Artículo original

Percepções de privacidade em sistemas nacionais de prontuários eletrônicos: o caso australiano

Percepciones de privacidad en los sistemas nacionales de registros electrónicos de salud: el caso australiano

Perceptions of privacy in national electronic health record systems: the Australian case

Ivan Luiz Marques Ricarte1* https://orcid.org/0000-0003-4832-9318

Faculdade de Tecnologia da Universidade Estadual de Campinas (FT-UNICAMP)

*Correspondencia: ricarte@unicamp.br

RESUMO

O objetivo deste trabalho é explorar questões de privacidade contempladas em sistemas nacionais de prontuários eletrônicos, tendo como 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, roubo de identidade e uso inadequado de informação por empresas de seguro ou empregadores. À medida que o paciente tem acesso à informação sobre sua saúde 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. Conclui-se que o prontuário eletrônico controlado pelo paciente 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 seus usos secundários.

Palavras-chave: Registros eletrônicos de saúde; privacidade; sistemas de saúde.

RESUMEN

Este trabajo tuvo como objetivo explorar los problemas de privacidad abordados por los sistemas nacionales de registros electrónicos de salud, para lo cual se efectuó un estudio de caso del sistema *My Health Record*, de Australia. Los problemas de privacidad se organizaron de acuerdo con un marco conceptual de privacidad informativa que incluyó prácticas de privacidad corporativa y comportamiento del cliente. Después de buscar bases de datos bibliográficas que cubren la salud, se seleccionaron y analizaron 18 artículos que abordaban las prácticas de privacidad del gobierno, las percepciones o actitudes de los usuarios, así como sus intenciones o comportamientos relacionados con la privacidad informativa. Con respecto a las prácticas de privacidad, se abordaron los aspectos de recopilación y almacenamiento de información del paciente, así como el grado de transparencia y control ejercido por el paciente sobre sus datos. En relación con la percepción de los pacientes, existe el temor de un acceso inadecuado a los datos, de robo de identidad y del uso indebido de la información por parte de las compañías de seguros o los empleadores. Dado que el paciente tiene acceso a información de salud, existe una demanda de una mejor alfabetización en salud, pero los profesionales de la salud temen que este acceso por parte de los pacientes puede generar confusión y preocupación innecesarias. Se concluye que el registro médico electrónico controlado por el paciente a nivel nacional puede ser un instrumento eficaz para empoderar a los ciudadanos a fin de controlar su salud y un motivador para expandir las condiciones de su alfabetización en salud. Sin embargo, los problemas de privacidad involucrados exigen una posición explícita y clara por parte de los gobiernos para garantizar la confidencialidad y el uso de los datos.

Palabras clave: Registros electrónicos de salud; privacidad; sistemas de salud.

ABSTRACT

The objective of this paper was to explore privacy issues addressed by national electronic health record systems, with a case study of Australia's My Health Record system. Privacy issues were organized according to a conceptual framework of informational privacy that included corporate privacy practices and customer behavior. After searching bibliographic databases covering health, 18 articles were selected and analyzed that addressed the government's privacy practices, users' perceptions or attitudes, as well as their intentions or behavior related to informational privacy. Regarding privacy practices, the aspects of collecting and storing patient information were addressed, as well as the degree of transparency and control exercised by the patient over their data. With regard to patients' perception, there is a fear of improper access to data as well as identity theft and misuse of information by insurance companies or employers, but this fear does not differ from that when information is available on paper support. Finally, as the patient has access to health information, there is a need for these patients to be able to understand what has been recorded, i.e. there is a demand for better health literacy, but health professionals fear that this access by patients may lead to unnecessary confusion and worry, leading to an increased workload. It is concluded that the patient-controlled electronic health record at the national level can be an effective instrument for empowering citizens to control their health and a motivator to expand the conditions of their health literacy. However, these privacy issues call for an explicit and clear position by governments to ensure the confidentiality of the data and secondary uses that may be made of this information.

