CBIS'24 XX Congresso Brasileiro de Informática em Saúde
08/10 a 11/10 de 2024 - Belo Horizonte/MG - Brasil

Aplicação de um modelo de maturidade para segurança do paciente em tecnologia da informação em saúde em hospitais brasileiros

Application of a health information technology safety maturity model in brazilian hospitals

Aplicación de un modelo de madurez para seguridad del paciente de tecnología de la información en salud en hospitales brasileños

Luiz Virginio[1], Julio Cesar dos Reis[2]

1 Aluno de Doutorado, Instituto de Computação da Unicamp, Campinas (SP), Brasil.
2 Professor Doutor, Instituto de Computação da Unicamp, Campinas (SP), Brasil.

Autor correspondente: Luiz Virginio
E-mail: luiz.virginio.jr@gmail.com

Resumo

Objetivo: este estudo apresenta a aplicação do Modelo de Maturidade em Segurança de Tecnologia de Informação em Saúde (HITSMM) em dois hospitais brasileiros. Método: Através de reuniões virtuais e entrevistas com líderes dos hospitais, avaliamos a aderência de cada hospital aos requisitos do HITSMM. Esses requisitos se alinham aos estágios específicos de maturidade, permitindo-nos determinar o nível atual de maturidade de cada hospital. Após as entrevistas, os líderes dos hospitais responderam a um questionário avaliando o HITSMM e sua percepção de seu impacto na segurança do paciente. Resultados: Embora ambos os hospitais possuam certificação Electronic Medical Record Adoption Model (EMRAM) Estágio 6, nossa avaliação os colocou no Estágio 2 na estrutura do HITSMM. Essa discrepância destaca a capacidade do HITSMM de avaliar aspectos de segurança não abordados pelo EMRAM. Conclusão: esse trabalho destaca o potencial do uso do HITSMM como uma nova ferramenta para melhorar a segurança da tecnologia em saúde.

Descritores: Tecnologia de Informação em Saúde; Segurança do Paciente; Modelo de Maturidade

Abstract

Objective: This study presents the application of the Healthcare Information Technology Security Maturity Model (HITSMM) in two Brazilian hospitals. Method: Through virtual meetings and interviews with hospital leaders, we assessed each hospital's adherence to the HITSMM requirements. These requirements align with specific maturity stages, allowing us to determine the current level of healthcare IT security maturity of each hospital. After the interviews, hospital leaders responded to a questionnaire evaluating the HITSMM and their perception of its impact on patient safety. Results: While both hospitals have Electronic Medical Record Adoption Model (EMRAM) Stage 6 certification, our assessment placed them in Stage 2 within the HITSMM framework. This discrepancy highlights the HITSMM's ability to assess security aspects not addressed by EMRAM. Conclusion: This work highlights the potential of using HITSMM as a new tool to improve healthcare IT security.

Keywords: Healthcare Information Technology, Patient Safety; Maturity Model

Resumen

Objetivo: Este estudio presenta la aplicación del Modelo de Madurez en Seguridad de Tecnología de la Información en Salud (HITSMM) en dos hospitales brasileños. Método: A través de reuniones virtuales y entrevistas con líderes de los hospitales, evaluamos la adhesión de cada hospital a los requisitos del HITSMM. Estos requisitos se alinean con etapas específicas de madurez, lo que nos permite determinar el nivel actual de madurez de la seguridad de TI en salud de cada hospital. Después de las entrevistas, los líderes de los hospitales respondieron un cuestionario evaluando el HITSMM y su percepción de su impacto en la seguridad del paciente. Resultados: Si bien ambos hospitales cuentan con la certificación Electronic Medical Record Adoption Model (EMRAM) Etapa 6, nuestra evaluación los ubicó en la Etapa 2 del HITSMM. Esta discrepancia destaca la capacidad del HITSMM para evaluar aspectos de seguridad que no aborda el EMRAM. Conclusión: Este trabajo destaca el potencial del uso del HITSMM como una nueva herramienta para mejorar la seguridad de la tecnología en salud.

Descriptores: Tecnología de Información en Salud; Seguridad del Paciente, Modelo de Madurez

Introduction

While Electronic Health Records (EHRs) hold promise for improved healthcare quality and efficiency [1], their implementation can introduce unforeseen risks if not handled properly [2,3,4,5,6]. Studies have documented potential downsides, including medication errors, unintended prescriptions, and misdirected tests [6,7,8].

As an approach to address this challenge, we developed the Health Information Technology Safety Maturity Model (HITSMM); a framework designed to enhance patient safety through the secure use of health information technologies. HITSMM is a maturity model structured in seven stages composed of a comprehensive list of requirements resulting from the proper combination of three different models: the Electronic Medical Record Adoption Model (EMRAM), Joint Commission International (JCI) information technology requirements, and the Safety Assurance Factors for EHR Resilience (SAFER) Guides.

The Joint Commission International (JCI) is an American accreditation body of healthcare organizations. It has a set of requirements dedicated to information management, which contains requirements specifically related to Health Information Technology (IT).

The SAFER Guides is a set of guides with recommended practices related to the safety and safe use of EHRs. It was designed to be a self-assessment for healthcare organizations. The recommended practices are organized into three domains: Safe Health IT, Using Health IT Safely, and Monitoring Safety [9].

