FACULDADE MAUÁ DE GOIÁS
Instituto de Ensino e Pesquisa do Planalto Central
Graduação em Sistemas de Informação - Bacharelado

LEANDRO ALVES LEÃO

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS EM SISTEMAS DE PRONTUÁRIO ELETRÔNICO: UMA REVISÃO NARRATIVA DA LITERATURA

Águas Lindas De Goiás
2018.2

FACULDADE MAUÁ DE GOIÁS
Instituto de Ensino e Pesquisa do Planalto Central
Graduação em Sistemas de Informação - Bacharelado

LEANDRO ALVES LEÃO

SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS EM SISTEMAS DE PRONTUÁRIO ELETRÔNICO: UMA REVISÃO NARRATIVA DA LITERATURA

Artigo científico apresentado à Faculdade Mauá de Goiás como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.
Orientadora: Luana Guimarães da Silva

Águas Lindas De Goiás
2018.2

Segurança Da Informação E Proteção De Dados Em Sistemas De Prontuário Eletrônico: Uma Revisão Narrativa Da Literatura

Leandro Alves Leão[1]
Luana Guimarães da Silva[2]

RESUMO

A digitalização de registros clínicos por meio de sistemas de prontuário eletrônico ampliou o acesso e a continuidade da informação em saúde, mas também expôs instituições hospitalares a riscos crescentes relacionados à confidencialidade, à integridade e à disponibilidade de dados sensíveis. No Brasil, essa preocupação intensificou-se com a sanção da Lei Geral de Proteção de Dados (LGPD), em 2018, que classifica dados de saúde como dados pessoais sensíveis sujeitos a exigências reforçadas de tratamento. Este estudo teve como objetivo analisar, por meio de revisão narrativa da literatura, as estratégias, os controles técnicos e organizacionais e os desafios relacionados à segurança da informação em sistemas de prontuário eletrônico, considerando publicações científicas veiculadas até o ano de 2018, nos idiomas português e inglês, em bases de dados acadêmicas reconhecidas. A análise evidenciou que controles como criptografia, autenticação multifator, controle de acesso baseado em papéis e trilhas de auditoria constituem a base técnica predominante nos estudos consultados, ao passo que tecnologias emergentes, como blockchain, começavam a ser exploradas como alternativa para reforçar a integridade e a rastreabilidade dos registros. Identificou-se, contudo, que a efetividade desses controles depende fortemente de fatores organizacionais e humanos, como treinamento de equipes e definição de políticas institucionais, e que instituições de menor porte enfrentam limitações significativas de recursos para investimento em segurança da informação. Conclui-se que a proteção de dados em prontuário eletrônico exige a articulação entre soluções técnicas, governança institucional e capacitação profissional, permanecendo como lacuna relevante a avaliação da efetividade prática de tais medidas em diferentes contextos assistenciais.

Palavras-chave: Segurança da informação; Prontuário eletrônico; Proteção de dados; Controle de acesso; Saúde digital.

[1] Acadêmico do curso de Sistemas da Informação da Faculdade Mauá de Goiás - Instituto de Ensino e Pesquisa do Planalto Central - Ltda.
[2] Orientador. Docentes dos cursos de Ciências da Saúde da Faculdade Mauá de Goiás - Instituto de Ensino e Pesquisa do Planalto Central - Ltda.

1 INTRODUÇÃO

A segurança da informação em saúde refere-se ao conjunto de práticas, políticas e controles técnicos voltados a garantir a confidencialidade, a integridade e a disponibilidade dos dados clínicos armazenados em sistemas de prontuário eletrônico, princípios classicamente reunidos no acrônimo CIA (MARTIN; IMBODEN; GREEN, 2015). A crescente digitalização de registros clínicos, motivada pela busca de continuidade assistencial e eficiência operacional, ampliou a superfície de exposição desses dados a acessos indevidos, falhas técnicas e incidentes cibernéticos (KRUSE et al., 2017a). No Brasil, a proteção desses dados passou a ser orientada, a partir de 2018, pela Lei Geral de Proteção de Dados (LGPD), que classifica dados de saúde como dados pessoais sensíveis, sujeitos a bases legais específicas de tratamento e a exigências reforçadas de segurança (BRASIL, 2018). Observa-se, assim, a convergência entre um cenário técnico de ampliação de riscos e um cenário regulatório de exigências crescentes quanto à proteção de dados sensíveis em saúde.

