. For each gap, we outlined specific actions the hospital should take to achieve compliance. By linking each requirement to its corresponding maturity stage, we were able to determine the hospital's overall HITSMM maturity level, reflecting its current health IT safety posture. Figure 6 presents an example of how we documented compliances and gaps with HITSMM requirements.

ID	Category	Requirement	Description	Stage	Compliance
CPOE.04	CPOE	Order sets	Evidence-based order sets shall be available in the EHR for common tasks and conditions and be updated regularly.	3	Compliant
CPOE.05	CPOE	Drug-allergy interaction checking on CPOE	Drug-allergy interaction checking shall occur during the entry of new medication orders.	3	Compliant
CPOE.06	CPOE	Drug-drug interaction checking on CPOE	Drug-drug interaction checking shall occur during the entry of new medication orders.	3	Not compliant
CPOE.07	CPOE	Duplicate order checking	Duplicate order checking shall occur for at least high risk medication, diagnostic tests, and procedure orders (excluding "as needed" medications).	3	Not compliant
CPOE.08	CPOE	Drug-condition checking	Drug-condition checking shall occur for important interactions between drugs and conditions.	4	Not compliant
CPOE.09	CPOE	Drug-patient age checking	Drug-patient age checking shall occur for important age-related medication issues.	4	Not compliant

Figure 6 - Documentation of HITSMM Application

Following the interviews, participants were invited to participate in a brief questionnaire gauging their satisfaction with HITSMM and its impact on health IT safety. The survey employed eight statements using a Likert scale format, where participants indicated their level of agreement with each statement.

Table 20 summarizes the questions included in the HITSMM satisfaction survey. Appendix B presents the complete questionnaire.

Table 20 - Statements applied in the HITSMM satisfaction questionnaire.

Number	Statement
Statement 1	IT can negatively impact patient safety when not properly developed and/or used.
Statement 2	IT can be used as an ally to improve patient safety.
Statement 3	Healthcare organizations must assess patient safety considering not only care processes, but also their information systems and the way people and processes interact with these systems.
Statement 4	HITSMM works as a guide for the progressive evolution of health IT safety.
Statement 5	HITSMM can be used to assess the current stage of a healthcare organization about the maturity of the use of IT in favor of patient safety.
Statement 6	HITSMM can promote improvements in patient safety through the adoption and safe use of technology.
Statement 7	HITSMM includes important IT-related aspects not evaluated by other certification and accreditation models, such as EMRAM-HIMSS and JCI.
Statement 8	The distribution of requirements over the HITSMM maturity stages is adequate, so more complex requirements are at higher stages.

6.2 HITSMM Application Results

6.2.1 Maturity Stage Evaluation

Our evaluation adopted a rigorous approach, defining hospital attainment of a specific stage only if complete compliance was achieved with all requirements within that stage and all preceding stages. This ensured a comprehensive assessment of health IT safety practices, leaving no room for gaps at any level.

Table 21 and Table 22 present the compliance of each Hospital A and Hospital B, respectively, for each maturity stage. The first collum presents a specific maturity stage, while the second and third columns present the percentage of compliant requirements and the percentage of no compliant requirements. Lines colored in green represents the stages which the Hospital A and B achieved 100% of compliance. Both hospitals achieved 100% of compliance for stages 1 and 2 but did not achieve 100% of compliance for subsequent stages. Therefore, the hospitals were classified on HITSMM's stage 2.

Table 21 - Hospital A Compliance for each stage of the HITSMM

Stage	Compliant	Not compliant
1	100%	0%
2	100%	0%
3	53%	47%
4	47%	53%
5	73%	27%
6	62%	38%
7	33%	67%

Table 22 - Hospital B Compliance for each stage of the HITSMM

Stage	Compliant	Not compliant
1	100%	0%
2	100%	0%
3	53%	47%
4	47%	53%
5	68%	32%
6	42%	58%
7	0%	100%

Table 23 and

Table 24 present the compliance of each Hospital A and Hospital B, for each HITSMM category. The first collum presents a specific category, while the second and third columns present the percentage of compliant requirements and the percentage of no compliant requirements. The hospitals achieved a very similar overall conformance.

Table 23. Hospital A Compliance for each category of the HITSMM

Category	Compliant	Not compliant
Clinical Communication	50%	50%
Clinical Documentation	88%	13%
Contingency Planning	70%	30%
CPOE	44%	56%
Interoperability	64%	36%
Laboratory and Blood Bank	100%	0%
Medical Imaging	100%	0%
Patient Identification	43%	57%
Pharmacy	65%	35%
Product Administration	92%	8%
System Configuration and Governance	57%	43%
Tests Results Reporting and Follow-up	42%	58%
Total	**64%**	**36%**

Table 24. Hospital B Compliance for each category of the HITSMM

Category	Compliant	Not compliant
Clinical Communication	75%	25%
Clinical Documentation	75%	25%
Contingency Planning	80%	20%
CPOE	61%	39%
Interoperability	18%	82%
Laboratory and Blood Bank	80%	20%
Medical Imaging	100%	0%
Patient Identification	29%	71%
Pharmacy	65%	35%
Product Administration	70%	30%
System Configuration and Governance	39%	61%
Tests Results Reporting and Follow-up	50%	50%
Total	**57%**	**43%**

6.2.2 HITSMM Satisfaction Evaluation

The second stage of our evaluation concerned the participants' perception of the usefulness of our proposal. To this end, one professional of each hospital answered a questionnaire to evaluate their satisfaction in relation to HITSMM through eight Likert scale statements. Therefore, for each statement, the participant indicated his/her agreement degree according to a Likert scale (strongly agree, agree, neutral, disagree, and strongly disagree). Table 25 presents the hospitals' responses to each statement in the questionnaire, which shows that HITSMM presented a very good satisfaction by the participants.

Table 25. Hospitals' responses to each statement on the HITSMM satisfaction assessment questionnaire

Statement	Hospital A Answer	Hospital B Answer
Statement 1: IT can negatively impact patient safety when not properly developed and/or used.	Agreed	Agreed
Statement 2: IT can be used as an ally to improve patient safety.	Strongly Agreed	Strongly Agreed
Statement 3: Healthcare organizations must assess patient safety considering not only care processes, but also their information systems and the way people and processes interact with these systems.	Strongly Agreed	Agreed
Statement 4: HITSMM works as a guide for the progressive evolution of health IT safety.	Strongly Agreed	Agreed
Statement 5: HITSMM can be used to assess the current stage of a healthcare organization about the maturity of the use of IT in favor of patient safety.	Strongly Agreed	Agreed
Statement 6: HITSMM can promote improvements for patient safety through the adoption and safe use of technology.	Strongly Agreed	Agreed
Statement 7: HITSMM includes important IT-related aspects not evaluated by other certification and accreditation models, such as EMRAM-HIMSS and JCI.	Strongly Agreed	Agreed
Statement 8: The distribution of requirements over the HITSMM maturity stages is adequate, so more complex requirements are at higher stages.	Strongly Agreed	Agreed

6.3 Discussion

Despite both hospitals achieving EMRAM Stage 6 validation, their HITSMM evaluations resulted in Stage 2 classifications. This discrepancy highlights HITSMM's

ability to assess safety aspects beyond the scope of EMRAM, addressing potential vulnerabilities not previously in EMRAM.

For instance, HITSMM enforces stricter safety measures, exemplified by its Stage 3 requirement prohibiting the simultaneous display of multiple patient records on the same screen. This requirement, absent in EMRAM, directly guards against potential patient misidentification, and associated medical errors.

Similarly, the findings for each category highlight the gaps between these two EMRAM stage 6 hospitals and the categories that involve requirements not yet assessed by EMRAM. For instance, the Clinical Documentation, Contingency Planning, Laboratory and Blood Bank, Medical Imaging, and Product Administration categories are extensively discussed in EMRAM stage 6 and exhibited a high level of compliance in both hospitals.

However, categories such as CPOE, Interoperability, Patient Identification, System Configuration and Governance, and Tests Results Reporting and Follow-up encompass several requirements that are not currently addressed by EMRAM, particularly in stage 6.

Table 26 presents some other examples of HITSMM requirements that are not addressed in EMRAM.

