Sistemas nacionais de prontuários eletrônicos frente à privacidade de dados

Ivan Luiz Marques Ricarte, ORCID 0000-0003-4832-9318
Faculdade de Tecnologia da Universidade Estadual de Campinas, Brasil
ricarte@unicamp.br

Resumo

Este trabalho analisa questões de privacidade contempladas em sistemas nacionais de prontuários eletrônicos, tendo com estudo de caso o sistema My Health Record, da Austrália. As questões de privacidade são organizadas conforme um arcabouço conceitual de privacidade informacional que contempla práticas de privacidade de empresas e comportamento de clientes. Após busca em bases de dados bibliográficos que cobrem a área da saúde, foram selecionados e analisados 18 artigos que abordavam as práticas de privacidade oferecidas pelo governo, as percepções ou atitudes de usuários, bem como suas intenções ou comportamento relacionados à privacidade informacional. Em relação às práticas de privacidade, foram abordados os aspectos de coleta e armazenamento da informação sobre os pacientes, bem como o grau de transparência e controle exercido pelo paciente sobre seus dados. No que se refere à percepção por parte dos pacientes, existe o receio de acesso inapropriado aos dados, bem como de roubo de identidade e de uso inadequado de informação por empresas de seguro ou empregadores, mas esse receio não difere daquele existente quando a informação está em suporte papel. Por fim, à medida que o paciente tem acesso à informação sobre sua saúde, há uma necessidade de que esses pacientes estejam capacitados a entender o que foi registrado, ou seja, há uma demanda por melhor literacia em saúde, mas profissionais de saúde receiam que esse acesso pelos pacientes possa levar a confusões e preocupações desnecessárias, levando consequentemente a um aumento de carga de trabalho. Conclui-se que o prontuário eletrônico controlado pelo paciente, em nível nacional, pode ser um instrumento efetivo de empoderamento do cidadão no controle de sua saúde e um motivador para ampliar as condições de sua literacia em saúde. No entanto, as questões de privacidade envolvidas demandam que haja um posicionamento explícito e claro, por parte dos governos, sobre a garantia da confidencialidade dos dados e usos secundários que poderão ser feitos dessa informação.

Palavras-chave: Prontuário eletrônico do paciente; Privacidade; Sistemas nacionais de saúde

National electronic health record systems and data privacy

Abstract

This paper analyzes privacy issues contemplated in national electronic health record systems, with the My Health Record system from Australia as a case study. Privacy issues are organized in accordance with a conceptual framework of informational privacy that addresses corporate privacy practices and customer behavior. After searching the bibliographic databases that cover the health area, 18 articles were selected and analyzed that addressed the privacy practices offered by the government, the perceptions or attitudes of users, as well as their intentions or behavior related to informational privacy. Regarding privacy practices, the aspects of collection and storage of information about patients, as well as the degree of transparency and control exercised by the patient about their data, were addressed. Concerning patient perception, there is a fear of inappropriate access to data as well as identity theft and misuse of information by insurance companies or employers, but not different from that of on paper. Finally, as the patient has access to information about their health, there is a need for these patients to be able to understand what has been registered, that is, there is a demand for better health literacy, but health professionals fear that this access by patients can lead to unnecessary confusion and worry, leading to an increase in workload. It is concluded that the patient-controlled electronic health record at the national level can be an effective tool to empower the citizen in controlling his health and a motivator to broaden the conditions of his health literacy. However, privacy issues involved demand that there be an explicit and clear position on the part of the governments on the guarantee of the confidentiality of the data and secondary uses that may be made of this information.