Key words: Electronic Health Records; Privacy; Health Systems

Recibido: 06/11/2019

Aceptado: 11/03/2020

Introdução

Sistemas de registros eletrônicos de saúde têm sido implantados, via de regra, de modo autônomo e independente por diferentes instituições de saúde, como estratégia para melhorar

seus processos internos e a assistência ao paciente. A integração desses registros de saúde, dispersos e fragmentados entre essas diversas instituições, constituiria o prontuário eletrônico do paciente, congregando, em meio digital, registros relativos ao estado de saúde de cada paciente, seguindo um padrão para a organização da informação, de modo a prover assistência de saúde de modo contínuo, eficiente e com qualidade.[1] 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.[2]

Uma das estratégias de integração dos registros eletrônicos de saúde é a implantação de um sistema nacional de prontuários eletrônicos. Nessa abordagem, o governo federal é responsável, seja por meio de aval ou de controle, por uma plataforma unificada que apoia a integração dos registros, contemplando os itens de informação que podem ser compartilhados entre os sistemas para prover a assistência de modo contínuo. 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.[3,4]

Nas iniciativas e tentativas de implantação desses sistemas nacionais de prontuários, a adesão pelos envolvidos tem mostrado ser uma barreira. Fragidis e Chatzoglou[4] destacam que um elemento crítico de sucesso dessas iniciativas é o compromisso de todos os envolvidos no processo (*stakeholders*), incluindo o paciente. Um paciente envolvido, que use esse recurso para levar suas informações para o profissional da saúde e que, consequentemente, deseja que esses profissionais complementem esses registros integrados, pode levar a uma maior utilização desses sistemas. 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. Por outro lado, aspectos relacionados à privacidade precisam ser explicitados e devidamente tratados.

Privacidade, por si, é um conceito complexo e multidimensional, com influências culturais e considerações individuais, como bem discutido por Solove.[5] Em seu esforço para conceituar privacidade, em uma abordagem pragmática e à luz das semelhanças de família de Wittgenstein, esse autor revisita as diferentes dimensões de privacidade como o direito de ser deixado a sós, do limite de acesso ao indivíduo, de sigilo, da personalidade, da intimidade e de controle sobre o fluxo de informação, que é o foco deste trabalho. Preocupações sobre

privacidade não são recentes, havendo manifestações sobre o tema desde o Século XIX com a disseminação da fotografia e seu uso em jornais impressos.[6] No entanto, o advento de serviços digitais na rede mundial e das redes sociais levanta novas questões sobre a privacidade na era digital, como o paradoxo da privacidade:[7] se, por um lado, as pessoas valorizam sua privacidade, por outro lado elas abrem mão de sua privacidade em troca de pequenas recompensas, como uma conta de correio gratuita ou simplesmente uma reação de seus contatos a uma fotografia ou comentário. Outra questão específica da privacidade na era digital está relacionada à ocorrência de problemas envolvendo uso inadequado ou acesso indevido a dados pessoais registrados em redes sociais, como o uso de dados de usuários de Facebook pela Cambridge Analytica[8] e o vazamento de fotos armazenadas como privativas nessa mesma rede social.[9] Mesmo com tantos aspectos envolvidos no conceito de privacidade, uma abordagem pragmática que tem sido utilizada juridicamente para essa definição é de que privacidade está relacionada ao controle e autonomia sobre a coleta, armazenamento e uso da informação, e que ela é violada quando a informação é coletada, armazenada ou utilizada contra a vontade do indivíduo.[10]

No caso de prontuários de pacientes, o caráter pessoal e sensível dos dados armazenados leva a questão da privacidade informacional a novos patamares de criticidade. Vários autores têm se debruçado sobre essa questão, abordando tanto recomendações para melhorar a segurança e privacidade no desenvolvimento[11] como os aspectos de segurança e privacidade abordados em pesquisas sobre esse tipo de sistema de informação.[12] No entanto, faltam estudos que abordem essas questões, bem como as percepções de pacientes e profissionais sobre elas, especificamente em sistemas nacionais de prontuários eletrônicos, nos quais o objetivo é prover acesso aos dados por um amplo conjunto de profissionais distribuídos em todo o território de um país.

O objetivo deste trabalho é explorar como os aspectos de privacidade são contempladas e percebidas em sistemas nacionais de prontuários eletrônicos. Para tanto, foi escolhido como um estudo de caso para essa análise o sistema nacional australiano,[13] 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 proposto por Beke, Eggers, e Verhoef.[10] 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 esta análise da privacidade informacional em sistemas de prontuários. Nesse arcabouço, apresentado esquematicamente na figura 1, 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",[14] 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.

