Análise de requisitos de privacidade e segurança em registros eletrônicos de saúde

Analysis of privacy and security requirements in electronic health records

Análisis de requisitos de privacidad y seguridad en registros sanitarios electrónicos

Rodrigo Tertulino[1], Naghmeh Ivaki[2]

1 Professor Adjunto em Redes de Computadores, Laboratório de Pesquisa em Engenharia de Software e Automação (LaPEA), Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, Natal (RN), Brasil.
2 Professora Assistente em Engenharia Informática, Centro de Informática e Sistemas da Universidade de Coimbra (CISUC), Departamento de Engenharia Informática, Universidade de Coimbra, Coimbra, Portugal.

Autor correspondente: Rodrigo Tertulino
E-mail: rrsilva@dei.uc.pt

RESUMO

Objetivo: O estudo oferece uma análise dos requisitos de privacidade e segurança presentes nos registros de prontuário eletrônico, enfatizando a relevância crucial da segurança e privacidade nos sistemas de saúde. **Método:** Estudo de caso descritivo-exploratório, realizado no sistema de prontuário eletrônico do cidadão usando na atenção primária à saúde. **Resultados:** Os resultados do estudo indicam que existem requisitos de segurança e privacidade que não são atendidos completamente pelo sistema, como integridade, acesso de emergência e anonimização, que precisam ser aprimoradas para atender à legislação e políticas de segurança. **Conclusão:** A pesquisa visa contribuir para a melhoria da segurança e preservação da privacidade nos dados dos pacientes nos registros eletrônicos de saúde, destacando a importância de implementar medidas adequadas para garantir a conformidade com as normas legais e promover a confiança dos pacientes no uso dessas tecnologias de saúde.

Descritores: Proteção da Privacidade; Segurança da informação; Prontuário Eletrônico do Paciente.

ABSTRACT

Objective: The study analyzes the privacy and security requirements in electronic medical records, emphasizing the crucial relevance of security and privacy in healthcare systems. **Method:** A descriptive-exploratory case study was carried out using the citizen's electronic medical record system used in primary health care. **Results:** The results of the study indicate that the system only partially meets security and privacy requirements, such as integrity, emergency access, and anonymization, which need to be improved to comply with legislation and security policies. **Conclusion:** The research aims to improve the security and privacy of patient data in electronic health records, highlighting the importance of implementing appropriate measures to ensure compliance with legal standards and promote patient confidence in using these health technologies.**Keywords:** Privacy Protection; Information security; Electronic Patient Record.

RESUMEN

Objetivo: El estudio ofrece un análisis de los requisitos de privacidad y seguridad presentes en los registros médicos electrónicos, enfatizando la relevancia crucial de la seguridad y la privacidad en los sistemas de salud. **Método:** Estudio de caso descriptivo-exploratorio, realizado en el sistema de historia clínica electrónica del ciudadano utilizado en la atención primaria de salud. **Resultados:** Los resultados del estudio indican que existen requisitos de seguridad y privacidad que el sistema no cumple completamente, como la integridad, el acceso de emergencia y la anonimización, que deben mejorarse para cumplir con la legislación y las políticas de seguridad. **Conclusión:** La investigación tiene como objetivo contribuir a mejorar la seguridad y privacidad de los datos de los pacientes en los registros médicos electrónicos, destacando la importancia de implementar medidas adecuadas para garantizar el cumplimiento de los estándares legales y promover la confianza de los pacientes en el uso de estas tecnologías sanitarias.

Descriptores: Protección de la Privacidad; Seguridad de la Información; Registro electrónico del paciente.

Introdução

Os sistemas de registros eletrônicos de saúde (RES) representam uma nova fronteira na melhoria dos cuidados de saúde para os pacientes, além de contribuir para a eficiência dos recursos dos sistemas de saúde[1]. Esses sistemas oferecem benefícios significativos, como facilitar o acesso às informações médicas, reduzir erros, otimizar o fluxo de trabalho dos profissionais de saúde e possibilitar uma melhor coordenação do tratamento entre diferentes prestadores de serviços de saúde. Outros benefícios dos RES incluem, procedimentos clínicos (redução de erros médicos), organizacionais (fornecendo benefícios financeiros e operacionais) e sociais (melhoria da saúde da população através de pesquisas médicas). Os RES são vistos como uma ferramenta importante para os governos, formuladores de políticas e autoridades de saúde, porque contêm dados longitudinais informações que podem ser compartilhadas para melhorar os serviços de saúde, segurança do paciente e pesquisa médica[2]. No entanto, esses sistemas têm preocupações ampliadas em relação à privacidade das pessoas e à confidencialidade de seus dados. Nesse contexto, as questões relacionadas à segurança e à privacidade emergem como preocupações e desafios predominantes no âmbito dos sistemas de saúde[3].