Keywords: Electronic Health Record; Privacy; National Health Systems

1 Introdução

Um prontuário eletrônico congrega, em meio digital, registros relativos ao estado de saúde de um paciente, seguindo um padrão para a organização da informação para prover assistência de saúde de modo contínuo, eficiente e com qualidade (Galvao & Ricarte, 2012). A continuidade da assistência, no entanto, só pode ser garantida quando houver alguma integração ou interoperabilidade entre os registros de um mesmo paciente em diferentes plataformas, com a informação sobre a saúde de cada indivíduo devidamente conectada (Tharmalingam, Hagens, & Zelmer, 2016). Sistemas nacionais de prontuários eletrônicos oferecem uma plataforma unificada para apoiar a integração desses registros, com o aval ou controle do governo federal. Vários países, entre os quais Dinamarca, Estados Unidos, Holanda, Noruega, Nova Zelândia e Suécia, têm buscado oferecer suas soluções para prover tais sistemas, seguindo diferentes abordagens decorrentes de opções políticas e de financiamento do sistema de saúde (Essén et al., 2018; Fragidis & Chatzoglou, 2018). Fragidis e Chatzoglou (2018) destacam que um elemento crítico de sucesso dessas iniciativas é o compromisso de todos os envolvidos no processo (*stakeholders*), incluindo o paciente. Nesse sentido, iniciativas nacionais nas quais os pacientes têm acesso e controle sobre seus registros de saúde podem trazer uma participação mais ativa por parte desses envolvidos e assim ampliar a aceitação no uso desses sistemas.

Uma preocupação que surge na implantação de um sistema nacional de prontuários eletrônicos é a privacidade informacional, ou seja, o grau de controle sobre se e como os dados sobre o paciente são coletados, armazenados, processados e disseminados. Preocupações sobre privacidade não são recentes, tendo surgido com o advento da fotografia e da disseminação de jornais impressos (Warren & Brandeis, 1890). No entanto, o advento das redes sociais e o consequente paradoxo da privacidade (Kokolakis, 2017), quando pessoas abrem mão de sua privacidade em troca de pequenas recompensas, e a ocorrência de problemas envolvendo o uso inadequado ou o acesso indevido a dados armazenados em redes sociais, como o uso de dados de usuários de Facebook pela Cambridge Analytica (Lee, 2018) e o vazamento de fotos armazenadas como privativas nessa mesma rede social (O'Sullivan, 2018), trazem novas dimensões às questões de privacidade na era digital.

O objetivo deste trabalho é analisar como questões de privacidade são contempladas em sistemas nacionais de prontuários eletrônicos. Para tanto, foi escolhido para essa análise o sistema nacional australiano (Australian Government. Australian Digital Health Agency, 2018), pela maturidade da experiência e pela disponibilidade de informação técnica. O governo australiano iniciou, em 2004, o esquema *HealthConnect* para promover a interoperabilidade dos sistemas de informação em saúde no país. A partir de uma avaliação desse esquema realizada em 2009, recomendou-se a criação de um prontuário eletrônico controlado pelo paciente, para melhorar a qualidade e a segurança da assistência em saúde, reduzir desperdícios e melhorar a continuidade da assistência. Em 2012 teve início a implantação do sistema *Personally Controlled Electronic Health Record* (PCEHR) e que, com algumas alterações implantadas em 2015, passou a ser denominado *My Health Record* (MyHR).

O arcabouço conceitual de privacidade informacional adotado para a análise foi o proposto por Beke, Eggers, e Verhoef (2018). Esse arcabouço contempla as práticas de privacidade de empresas e as intenções ou comportamento de clientes e, apesar de não ser especificamente par a área da saúde, pode ser aplicado para a análise da privacidade informacional em sistemas de prontuários. Nesse arcabouço, as práticas de privacidade adotadas por empresas incluem aspectos tais como o modo que a informação é coletada, como é armazenada, como é utilizada, o grau de transparência oferecido e o grau de controle exercido pelo cliente. Intenções ou comportamento de clientes incluem liberar o acesso à informação, aceitar ou adotar inovações direcionadas por dados, e os tipos de transações ou interações realizadas com os sistemas. Essas duas dimensões são mediadas pelas atitudes e

percepções dos clientes em relação às práticas de privacidade das empresas, envolvendo as preocupações com a privacidade por parte dos clientes e o chamado "cálculo de privacidade" (Dinev & Hart, 2006), para ponderar o balanço entre o nível de privacidade desejado e o benefício que é esperado com a disponibilização do acesso à informação. Esses aspectos são ainda influenciados por características como reputação da empresa, experiências anteriores de clientes e fatores como cultura e legislação local.