Table 26 - Examples of HITSMM requirements that are not addressed in EMRAM

Category	Requirement	HITSMM Maturity Stage
Patient Identification	The organization shall have policies and procedures to ensure the prevention and identification of duplicate patient records, as well as to perform the merging of duplicate records. Duplicate registration prevention activities include, but are not limited to: - Register patients using standardized procedures. - Train employees to search for patients in the system before creating a new record.	3
Patient Identification	The hospital shall have organizational policies to monitor the use of test patients in the production environment. When they do exist, they shall have unambiguously assigned "test" names (e.g., including numbers) and shall be clearly identifiable as test patients (e.g., different background color for patient header).	3
Clinical Documentation	Use of abbreviations and acronyms shall be minimized and standardized by the organization.	4
Interoperability	The operational status of the system interface shall be clear to its users regarding clinical use, such as knowing when the interface cannot transmit or receive messages, alerts, or crucial information.	4
CPOE	"TALLman lettering" shall be used to prevent from order entry errors due to orthographically similar medication names (sound alike, look alike).	5
System Configuration and Governance	The hospital shall have policies to ensure that the EHR is configured to make it difficult to confuse the live version of the EHR with other versions (training, test, and read-only backup versions). For example, the screen background color	5

	or the color of the patient headers could be different, policy and process for creating and naming test patients.	
System Configuration and Governance	The hospital shall develop a process to regulate the proper use of copy and paste.	6
System Configuration and Governance	The hospital shall monitor compliance with the use of guidelines for copy and paste actions and implement corrective actions, as needed.	6
System Configuration and Governance	The hospital shall have a mechanism for internal reporting of EHR-related safety hazards. Such mechanism should be for anonymous and no-fault. The hospital shall have formal process for addressing reported problems and for reporting problems externally to the developer. The user who reported the issue should be notified of the outcome when appropriate.	7
CPOE	The system should alert not only on electronic prescription but also when registering a new allergy, clinical conditions and test results.	7

Both hospitals exhibited instances where higher stages displayed greater compliance than lower stages. This is particularly evident in Hospital A, where conformance for stages 5 and 6 was 73% and 62% respectively, while conformance for stages 3 and 4 was 53% and 47% respectively. This can be attributed to the fact that some complex requirements specified in stages 5 to 7, like technology-enabled bedside administration, are already covered by EMRAM certification.

It's worth noting that the HITSMM application was conducted remotely due to the focus on validating the model's applicability and suitability. Additionally, both hospitals had previously undergone EMRAM certification, familiarizing them with the evaluation process. In scenarios where the goal is to apply HITSMM for a more detailed evaluation to support a consulting project, an in-person assessment is recommended to observe care processes and better evaluate conformance with HITSMM requirements. A comprehensive evaluation could take approximately three days, with seven to eight hours of assessment per day.

We observe that the size of the hospital being evaluated can influence the results of the HITSMM evaluation, particularly regarding requirements associated with technology-enabled bedside administration. For instance, HITSMM stage 5 mandates technology-enabled bedside administration in at least 25% of inpatient beds, while stages 6 and 7 require 50% and 95%, respectively. In hospitals with numerous inpatient units, implementing this technology in one or a few units might not reach the 95% or 50% threshold. Conversely, a hospital with only one inpatient unit would likely implement the requirement across the entire unit, easily surpassing the 95% mark for technology-enabled bedside administration compared to larger hospitals.

6.4 Final Remarks

This chapter presented the results of the third phase of our investigation: the application of HITSMM in practice. We applied HITSMM in two Brazilian hospitals already certified on EMRAM stage 6. Our goal was to analyze if our model was able to evaluate other aspects of Health IT safety not addressed by the previous evaluation these hospitals have been submitted in EMRAM validation. Furthermore, we aimed to investigate the satisfaction of these hospitals in using HITSMM as a framework to evaluate and provide a roadmap to improve their maturity in Health IT safety. The participants' feedback was able to confirm that our model is a potential tool for enhancing Health IT safety.

Chapter 7
Conclusion

Literature have shown that maturity models regarding IT and patient safety are not comprehensive and lack details. Therefore, it is important to conduct studies to address recommendations for safe development, implementation, and use of IT to avoid patient harm. In this Ph.D. thesis, we developed the HITSMM, a framework designed to enhance patient safety through the secure use of health information technologies. To the best of our knowledge, there is no maturity model in literature focused on this domain.

This chapter consolidates the research findings of our investigation, presenting the main contributions and the answers for our Research Questions. We also present the how we are disseminating our results through journals and conference publications. Then, we present the main future perspectives for further studies. Finally, we present the final remarks of this Ph.D. thesis.

7.1 Research Findings

The first phase of our investigation aimed to develop mappings between EMRAM and JCI, and between EMRAM and SAFER Guides. The EMRAM-JCI Mapping identifies relations between JCI and EMRAM requirements, as well as the JCI requirements that can be supported by Health IT. The identification of relations between JCI and EMRAM requirements can facilitate the management of JCI and EMRAM conformance by healthcare organizations.

EMRAM requires many criteria also required by JCI. However, the maturity model usually specifies the use of a technology, which is not required by JCI (the technology-enabled bedside product administration, for example). In other words, in many cases, implementing an EMRAM requirement can also accomplish a JCI requirement. Therefore, healthcare organizations can use the results of this Ph.D. thesis to identify technologies they can implement to ensure compliance with both validations.

In addition, healthcare organization can use Health IT implementations to achieve many JCI requirements, even when that Health IT are not required by EMRAM. That can be obtained through the JCI requirements that can be supported by Health IT identified our investigation. Therefore, another important finding of this Ph.D. thesis is the identification of JCI requirements associated to Health IT that are not currently required by EMRAM. Those requirements can be used to promote the evolution of this maturity model.

The EMRAM-SAFER Guides Mapping identified relations between EMRAM and SAFER Guides requirements. Despite EMRAM is more focused on Health IT maturity in organizations, it includes important requirements strictly related to patient safety, such as the technology-enabled bedside administration which is not covered by SAFER Guides. On the other side, most of SAFER Guides requirements are not addressed by EMRAM. These results are useful as a source for the improvement of both methods. Furthermore, healthcare organizations can use our achieved results to identify technologies and implement them to ensure compliance with both validations.

Our comparative analysis of EMRAM, JCI, and SAFER Guides revealed significant strengths and weaknesses in each model's approach to Health IT safety, which were able to answer our first Research Question (RQ1). While these frameworks offer valuable insights, their individual limitations highlighted the need for a more specific maturity model that can effectively address in evaluate and guide healthcare organizations in improving patient safety through Health IT.

As part of HITSMM development, the mappings between EMRAM, JCI and SAFER Guides were used in a complementary manner to develop this new maturity model. The HITSMM can be used by healthcare organizations to evaluate what is its current maturity stage regarding Health IT and patient safety, as well as to identify recommendations to improve its maturity by implementing HITSMM requirements. Therefore, it is possible to use HITSMM as a guide to continuously improve patient safety through the safe use of safe technologies.

The development of a HITSMM capitalizes on the strengths of EMRAM, JCI, and SAFER Guides. This model can enhance Health IT safety while reducing implementation complexity once its structure in maturity stages provides a clear roadmap for continuous improvement, enabling healthcare organizations to evolve their maturity incrementally.

These findings addressed our second Research Question (RQ2), demonstrating that HITSMM offers a more effective approach to evaluating and improving Health IT safety compared to using EMRAM, JCI, or SAFER Guides individually.

To highlight the benefits of HITSMM in comparison of EMRAM, JCI and SAFER Guides individually, we recall the strengths and weaknesses presented in Table 14 and relate them with the main differentials of our model (Table 27).

Table 27 - Advantages of HITSMM in comparison to EMRAM, JCI, and SAFER Guides

Model	Advantages of HITSMM
EMRAM	HITSMM is focused on Patient Safety. HITSMM includes SAFER Guides and JCI requirements that are not addressed by EMRAM.
JCI	HITSMM is structured as a maturity model. HITSMM is focused on Information Technology and Patient Safety. HITSMM includes many requirements from EMRAM and SAFER Guides that are not addressed by JCI.
SAFER Guides	HITSMM is structured as a maturity model. HITSMM includes EMRAM safety patient requirements that are not addressed by SAFER Guides.

We applied HITSMM to assess the health IT safety maturity stage of two Brazilin hospitals. Additionally, we evaluated participant satisfaction with the HITSMM model itself. The HITSMM application in fact presented the maturity stage of the hospitals and participants' feedback revealed high satisfaction with our framework, suggesting its significant potential as a tool for enhancing Health IT safety. This result serves an answer to our third Research Question (RQ3), which focus on verifying whether HITSMM can identify and measure the maturity level of healthcare organizations regarding Health IT safety practices.

7.2 Dissemination of Results

This Ph.D. thesis draws upon the authors' research, resulting in publications and submissions to journals and conferences. Much of the material presented here has already appeared in, or been submitted for publication in, journal and conference articles during the Ph.D. program. A list of these accepted or submitted articles follows:

- VIRGINIO, L. & DOS REIS, J. C. 2019. Finding Relations Between Requirements for Healthcare Information Systems Use in Hospitals: A Study on EMRAM and JCI. In Proceedings of the 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI).
- VIRGINIO, L. & DOS REIS, J. C. 2020. Health IT and Patient Safety: Finding Relations Between EMRAM and SAFER Guides. In the Proceedings of the XVII Congresso Brasileiro de Informática em Saúde (CBIS 2020).
- VIRGINIO, L. & DOS REIS, J. C. 2021. HITSMM: A Maturity Model for Health Information Technology Safety. In Proceedings of the XVIII Congresso Brasileiro de Informática em Saúde (CBIS 2021).
- VIRGINIO, L. & DOS REIS, J. C. 2024. Application of a Health IT Safety Maturity Model in Brazilian Hospitals. Accepted in the XX Congresso Brasileiro de Informática em Saúde, CBIS 2024. 2024.
- VIRGINIO, L. & DOS REIS, J. C.. Improving Patient Safety Maturity in Healthcare Organizations Using Information Technology. Submitted to an International Journal.

7.3 Future Perspectives

Future research can address the limitations of this study by expanding the reference models to include those like ONA, ISO, and other HIMSS maturity models. This would allow for a more comprehensive evaluation of Health IT safety maturity, incorporating aspects such as artificial intelligence, telemedicine, and patient-facing IT applications.