A magnitude dos riscos associados à digitalização de dados clínicos pode ser observada em levantamentos oficiais do período. De acordo com dados do Departamento de Saúde e Serviços Humanos dos Estados Unidos (HHS), por meio de seu Escritório de Direitos Civis, foram registradas 265 violações de dados de saúde envolvendo 500 ou mais indivíduos apenas no ano de 2015, afetando mais de 113 milhões de pessoas, das quais a maior parte decorreu de incidentes de invasão e ataques cibernéticos a servidores de rede (U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, 2016). Em consonância com esse cenário, o Ponemon Institute (2016) constatou que o custo médio por registro violado no setor de saúde alcançou 402 dólares em 2016, o mais elevado entre os dezesseis setores econômicos analisados no estudo, muito acima da média global de 158 dólares por registro. Tais dados evidenciam que instituições de saúde figuravam, já naquele período, entre os alvos mais frequentes e financeiramente mais onerosos de incidentes de segurança da informação.

Embora a adoção de prontuários eletrônicos amplie o acesso e a continuidade da informação clínica, a literatura aponta uma lacuna relevante quanto à efetiva implementação de controles de segurança adequados em instituições de saúde. Jayabalan e O'Daniel (2016) observam que, apesar da existência de diversos modelos de controle de acesso descritos na literatura técnica, sua adoção prática permanece heterogênea entre instituições, muitas das quais mantêm mecanismos insuficientes para restringir o acesso indevido a dados sensíveis. Diante desse cenário, questiona-se: quais estratégias, controles técnicos e desafios têm sido relatados na literatura científica para garantir a segurança da informação em sistemas de prontuário eletrônico?

A realização desta revisão narrativa justifica-se pela relevância crescente do tema diante da intensificação de incidentes cibernéticos no setor de saúde e da entrada em vigor de exigências legais específicas para o tratamento de dados sensíveis no Brasil, campo ainda pouco consolidado na literatura nacional em Sistemas de Informação aplicados à saúde. Esta revisão busca contribuir para a sistematização de um conhecimento tecnicamente disperso entre diferentes comunidades de pesquisa, como a Ciência da Computação, a Ciência da Informação e a Administração em Saúde, favorecendo a compreensão integrada dos controles técnicos e organizacionais discutidos na literatura internacional do período analisado.

No campo dos Sistemas de Informação, a compreensão sobre estratégias de segurança da informação aplicadas a prontuários eletrônicos possui aplicação direta no planejamento de arquiteturas de dados, na definição de políticas de governança de tecnologia da informação e na escolha de controles técnicos de autenticação, criptografia e auditoria adotados por instituições de saúde (KRUSE et al., 2017b). Para os profissionais das equipes assistenciais, por sua vez, a compreensão sobre práticas seguras de manuseio de dados em prontuários eletrônicos é essencial para o cumprimento de responsabilidades éticas e legais relacionadas ao sigilo profissional, subsidiando também sua participação em processos institucionais de governança de dados clínicos (MARTIN; IMBODEN; GREEN, 2015).

Em termos de impacto social, o fortalecimento da segurança da informação em saúde contribui para a proteção da privacidade e da dignidade dos pacientes, para a redução de prejuízos institucionais decorrentes de incidentes de segurança e para o fortalecimento da confiança da população em serviços de saúde digitalizados (PONEMON INSTITUTE, 2016). Tal contribuição adquire relevância particular em instituições públicas e de menor porte, nas quais a limitação de recursos técnicos e financeiros pode ampliar a exposição a incidentes de segurança, com potenciais repercussões sobre a continuidade da assistência prestada à população (MEHRAEEN et al., 2016).