A segurança das informações e a privacidade dos pacientes são aspectos fundamentais em qualquer sistema de prontuário eletrônico do paciente, incluindo os RES[10]. Logo, a confidencialidade dos dados dos pacientes é essencial para construir uma relação de confiança entre pacientes e profissionais de saúde. Consequentemente, sistemas de prontuário eletrônico armazenam informações sensíveis sobre a saúde dos indivíduos, incluindo diagnósticos, histórico de tratamento, prescrições e outras informações médicas[2]. Assim, a garantia de que esses dados são acessíveis apenas por profissionais autorizados é essencial para proteger a privacidade dos pacientes. Além disso, a segurança e privacidade das informações dos pacientes são consideradas as principais preocupações e desafios do sistema de saúde[12].

Logo, estas preocupações afetam o interesse dos pacientes em divulgar os seus dados de saúde e podem ter consequências fatais. Consequentemente, a privacidade e segurança das informações armazenadas no RES são cruciais para o funcionamento

eficaz do sistema de saúde e o bem-estar dos pacientes. Todavia, os RES contêm dados pessoais e sensíveis dos pacientes, tornando imperativo garantir sua proteção adequada[9].

A importância da preservação da privacidade nos dados e da segurança da informação em sistemas de prontuário eletrônico do paciente como o e-SUS PEC vai muito além da conformidade legal. Ela é essencial para a confiança dos pacientes, a integridade das decisões médicas, a continuidade do atendimento e o avanço da pesquisa médica. Portanto, investir em tecnologias seguras, treinamento adequado para profissionais de saúde e conscientização dos pacientes é crucial para garantir um sistema de saúde digital seguro, eficiente e centrado no paciente[26].

Em resumo, o estudo tem como objetivos primordiais a descrição dos requisitos fundamentais de privacidade e segurança visando assegurar a integridade dos registros eletrônicos de saúde, a análise dos desafios inerentes à proteção da privacidade dos pacientes em ambientes de prontuário eletrônico, a identificação de lacunas a serem aprimoradas para o cumprimento das legislações e políticas de segurança, e a proposição de mecanismos para aprimorar a segurança, por meio da sugestão de um conjunto de técnicas que possam fortalecer a segurança dos sistemas e garantir uma maior preservação da privacidade nos dados dos pacientes. A próxima seção abordará detalhadamente os métodos empregados neste estudo.

Métodos

No contexto da saúde, os sistemas de saúde têm sido baseados em implementações de software fragmentadas, sem considerar aspectos de privacidade e segurança[2]. Consequentemente, a necessidade de arquiteturas de referência na área da saúde tornou-se objeto de estudo na última década devido ao crescente número de instituições e países que começaram a utilizar este tipo de sistema de forma mais sistemática[8]. Assim, neste estudo, trabalhamos na realização de uma análise exploratória para analisar os requisitos de segurança e privacidade contidos no PEC e-SUS APS. Para realizar essa análise foi desenvolvido uma Matriz de Rastreabilidade de Requisitos (RTM)[16].

Para revisão dos requisitos de segurança e privacidade, utilizou-se o estudo[21]. Como resultado, o principal objetivo deste estudo de mapeamento sistemático é fornecer uma visão geral das pesquisas recentes sobre requisitos de privacidade e segurança nos RES. Os requisitos de segurança que compõe o estudo e que se faz necessário em um sistema de RES, são: **Integridade, Transmissão Segura, Autenticação, *Logoff* Automático, Auditoria, Controle de acesso, Consentimento, Acesso de Emergência, e Anonimização**.

Portanto, o estudo teve como objetivo compreender as tendências atuais e futuras de privacidade e segurança dos sistemas RES. Assim, com este estudo foi possível determinar os principais requisitos de privacidade e segurança que devem fazer parte destes sistemas.

A análise foi realizada na cidade de Mossoró, RN. Foram analisados PEC e-SUS APS instalados nas unidades básicas de saúde (UBS) do município com o apoio da secretaria de saúde do município[15].