Adaptado de Beke, Eggers e Verhoef.[10]

Fig. 1 - Arcabouço conceitual para privacidade.

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 e a discussão relacionados a essa análise.

Métodos

A abordagem utilizada para avaliar a percepção de questões de privacidade pelos participantes e usuários de um sistema nacional de prontuários eletrônicos foi a análise documental exploratória por meio de um estudo de caso sobre o sistema australiano. Não foi o objetivo realizar uma revisão sistemática sobre alguma questão específica relacionada à privacidade, mas sim um levantamento de percepções por meio das publicações.

Foram realizadas pesquisas bibliográficas referentes à iniciativa australiana do sistema nacional de prontuários eletrônicos na base bibliográfica PubMed e no recurso de busca integrada do Sistema de Bibliotecas da Universidade Estadual de Campinas, que congrega 106 distintas bases de dados bibliográficos em diferentes áreas do conhecimento. Em PubMed foi utilizado o recurso de busca avançada com os descritores MeSH *Australia* e *electronic health record* (prontuário eletrônico do paciente). O recurso de busca integrada do Sistema de Bibliotecas da Universidade Estadual de Campinas não possibilita a especificação de descritores MeSH e, nesse caso, foi realizada a busca ampla por resultados contendo esses mesmos termos.

Ao conjunto de artigos resultantes foram aplicados critérios adicionais de exclusão e inclusão. O primeiro critério de exclusão foi ignorar os artigos 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 avaliada a pertinência ao tema pela análise de título e, posteriormente, do conteúdo do resumo. Finalmente, o texto integral foi analisado para decidir se o trabalho em questão abordava, de alguma maneira, a percepção de privacidade no uso do sistema nacional de prontuários eletrônicos da Austrália. A inclusão de novos artigos deu-se pela técnica de *snowballing*,[15] ou seja, pela análise de artigos mais recentes que citaram os artigos selecionados.

A análise do conteúdo dos artigos selecionados para a revisão final foi realizada 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). Por exemplo, foram criados os rótulos Uso, Transparência, Controle, Coleta e Armazenamento e esses, por sua vez, foram agregados no rótulo Práticas de privacidade (Fig. 2). Similarmente, os rótulos para Percepções ou atitudes e para Intenções ou comportamento também foram criados.

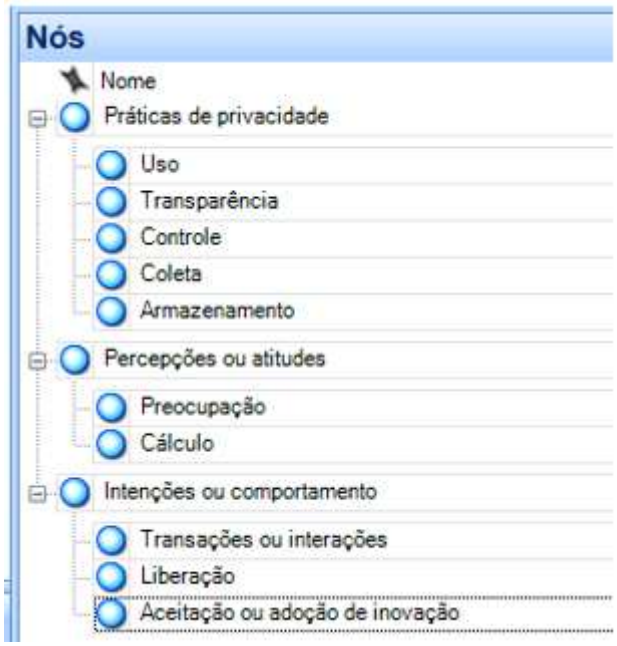

Fig. 2 - Rótulos para análise conteúdo no software NVivo.

Os artigos selecionados foram carregados como fontes internas no software e, para cada artigo, foram rotulados os fragmentos de texto que constituíam evidências para cada aspecto do arcabouço conceitual, conforme 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. O software permite que, a partir desses registros, sejam levantados relatórios com as evidências organizadas pelos nós.

Para efeitos de aplicação do arcabouço conceitual de privacidade, considerou-se que o governo seria a empresa provedora do serviço, enquanto que clientes são tanto pacientes como profissionais de saúde que precisam ter acesso à informação para prover a assistência.