O restante deste artigo apresenta a metodologia utilizada para levantar informação publicada sobre o sistema australiano e para realizar a análise de dados sobre os aspectos de privacidade, bem como os resultados obtidos nessa análise.

2 Métodos

A abordagem utilizada para avaliar a percepção de questões de privacidade pelos participantes e usuários do sistema australiano de prontuários eletrônicos foi a análise exploratória por meio de uma revisão de literatura. Não foi o objetivo realizar uma revisão sistemática, mas um levantamento de percepções por meio das publicações.

Foram realizadas pesquisas bibliográficas referentes à iniciativa australiana do sistema nacional de prontuários eletrônicos na base PubMed e no Sistema de Bibliotecas da Unicamp (106 bases). Em PubMed foi utilizado o recurso de busca avançada com os descritores MeSH *Australia* e *electronic health record* (prontuário eletrônico do paciente). No Sistema de Bibliotecas da Unicamp não havia a possibilidade de especificar descritores MeSH e, nesse caso, foi realizada a busca ampla por resultados contendo esses termos.

Aos artigos resultantes foram aplicados critérios de exclusão. O primeiro critério foi ignorar resultados publicados em data anterior a 2012, pois este foi o ano de implantação da iniciativa australiana e, portanto, resultados anteriores a essa data não se aplicariam ao atual estágio do sistema. Aos resultados remanescentes foi aplicada a análise de título e, posteriormente, de resumo. Finalmente, o texto integral foi analisado para decidir se o trabalho em questão abordava, de alguma maeira, a percepção de privacidade.

O conteúdo dos artigos selecionados para a revisão final foi analisado com apoio do software NVivo (versão 10). Para tanto, o arcabouço conceitual de privacidade informacional foi traduzido em um conjunto de rótulos organizados hierarquicamente (na terminologia desse software, foram representados como nós) e, em cada artigo analisado (fontes), evidências para cada aspecto foram registradas, seguindo a abordagem metodológica da análise de conteúdo. Desse modo, ao fim desse procedimento de análise, os registros associados a cada aspecto da privacidade informacional foram devidamente levantados. Para efeitos de aplicação do arcabouço conceitual, considerou-se que o governo seria a empresa provedora do serviço, enquanto que clientes são tanto os pacientes como os profissionais de saúde que precisam ter acesso à informação para prover a assistência.

3 Resultados

A busca teve 1301 resultados na base de dados PubMed e 84.199 resultados no Sistema da Biblioteca da Unicamp. Após a aplicação de critérios de exclusão pela data de publicação e pela análise de título e resumos, foram selecionados 31 artigos para avaliação do texto integral. Desses, 13 artigos foram excluídos por não abordar, na análise do texto integral, referências aos tópicos de interesse relacionados à percepção da privacidade informacional. Os resultados obtidos na análise dos 18 artigos restantes que efetivamente continham indicações referentes ao arcabouço conceitual de privacidade informacional são sintetizados a seguir.

3.1 Práticas de privacidade

A informação coletada e armazenada em MyHR pode ser oriunda de diversas fontes, que necessariamente precisam estar registradas no sistema para ter esse acesso (Nøhr et al., 2017; Pearce & Bainbridge, 2014). Há dados que são inseridos pelo próprio governo, por meio da informação do programa Medicare, e há dados clínicos que são carregados a partir dos sistemas de informação clínica de cada instituição ou profissional de saúde (Bidargaddi, Van Kasteren, Musiat, & Kidd, 2018). Desses dados clínicos, o mínimo que se espera que esteja presente é o Sumário de saúde compartilhado, tipicamente criado pelo clínico geral do paciente, mas que pode ser criado por um enfermeiro registrado ou por um agente de saúde aborígene (Hemsley et al., 2017; Pearce & Bainbridge, 2014). Os pacientes podem complementar essas informações com notas pessoais de saúde, informação sobre a existência e localização de diretivas de cuidados antecipados, e detalhes de contatos de emergência (Pearce & Bainbridge, 2014).