No geral, o estudo fornece uma análise abrangente dos requisitos de privacidade e segurança que estão presentes no PEC e-SUS APS. Sendo assim, destacando a importância da segurança e da privacidade nos sistemas de saúde. Na próxima seção apresentaremos uma discussão acerca dos resultados do artigo.

Resultados e Discussão

Analisamos o PEC no sistema de atenção primária (e-SUS APS) para detalhar como esses sistemas lidam com políticas e leis relativas à preservação da privacidade dos usuários. Para entender melhor como o sistema foi implementado e como seus componentes são representados dentro do PEC do e-SUS, realizamos um diagrama de implantação, figura 1. Assim, na imagem destacamos os principais módulos que fazem parte do PEC do e-SUS APS[11]. Logo em seguida, a descrição dos módulos que compõem o sistema é discutida.

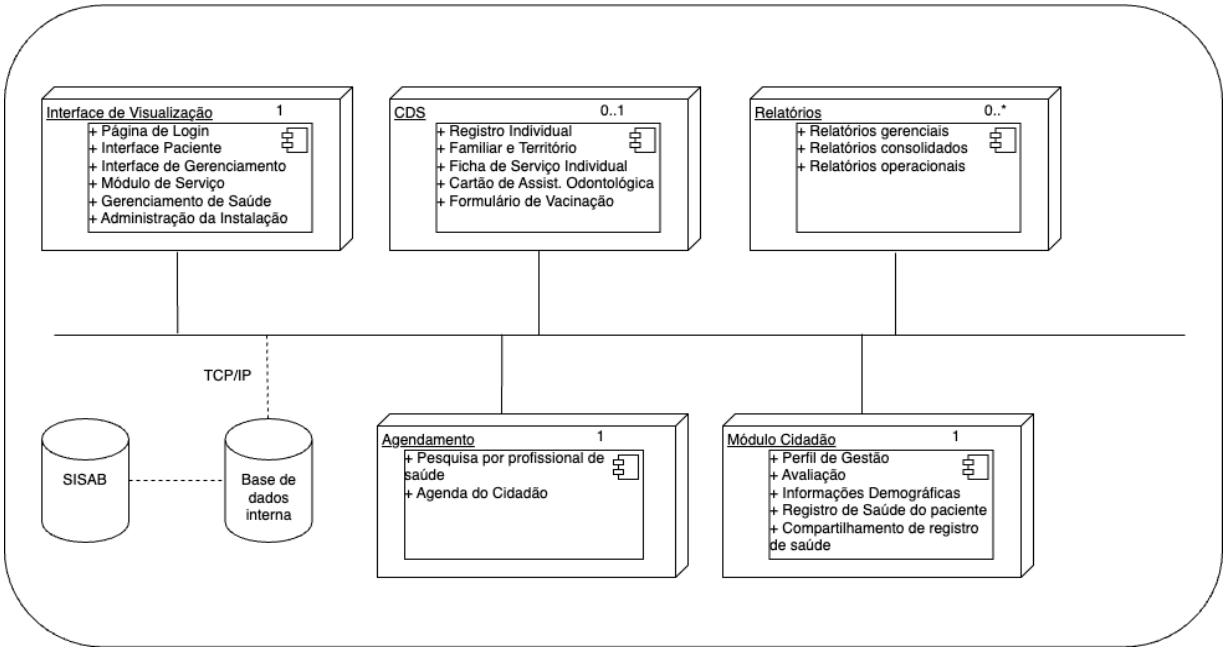

Figura 1 – Diagrama de visualização de implantação PEC e-SUS APS.

No Brasil, diversas dificuldades estão relacionadas à informatização dos sistemas de atenção primária à saúde administrados pelos governos municipais. Por isso, o **CDS** é uma forma de cadastrar pacientes quando o sistema não possui conexão com a internet. Portanto, a coleta simplificada de dados é um dos componentes do PEC e-SUS APS, utilizada principalmente em serviços de saúde que não possuem sistema informatizado para uso rotineiro no trabalho.

A **interface de visualização** é responsável pela página de login dos usuários utilizando o PEC do E-SUS. Além disso, também fornece acesso aos módulos internos de configuração e parametrização do sistema.