Resultados e discussão

A busca realizada teve 1 301 resultados na base de dados PubMed e 84 199 resultados no Sistema da Biblioteca da Universidade Estadual de Campinas. 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 aspectos de interesse apresentados no arcabouço de privacidade informacional. Os 18 artigos efetivamente selecionados não necessariamente abordavam a privacidade como foco central, mas poderiam abordar outros aspectos do MyHR e, indiretamente, fazer referências a questões relacionadas à privacidade, segundo o arcabouço conceitual adotado para direcionar este estudo.

A tabela sumariza quais foram os 18 artigos analisados e quais aspectos cada um abordava. Os resultados obtidos na análise dos artigos selecionados são sintetizados a seguir, organizados segundo as três dimensões desse arcabouço, quais sejam: práticas institucionais de privacidade, percepções ou atitudes relacionadas à privacidade e intenções ou comportamento de usuários em relação à privacidade.

Tabela - Síntese dos artigos analisados e aspectos endereçados por cada um

Primeiro autor, ano	Coleta	Armaz	Transp	Contr	Uso	Preoc	Calc	Liber	Aceit	Inter
Andrews, 2014 (29)						X	X		X	
Bidargaddi, 2017 (17)	X									
Bidargaddi, 2018 (25)				X	X					
Carroll, 2017 (27)				X		X	X	X		

Essén , 2018 (3)			X							
Garrety, 2014 (24)				X						
Garrety, 2016 (18)	X								X	
Hanna, 2017 (22)		X							X	X
Hemsley, 2017 (20)	X								X	X
Kerai, 2014 (23)			X	X		X		X	X	X
Lehnbom, 2014 (26)				X		X		X		
Mendelson, 2016 (21)		X			X					
Nohr, 2017 (16)	X	X	X	X						
Parsons, 2016 (31)								X	X	
Pearce, 2014 (19)	X	X	X	X	X					X
Srur, 2012 (28)					X		X			
van Kasteren, 2017 (30)						X		X		
Walsh, 2017 (32)										X

Os aspectos envolvidos incluem as dimensões das práticas institucionais de privacidade (coleta, armazenamento [armaz], transparência [transp], controle [contr], uso), de percepções ou atitudes relacionadas à privacidade (preocupação [preoc], cálculo de privacidade [calc]) e de intenções ou comportamento de usuários em relação à privacidade (liberação [liber], aceitação [aceit] e interação [inter]).

Práticas institucionais de privacidade

As práticas institucionais de privacidade compreendem estratégias de coleta, armazenamento, uso, transparência e controle dos dados dos indivíduos.

No que se refere à coleta de dados em um prontuário, um dos aspectos que interfere na privacidade informacional é que nem sempre o paciente sabe que suas informações estão sendo coletadas. A informação coletada e armazenada em MyHR pode ser oriunda de diversas fontes, a partir de usuários ou instituições que necessariamente precisam estar registradas no sistema para ter essa permissão de acesso. As evidências coletadas dos artigos analisados confirmam essa é, efetivamente, a condição presente em MyHR. Nohr et al.[16] afirmam que os dados clínicos são produzidos e mantidos em sistemas de atenção primária (clínicos gerais), secundária (especialistas) e terciária (hospitais), que alimentam o sistema MyHR com sumários desses dados. Bidargaddi e Kidd[17] corroboram esse mecanismo de coleta, ao afirmar que há dados que são inseridos pelo próprio governo, por meio da informação do programa de saúde público (Medicare), e há dados clínicos que são carregados a partir dos sistemas de informação clínica de cada instituição, sejam hospitais, clínicas ou consultórios de profissionais de saúde, podendo essa informação ser carregada automaticamente ou a partir de requisições dos usuários, a depender das características dos sistemas locais conectados ao sistema MyHR. Assim, cada instituição pode ter seu sistema de registro eletrônico, mas é preciso que esse sistema seja capaz de carregar parte dos dados para o sistema nacional de prontuários.