Additionally, future studies may explore the applicability of the HITSMM to outpatient settings such as ambulatory clinics, laboratories, and diagnostic imaging centers. This would require tailoring the model to address the unique IT safety challenges faced by these settings.

Research could investigate the relationship between Health IT safety maturity and patient outcomes. This would involve analyzing data from hospitals with varying levels of HITSMM maturity to determine if higher maturity levels correlate with improved patient safety outcomes.

Finally, future studies could focus on developing strategies to implement and sustain high levels of Health IT safety maturity in healthcare organizations. This could involve creating educational resources, providing technical assistance, and establishing ongoing monitoring and evaluation processes.

Another potential avenue for future research could be the extraction of software requirements from the HITSMM. These requirements could serve as a valuable tool for IT developers, enabling them to assess and enhance the safety and quality of their health IT products in alignment with the maturity model.

We applied the HITSMM in two hospitals and highlight the importance to apply it in a greater number of organizations to obtain a better conclusive validation process. Applying the HITSMM in a greater number of organizations might help us understanding further details of the process application and results usability.

This application was limited to investigating the organization's current maturity stage. It did not include a process to evaluate the necessary adjustments for achieving a higher HITSMM maturity stage, nor did it address how to implement those adjustments.

We understand that it is important to conduct further studies with the goal of applying HITSMM in more different healthcare organizations and measure their results in patient safety. This can be accomplished by performing the three proposed steps: (1) verifying the organization’s current maturity stage; (2) analyzing results and necessary adjustments; (3) stablishing a new maturity stage target; (4) applying adjustments according to maturity stage target; (5) verifying if the maturity stage target was reached; and (6) analyze the results of maturity stage increasing.

In the first step, we should analyze the compliance of the organization for each HITSMM requirements to verify its current maturity stage. The goal of step two is to analyze the non-conformities and verify which adjustments should be performed to be fully compliant. Those adjustments may include process changes, software and/or hardware acquisition, EHR parametrizations, etc.

In the third step, the organization stablishes a maturity stage target according to their priorities and capability of performing improvements. In the step four, the organization must implement all adjustments necessary to reach the stablished target. To evaluate if the target was reached, the organization should apply HITSMM conformity test again in the fifth step.

The goal of step six is to analyze the improvements obtained with the maturity stage increasing. For example, the organization can verify whether Key Performance Indicators (KPIs) related to patient safety, such as number of computerized provider order entry mistakes, have improved after adjustments implementation. The six proposed steps can be repeated until the obtaining of the higher maturity stage.

As previously mentioned, conducting the evaluation process in person is crucial for a more detailed assessment that can support a consulting project. A comprehensive evaluation could take approximately three days, with seven to eight hours of assessment per day. Additionally, involving and engaging all stakeholders related to the requirements being evaluated is essential, such as IT professionals and clinical managers.

7.4 Final Remarks

This Ph.D. thesis addressed the critical need for a more specific framework to ensure patient safety through the secure use of Health IT. Recognizing the limitations of existing maturity models (EMRAM, JCI, SAFER Guides) in their individual focus, we developed a novel approach: the HITSMM. This new model bridges these gaps by leveraging the strengths of each of these three existing models to provide a holistic roadmap for healthcare organizations seeking to improve their Health IT safety practices.

Our research yielded significant findings. First, we established crucial mappings between EMRAM, JCI, and SAFER Guides, revealing areas for improvement within each

framework. Second, we developed and successfully implemented HITSMM in two Brazilian hospitals, demonstrating its effectiveness in assessing current Health IT safety maturity and identifying areas for improvement.

While this Ph.D. thesis lays a strong foundation, future research holds exciting possibilities for expanding HITSMM's impact. The application in two hospitals serves as a springboard for broader validation. Implementing HITSMM in a larger and more diverse set of healthcare organizations will provide further insights into its usability and effectiveness across different settings. Furthermore, this research paves the way for investigating the relationship between HITSMM implementation and measurable improvements in patient safety outcomes. By incorporating a longitudinal study design that tracks changes in patient safety KPIs following HITSMM implementation, future research can definitively establish the model's real-world impact.

Ultimately, the proposed HITSMM offers a practical roadmap that empowers healthcare organizations to leverage HITSMM as a powerful tool for safeguarding patient well-being in the digital age.

References

[1] Chaudhry B. Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care. Ann Intern Med. 2006 May;144(10):742.

[2] Myers RB, Jones SL, Sittig DF. Review of reported clinical information system adverse events in US food and drug administration databases. Appl Clin Inform. 2011;2(1):63–74.

[3] Koppel R, Metlay JP, Cohen A, Abaluck B, Localio AR, Kimmel SE, et al. Role of computerized physician order entry systems in facilitating medication errors. JAMA. 2005 Mar 9;293(10):1197–203.

[4] Johnson CW. Politics and patient safety don't mix: understanding the failure of large-scale software procurement in healthcare. IET Conf Proc. 2009;33(1).

[5] Harrison MI, Koppel R, Bar-Lev S. Unintended Consequences of Information Technologies in Health Care - An Interactive Sociotechnical Analysis. J Am Med Inform Assoc. 2007;542–9.

[6] Virginio Junior LA, Ricarte ILM. Identification of Patient Safety Risks Associated with Electronic Health Records: A Software Quality Perspective. Stud Health Technol Inform. 2015;216:55–9.

[7] Magrabi F, Liaw ST, Arachi D, Runciman W, Coiera E, Kidd MR. Identifying patient safety problems associated with information technology in general practice: an analysis of incident reports. BMJ Qual Saf. 2015;bmjqs-2015-004323.

[8] Magrabi F, Baker M, Sinha I, Ong MS, Harrison S, Kidd MR, et al. Clinical safety of England's national programme for IT: A retrospective analysis of all reported safety events 2005 to 2011. Int J Med Inform. 2015;84(3):198–206.

[9] Sittig DF, Ash JS, Singh H. The SAFER guides: Empowering organizations to improve the safety and effectiveness of electronic health records. Am J Manag Care. 2014;20(5):418–23.

[10] Wendler R. The maturity of maturity model research: A systematic mapping study. Inform Software Tech. 2012;54(12):1317–33. doi: 10.1016/J.INFSOF.2012.07.007.

[11] Kolukısa Tarhan A, Garousi V, Turetken O, Söylemez M, Garossi S. Maturity assessment and maturity models in health care: A multivocal literature review. Digital Health. 2020;6. doi: 10.1177/2055207620914772.

[12] Carvalho JV, Rocha Á, van de Wetering R, Abreu A. A Maturity model for hospital information systems. J Bus Res. 2019;94(August 2017):388–99.

[13] World Health Organization. Patient safety [Internet]. World Health Organization; [cited 2015 Mar 31]. Available from: http://www.euro.who.int/en/health-topics/Health-systems/patient-safety/patient-safety

[14] Agency for Healthcare Research and Quality. AHRQ patient safety network - Glossary [Internet]. 2016 [cited 2016 Jul 7]. Available from: https://psnet.ahrq.gov/glossary/p

[15] Institute of Medicine. Patient Safety: Achieving a New Standard for Care. Washington, D.C.: National Academies Press; 2004. 1-432 p.

[16] Runciman W, Hibbert P, Thomson R, Van Der Schaaf T, Sherman H, Lewalle P. Towards an International Classification for Patient Safety: key concepts and terms. Int J Qual Health Care. 2009;21(1):18–26.

[17] Meeks DW, Takian A, Sittig DF, Singh H, Barber N. Exploring the sociotechnical intersection of patient safety and electronic health record implementation. J Am Med Inform Assoc. 2014;21(e1)–34.

[18] Menon S, Singh H, Meyer AND, Belmont E, Sittig DF. Electronic health record-related safety concerns: A cross-sectional survey. J Healthc Risk Manag. 2014;34(1):14–26.

[19] Sittig DF, Singh H. A red-flag-based approach to risk management of EHR-related safety concerns. J Health Risk Manag. 2013;33(2):21–6.

[20] Magrabi F, Ong MS, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. J Am Med Inform Assoc. 2010;17(6):663–70.

[21] Lei J, Guan P, Gao K, Lu X, Chen Y, Li Y, et al. Characteristics of health IT

outage and suggested risk management strategies: an analysis of historical incident reports in China. Int J Med Inform. 2014;83(2):122–30.

[22] Meeks DW, Smith MW, Taylor L, Sittig DF, Scott JM, Singh H. An analysis of electronic health record-related patient safety concerns. J Am Med Inform Assoc. 2014;1–7.

[23] Warm D, Edwards P. Classifying health information technology patient safety related incidents - an approach used in Wales. Appl Clin Inform. 2012;3(2):248–57.

[24] Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19(1):45–53.

[25] Lawler EK, Hedge A, Pavlovic-Veselinovic S. Cognitive ergonomics, socio-technical systems, and the impact of healthcare information technologies. Int J Ind Ergon. 2011;41(4):336–44.

[26] Horsky J, Schiff GD, Johnston D, Mercincavage L, Bell D, Middleton B. Interface design principles for usable decision support: A targeted review of best practices for clinical prescribing interventions. J Biomed Inform. 2012;45(6):1202–16.

[27] Paulk MC, Curtis B, Chrissis MB. Capability maturity model for software. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst; 1991.