O módulo de **relatórios** permite que funcionários das UBS e gestores visualizem as ações de saúde realizadas no território de forma resumida e sistematizada. Com isso, diversos relatórios são divididos em consolidados, de produção e operacionais.

O módulo de **agendamento** é utilizado para organizar a agenda dos profissionais da UBS. É a principal ferramenta utilizada pelos funcionários nas recepções das UBS. Este módulo está disponível no PEC e foi desenhado considerando os avanços

tecnológicos e o crescente acesso constante da população aos smartphones, tendo assim acesso aos aplicativos móveis.

O módulo **cidadão** é onde os usuários com acesso aos registros dos pacientes podem acessar, adicionar e alterar informações. Além disso, para armazenar as informações, o PEC do E-SUS utiliza um banco de dados para armazenamento local e as transmite ao SISAB nacional por meio de agendamento.

Assim, o **SISAB** é o atual sistema nacional de informação para processamento e difusão de dados e informação de ações que visa construir conhecimento e tomar decisões[14].

A estrutura dos campos, atributos e elementos do PEC e-SUS APS está disponível como material suplementar no site https://zenodo.org/doi/10.5281/zenodo.10960834. Esse recurso pode fornecer informações detalhadas sobre a organização e características do sistema, auxiliando na compreensão e análise dos requisitos de segurança e privacidade relacionados ao prontuário eletrônico.

Para realizar nossa análise, desenvolvemos uma matriz de rastreabilidade de requisitos (RTM) que é o processo de rastreamento dos requisitos aplicáveis a vários artefatos de desenvolvimento de software[23]. Além disso, a rastreabilidade de requisitos é um elemento vital da engenharia de requisitos (ER), pois pode fornecer visibilidade dos fatores necessários ao procedimento de desenvolvimento de software e sistema, o que contribui para uma melhor compreensão do sistema de software em desenvolvimento ou já desenvolvidos.

Realizamos o RTM no PEC do e-SUS APS para verificar se o sistema segue os requisitos de segurança e privacidade[21]. A descrição dos requisitos de segurança e privacidade analisados e os resultados da análise estão descritas na Tabela 1.

Na próxima seção, apresentaremos soluções propostas para garantir a preservação e privacidade nos dados dos pacientes e os resultados da nossa análise sobre os desafios enfrentados em sistemas de prontuário eletrônico.

Análise dos resultados

A análise dos resultados da pesquisa sugere necessário um esforço contínuo para aprimorar a segurança e privacidade dos sistemas de prontuário eletrônico, garantindo que as informações dos pacientes sejam protegidas e acessíveis apenas por profissionais autorizados. Isso contribuirá para a melhoria da qualidade dos serviços de saúde e para a confiança dos pacientes no sistema de saúde na totalidade.

Os resultados da pesquisa indicaram que o sistema ainda precisa ser aprimorado para atender completamente às legislações e políticas de privacidade e segurança em vigor. Foram identificados requisitos de segurança e privacidade que ainda não são atendidos pelo sistema, como o acesso de emergência, anonimização e integridade. Consequentemente, a falta de acesso de emergência em um sistema de prontuário eletrônico pode ter um impacto negativo na segurança e privacidade dos pacientes[32]. Isso ocorre porque, em emergências, os profissionais de saúde podem precisar acessar rapidamente as informações do paciente para tomar decisões críticas de tratamento. Se o acesso de emergência não estiver disponível ou for limitado, isso pode atrasar o tratamento e colocar a vida do paciente em risco.

Logo, soluções baseadas em biometria para controle de acesso durante circunstâncias de emergência, na qual o fornecimento da impressão digital da vítima, permitiria que os profissionais de saúde, acessem algumas partes dos dados do PEC, incluindo tipo sanguíneo, alergias, medicação atual, histórico médico e informações de contato. Assim, mecanismos como *biometric identification*[33] e *watermarking-based*[34] podem contribuir para fortalecer a proteção dos dados dos pacientes, garantir o acesso autorizado apenas a profissionais de saúde qualificados.

Portanto, é importante que os sistemas de prontuário eletrônico tenham medidas de segurança e privacidade adequadas, incluindo acesso de emergência, para garantir a proteção das informações do paciente e a segurança do tratamento médico.