The Healthcare Information and Management Systems Society (HIMSS) Analytics developed the Electronic Medical Record Adoption Model (EMRAM), which is composed of eight stages (from zero to seven). The goal of EMRAM is to measure the adoption and utilization of EHR functions in hospitals, focusing especially on patient safety, patient satisfaction, information security, and clinician support.

This study presents the application of the HITSMM in two Brazilian hospitals. This work builds upon three of our previous studies: (1) identification of relations between EMRAM and Joint Commission International (JCI) [10]; (2) identification of

relations between EMRAM and SAFER Guides [11]; and (3) development of HITSMM [12].

The HITSMM is composed by 138 requirements. These requirements are grouped into 12 thematic categories: Patient Identification, Clinical Documentation, Computerized Provider Order Entry (CPOE), Pharmacy, Product Administration, test results Reporting and Follow-up, Laboratory and Blood Bank, Medical Imaging, Clinical Communication, Contingency Planning, Interoperability; System Configuration and Governance.

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. Table 1 presents the main aspects evaluated in each HITSMM maturity stages.

A strategy used to increase maturity in each subsequent stage was distributing 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. Stage 4 adds 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. More details concerning HITSMM development can be found at our study [12].

Table 1 - 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.

Methods

To evaluate HITSMM application, we proposed an approach to apply the model in two private hospitals. To protect the confidentiality of the two participating hospitals, we have not identified them in this document. We will refer to them as Hospital A and Hospital B. We selected hospitals that have already been validated on EMRAM Stage 6 once we would like to investigate whether the participants believe that HITSMM can evaluate a more comprehensive set of requirements related to patient safety than EMRAM.

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 1 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 1 - 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 2 summarizes the questions included in the HITSMM satisfaction survey. All participants provided informed consent after reviewing and agreeing to the terms outlined in our consent form. This form explicitly stated that no identifying information would be published in connection with this study.

Table 2 - 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.

Results

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 3 and Table 4 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 3 - 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 4 - 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 5 and Table 6 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 5 - 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 6 - 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%**

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 7 presents the hospitals' responses to each statement in the questionnaire, which shows that HITSMM presented a very good satisfaction by the participants.

Table 7 - 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

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

Table 8 - 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 with regard to 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 or the color of the patient headers could be different, policy and process for creating and naming test patients.	5
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

Applying the HITSMM in a greater number of organizations might help us understanding further details of the process application and results usability. Additionally, the 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.

Notably, participants feedback indicated high satisfaction with HITSMM, underscoring its potential as a valuable tool for improving healthcare technology safety. We understand that it is important to conduct further studies with the goal of applying HITSMM in 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 establishes a maturity stage target according to their priorities and capability of making improvements. In step four, the organization must implement all adjustments necessary to reach the established target. To evaluate if the target was reached, the organization should apply HITSMM conformity test again in the fifth step.

Step six aims 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 the number of computerized provider order entry mistakes, have improved after adjustments implementation. The six proposed steps can be repeated until the higher maturity stage is obtained.

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 work, we conducted the application of HITSMM, a framework designed to enhance patient safety through the secure use of health information technologies. This study employed the HITSMM model to assess the health IT safety maturity stage in two hospitals. Additionally, we evaluated participant satisfaction with the HITSMM model itself.

We found that the HITSMM can be used by healthcare organizations to evaluate what is its current maturity stage regarding Health IT and patient safety. Also, it is useful to identify recommendations to improve its maturity by implementing HITSMM requirements. HITSMM can be used as a guide to continuously improve patient safety through the safe use of safe technologies.

Acknowledgment

This work was supported by the National Council for Scientific and Technological Development. We are grateful for the valuable partnership of FOLKS in this study.

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

References

1. B. Chaudhry, "Systematic Review: Impact of Health Information Technology on Quality, Efficiency, and Costs of Medical Care," Ann. Intern. Med., vol. 144, no. 10, p. 742, May 2006.

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. J Am Med Assoc [Internet]. 2005 Mar 9 [cited 2014 Dec 11];293(10):1197–203. Available from: http://archpsyc.jamanetwork.com/article.aspx?articleid=200498

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

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

6. L. A. Virginio and I. L. M. Ricarte. Identification of Patient Safety Risks Associated with Electronic Health Records: A Software Quality Perspective. Stud. Health Technol. Inform, V. 216, p. 55–9, 2015.

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 [Internet]. 2015;(November):bmjqs-2015-004323. Available from: http://qualitysafety.bmj.com/lookup/doi/10.1136/bmjqs-2015-004323

8. Magrabi F, Baker M, Sinha I, Ong M-S, 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 [Internet]. 2015;84(3):198–206. Available from: http://linkinghub.elsevier.com/retrieve/pii/S1386505614002482

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. 12th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics, CISP-BMEI 2019. 2019.

11. Virginio L., Dos Reis, J. C. Health IT and Patient Safety: Finding Relations Between EMRAM and SAFER Guides. o XVII Congresso Brasileiro de Informática em Saúde, CBIS 2020. 2020.

12. Virginio L., Dos Reis, J. C. Improving Patient Safety Maturity in Healthcare Organizations Using Information Technology. Submitted to an international jornal