Entre os dados clínicos registrados no sistema nacional, o mínimo que se espera que esteja presente é o Sumário de Saúde Compartilhado, o único item do prontuário que, seguramente, estará disponível para qualquer profissional de saúde atuando na assistência de um paciente. Esse sumário é o elemento central do prontuário nacional, sendo complementado por outros documentos clínicos e notas.[18] Tipicamente, esse sumário é criado pelo clínico geral do paciente, mas, no caso da Austrália, pode também ser criado por um enfermeiro registrado ou por um agente de saúde aborígene, segundo *Pearce* e *Bainbridge*[19] e *Hemsley* et al.[20]. Os documentos clínicos complementares incluem sumários de altas, sumários de eventos, cartas de referências (encaminhamentos a especialistas) e cartas de especialistas, emitidas após suas

consultas.[19] Os pacientes podem complementar as informações em seus prontuários com notas pessoais de saúde, informação sobre a existência e, se existir, a localização de diretivas de cuidados antecipados, e detalhes de contatos de emergência[19]. As notas de pacientes tipicamente contêm informações sobre alergias, reações adversas e medicamentos correntes.[16]

Outra prática institucional relacionada à privacidade diz respeito ao modo e estratégias utilizadas pelas empresas para armazenar os dados coletados. Nesse quesito, MyHR adota um modelo de repositórios distribuídos. Segundo Nohr et al.,[16] a infraestrutura central de MyHR gerencia a localização e transferência de dados do sistema distribuído, com vários repositórios estabelecidos para coletar e armazenar os dados clínicos. Embora existam diversos repositórios estabelecidos pelo sistema nacional para manter os documentos clínicos, outras organizações podem definir e utilizar seus próprios repositórios, como foi o caso do sistema australiano de Medicare.[19] *Mendelson* e *Wolf*[21] alertam que o órgão governamental responsável por manter essa infraestrutura, a *Australian Digital Health Agency*, terceirizou diversas de suas funções para companhias privadas, o que gerou desconfianças sobre possíveis usos da informação para outros fins que não a assistência em saúde. Sobre esse modelo distribuído e descentralizado, Hanna et al.[22] alertam que é essencial que o sistema armazene toda a informação relevante sobre a saúde do paciente, sob o risco, caso contrário, de ser mais um local a ser consultado durante a assistência, agravando ainda mais a fragmentação já existente dessa informação.

A prática institucional da transparência diz respeito a permitir que os usuários saibam quais dados estão armazenados e para que fins serão utilizados. Segundo *Essén* et al.[3] na Austrália, como em muitos outros países, todos os cidadãos têm por lei o direito de conhecer quais dados clínicos sobre si estão armazenados em qualquer sistema, embora em alguns países o acesso à informação não seja simples. No caso da Austrália, o cidadão tem pleno acesso aos dados de sua saúde que estão armazenados no sistema MyHR.[16] A maior parte dos pacientes acredita que esse acesso permite que eles verifiquem se há erros em seus registros de sua saúde, além de melhorar o conhecimento sobre a própria saúde e o relacionamento com seus provedores de saúde.[23] Outro mecanismo de transparência disponível é o registro de acessos (*log*), que os usuários podem acessar por meio do portal do paciente.[16] Assim, cada usuário pode saber quando seus registros de saúde foram acessados e de onde ocorreu esse acesso. No entanto, esse acesso não é registrado por indivíduo, mas apenas em nível de qual organização

ele ocorreu,[16] embora legalmente o paciente possa solicitar às organizações o registro de quais indivíduos fizeram os acessos.[19]

A prática institucional de oferecer aos usuários controle sobre os seus dados armazenados pela organização é uma maneira de aumentar a sensação de autonomia e torná-los mais cooperativos na disponibilização de dados.[10] Nesse sentido, o sistema MyHR oferece amplo controle aos pacientes, uma vez que, à exceção do Sumário de Saúde Compartilhado, qualquer usuário pode limitar quais documentos adicionais serão incluídos e quem poderá ter acesso a eles.[24] *Bidargaddi* et al.[25] confirmam que alguns registros, como os registros de saúde da prática geral, exigem ações do clínico geral e do paciente antes de serem carregados ao sistema. Embora a iniciativa de solicitar que um documento não seja incluído caiba ao paciente, espera-se que os profissionais de saúde usem o bom senso e solicitem permissão dos pacientes antes de adicionar informação sensível, como no caso de doenças sexualmente transmissíveis.[19] Em fato, um estudo quantitativo por *Lehnbom*, *Brien* e *McLachlan*[26] revelou que um quarto dos usuários exerceriam essa possibilidade de não incluir informações sensíveis em seu prontuário. Por outro lado, em relação aos documentos já carregados no sistema, por se tratar de um prontuário, nenhum registro pode ser removido do sistema. Segundo *Nohr* et al.,[16] não é possível remover documentos, mas apenas restringir o acesso a eles; o acesso pode ser liberado posteriormente, se o paciente assim o desejar.