Para responder a essa questão, realizou-se uma revisão narrativa da literatura, reunindo e discutindo, de forma qualitativa, estudos científicos publicados até o ano de 2018, nos idiomas português e inglês, em bases de dados acadêmicas reconhecidas na área de Computação, Sistemas de Informação e Saúde, como PubMed/MEDLINE, IEEE Xplore, Scopus e SciELO, utilizando o Google Acadêmico como ferramenta auxiliar de localização e conferência bibliográfica. Foram utilizados descritores relacionados a "information security", "electronic health records", "access control", "data protection" e "segurança da informação", isoladamente e em combinações pertinentes por meio dos operadores booleanos AND e OR, sendo considerados estudos que relacionassem explicitamente segurança da informação,

proteção de dados e prontuário eletrônico em saúde, e excluídas publicações duplicadas, trabalhos posteriores ao período definido, textos em outros idiomas e estudos sem aderência direta à questão investigada. Diante desse contexto, o presente estudo tem como objetivo analisar as estratégias, os controles técnicos e organizacionais e os desafios relacionados à segurança da informação e à proteção de dados em sistemas de prontuário eletrônico, mapeando os principais controles relatados na literatura, identificando os principais riscos e incidentes associados a esses sistemas e apontando lacunas de pesquisa relacionadas à governança e à segurança de dados clínicos.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Conceitos fundamentais e bases teóricas

A segurança da informação em saúde fundamenta-se, classicamente, na tríade confidencialidade, integridade e disponibilidade, princípios que orientam a definição de controles técnicos e organizacionais aplicados a sistemas de prontuário eletrônico (MARTIN; IMBODEN; GREEN, 2015). A confidencialidade relaciona-se à restrição de acesso a dados clínicos apenas a indivíduos autorizados; a integridade, à garantia de que os registros não sejam alterados de forma indevida; e a disponibilidade, à possibilidade de acesso tempestivo à informação por profissionais autorizados no momento do atendimento (MARTIN; IMBODEN; GREEN, 2015). Kruse et al. (2017a) acrescentam a essa base conceitual a distinção entre salvaguardas administrativas, físicas e técnicas, categorias que estruturam, no contexto normativo estadunidense, as exigências de segurança aplicáveis a sistemas de informação em saúde.

No contexto brasileiro, a Lei Geral de Proteção de Dados Pessoais estabelece que dados de saúde constituem categoria de dados pessoais sensíveis, sujeitos a bases legais específicas de tratamento e a exigências reforçadas de segurança, cabendo aos agentes de tratamento adotar medidas técnicas e administrativas aptas a proteger tais dados de acessos não autorizados e de situações de destruição, perda, alteração ou comunicação indevida (BRASIL, 2018). Observa-se, portanto, convergência entre a tríade conceitual identificada na literatura internacional do período e as exigências legais posteriormente formalizadas no ordenamento brasileiro, ainda que os estudos técnicos aqui analisados sejam anteriores à própria promulgação da lei, o que reforça a continuidade histórica das preocupações com confidencialidade, integridade e disponibilidade de dados clínicos.

2.2 Funcionamento, controles técnicos e organizacionais

Entre os controles técnicos frequentemente discutidos na literatura, destacam-se mecanismos de controle de acesso baseado em papéis (role-based access control), criptografia de dados e trilhas de auditoria que permitem rastrear acessos e alterações realizadas em prontuários eletrônicos. Jayabalan e O'Daniel (2016), em revisão sistemática de dez anos de produção científica sobre o tema, identificam que os modelos de controle de acesso evoluíram de abordagens estritamente baseadas em papéis funcionais para modelos que incorporam dimensões contextuais, como localização e horário do acesso, de modo a proporcionar uma proteção mais granular da privacidade do paciente. Kruse et al. (2017b), por sua vez, ao examinarem vinte e cinco estudos sobre técnicas de segurança para prontuários eletrônicos, constatam que firewalls e criptografia figuram entre os mecanismos mais frequentemente relatados, ressalvando que nenhuma solução isolada é suficiente para prevenir a totalidade dos incidentes de violação de dados em ambientes de saúde.