Além disso, a anonimização é uma técnica que remove informações pessoais identificáveis de um registro eletrônico de saúde, tornando-o menos identificável e mais seguro. Portanto, é importante que os sistemas de prontuário eletrônico tenham medidas de segurança e privacidade adequadas, incluindo anonimização. A de-identificação é uma

técnica que permite a anonimização e, consequentemente remover determinadas informações para que não seja mais possível identificar o usuário. Sendo assim, se faz necessário que o sistema forneça de-identificação dos dados contidos dos pacientes.

Tabela 1 - Matriz de rastreabilidade com os resultados dos requisitos de segurança e privacidade PEC e-SUS

Requisito	Categoria	Módulo Software	Resultado	Comentários
Controle de Acesso	Privacidade	e-SUS APS gerenciamento/Perfil	Encontrado	O modelo de controle de acesso utilizado pelo sistema e- SUS PEC é baseado em funções, dependendo do perfil profissional, como médicos ou enfermeiros, terem acesso a todas as informações do paciente.
Acesso de Emergência	Privacidade	Não Atribuído	Não Encontrado	Nenhum
Anonimização	Privacidade	Cidadão\Visualizar cidadão	Não Encontrado	As informações pessoais de saúde (PHI) não são anonimizadas, podendo revelar informações privadas, como (CPF, Raça, Telefone, PIS/PASEP e Tipo de Sangue)
Anonimização	Privacidade	Cidadão\Visualizar cidadão\Folha de Rosto	Não Encontrado	Para acessar informações pessoais, é necessário insira uma justificativa para visualização dos registos médicos. No entanto, as informações que o PHI adere podem ser visualizadas para outro usuário.
Auditoria	Segurança	Base de dados interna	Encontrado	Caso o profissional deseje visualizar o prontuário através do módulo cidadão, é obrigatório cadastrar uma justificativa de acesso às informações clínicas no momento do atendimento ou na ausência do cidadão na UBS. Está justificativa é registada no banco de dados para utilização posterior, no caso de auditoria em relação ao sigilo do cidadão dados clínicos sensíveis.
Integridade	Segurança	Não atribuído	Não Encontrado	A integridade da base de dados é de responsabilidade da secretaria municipal responsável pela instalação do sistema. Para garantir a integridade dos dados e o correto funcionamento do sistema, as informações devem ser inseridas ou importadas por meio do e-SUS APS PEC. Além disso, os dados não são criptografados nativamente pelo sistema. Não foram identificados mecanismos de criptografia, que não garantam a

				integridade completa das informações do usuário no sistema. Os dados armazenados no e-SUS PEC não são criptografados por padrão. Por isso, esta tarefa é de responsabilidade do administrador do sistema responsável para instalação e manutenção do sistema.
Transmissão Segura	Segurança	Gerenciamento\ Gerenciamento município	Encontrado	A transmissão de dados para a rede nacional de dados de saúde é criptografada por meio de certificação digital A1 configurável por meio de chave fornecida pelo governo (Departamento de Informática do SUS - DATASUS).
Autenticação	Segurança	Página de Login	Encontrado	O controle de acesso é baseado em usuário e senha. Além de ser o padrão para login no sistema e-SUS PEC. No entanto, a página de login não tem criptografia (http://localhost:8080/). O processo de autenticação também pode ser feito pelo gov.br no PEC e-SUS.
Consentimento	Privacidade	Cidadão	Encontrado	Os pacientes podem escolher como seus dados clínicos serão disponibilizados na rede de saúde. Por padrão, seus dados ficam visíveis para todos os atendimentos, caso o cidadão discorde, deverá optar por marcar a opção "Desativar compartilhamento de prontuários deste cidadão".
Automático Logoff	Segurança	Instalador\configurações de instalação\segurança	Encontrado	Prazo para redefinição de senha dos profissionais de acesso ao PEC. Tempo limite para encerramento da sessão por inatividade do sistema. O número máximo de tentativas consecutivas de login com autenticação inválida. Solicitação manual para redefinir senhas para todos os usuários do sistema.

Logo, mecanismos como: *Privacy Preserving Data Publishing* (PPDP)[27] e *Distributed Common Identity for the Integration of Regional Health Data* (DCIFIRHD)[28]. ambos os mecanismos poderiam ser utilizados para fornecer anonimização das informações.

A integridade dos dados é essencial para garantir que as decisões médicas sejam baseadas em informações precisas e confiáveis. Se as informações do paciente forem alteradas ou corrompidas de forma não autorizada, isso pode levar a diagnósticos incorretos, tratamentos inadequados e outros problemas de saúde.