[28] Tabrizi JS, Gharibi F, Wilson AJ. Advantages and Disadvantages of Health Care Accreditation Models. Health Promot Perspect. 2011 Jul 25;1(1):1-31. doi: 10.5681/hpp.2011.001.

[29] Sittig DF, Salimi M, Aiyagari R, Banas C, Clay B, Gibson KA, et al. Adherence to recommended electronic health record safety practices across eight health care organizations. J Am Med Inform Assoc. 2018;25(7):913–8.

[30] Ozkan S, Byakal N, Sincan M. Assessing Hospital Information Systems Processes: A Validation of PRISE Information Systems Success Model in Healthcare. Inf Syst. 2008.

[31] Flott K, Callahan R, Darzi A, Mayer E. A Patient-Centered framework for evaluating digital maturity of health services: A systematic review. J Med Internet Res. 2016;18(4).

[32] Carvalho JV, Rocha Á, Abreu A. Maturity Models of Healthcare Information Systems and Technologies: a Literature Review. J Med Syst. 2016;40(6):1–10.

[33] Carvalho JV, Rocha Á, Abreu A. Maturity Assessment Methodology for HISMM - Hospital Information System Maturity Model. J Med Syst. 2019;43(2).

[34] Gomes J, Romão M. Information System Maturity Models in Healthcare. J Med Syst. 2018 Oct 16;42(12):235. doi: 10.1007/s10916-018-1097-0. PMID: 30327955.

[35] Virginio Junior LA. Investigação de estratégias para mitigação de riscos para a segurança do paciente associados aos sistemas de registro eletrônico em saúde. 2016. Dissertação (mestrado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, Campinas, SP.

[36] Kutza JO, Hübner U, Holmgren AJ, Esdar M. Patient Safety Informatics: Criteria Development for Assessing the Maturity of Digital Patient Safety in Hospitals. Stud Health Technol Inform. 2022 May 25;294:885-889. doi: 10.3233/SHTI220618. PMID: 35612236.

[37] Sittig DF, Wright A, Coiera E, Magrabi F, Ratwani R, Bates DW, Singh H. Current challenges in health information technology-related patient safety. Health Informatics J. 2020 Mar;26(1):181-189. doi: 10.1177/1460458218814893. PMID: 30537881.

[38] Taheri Moghadam S, Hooman N, Sheikhtaheri A. Patient Safety Classifications for Health Information Technology (HIT) and Medical Devices: A Review on Available Systems. Stud Health Technol Inform. 2022 May 16;293:153-160. doi: 10.3233/SHTI220362. PMID: 35592975.

[39] McInerney C, Benn J, Dowding D, Habli I, Jenkins DA, McCrorie C, Peek N, Randell R, Williams R, Johnson OA. Patient Safety Informatics: Meeting the Challenges of Emerging Digital Health. Stud Health Technol Inform. 2022 Jun 6;290:364-368. doi: 10.3233/SHTI220097. PMID: 35673036.

[40] Virginio Junior LA, Dos Reis JC. Finding Relations Between Requirements for Healthcare Information Systems Use in Hospitals: A Study on EMRAM and JCI. 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI). 2019:1-6. doi: 10.1109/CISP-BMEI48845.2019.8965782.

[41] Virginio Junior LA, Dos Reis JC. Health IT and Patient Safety: Finding Relations Between EMRAM and SAFER Guides. XVII Congresso Brasileiro de Informática em Saúde, CBIS 2020. 2020.

Appendix A – HITSMM's Table of Requirements

ID	Category	Sub-Category	Requirement Title	Requirement Description	Maturity Stage
CDOC.01	Clinical Documentation	Structured Data	Coded Allergy	Coded allergen and reaction information (or "no known allergies") are entered and updated in the EHR prior to any order entry.	1
CDOC.04	Clinical Documentation	Clinical Documentation	Nursing documentation into the EHR	Nursing shall use the EHR to record vital signs, hydric balance, nursing notes and evolution, care plans, risk assessment, nursing diagnoses, nursing prescription, nursing procedures check, medication administration.	1
CDOC.07	Clinical Documentation	Nursing Documentation	Medication reconciliation	Medication reconciliation shall be supported by the EHR and be performed during the admission, transfer and discharge processes, including reconciliation for medications that will be used at home after discharge.	1
CDOC.08	Clinical Documentation	Medical Documentation	Medical documentation	Medical documentation for physicians shall be electronic (clinical history, physical examination, evolution, list of problems and diagnosis, surgical description, discharge summary, etc.).	1
CPOE.01	CPOE	Structured Data	Structured CPOE	The hospital shall use a structured CPOE and prescribers shall avoid using of free-text.	1
CDOC.02	Clinical Documentation	Organizational Policies	Delegation or transcription tasks	The organization shall have a written policy and procedure in place regarding delegation or transcription tasks (order entry, clinical documentation, transcription of results, etc.). For example, all transcription activities shall include review and approval process by the person in charge before being released in the EHR.	2
CDOC.05	Clinical Documentation	Nursing Documentation	Structured nursing documentation	Nursing documentation shall have structured data in such a way that it is possible to interact with nursing decision support mechanisms.	2
CDOC.09	Clinical Documentation	Medical Documentation	Medical documentation based on templates	The system shall offer structured templates for physicians, so that this data can be used in decision support mechanisms and data analysis.	2

CDOC.10	Clinical Documentation	Medical Documentation	Coded Data	Part of the patient's information shall be coded using a national or international medical vocabulary such as CID, SNOMED or LOINC.	2
CPOE.02	CPOE	Electronic Communication	Electronic communication of orders	Order entry information is electronically communicated to the laboratory, radiology, pharmacy, etc..	2
CPOE.03	CPOE	Electronic Communication	Status of orders	Health professionals shall manage status of orders in order to verify if they were properly received and met by the laboratory, radiology, pharmacy, etc..	2
MEDIMG.01	Medical Imaging	Medical Imaging	Access to EHR by RIS	RIS shall allow radiologist to access the EHR while reviewing an imaging examination.	2
MEDIMG.02	Medical Imaging	Medical Imaging	PACS implementation	The hospital shall have full implementation of PACS so that all diagnostic modalities are in digital format.	2
PID.01	Patient Identification	Configuration	Master Patient Index	The hospital shall have a Master Patient Index (MPI) in order to identify patients uniquely in all clinical information systems.	2
PHARM.17	Pharmacy	Pharmacy	Decision support in dispensation	The pharmacy information system shall provide decision support mechanisms in the dispensing process so that there is verification and alerts for errors during dispensing. There shall be minimal support for duplicities, incorrect medications, and incorrect doses.	2
PRADM.02	Product Administration	Medication Administration	Resuscitation medication in the medication administration module	Resuscitation medications performed on paper order must be included in the medication administration module once the patient is stable.	2
PRADM.03	Product Administration	Medication Administration	Medication administration registered in the medication administration module	The medication administration module shall be updated after the medication is checked and administered to the patient, indicating the person responsible for administration, status of the medication and exact time of administration.	2
TRRF.01	Tests Results Reporting and Follow-up	Structured Data	Structured laboratory results in the EHR	Laboratory results shall be structured and accessible in the EHR.	2
TRRF.02	Tests Results Reporting and Follow-up	Structured Data	Image Reports in the EHR	The results, reports and images of radiology exams and diagnostic imaging shall be accessible integrated to EHR.	2

TRRF.04	Tests Results Reporting and Follow-up	Integration	Pathological anatomy reports integrated into EHR	Pathological anatomy reports shall be integrated into the EHR, preferably in a structured manner.	2
TRRF.05	Tests Results Reporting and Follow-up	Integration	Microbiology reports integrated into EHR	Microbiology reports shall be integrated into the EHR.	2
CDOC.06	Clinical Documentation	Nursing Documentation	Clinical decision support for nursing	The EHR shall provide decision support for nursing, offering intelligent forms for assessing risks, scales and indexes, vital signs, nursing diagnosis, nursing interventions, etc.	3
CDOC.14	Clinical Documentation	Document Management	Scanning of documents without clinical relevance	All documents with no clinical relevance on paper (consent terms, for example) shall be digitized and attached to the EHR within 72 hours of discharge.	3
CDOC.15	Clinical Documentation	Document Management	Scanning of documents with clinical relevance	All documents with clinical relevance generated on paper must be digitized and attached to the EHR within 24 hours of its creation.	3
CPOE.05	CPOE	CDS	Drug-allergy interaction checking on CPOE	Drug-allergy interaction checking shall occur during the entry of new medication orders.	3
CPOE.06	CPOE	CDS	Drug-drug interaction checking on CPOE	Drug-drug interaction checking shall occur during the entry of new medication orders.	3
CPOE.07	CPOE	CDS	Duplicate order checking	Duplicate order checking shall occur for at least high-risk medication, diagnostic tests, and procedure orders (excluding "as needed" medications).	3
INTER.03	Interoperability	Configuration	Use standard clinical vocabularies	The hospital shall use standard clinical vocabularies in system-to-system interfaces to connect applications.	3
INTER.04	Interoperability	Evaluation and Testing	Transmission without loss	System-to-system interfaces shall be properly configured and tested to ensure that data elements are transmitted without loss of or changes to information content (for example, truncation of free text data).	3