Em direção complementar, Azaria et al. (2016) propõem, no sistema denominado MedRec, o uso de tecnologia blockchain para gerenciamento de acesso e permissões sobre dados médicos, de modo a garantir um registro descentralizado, auditável e resistente a alterações não autorizadas do histórico de acessos aos prontuários. Essa proposta representa uma ruptura em relação aos modelos tradicionais de controle de acesso centralizado discutidos por Jayabalan e O'Daniel (2016), na medida em que desloca a garantia de integridade de um servidor único para um registro distribuído entre múltiplos nós da rede. Já Mehraeen et al. (2016), ao analisarem desafios de segurança em ambientes de computação em nuvem aplicados à saúde, destacam que a autenticação, a autorização e o controle de acesso permanecem como preocupações centrais também nesse modelo de infraestrutura, no qual o armazenamento de dados clínicos passa a depender adicionalmente da confiabilidade de provedores terceirizados.

2.3 Riscos, incidentes e vulnerabilidades associados a sistemas de prontuário eletrônico

Kruse et al. (2017a), em revisão sistemática sobre tendências de cibersegurança em saúde, constatam que o setor permanece, de forma consistente, atrás de outros setores econômicos quanto à maturidade de suas práticas de segurança da informação, recomendando a adoção de protocolos claros de atualização de software, segmentação de redes e capacitação de funcionários sobre conteúdos suspeitos. Esse diagnóstico dialoga diretamente com os dados oficiais apresentados na introdução deste trabalho, segundo os quais a maior parte dos indivíduos afetados por violações de dados de saúde em 2015 esteve associada a incidentes de

invasão de servidores de rede, e não a falhas pontuais de dispositivos isolados (U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES, 2016).

Martin, Imboden e Green (2015) deslocam parte da análise dos riscos técnicos para fatores organizacionais, ao proporem um arcabouço teórico que explica a conformidade e a não conformidade de pequenas instituições de saúde estadunidenses às exigências da normativa de segurança então vigente. Os autores identificam quatro categorias de fatores determinantes: capacidade de recursos, ambiente de fiscalização, pressões sociais e normativas, e fatores organizacionais internos, evidenciando que a vulnerabilidade de instituições de menor porte decorre menos da ausência de conhecimento técnico e mais de restrições estruturais de recursos e de fiscalização insuficiente. Essa perspectiva amplia a compreensão dos riscos para além da dimensão estritamente tecnológica enfatizada por Kruse et al. (2017b), incorporando explicitamente a dimensão institucional como fator de vulnerabilidade.

2.4 Evidências e abordagens identificadas na literatura consultada

Os estudos analisados apresentam convergência quanto à centralidade do controle de acesso como mecanismo técnico prioritário na proteção de dados de prontuário eletrônico, ainda que proponham abordagens distintas para sua implementação. Enquanto Jayabalan e O'Daniel (2016) sistematizam modelos consolidados de controle de acesso baseados em papéis e atributos, Azaria et al. (2016) apresentam uma prova de conceito de arquitetura descentralizada baseada em blockchain, sugerindo que a integridade e a auditabilidade dos registros de acesso podem ser reforçadas por mecanismos que independem de uma autoridade central única. Tratava-se, à época, de uma proposta ainda exploratória, cuja maturidade tecnológica e viabilidade de adoção em larga escala por instituições de saúde não haviam sido plenamente estabelecidas nos estudos consultados.