Logo, a integridade dos dados é identificada como um elemento-chave na garantia da qualidade das informações clínicas, destacando-se a importância de abordagens abrangentes para garantir a integridade, autenticidade e não repúdio dos dados registrados. Além disso, a falta de integridade pode afetar a continuidade do atendimento, pois pode haver uma interrupção no tratamento se as informações do paciente não estiverem disponíveis quando necessário. Portanto, é importante que os sistemas de prontuário eletrônico tenham medidas de segurança e privacidade adequadas, incluindo garantia de integridade dos dados. Dessa forma, o uso de mecanismos para fornecer integridade dos dados como *Blockchain*[30], *Intelligent Framework for Securing Healthcare* (IFHDS)[31] e *Personally Controlled Electronic Health Record* (PCEHR)[29] poderiam garantir integridade dos dados armazenados, transmitidas e gerenciados pelo PEC e-SUS APS.

Consequentemente, as ameaças potenciais associadas à alteração não autorizada dos dados do paciente são identificadas como preocupações significativas, com implicações diretas na precisão dos diagnósticos, eficácia dos tratamentos e continuidade do atendimento. A análise ressalta a necessidade premente de medidas robustas de segurança e privacidade, incluindo garantias específicas para a integridade dos dados, como meio essencial para salvaguardar a confiança contínua nos registros eletrônicos de saúde. Assim, a implementação dessas salvaguardas não apenas protege a confidencialidade das informações, mas também reforça a base para decisões médicas críticas, contribuindo para a segurança e eficácia dos cuidados de saúde. Na próxima

seção, apresentaremos a conclusão do estudo e discutiremos possíveis trabalhos futuros que podem ser desenvolvidos com base em nossas descobertas.

Conclusão

A confidencialidade dos dados dos pacientes é essencial para construir uma relação de confiança entre pacientes e profissionais de saúde. Sistemas de registro eletrônico de saúde armazenam informações sensíveis sobre a saúde dos indivíduos, incluindo diagnósticos, histórico de tratamento, prescrições e outras informações médicas.

A garantia de que esses dados são acessíveis apenas por profissionais autorizados é essencial para proteger a privacidade dos pacientes. Consequentemente, o estudo realizado no PEC e-SUS APS identificou que requisitos como a acesso de emergência, anonimização e integridade ainda não são atendidos completamente pelo sistema. Portanto, para aprimorar o sistema de PEC e-SUS APS, é necessário implementar medidas de segurança e privacidade que atendam às legislações e políticas de segurança, como a Lei Geral de Proteção de Dados (LGPD)[13] e a ISO 18308:2011[22] que trata dos requisitos de informática em saúde para uma arquitetura de registros eletrônicos de saúde.

Além disso, como medidas de segurança e privacidade, é importante garantir que os profissionais de saúde sejam treinados para utilizar o sistema de forma segura e que os pacientes sejam informados sobre como suas informações serão protegidas.

Também se faz necessário, fornecer transparência na comunicação com os pacientes sobre a proteção de suas informações. Logo, o estudo fornece uma análise abrangente dos requisitos de privacidade e segurança que estão presentes no PEC e-SUS APS, destacando a importância da segurança e da privacidade nos sistemas de saúde.

Com base nos resultados do estudo, é possível identificar áreas que precisam ser aprimoradas para garantir a segurança e preservação da privacidade nos dados dos pacientes. Portanto, é importante garantir que as informações dos pacientes sejam protegidas e acessíveis apenas por profissionais autorizados. Como forma de contornar a

falta dos requisitos identificados no estudo, sugerimos o uso dos mecanismos citados para melhorar integridade, anonimização e acesso de emergências no PEC e-SUS APS.

O estudo também destaca que a confiança dos pacientes na segurança de seus dados é essencial para impulsionar a inovação em saúde. Em resumo, o estudo é importante para garantir a segurança e preservação da privacidade nos dados dos pacientes em sistemas de prontuário eletrônico, contribuindo para a melhoria da qualidade dos serviços de saúde.

Por fim, como trabalho futuro, pretendemos desenvolver uma arquitetura de referência para implementação de requisitos de privacidade e segurança em sistemas de registro eletrônico de saúde.

Agradecimentos

A secretaria municipal de saúde, Mossoró-RN, gentilmente permitiu acesso ao sistema através do gestor da secretaria por meio de convênio firmado entre o Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN) e do município para fins de pesquisa, sem os quais não seria possível realizar os testes no PEC e-SUS APS.