O usuário exerce esse controle de acesso a documentos por meio do portal do paciente, onde há opções para definir as restrições de acesso ao próprio registro.[19] A maioria dos provedores de serviço de saúde estão de acordo com esse modelo de controle de acesso.[27] Por padrão, qualquer profissional da saúde em atendimento a um paciente, ciente de seu identificador, pode ter acesso aos documentos no prontuário; como medida de segurança adicional, o paciente pode definir um código de acesso adicional de restrição de acesso.[19] No entanto, em caso de emergência, o prestador de serviço pode sobrepassar o controle de acesso.[19] Segundo *Kerai*, *Wood* e *Martin*,[23] a quase totalidade dos pacientes dispõem-se a abrir totalmente o acesso a seus clínicos gerais.

O último aspecto relacionado às práticas institucionais de privacidade é qual o uso que é feito dos dados coletados e armazenados. No caso de MyHR, os dados devem em princípio ser usados exclusivamente para fins assistenciais e terapêuticos, em benefício dos pacientes. Em situações normais, os dados são acessados por meio dos portais de pacientes e de provedores de serviços de saúde;[19] aplicativos de software de terceiros devem se conectar ao sistema por

meio do portal de provedores.[25] No entanto, existe a possibilidade de usos não-terapêuticos dos dados. Por exemplo, a legislação referente a MyHR requer que o operador do sistema esteja preparado para fornecer dados anonimizados.[21] Similarmente, há previsão para o uso de dados de MyHR podendo ser usados em cortes e tribunais.[21] Esse uso secundário dos dados levanta diversas questões éticas e legais, e grupos não-governamentais ligados a questões de privacidade têm questionado, desde a implantação do sistema, essa possibilidade.[28]

Percepções ou atitudes relacionadas à privacidade

As percepções ou atitudes de consumidores em relação à privacidade frequentemente atuam como mediadores entre as práticas institucionais de privacidade e o comportamento dos usuários.[10] Incluem-se nessa dimensão do arcabouço conceitual as preocupações dos consumidores em respeito à privacidade e o cálculo de privacidade.

Em relação às preocupações com a privacidade, a confiança no sistema MyHR não é incondicional. Andrews, Gajanayake e Sahama[29] detectaram, em seus estudos, que os usuários apresentaram preocupação moderada sobre a segurança oferecida pelo sistema MyHR e a garantia de que seus dados permaneceriam confidenciais. Similarmente, *Kerai*, *Wood* e *Martin*[23] observaram que o receio do acesso por pessoal não autorizado, como agências governamentais, companhias de seguro e companhias farmacêuticas, é causa de preocupação por parte dos usuários. No entanto, aparentemente essa preocupação não tem como causa primária o sistema nacional de prontuário eletrônico, pois são manifestações similares àquelas que os pacientes sentem em relação ao sistema tradicional em papel. Estudo de *Lehnbom*, *Brien* e *McLachlan*[26] em 2014 revelou que 46 % dos participantes acreditavam que o risco de furto de dados seria maior com os prontuários eletrônicos do que com prontuários em papel; já em 2016, estudo similar realizado por *Carroll* e *Butler-Henderson*[27] revelou que essa proporção era de 40 %, enquanto 30 % dos participantes acreditavam que esse risco seria maior com os prontuários em papel. As preocupações usuais dos usuários em relação a seus registros incluem a sua visão por pessoal não autorizado, o roubo intencional de identidade e o uso inapropriado dos dados por companhias de seguro e empregadores.[26] Apesar das preocupações dos usuários sobre a privacidade e a segurança dos dados, há confiança suficiente confiança da população no governo de que o sistema MyHR será seguro.[30]