Mehraeen et al. (2016), ao sistematizarem duzentos e dez artigos sobre segurança em computação em nuvem na saúde, identificam padrões recorrentes de vulnerabilidade relacionados à gestão de identidade e à ação de agentes maliciosos externos, resultado que converge com os achados de Kruse et al. (2017a) quanto à predominância de incidentes de invasão entre as causas de violação de dados no período. Por outro lado, Martin, Imboden e Green (2015) e Kruse et al. (2017b) evidenciam, de forma complementar, que a adoção de controles técnicos adequados não é suficiente isoladamente, sendo necessária a articulação entre tecnologia, políticas institucionais e capacitação de equipes para a efetiva proteção dos dados clínicos.

2.5 Desafios, controvérsias e limitações

Entre os principais desafios identificados na literatura, destaca-se a dificuldade de equilibrar segurança da informação e agilidade no acesso a dados clínicos em situações de urgência, nas quais controles excessivamente restritivos podem comprometer a celeridade do atendimento, tensão já observada nos modelos de controle de acesso contextual discutidos por Jayabalan e O'Daniel (2016). Some-se a isso a limitação de recursos técnicos e financeiros de muitas instituições de saúde, especialmente as de menor porte, para investimento em infraestrutura de segurança da informação adequada, conforme evidenciado por Martin, Imboden e Green (2015) em seu estudo sobre conformidade de pequenas instituições estadunidenses.

Parte da literatura questiona a efetividade de abordagens puramente técnicas de segurança da informação quando não acompanhadas de mudanças organizacionais nas instituições de saúde. Kruse et al. (2017a) apontam o fator humano, incluindo a insuficiência de treinamento de funcionários, como uma das principais vulnerabilidades associadas a incidentes de segurança no setor, resultado que reforça, sob outra perspectiva, a análise institucional proposta por Martin, Imboden e Green (2015). Observa-se ainda que, no período analisado, a proposta de utilização de blockchain apresentada por Azaria et al. (2016) permanecia em estágio exploratório, sem evidências consolidadas sobre seu desempenho, escalabilidade e custo de implementação em ambientes hospitalares reais, o que constitui uma limitação relevante das evidências então disponíveis.

2.6 Lacunas de pesquisa e perspectivas futuras

Como direções futuras, a literatura aponta a necessidade de estudos que avaliem a efetividade prática de controles técnicos de segurança da informação em diferentes portes e contextos institucionais, avançando além de revisões conceituais para investigações empíricas de implementação (KRUSE et al., 2017b). Destaca-se também a relevância de pesquisas voltadas ao desenvolvimento de soluções de segurança da informação de menor custo, acessíveis a instituições com recursos limitados, tal como sugerido por Martin, Imboden e Green (2015) a partir da constatação de que restrições financeiras constituem barreira relevante à conformidade de pequenas instituições de saúde.

Adicionalmente, a maturação de tecnologias emergentes como o blockchain, ainda em estágio inicial de exploração nos estudos analisados (AZARIA et al., 2016), constitui uma lacuna de pesquisa a ser aprofundada quanto à sua viabilidade prática em larga escala. No contexto brasileiro, a promulgação da Lei Geral de Proteção de Dados em 2018 (BRASIL,

2018), posterior à maior parte dos estudos técnicos internacionais aqui analisados, aponta para a necessidade de investigações futuras que avaliem a efetividade prática de frameworks de conformidade legal em instituições de saúde nacionais de diferentes portes, tema ainda não consolidado na literatura científica consultada.

3 CONCLUSÃO

A presente revisão narrativa teve como objetivo analisar as estratégias, os controles técnicos e organizacionais e os desafios relacionados à segurança da informação e à proteção de dados em sistemas de prontuário eletrônico. A literatura analisada evidencia que a proteção de dados clínicos apoia-se predominantemente em controles de acesso baseados em papéis, criptografia e trilhas de auditoria, complementados, em estudos mais exploratórios, por propostas de arquiteturas descentralizadas baseadas em blockchain, sem que estas últimas tivessem alcançado, no período analisado, maturidade suficiente para adoção consolidada.