Referências

1. N. Menachemi and T.H. Collum, Benefits and drawbacks of electronic health records systems, Risk Management and Healthcare Policy 4 (2011) 47-55. https://doi: 10.2147/RMHP.S12985.
2. Jigna J. Hathaliya and Sudeep Tanwar. An exhaustive survey on security and privacy issues in healthcare 4.0. Computer Communications, 153:311 – 335, 2020. ISSN 0140-3664. https://doi.org/https://doi.org/10. 1016/j.comcom.2020.02.018.
3. Arash Ghazvini and Zarina Shukur. Security challenges and success factors of electronic healthcare system. Procedia Technology, 11:212 – 219, 2013. ISSN 2212-0173. http://www.sciencedirect.com/science/article/pii/S221201731300337X.
4. M. Wazid et al. A Novel Authentication and Key Agreement Scheme for Implantable Medical Devices Deployment. IEEE J Biomed Health Inform, 22(4):1299–1309, 07 2018.
5. H. M. Hussien et al. A systematic review for enabling of develop a blockchain tech- nology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. Journal of Medical Systems. https: //doi.org/10.1007/s10916-019-1445-8.
6. B. F. Smaradottir. Security management in electronic health records: Attitudes and experiences among health care professionals. In 2018 International Conference on Computational Science and Computational Intelligence (CSCI), pages 715–719, 2018. https://doi.org/10.1109/CSCI46756.2018.00143.

7. Buket Yüksel, Alptekin Küpçü, and Öznur Özkasap. Research issues for privacy and security of electronic health services. Future Generation Com- puter Systems. https://doi.org/10.1016/j.future.2016.08.011.
8. Omar El-Gayar and Ahmed Elnoshokaty. Factors and design features influencing the continued use of wearable devices. Journal of Healthcare Informatics Research, 7(3):359–385, Sep 2023. ISSN 2509-498X. https://doi.org/10.1007/s41666-023-00135-4.
9. Araujo, J. R. De; araujo filho, d. C. De; machado, l. D. S.; martins, r. M. G; cruz, R. de S. B. L. C. Sistema e-SUS AB: percepções dos enfermeiros da Estratégia Saúde da Família. 2019. Disponível em: https://scielosp.org/pdf/sdeb/2019. Acesso em: 16 set. 2020.
10. Marin, H. F. Sistemas de informação em saúde: considerações gerais. Journal of Health Informatics, [s. l.], v. 1, n. 2, p. 20-24, jan./mar., 2010.
11. Postal L, Celuppi IC, Lima G dos S, Felisberto M, Lacerda TC, Wazlawick RS, et al.. Sistema de agendamento online: uma ferramenta do PEC e-SUS APS para facilitar o acesso à Atenção Primária no Brasil. Ciência saúde coletiva [Internet]. 2021Jun;26(6):2023–34. Disponível em: https://doi.org/10.1590/1413-81232021266.38072020
12. Bredariol Junior JB, et al. Grau de maturidade da segurança da informação na visão dos gestores da rede pública de hospitais federais do Brasil. Revista Ibérica de Sistemas e Tecnologias de Informação, 2021;E41: 232-243.
13. Alves JC. Breves considerações à Lei Geral de Proteção de Dados (LGPD) e sua consonância com o direito fundamental à saúde em tempos de pandemia do novo coronavírus. Revista de Direito e Atualidades. 2021;1(1).
14. Thaísa Cardoso Lacerda, Jades Fernando Hammes, Miliane Fantonelli, Eduardo Monguilhott Dalmarco, and Raul Sidnei Wazlawick. e-sus aps strategy: Case of success on primary care informatization in brazil. Journal of Health Informatics, 12(4), nov. 2020. URL https://jhi.sbis.org.br/index.php/jhi-sbis/article/view/754.
15. Ministério da Saúde. Prontuário eletrônico do cidadão v5.0 - instalação do sistema. Disponível em: https://saps-ms.github.io/Manual-eSUS-APS/docs/PEC/PEC-02-instalacao/. accessed: 12.06.2023, 2023.
16. Mamta Madan, Meenu Dave, and Anisha Tandon. Importance of RTM for testing a web-based project. In 2018 7th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pages 816–818, 2018. https://doi.org/10.1109/ICRITO.2018.8748299.
17. Orlena CZ Gotel and CW Finkelstein. An analysis of the requirements traceability problem. In Proceedings of ieee international conference on requirements engineering, pages 94–101. IEEE, 1994.
18. Poyraz et al Software requirement traceability analysis using text mining methods. In 2017 25th Signal Processing and Communications Applications Conference (SIU), pages 1–4, 2017. https://doi.org/10.1109/SIU.2017.7960424.
19. Serin Jeong, Heetae Cho, and Seonah Lee. Agile requirement traceability matrix. In Proceedings of the 40th International Conference on Software Engineering: Companion Proceeedings, ICSE '18, page 187–188, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450356633. https://doi.org/10.1145/3183440.3195089.
20. Bangchao Wang, Rong Peng, Yuanbang Li, Han Lai, and Zhuo Wang. Requirements traceability technologies and technology transfer decision support: A systematic review. Journal of Systems and Software, 146:59–79, 2018. ISSN 0164-1212. https://doi.org/https://doi.org/10.1016/