INTER.05	Interoperability	Evaluation and Testing	System-to-system interfaces testing	System-to-system interfaces shall be tested before going into production and after changes to hardware, software, or content (e.g., the allowable list of data elements to be exchanged) on either side of the interface. The hardware and software environment for interface testing shall be physically separate from the live environment.	3
PID.02	Patient Identification	Organizational Policies	Prevention and identification of duplicate patient records	The organization shall have policies and procedures to ensure the prevention and identification of duplicate patient records, as well as to perform the merging of duplicate records. Duplicate registration prevention activities include, but are not limited to: - Register patients using standardized procedures; - Train employees to search for patients in the system before creating a new record.	3
PID.03	Patient Identification	Configuration	Temporary unique patient ID	During patient admission, the organization shall have a process for assigning a unique "temporary" ID to patients in the event that the system is unavailable or the patient is unable to provide their information. There shall be a process to update the patient identification as soon as they are available, as well as a process to merge medical records, in case the patient whose temporary ID was created already had a patient record.	3
PID.04	Patient Identification	Organizational Policies	Patient identification in information from external sources	The hospital shall have organizational policies and activities to ensure correct patient identification of information from external sources (e.g., tests results from external labs).	3
PID.05	Patient Identification	Organizational Policies	Use of test patients in production environment	The hospital shall have organizational policies to monitor the use of test patients in the production environment. When they do exist, they shall have unambiguously assigned "test" names (e.g., including numbers) and shall be clearly identifiable as test patients (e.g., different background color for patient header).	3

PID.06	Patient Identification	Evaluation and Testing	Usability testing for safe patient identification	The hospital shall perform EHR usability testing in order to verify aspects like: - Clinicians have the ability to create personalized electronic lists of their patients according to several criteria (e.g., user, location, time, service). - Patient names on adjacent lines in the EHR display are visually distinct. - The user interfaces of the training, test, and read-only backup environments of the EHR are clearly different from the production version to prevent inadvertent entry or review of patient information in the wrong system. - Patients who are deceased are clearly identified as such. - Critical patient identification information shall be visible in a header.	3
PID.07	Patient Identification	Configuration	Display of two or more patient's records	The EHR shall limit the number of patient records that can be displayed on the same computer at the same time to one. Otherwise, the hospital shall have policies and training of professionals to avoid the use of these resources, since they may imply the registration of information in the incorrect patient record.	3
PRADM.01	Product Administration	Medication Administration	Medication of procedures that have already occurred in the medication administration module	All medications (including the anesthetic record) administered to the patient during medical procedures, must be recorded in the administration module at the time the patient is in the next level of care (for example, after the patient leaves the Surgical Center).	3
SCG.19	System Configuration and Governance	Pervasiveness of Use	All clinicians using EHR	All healthcare professionals (> 95%) shall use the EHR to record patient information, including doctors, nurses, nutritionists, clinical pharmacists and psychologists.	3
SCG.20	System Configuration and Governance	Pervasiveness of Use	Use of CPOE	The electronic prescription shall be used to order all medications, diagnostic tests and procedures. At least 95% of the prescriptions must be carried out electronically.	3
TRRF.06	Tests Results Reporting and Follow-up	Usability	Codification for text-based test reports	Predominantly text-based test reports (e.g. radiology or pathology reports) shall have a coded (e.g. abnormal/normal at a minimum) interpretation associated with them.	3

CDOC.16	Clinical Documentation	Organizational Policies	Abbreviations and acronyms	Use of abbreviations and acronyms shall be minimized and standardized by the organization.	4
CPOE.04	CPOE	CDS	Order sets	Evidence-based order sets shall be available in the EHR for common tasks and conditions and be updated regularly.	4
CPOE.08	CPOE	CDS	Drug-condition checking	Drug-condition checking shall occur for important interactions between drugs and conditions.	4
CPOE.09	CPOE	CDS	Drug-patient age checking	Drug-patient age checking shall occur for important age-related medication issues.	4
CPOE.10	CPOE	CDS	Dose range checking for single dose	Dose range checking for single dose shall occur before medication orders are submitted for dispensing.	4
CPOE.11	CPOE	CDS	Dose range checking for daily dose	Dose range checking for daily dose shall occur before medication orders are submitted for dispensing.	4
CPOE.17	CPOE	CPOE	Additional steps after prescription	The clinician is informed during the ordering process when additional steps are needed to complete the order being requested. For example: when non-formulary medications require additional pre-approval and "send out" tests require special forms or procedures.	4
INTER.06	Interoperability	Organizational Policies	Policies and procedures to describe how to stop and restart the exchange of data	The hospital shall have policies and procedures to describe how to stop and restart the exchange of data across the interface in an orderly manner. For example, to ensure that all system interface buffers are empty prior to stopping or restarting the system, as well as buffers are of adequate size and behavior to prevent any loss of data (for example, in case of disconnection of interfaces while the sending system continues to produce data for transmission).	4
INTER.07	Interoperability	Training and Support	Training staff on system-to-system interface	The hospital shall train assigned staff on all system-to-system interface maintenance and monitoring activities or have appropriate access to qualified personnel. System and application operator manuals for quick reference are developed, readily available, and up-to-date.	4
INTER.08	Interoperability	Organizational Policies	Documentation of data exchange needs	The hospital shall document data exchange needs and include how data will be used and who is responsible for maintaining the interface and the systems connected to it. The organization shall maintain a comprehensive data dictionary that includes, for each data element:	4

				▪ Data type (e.g., coded, text, numeric) ▪ Data definition ▪ Clinical vocabularies ▪ Metadata (e.g., creator, date created, users)	
INTER.09	Interoperability	Usability	Operational status of the system interface	The operational status of the system interface shall be clear to its users with regard to clinical use, such as knowing when the interface cannot transmit or receive messages, alerts, or crucial information.	4
PHARM.01	Pharmacy	Pharmacy	Medication unitarization	The drug unitarization process shall have a technology-based mechanism to ensure that each drug has been unitarized correctly.	4
PHARM.02	Pharmacy	Pharmacy	Medication storage	The drug storage process shall have a technology-based mechanism to ensure that each drug has been stored in the correct location.	4
TRRF.07	Tests Results Reporting and Follow-up	Management	Tracking of send-out tests	"Send-out" (or reference lab) tests shall be electronically tracked, and their results shall be incorporated into the EHR, with a coded test name, result value, and interpretation.	4
TRRF.08	Tests Results Reporting and Follow-up	Organizational Policies	Organizational policies related to tests results	The hospital shall have organizational policies in order to: - Identify the responsible for test result follow-up. - Identify workflows that are particularly vulnerable to mishandling of test results (handoffs between clinicians, care transitions between clinical settings, etc.). - Perform usability testing in order to verify that the display of test results meets intended clinical users. - Define which abnormal test results should be sent as high priority alerts to minimize "alert fatigue". - Establish expectations for timely review of test results and specifically address planned and unplanned absences.	4
TRRF.09	Tests Results Reporting and Follow-up	Electronic Communication	Communication of abnormal tests results	Clinicians shall be electronically notified about abnormal tests results and results notifications remain in clinician inboxes until a clinician action occurs to address them.	4

TRRF.10	Tests Results Reporting and Follow-up	Electronic Communication	Results forwarding	The hospital shall have mechanisms to forward results and results notifications from one clinician to another.	4
TRRF.11	Tests Results Reporting and Follow-up	Electronic Communication	Reminders for clinicians	The EHR has the capability for clinicians to set reminders for themselves and other responsible clinical staff for future tasks to facilitate test result follow-up.	4
TRRF.12	Tests Results Reporting and Follow-up	Organizational Policies	Tests results reporting and follow-up monitoring	The hospital shall monitor and address test results sent to the wrong clinician or never transmitted to any clinician (e.g., due to an interface problem or patient/provider misidentification).	4
CCOM.01	Clinical Communication	Organizational Policies	Delivering of urgent clinical information	The hospital shall have policies to ensure that urgent clinical information is delivered to clinicians in a timely manner and use of messaging systems is appropriated: - Evaluation of verbal delivery of critical information that supplements use of the EHR. - Address timely electronic delivery of important clinical information. For example, hospital discharge summaries are delivered to clinicians responsible for follow-up. - Policies on clinician-to-clinician messaging that specifies what should and should not be transmitted.	5
CCOM.02	Clinical Communication	Evaluation and Testing	Usability of electronic communication	The hospital shall perform usability tests in order to ensure that: - The EHR includes the capability for clinicians to look up the status of their electronic communications (e.g., sent, delivered, opened, acknowledged). - Messages clearly display the individual who initiated the message and the time and date it was sent. - The EHR facilitates accurate routing of clinician-to-clinician messages and enables forwarding of messages to other clinicians. - Electronic message systems include the capability to indicate the urgency of messages. - Both EHR design and organizational policy facilitate clear identification of clinicians who are responsible for action or follow-up in response to a message.	5