Em resposta à questão norteadora, observa-se que as estratégias relatadas na literatura combinam dimensões técnicas e organizacionais: de um lado, mecanismos de autenticação, controle de acesso e auditoria; de outro, políticas institucionais, capacitação de equipes e alocação de recursos, sendo esta segunda dimensão apontada como determinante da efetividade da primeira. Do ponto de vista científico, a revisão contribui para consolidar um campo tecnicamente disperso, evidenciando convergências entre estudos de diferentes tradições disciplinares quanto à centralidade do controle de acesso e à insuficiência de soluções puramente tecnológicas. Do ponto de vista prático, os achados reforçam, no âmbito dos Sistemas de Informação em saúde, a relevância de decisões de governança que articulem investimento técnico, políticas institucionais e capacitação profissional.

Entre as limitações identificadas, destacam-se a concentração das evidências disponíveis em contextos institucionais estadunidenses, a escassez de estudos empíricos sobre a efetividade prática dos controles relatados e a ausência, no período analisado, de investigações específicas sobre a aplicação de exigências legais brasileiras a sistemas de prontuário eletrônico, uma vez que a Lei Geral de Proteção de Dados é posterior à maior parte da literatura técnica consultada. Tais lacunas indicam a necessidade de investigações futuras voltadas à avaliação empírica de frameworks de conformidade em instituições de saúde brasileiras, ao desenvolvimento de soluções de segurança de menor custo para instituições de recursos limitados e ao amadurecimento de tecnologias emergentes, como o blockchain, aplicadas à proteção de dados clínicos.

REFERÊNCIAS

AZARIA, A.; EKBLAW, A.; VIEIRA, T.; LIPPMAN, A. MedRec: using blockchain for medical data access and permission management. In: INTERNATIONAL CONFERENCE ON OPEN AND BIG DATA (OBD), 2., 2016, Viena. Proceedings [...]. [S. l.]: IEEE, 2016. p. 25-30. Disponível em: https://doi.org/10.1109/OBD.2016.11. Acesso em: março de 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: setembro de 2018.

JAYABALAN, M.; O'DANIEL, T. Access control and privilege management in electronic health record: a systematic literature review. Journal of Medical Systems, v. 40, n. 12, art. 261, 2016. Disponível em: https://doi.org/10.1007/s10916-016-0589-z. Acesso em: junho de 2018.

KRUSE, C. S.; FREDERICK, B.; JACOBSON, T.; MONTICONE, D. K. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technology and Health Care, v. 25, n. 1, p. 1-10, 2017a. Disponível em: https://doi.org/10.3233/THC-161263. Acesso em: novembro de 2018.

KRUSE, C. S.; SMITH, B.; VANDERLINDEN, H.; NEALAND, A. Security techniques for the electronic health records. Journal of Medical Systems, v. 41, n. 8, art. 127, 2017b. Disponível em: https://doi.org/10.1007/s10916-017-0778-4. Acesso em: outubro de 2018.

MARTIN, N. L.; IMBODEN, T.; GREEN, D. T. HIPAA security rule compliance in small healthcare facilities: a theoretical framework. Issues in Information Systems, v. 16, n. 1, p. 180-188, 2015. Disponível em: https://doi.org/10.48009/1_iis_2015_180-188. Acesso em: agosto de 2018.

MEHRAEEN, E.; GHAZISAEEDI, M.; FARZI, J.; MIRSHEKARI, S. Security challenges in healthcare cloud computing: a systematic review. Global Journal of Health Science, v. 9, n. 3, p. 157-166, 2016. Disponível em: https://doi.org/10.5539/gjhs.v9n3p157. Acesso em: abril de 2018.

PONEMON INSTITUTE. 2016 cost of data breach study: global analysis. Traverse City: Ponemon Institute, 2016. Disponível em: https://www.ponemon.org/research/ponemon-library/. Acesso em: dezembro de 2018.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES. Office for Civil Rights. Breaches affecting 500 or more individuals. Washington, DC: HHS, 2016. Disponível em: https://ocrportal.hhs.gov/ocr/breach/breach_report_hip.jsf. Acesso em: fevereiro de 2018.