No que se refere ao armazenamento, MyHR adota um modelo de repositórios distribuídos, com operadores registrados que mantém a informação carregada no sistema (Mendelson & Wolf, 2016; Nøhr et al., 2017; Pearce & Bainbridge, 2014). O responsável por essa infraestrutura é a *Australian Digital Health Agency*, um órgão governamental que, no entanto, terceirizou várias de suas funções para uma companhia privada (Mendelson & Wolf, 2016).

A transparência, em princípio, é garantida, pois todos os pacientes têm acesso aos dados de sua saúde que estão armazenados no sistema (Essén et al., 2018; Nøhr et al., 2017). Ademais, todos os acessos ao sistema são registrados e os pacientes podem verificar quais instituições acessaram os seus dados (Nøhr et al., 2017; Pearce & Bainbridge, 2014). No entanto, alguns autores questionam o quanto desse acesso pode efetivamente ser compreendido pelos pacientes, seja por questões de usabilidade do sistema (Walsh et al., 2017), seja pelas limitações impostas pelas condições de saúde desses pacientes (Hemsley et al., 2017; Kerai, Wood, & Martin, 2014).

Em relação ao controle que o paciente exerce sobre quem pode ter acesso aos seus dados, aparentemente é completo (Nøhr et al., 2017). Com a exceção do Sumário de saúde compartilhado, todos os documentos adicionais podem ser liberados, restritos com um código de acesso ou totalmente escondidos por meio das restrições de acesso definidas pelo paciente (Garrety, McLoughlin, Wilson, Zelle, & Martin, 2014); dados não podem ser removidos. Há, no entanto, situações previstas na legislação nas quais esses controles de acesso podem ser desconsiderados pelo governo (Mendelson & Wolf, 2016) ou no atendimento de emergência (Pearce & Bainbridge, 2014).

Sobre o uso dos dados, deveria em princípio ser exclusivamente para fins terapêuticos, em benefício dos pacientes. No entanto, grupos ligados à privacidade têm questionado a possibilidade de

usos secundários desses dados desde a implantação do sistema (Srur & Drew, 2012) e, efetivamente, há brechas na legislação para permitir o acesso aos dados para uso em processos legais e para a vigilância sanitária (Mendelson & Wolf, 2016).

3.2 Percepções ou atitudes relacionadas à privacidade

Como seria de se esperar, diversos estudos identificaram nos usuários alguma preocupação moderada sobre a segurança oferecida por tal sistema e a garantia de que seus dados permaneceriam confidenciais (Andrews, Gajanayake, & Sahama, 2014; Kerai et al., 2014), mas não muito diferente do que sentem em relação ao sistema tradicional em papel (Carroll & Butler-Henderson, 2017). Entre os receios estão o acesso inapropriado, o roubo de identidade, o uso inadequado da informação por empresas de seguro ou empregadores (Lehnbom, Brien, & McLachlan, 2014). Apesar disso, parece haver confiança suficiente no governo para levar os pacientes a usar o sistema (van Kasteren, Maeder, Williams, & Damarell, 2017).

Sobre o cálculo da privacidade, será preciso esperar mais tempo com o sistema em plena adoção para que os benefícios possam ser contrapostos ao que se perdeu de privacidade na utilização do sistema (Andrews et al., 2014; Srur & Drew, 2012).

3.3 Intenções ou comportamento de usuários em relação à privacidade

No que se refere à liberação de acesso à informação em MyHR, a grande maioria dos usuários acredita que o clínico geral deve ter acesso completo aos dados, mas não necessariamente outros profissionais de saúde (Kerai et al., 2014; Lehnbom et al., 2014). Mesmo pacientes infectados com HIV consentem em compartilhar essa informação em nome de uma assistência mais abrangente (Parsons & Ryder, 2016).