CCOM.03	Clinical Communication	Organizational Policies	Access to current patient and clinician contact information	The hospital shall have policies to ensure that clinicians are able to electronically access current patient and clinician contact information (e.g., email address, telephone and fax numbers) and identify clinicians currently involved in a patient's care. - The organization shall maintain up-to-date patient care team information within the EHR. - The organization has a process for patients to review and correct their contact information listed in the EHR, including their preferred method of communication.	5
CCOM.04	Clinical Communication	Organizational Policies	Clinical communications documented into the EHR	The hospital shall ensure that all clinician-to-clinician communications that contains any information about a patient's diagnosis, treatment, or care is documented into or scanned into the EHR. If clinical messaging systems external to the EHR are used, copies of patient-related messages are stored in the EHR.	5
CDOC.11	Clinical Documentation	Medical Documentation	Clinical protocols	The hospital shall use computerized clinical protocols with clinical decision support for physicians. The EHR shall be able to propose conducts from the information recorded by the physician in the patient's chart, usually a prescription set containing medications, nursing care and / or examination requests. The hospital shall have at least one computerized clinical protocols implemented.	5
CONT.01	Contingency Planning	Configuration	Redundancy for hardware	The hospital shall have duplication/redundancy for hardware that run applications critical to the organization's operation. - The organization shall maintain a redundant path to the Internet consisting of two different cables, in different trenches, provided by two different Internet providers. - The organization maintains a redundant datacenter with current patient data. - If using a remotely hosted EHR (e.g., cloud-based solution), the hospital shall require that its EHR provider back up data with tape, Internet, redundant drives, or any means necessary to allow full recovery from incidents.	5

CONT.02	Contingency Planning	Configuration	Uninterruptible Power Supply	An Uninterruptible Power Supply (UPS), electric generator and sufficient fuel shall be available to support the EHR during an extended power outage. Both shall be kept in secure locations and tested regularly.	5
CONT.03	Contingency Planning	Management	Back-up of patient data	The hospital shall back-up all patient data and software application configurations critical to the organization's operations. The back-up shall be encrypted.	5
CONT.04	Contingency Planning	Organizational Policies	Policies on EHR downtimes and recovery processes	The hospital shall have policies and procedures on EHR downtimes and recovery processes to ensure continuity of operations with regard to safe patient care and critical business operations. The policies shall include at least: - When a downtime should be called. - Who will be in charge during the downtime (both on the clinical and technical side). - How everyone will be notified. - What are the procedures to recovery. The EHR downtime policy is reviewed at least every 2 years.	5
CONT.05	Contingency Planning	Management	Testing and monitoring contingency planning	The hospital shall have a testing and monitoring strategy to prevent and manage EHR downtime events. According to a formal procedure, the hospital shall conduct a simulation periodically to verify that all contingencies are functioning properly during system downtime.	5

CONT.06	Contingency Planning	Configuration	Summary reports on read-only EHR	The hospital shall have summary reports on a read-only EHR available in PC/workstations on the wards/floors when the system is down. These PC/workstations shall be connected to a generator circuit or UPS and direct connected to a printer on a generator circuit or UPS.	5
CONT.07	Contingency Planning	Organizational Policies	Documentation of medical record when the system is unavailable	The hospital shall have a formal process that specifies how the medical record is documented when the system is unavailable and how the documentation generated during the system downtimes is updated in the system when it is available again.	5
CONT.08	Contingency Planning	Organizational Policies	Patient identification during downtimes	The hospital shall have policies and procedures in place to ensure accurate patient identification when preparing for, during, and after downtimes. There shall be a mechanism in place to register new patients during downtime, including assignment of unique temporary patient record numbers along with a process for reconciling these new patient IDs once the EHR comes back online.	5
CONT.09	Contingency Planning	Organizational Policies	Communication during downtimes	A communication strategy that does not rely on the computing infrastructure exists for downtime and recovery periods.	5
CONT.10	Contingency Planning	Training and Support	Training of staff for downtimes	Staff shall be trained and tested on downtime and recovery procedures. The organization shall conduct unannounced EHR "downtime drills" at least once a year.	5
CPOE.12	CPOE	CDS	Drug-diet checking	The CPOE shall have alerts of drug-diet interaction during the prescription. For example, medications that should be taken with empty stomach, alert for medication that have their absorption decreased or increased in the presence of food in the stomach, etc.	5
CPOE.13	CPOE	CDS	Drug-lab results checking	The CPOE shall have alerts of drug-lab results interaction during the prescription.	5

CPOE.18	CPOE	CPOE	TALLman lettering	"TALLman lettering" shall be used to prevent from order entry errors due to orthographically similar medication names (sound alike, look alike).	5
INTER.10	Interoperability	Management	Monitoring of the performance and use of system interfaces	The organization shall monitor the performance and use of system interfaces regularly, including monitoring the interface error log and the volume of transactions over the interface.	5
INTER.11	Interoperability	Evaluation and Testing	Interface errors detection	When interface errors are detected, they shall be reported, fixed, and used to construct new test cases to improve the interface testing.	5
LABBL.01	Laboratory and Blood Bank	Laboratory and Blood Bank	Samples collection	At the point of collection of samples, the hospital shall use technology-enabled to scan blood specimens/samples before collection in order to verify patient identification errors. The process shall be implemented for at least 25% of the volume of samples collection.	5
LABBL.04	Laboratory and Blood Bank	Laboratory and Blood Bank	Blood product verification	At the time of association of the blood product with the prescription / order, the system shall verify that the product match with the prescription.	5
LABBL.05	Laboratory and Blood Bank	Laboratory and Blood Bank	Disassociation of blood products	The blood bank shall have a process that allows a particular blood product to be disassociated to a prescription if it has not been administered.	5
PHARM.03	Pharmacy	Clinical Pharmacy	Pharmacy evaluation	The hospital shall have a formal procedure for reviewing prescriptions before dispensing and the first dose with system support. At least 25% of prescriptions must be reviewed before dispensing.	5
PHARM.04	Pharmacy	Clinical Pharmacy	Pharmacy evaluation	The hospital shall have a formal procedure for reviewing prescriptions before dispensing and the first dose with system support. At least 50% of prescriptions must be reviewed before dispensing.	5
PHARM.07	Pharmacy	Clinical Pharmacy	Clinical pharmacy documentation	During the second line validation by the clinical pharmacy, all changes and review notes shall be recorded in the EHR and made available to all other health professionals.	5
PHARM.08	Pharmacy	Clinical Pharmacy	Duplicate orders alerts for pharmacy	The pharmacy system shall provide duplicate orders alerts.	5
PHARM.09	Pharmacy	Clinical Pharmacy	Allergy orders alerts for pharmacy	The pharmacy system shall provide drug-allergy interaction alerts.	5

PHARM.10	Pharmacy	Clinical Pharmacy	Drug-drug interaction alerts for pharmacy	The pharmacy system shall provide drug-drug interaction alerts.	5
PHARM.11	Pharmacy	Clinical Pharmacy	Dose range alerts for pharmacy	The pharmacy system shall provide dose range alerts.	5
PHARM.12	Pharmacy	Clinical Pharmacy	Cumulative dose alerts for pharmacy	The pharmacy system shall provide cumulative dose alerts.	5
PHARM.13	Pharmacy	Clinical Pharmacy	Drug-food interaction alerts for pharmacy	The pharmacy system shall provide drug-food interaction alerts.	5
PHARM.14	Pharmacy	Clinical Pharmacy	Drug-lab interaction alerts for pharmacy	The pharmacy system shall provide drug-lab alerts.	5
PHARM.15	Pharmacy	Clinical Pharmacy	Drug-condition interaction alerts for pharmacy	The pharmacy system shall provide drug-condition alerts.	5
PHARM.16	Pharmacy	Clinical Pharmacy	Drug-patient age checking for pharmacy	The pharmacy system shall provide drug-patient age alerts.	5
PRADM.04	Product Administration	Medication Administration	5 rights at the bedside medication administration	The organization shall implement a process for Technology-Enabled Bedside Product Administration using the patient's wristband identification code and the medications to be administered. The system of bedside administration shall automatically check the 5 rights of medication administration: patient, medication, data/hour, route and dose. This process should be implemented for a minimum of 25% of the total administration volume.	5
PRADM.07	Product Administration	Medication Administration	Confirmation after administration	Medications administered via bedside administration should be updated in the system only after the patient has actually received them (not before).	5

PRADM.08	Product Administration	Medication Administration	Bedside administration of human milk	Human milk shall be included in the Technology-Enabled Bedside Product Administration process, so that its identification code is scanned to check for possible errors in patient identification, dose, etc. The process shall be implemented for at least 25% of the volume of administrations.	5
PRADM.11	Product Administration	Medication Administration	Bedside administration of blood products	Blood products must be identified with a barcode and scanned at the bedside prior to administration to check for possible error of patient identification, dose, etc. The process shall be implemented for at least 25% of the volume of administrations.	5
SCG.01	System Configuration and Governance	Configuration	EHR access points	The hospital shall have an adequate number of EHR access points in all clinical areas and organizational policies that set minimum standards for EHR access by clinicians (for example, clinicians walk no more than 50 feet to access an EHR).	5
SCG.02	System Configuration and Governance	Configuration	Live version of the EHR versus other versions	The hospital shall have policies to ensure that the EHR is configured to make it difficult to confuse the live version of the EHR with other versions (training, test, and read-only backup versions). For example, the screen background color or the color of the patient headers could be different, policy and process for creating and naming test patients.	5
SCG.03	System Configuration and Governance	Evaluation and Testing	Testing of health information technology	Health information technology systems shall be tested before and after implementation for usability, effectiveness, security information and patient safety.	5
SCG.04	System Configuration and Governance	Evaluation and Testing	Data integrity during and after major system changes	The hospital shall have processes in place to ensure data integrity during and after major system changes, such as upgrades to hardware, operating systems, or browsers. For example, application changes (e.g., from one EHR system to another); format changes (e.g., from free text to structured data), coding system changes (e.g., from ICD-9 to ICD-10), storage mechanism changes (e.g., from magnetic tapes to solid state hard drives), data used for reporting ((e.g., length of stay, readmission rates, etc.).	5
SCG.05	System Configuration and Governance	Training and Support	Training before using the system	All users shall be trained before using the system and before any changes to the system. EHR safety shall be covered in EHR training.	5