j.jss.2018.09.001.
21. Rodrigo Tertulino, Nuno Antunes, and Higor Morais. Privacy in electronic health records: a systematic mapping study. Journal of Public Health, Jan 2023. ISSN 1613-2238. https://doi.org/10.1007/s10389-022-01795-z.
22. ISO. Health informatics — requirements for an electronic health record architecture, 2011. URL https://www.iso.org/standard/52823.html.
23. Orlena CZ Gotel and CW Finkelstein. An analysis of the requirements traceability problem. In Proceedings of ieee international conference on requirements engineering, pages 94–101. IEEE, 1994.
24. HIPAA (2013b) Summary of the HIPAA Privacy Rule. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf Acessado em 22/09/2022.
25. GDPR (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/ EC (General Data Protection Regulation). http://eurlex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC
26. Shah S. M., Khan R. A. (2020) Secondary use of electronic health record: Opportunities and challenges. IEEE Access 8:136947– 136965. https://doi.org/10.1109/ACCESS.2020.3011099
27. Poulis G., Loukides G., Skiadopoulos S., Gkoulalas-Divanis A. (2017) Anonymizing datasets with demographics and diagnosis codes in the presence of utility constraints. J. Biomed. Inform. 65:76–96. https://doi.org/10.1016/j.jbi.2016.11.001.
28. Kho A. N., Cashy J. P., Jackson K. L., Pah A. R., Goel S., Boehnke J., Humphries J. E., Kominers S. D., Hota B. N., Sims S. A., Malin B. A., French D. D., Walunas T. L., Meltzer D. O., Kaleba E. O., Jones R. C., Galanter W. L. (2015) Design and implementation of a privacy preserving electronic health record linkage tool in Chicago. J. Am. Med. Inform. Assoc. 22(5):1072– 1080. https://doi.org/10.1093/jamia/ocv038
29. Mamun Q., Rana M. (2017) A robust authentication model using multi-channel communication for eHealth systems to enhance privacy and security. In: 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 255–260 https://doi.org/10.1109/IEMCON.2017. 8117210
30. Sun Y., Zhang R., Wang X., Gao K., Liu L. (2018) A decen- tralizing attribute-based signature for healthcare blockchain. In: 2018 27th International Conference on Computer Communication and Networks (ICCCN), pp. 1–9 https://doi.org/10.1109/ ICCCN.2018.8487349
31. Essa Y. M., Hemdan E. E. D., El-Mahalawy A., Attiya G., El-Sayed A. (2019) IFHDS: Intelligent framework for securing healthcare bigdata. J. Med. Syst. 43(5):124. https://doi.org/10.1007/s10916-019-1250-4
32. Bhoomi, Gupta., Deepika, Bansal. Electronic Health Record Systems for Enhanced Medical Care: A Survey. (2023).257-262. doi: 10.1109/ICISCoIS56541.2023.10100356
33. Díaz-Palacios, José R., Víctor J. Romo-Aledo, and Amir H. Chinaei. "Biometric access control for e-health records in pre-hospital care." *Proceedings of the joint EDBT/ICDT 2013 workshops*. 2013.
34. Alghazo JM. Intelligent Security and Privacy of Electronic Health Records Using Biometric Images. Curr Med Imaging Rev. 2019;15(4):386-394. doi: 10.2174/1573405615666181228121535. PMID: 31989908.