De modo geral, as pessoas tendem a aceitar bem a proposta desse sistema, antevendo melhor assistência em saúde e maior controle sobre a própria saúde (Hanna, Gill, Newstead, Hawkins, & Osborne, 2017). No entanto, a falta de informação sobre proteções e riscos à privacidade podem influenciar negativamente na ampla adoção do sistema (Hemsley et al., 2017).

Por fim, no que se refere às transações ou interações com o sistema, o acesso e o controle sobre as informações da própria saúde demandam que o paciente tenha conhecimento suficiente para compreender as informações e as consequências de liberar ou restringir o seu acesso a profissionais da assistência em saúde – o conceito da literacia em saúde (Hanna et al., 2017). Por outro lado, profissionais de saúde receiam que esse acesso pelos pacientes possa levar a confusões e preocupações desnecessárias, levando consequentemente a um aumento de carga de trabalho (Kerai et al., 2014).

4 Conclusão

O prontuário eletrônico controlado pelo paciente, em nível nacional, pode ser um instrumento efetivo de empoderamento do cidadão no controle de sua saúde e um motivador para ampliar as condições de sua literacia em saúde. No entanto, as questões de privacidade envolvidas demandam que haja um posicionamento explícito e claro, por parte dos governos, sobre a garantia da confidencialidade dos dados e usos secundários que poderão ser feitos dessa informação, bem como sobre as atitudes que serão tomadas contra os abusadores da privacidade na improvável ocorrência de sua violação.

5 Referências

Andrews, L., Gajanayake, R., & Sahama, T. (2014). The Australian general public's perceptions of having a personally controlled electronic health record (PCEHR). *International Journal of Medical Informatics*, *83*(12), 889–900. https://doi.org/10.1016/j.ijmedinf.2014.08.002

Australian Government. Australian Digital Health Agency. (2018). My Health Record. Retrieved September 12, 2018, from https://www.myhealthrecord.gov.au/

Beke, F. T., Eggers, F., & Verhoef, P. C. (2018). Consumer Informational Privacy: Current Knowledge and Research Directions. *Foundations and Trends® in Marketing*, *11*(1), 1–71. https://doi.org/10.1561/1700000057

Bidargaddi, N., Van Kasteren, Y., Musiat, P., & Kidd, M. R. (2018). Developing a third-party analytics application using Australia's national personal health records system: Case study. *Journal of Medical Internet Research*, *20*(4). https://doi.org/10.2196/medinform.7710

Carroll, J., & Butler-Henderson, K. (2017). MyHealthRecord in Australian Primary Health Care: An Attitudinal Evaluation Study. *Journal of Medical Systems*, *41*(10). https://doi.org/10.1007/s10916-017-0807-3

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Essén, A., Scandurra, I., Gerrits, R., Humphrey, G., Johansen, M. A., Kiergegaard, P., … Ancker, J. S. (2018). Patient access to electronic health records: Differences across ten countries. *Health Policy and Technology*, *7*(1), 44–56. https://doi.org/10.1016/j.hlpt.2017.11.003

Fragidis, L. L., & Chatzoglou, P. D. (2018). Implementation of a nationwide electronic health record (EHR): The international experience in 13 countries. *International Journal of Health Care Quality Assurance*, *31*(2), 116–130. https://doi.org/10.1108/IJHCQA-09-2016-0136

Galvao, M. C. B., & Ricarte, I. L. M. (2012). *Prontuário do Paciente*. Rio de Janeiro: Guanabara-Koogan.