SCG.06	System Configuration and Governance	Training and Support	Users support	The organization shall have organizational policies to ensure that EHR users can obtain support from the IT team and digital health to solve problems related to technology (hardware, software, network, etc.).	5
SCG.07	System Configuration and Governance	Organizational Policies	Recording criticisms and suggestions associated with the EHR	The hospital shall have organizational policies to ensure that EHR users are able to notify technology-related problems (hardware, software, network/ISP, etc.) and make improvements suggestions.	5
SCG.08	System Configuration and Governance	Optimization	Governance of criticisms and suggestions	The hospital shall have a formal strategy for governance of criticisms and suggestions from users, as well as prioritizing requests and deciding to adopt suggestions.	5
SCG.21	System Configuration and Governance	Pervasiveness of Use	Patient wristband scan error record	The organization shall be able to register in the EHR when a bedside administration could not be performed using Technology-Enabled Bedside Product Administration due to errors in reading the patient's wristband. The hospital must still be able to verify the scan percentage of the wristband, and this percentage must be equal to or greater than 25%.	5
CDOC.12	Clinical Documentation	Medical Documentation	Clinical protocols	The hospital shall use computerized clinical protocols with clinical decision support for physicians. The EHR shall be able to propose conducts from the information recorded by the physician in the patient's chart, usually a prescription set containing medications, nursing care and / or examination requests. The hospital shall have at least three computerized clinical protocols implemented.	6
CPOE.14	CPOE	CDS	Health maintenance alerts	The system should provide alerts for maintaining the patient's health condition during the prescription or recording of clinical documentation. For example, when prescribing exams or registering clinical documentation, the system can alert the doctor to a recommendation for a mammogram exam for a woman over 50.	6

CPOE.15	CPOE	CDS	Security alert when requesting exams and procedures	The Electronic Prescription must provide mechanisms for checking certain patient conditions when requesting tests and procedures. For example, alerting when requesting an MRI if the patient has any metal in the body, or alerting in case of the procedure exceeds the limit of exposure to radiation.	6
LABBL.02	Laboratory and Blood Bank	Laboratory and Blood Bank	Samples collection	At the point of collection of samples, the hospital shall use technology-enabled to scan blood specimens/samples before collection in order to verify patient identification errors. The process shall be implemented for at least 50% of the volume of samples collection.	6
PHARM.05	Pharmacy	Clinical Pharmacy	Pharmacy evaluation	The hospital shall have a formal procedure for reviewing prescriptions before dispensing and the first dose with system support. 100% of prescriptions must be reviewed before dispensing. The process must be in operation 24 hours a day 7 days a week.	6
PRADM.05	Product Administration	Medication Administration	5 rights at the bedside medication administration	The hospital shall implement a process for Technology-Enabled Bedside Product Administration using the patient's wristband identification code and the medications to be administered. The system of bedside administration shall automatically check the 5 rights of medication administration: patient, medication, data/hour, route and dose. This process should be implemented for a minimum of 50% of the total administration volume.	6
PRADM.09	Product Administration	Medication Administration	Bedside administration of human milk	Human milk shall be included in the Technology-Enabled Bedside Product Administration process, so that its identification code is scanned to check for possible errors in patient identification, dose, etc. The process shall be implemented for at least 50% of the volume of administrations.	6

PRADM.12	Product Administration	Medication Administration	Bedside administration of blood products	Blood products must be identified with a barcode and scanned at the bedside prior to administration to check for possible error of patient identification, dose, etc. The process shall be implemented for at least 50% of the volume of administrations.	6
SCG.16	System Configuration and Governance	Copy/Paste	Copy and paste process	The hospital shall develop a process to regulate the proper use of copy and paste.	6
SCG.17	System Configuration and Governance	Copy/Paste	Training for using copy and paste actions	The hospital shall provide education and training on the proper use of copy and paste actions to all professionals who record on the EHR.	6
SCG.18	System Configuration and Governance	Copy/Paste	Copy and paste compliance monitoring	The hospital shall monitor compliance with the use of guidelines for copy and paste actions and implement corrective actions, as needed.	6
SCG.22	System Configuration and Governance	Pervasiveness of Use	Patient wristband scan error record	The organization shall be able to register in the EHR when a bedside administration could not be performed using Technology-Enabled Bedside Product Administration due to errors in reading the patient's wristband. The hospital must still be able to verify the scan percentage of the wristband, and this percentage must be equal to or greater than 50%.	6
TRRF.03	Tests Results Reporting and Follow-up	Usability	Display of laboratory results over time	The EHR shall incorporate tools and reports that enable selected laboratory results to be graphed and displayed to view trends over time. The associated graphs shall follow standardized display criteria.	6
CDOC.03	Clinical Documentation	CDS	Clinical reference materials directly from the EHR	Tha hospital shall provide clinical reference materials directly from the EHR. Reference materials shall be accessible through info buttons, for example, in the order entry screen/module. Examples include: medication monographs (such as Micromedex), dosing calculators, diagnostic guides, laboratory reference materials, image atlases, anatomical diagrams, patient education materials, and disease-specific treatment guidelines.	7

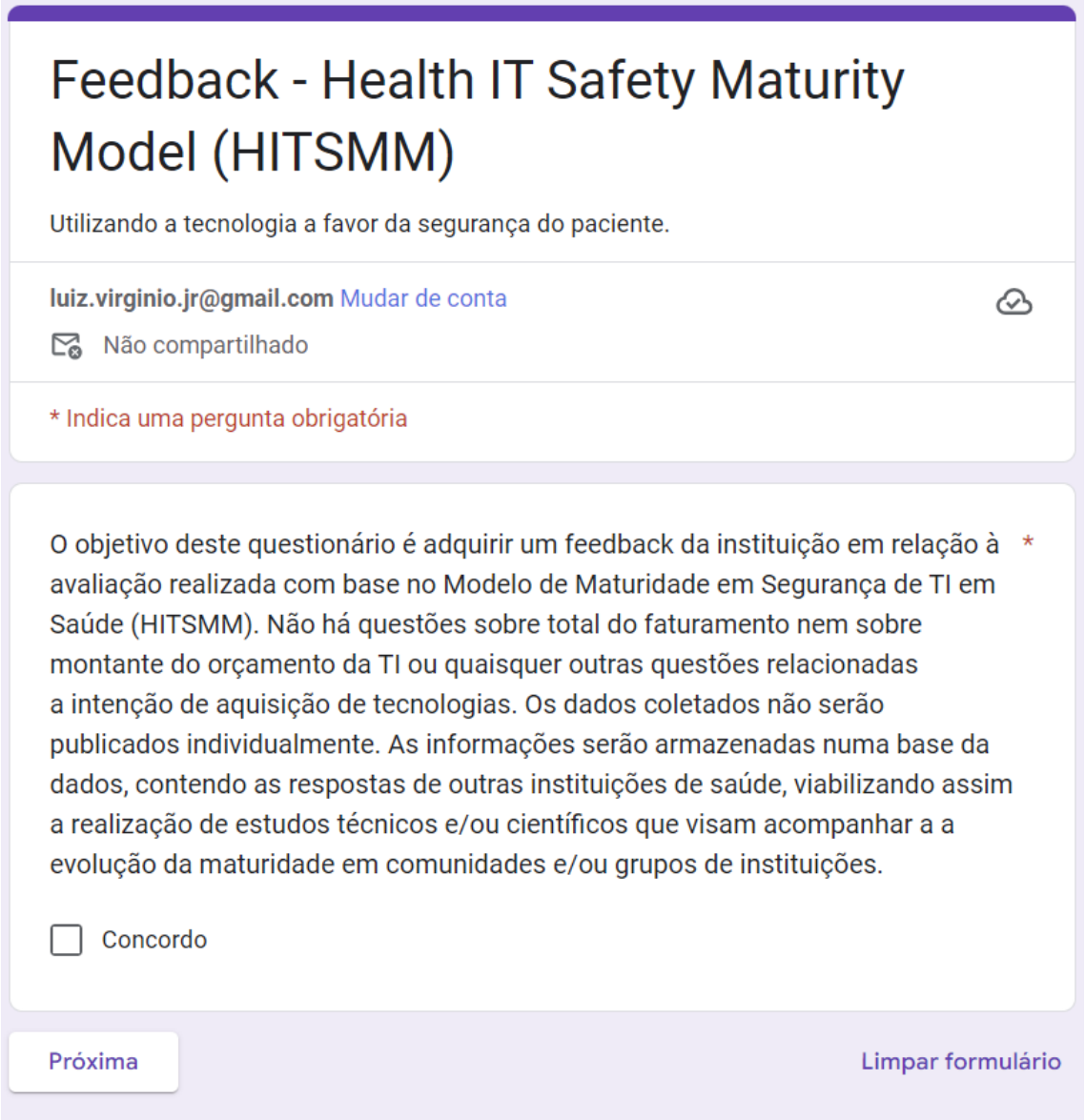
CDOC.13	Clinical Documentation	Medical Documentation	Clinical protocols	The hospital shall use computerized clinical protocols with clinical decision support for physicians. The EHR shall be able to propose conducts from the information recorded by the physician in the patient's chart, usually a prescription set containing medications, nursing care and / or examination requests. The hospital shall have at least five computerized clinical protocols implemented.	7
CPOE.16	CPOE	CDS	Alerts when recording allergies, medical conditions and test results	The system should alert not only on electronic prescription but also when registering a new allergy, clinical conditions and test results.	7
INTER.01	Interoperability	Configuration	Support and use standardized protocols	The EHR shall support and use standardized protocols for exchanging data with other organizations.	7
INTER.02	Interoperability	Electronic Communication	Exchanging clinical information with external organizations	The hospital shall have the capacity to exchange clinical information with external organizations that have the same capacity. The organization shall be able to export standardized clinical documents and / or perform automated data exchange through the EHR.	7
LABBL.03	Laboratory and Blood Bank	Laboratory and Blood Bank	Samples collection	At the point of collection of samples, the hospital shall use technology-enabled to scan blood specimens/samples before collection in order to verify patient identification errors. The process shall be implemented for at least 95% of the volume of samples collection.	7
PHARM.06	Pharmacy	Clinical Pharmacy	Retrospective pharmacy evaluation	The hospital shall have a formal process to monitor medications that have been administered without reviewing by the clinical pharmacy. Such prescriptions shall be retrospectively reviewed until the next day prior to the first scheduled medication administration for that patient.	7
PRADM.06	Product Administration	Medication Administration	5 rights at the bedside medication administration	The hospital shall implement a process for Technology-Enabled Bedside Product Administration using the patient's wristband identification code and the medications to be administered. The system of bedside administration shall automatically check the 5 rights of medication administration: patient, medication, data/hour, route and dose.	7