Garrety, K., McLoughlin, I., Wilson, R., Zelle, G., & Martin, M. (2014). National electronic health records and the digital disruption of moral orders. *Social Science and Medicine*, *101*, 70–77. https://doi.org/10.1016/j.socscimed.2013.11.029

Hanna, L., Gill, S. D., Newstead, L., Hawkins, M., & Osborne, R. H. (2017). Patient perspectives on a personally controlled electronic health record used in regional Australia: 'I can be like my own doctor.' *Health Information Management Journal*, *46*(1), 42–48. https://doi.org/10.1177/1833358316661063

Hemsley, B., McCarthy, S., Adams, N., Georgiou, A., Hill, S., & Balandin, S. (2017). Legal, ethical, and rights issues in the adoption and use of the "My Health Record" by people with communication disability in Australia. *Journal of Intellectual & Developmental Disability*, 1–9. https://doi.org/10.3109/13668250.2017.1294249

Kerai, P., Wood, P., & Martin, M. (2014). A pilot study on the views of elderly regional Australians of personally controlled electronic health records. *International Journal of Medical Informatics*, *83*(3), 201–209. https://doi.org/10.1016/j.ijmedinf.2013.12.001

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers and Security*, *64*, 122–134. https://doi.org/10.1016/j.cose.2015.07.002

Lee, D. (2018). Facebook sued by top prosecutor over Cambridge Analytica. *BBC News*. Retrieved from https://www.bbc.com/news/technology-46627133

Lehnbom, E. C., Brien, J. E., & McLachlan, A. J. (2014). Knowledge and attitudes regarding the personally controlled electronic health record: An Australian national survey. *Internal Medicine Journal*, *44*(4), 406–409. https://doi.org/10.1111/imj.12384

Mendelson, D., & Wolf, G. (2016). "My [Electronic] Health Record" – Cui Bono (for Whose Benefit)? *Journal of Law and Medicine*, *24*(2), 283–296. Retrieved from https://ssrn.com/abstract=2881787

Nøhr, C., Parv, L., Kink, P., Cummings, E., Almond, H., Nørgaard, J. R., & Turner, P. (2017). Nationwide citizen access to their health data: Analysing and comparing experiences in Denmark, Estonia and Australia. *BMC Health Services Research*, *17*(1), 1–11. https://doi.org/10.1186/s12913-017-2482-y

O'Sullivan, D. (2018). Facebook reveals bug exposed 6.8 million users' photos. *CNN International Edition*. Retrieved from https://edition.cnn.com/2018/12/14/tech/facebook-private-photos-exposed-bug/index.html

Parsons, B. F., & Ryder, N. (2016). High uptake of shared electronic health records among HIV-infected patients at an Australian sexual health clinic. *Sexual Health*, *13*(4), 393–394. https://doi.org/10.1071/SH16035

Pearce, C., & Bainbridge, M. (2014). A personally controlled electronic health record for Australia. *Journal of the American Medical Informatics Association*, *21*(4), 707–713. https://doi.org/10.1136/amiajnl-2013-002068

Srur, B. L., & Drew, S. (2012). Challenges in designing a successful e-health system for Australia. In *2012 International Symposium on Information Technologies in Medicine and Education* (pp. 480–484). Hokodate, Japan: Institute of Electrical and Electronics Engineers. https://doi.org/10.1109/ITiME.2012.6291347

Tharmalingam, S., Hagens, S., & Zelmer, J. (2016). The value of connected health information: Perceptions of electronic health record users in Canada. *BMC Medical Informatics and Decision Making*, *16*(1), 1–9. https://doi.org/10.1186/s12911-016-0330-3

van Kasteren, Y., Maeder, A., Williams, P. A., & Damarell, R. (2017). Consumer perspectives on My Health Record: A review. *Studies in Health Technology and Informatics*, *239*(March 2016), 146–152. https://doi.org/10.3233/978-1-61499-783-2-146

Walsh, L., Hemsley, B., Allan, M., Adams, N., Balandin, S., Georgiou, A., … Hill, S. (2017). The E-health Literacy Demands of Australia's My Health Record: A Heuristic Evaluation of Usability. *Perspectives In Health Information Management*, *14*(Fall), 1–28. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cmedm&AN=29118683&site=ehost-live

Warren, S., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 1–22. https://doi.org/10.2307/1321160