				This process should be implemented for a minimum of 95% of the total administration volume.	
PRADM.10	Product Administration	Medication Administration	Bedside administration of human milk	Human milk shall be included in the Technology-Enabled Bedside Product Administration process, so that its identification code is scanned to check for possible errors in patient identification, dose, etc. The process shall be implemented for at least 95% of the volume of administrations.	7
PRADM.13	Product Administration	Medication Administration	Bedside administration of blood products	Blood products must be identified with a barcode and scanned at the bedside prior to administration to check for possible error of patient identification, dose, etc. The process shall be implemented for at least 95% of the volume of administrations.	7
SCG.09	System Configuration and Governance	Optimization	Reporting of EHR-related safety hazards	The hospital shall have a mechanism for internal reporting of EHR-related safety hazards. Such mechanism should be for anonymous and no-fault. The hospital shall have formal process for addressing reported problems and for reporting problems externally to the developer. The user who reported the issue should be notified of the outcome when appropriate.	7
SCG.10	System Configuration and Governance	Human Resources	Committees to discuss health IT safety	The hospital shall have formal and operational committees formed to discuss aspects related to health IT safety in the hospital.	7
SCG.11	System Configuration and Governance	Human Resources	Highest level decision makers as part of committees	The highest level decision makers (e.g. boards of directors, owners of physician practices) are committed to promoting a culture of safety that incorporates the safety and safe use of EHRs.	7

SCG.12	System Configuration and Governance	Evaluation and Testing	CDS content evaluation	The hospital shall have policies to evaluate CDS content that include, but is not limited to: - Order sets quality and update; - Quality of the rules for alerts (check if the rules are correct, updated and appropriate to the clinical context); - Assessment of the adequacy of clinical knowledge bases (context in which they are being used, need for version updates, etc.).	7
SCG.13	System Configuration and Governance	Evaluation and Testing	CDS presentation adequacy evaluation	The hospital shall have policies to evaluate CDS presentation adequacy that include, but is not limited to: - Evaluation if CDS alerts are displayed in the relevant clinical context. - Evaluation of interruptive alerts (e.g., pop-ups at the time of ordering). These kinds of alerts shall be used with discretion and only for high risk and/or priority conditions. - Review interactions so that only the most significant interaction-related alerts, as determined by the organization, are presented to clinicians; - Evaluation of clarity of questions posed to users.	7
SCG.14	System Configuration and Governance	Evaluation and Testing	CDS adherence evaluation	The hospital shall have policies to evaluate the adherence of CDS mechanisms implemented that include, but are not limited to: - Assess the occurrence of alert fatigue. - Assess adherence to computerized protocols. - Assess frequency of access to content offered by clinical knowledge bases.	7
SCG.15	System Configuration and Governance	CDS	Key metrics related to CPOE and CDS	Key metrics related to CPOE and CDS (e.g., override rates) are defined, monitored, and acted on to optimize safety and use. For example: ▪ CPOE use rate ▪ Frequency (i.e., volume) of orders that generate an alert ▪ Override rate (i.e., percent of alerts that are overridden) in comparison to alert volume ▪ Percent of all orders requiring modification by someone other than the ordering provider ▪ Types of alerts and percent of overrides ▪ Usage of evidence-based order sets	7

				▪ Clinician satisfaction with CDS alert functionality ▪ Results of any CPOE evaluation tool	
SCG.23	System Configuration and Governance	Pervasiveness of Use	Patient wristband scan error record	The organization shall be able to register in the EHR when a bedside administration could not be performed using Technology-Enabled Bedside Product Administration due to errors in reading the patient's wristband. The hospital must still be able to verify the scan percentage of the wristband, and this percentage must be equal to or greater than 95%.	7

Appendix B - HITSMM Satisfaction Questionnaire



Feedback - Health IT Safety Maturity Model (HITSMM)

Utilizando a tecnologia a favor da segurança do paciente.

luiz.virginio.jr@gmail.com Mudar de conta

Não compartilhado

* Indica uma pergunta obrigatória

O objetivo deste questionário é adquirir um feedback da instituição em relação à avaliação realizada com base no Modelo de Maturidade em Segurança de TI em Saúde (HITSMM). Não há questões sobre total do faturamento nem sobre montante do orçamento da TI ou quaisquer outras questões relacionadas a intenção de aquisição de tecnologias. Os dados coletados não serão publicados individualmente. As informações serão armazenadas numa base da dados, contendo as respostas de outras instituições de saúde, viabilizando assim a realização de estudos técnicos e/ou científicos que visam acompanhar a a evolução da maturidade em comunidades e/ou grupos de instituições. *

Concordo

Próxima

Limpar formulário

Dados do Hospital e Participante

Nome do Hospital *

Sua resposta

Perfil do Hospital *

- ○ Filantrópico com perfil público (mais de 80% SUS)
- ○ Filantrópico com perfil privado (menos de 80% SUS)
- ○ Privado
- ○ Público de gestão direta
- ○ Público com gestão terceirizada

Certificação e Acreditações

- ☐ HIMSS Analytics EMRAM estágio 6
- ☐ HIMSS Analytics EMRAM estágio 7
- ☐ Joint Commission International (JCI)
- ☐ Qmentum (Canadense)
- ☐ ONA I
- ☐ ONA II
- ☐ ONA III
- ☐ NIAHO

Quantidade de Leitos *

Sua resposta

Nome do participante *

Sua resposta

Cargo/função do participante no hospital *

Sua resposta

Voltar Próxima Limpar formulário

Indique seu grau de concordância com as afirmações abaixo: *

	Discordo totalmente	Discordo	Indiferente	Concordo	Concordo totalmente
A Tecnologia da Informação pode impactar negativamente na segurança do paciente quando não desenvolvida e/ou utilizada de forma adequada.	○	○	○	○	○
A Tecnologia da Informação pode ser utilizada como uma aliada para melhoria da segurança do paciente.	○	○	○	○	○
É importante que as instituições de saúde avaliem a segurança do paciente considerando não apenas os processos assistenciais, mas também seus sistemas de informação e a forma que as pessoas e processos interagem com esses sistemas.	○	○	○	○	○

O HITSMM funciona como um guia orientador para uma evolução progressiva.	○	○	○	○	○
O HITSMM pode ser utilizado para avaliar o estágio atual da instituição em relação à maturidade do uso da tecnologia da informação a favor da segurança do paciente.	○	○	○	○	○
O HITSMM é capaz de promover melhorias para a segurança do paciente por meio da adoção e uso seguro da tecnologia.	○	○	○	○	○
O HITSMM inclui aspectos importantes relacionados à TI e que ainda não são avaliados por outros modelos de certificação e acreditação, tais como EMRAM-HIMSS e JCI.	○	○	○	○	○

A distribuição dos requisitos ao longo dos estágios está adequada, de forma que requisitos mais complexos estão em estágios mais altos.	◯	◯	◯	◯	◯

Existe algum aspecto relacionado à TI e segurança do paciente que você considera que não está sendo avaliado no HITSMM ? Se sim, indique quais são. *

Sua resposta

Por favor, indique suas críticas e sugestões de melhoria para o HITSMM.

Sua resposta

Comentários gerais

Sua resposta

Voltar Enviar Limpar formulário