Em relação aos aspectos ligados ao cálculo da privacidade, o consenso é de que não houve ainda tempo hábil de uso do sistema para que seus participantes, sejam pacientes ou profissionais de saúde, possam avaliar os benefícios advindos do compartilhamento dessas informações de saúde. Srur e Drew[28] apontam que os envolvidos estão identificando riscos potenciais e avaliando a satisfação e confiança no sistema, e que os benefícios efetivos só serão mensuráveis no futuro. Andrews, Gajanayake e Sahama[29] ressaltam que não há preditores fortes que permitam avaliar quão útil será o sistema ou quão fácil será utilizá-lo, fatores essenciais para encorajar o seu uso. *Carroll* e *Butler-Henderson*[27] levantam, em seu estudo, um interessante aspecto nesse dilema: enquanto 66 % dos participantes acham que o profissional da saúde pode prestar melhor assistência com acesso ao sistema MyHR, menos da metade deles acham que um prestador de serviço precisaria desse acesso. Como ressaltam Garrety et al.[24] será imperativo que os usuários entendam que, com o direito de controlar o acesso aos seus documentos no sistema MyHR, vem a responsabilidade de que a informação incompleta possa prejudicar sua assistência. Assim, será preciso esperar mais tempo com o sistema em plena adoção para que esses benefícios possam ser contrapostos ao que se perdeu de privacidade na utilização do sistema.

Intenções ou comportamento de usuários em relação à privacidade

A dimensão de intenções ou comportamento de usuários em relação às práticas de privacidade incluem a liberação de acesso à informação, aceitação ou adoção de inovações direcionadas por dados e as transações ou interações com o sistema.

Em avaliações preliminares sobre a intenção de liberar o acesso aos dados em MyHR, a maioria dos pacientes acredita que dará acesso completo aos dados ao seu clínico geral: em estudo de *Kerai*, *Wood* e *Martin*,[23] 95 % dos respondentes responderam que abririam totalmente seus registros ao seu médico pessoal. Similarmente, em estudo de van *Kasteren* et al.,[30] 97 % dos pacientes abririam seus registros aos seus clínicos gerais e 91 % com seus especialistas, mas apenas 66 % fariam isso com qualquer provedor de assistência. Números similares foram obtidos em estudo de *Lehnbom*, *Brien* e *McLachlan*,[26] segundo o qual 56 % dos pacientes respondentes abririam o acesso de seus registros a qualquer provedor de saúde envolvido em sua assistência; entre os restantes, 97 % o fariam com seu clínico geral, 91 % com especialistas, 49 % para os farmacêuticos e 38 % com os dentistas. *Carroll* e *Butler-Henderson*,[27] por outro lado, levantaram que 48 % dos pacientes concordavam ou fortemente

concordavam que um provedor de assistência deveria ter acesso completo aos registros do MyHR, embora ninguém discordasse totalmente dessa afirmação. Mesmo entre pacientes de grupos mais vulneráveis, como aqueles infectados com HIV, conforme estudo de *Parsons* e *Ryder*,[31] a maioria dos pacientes concorda que seus registros sejam incluídos no sistema, com a sensação de que o compartilhamento dessa informação promoverá uma assistência mais abrangente.

No que se refere à aceitação ou adoção de inovações, de modo geral, as pessoas envolvidas tendem a aceitar bem a proposta de um sistema nacional de prontuário eletrônico, antevendo melhor assistência em saúde e maior controle sobre a própria saúde.[22] O estudo de *Kerai*, *Wood* e *Martin*[23] com pacientes idosos mostrou que 85 % dos entrevistados achavam que ter um sistema nacional era uma boa ideia. No entanto, no início da implantação do sistema, a adoção foi lenta, com menos de 3 % de adesão da população ao final do primeiro ano do sistema.[18] Fatores que podem influenciar negativamente na ampla adoção do sistema são a falta de informação à população sobre mecanismos de proteção e os riscos à privacidade[20] e se o sistema não atender adequadamente às necessidades de saúde da população.[29]

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 que estão lá registradas, o que envolve o conceito da literacia em saúde.[22] Autores como *Walsh* et al.[32] questionam o quanto desse acesso pode efetivamente ser compreendido pelos pacientes, seja por questões de usabilidade do sistema seja pelas limitações impostas pela capacidade de compreensão da informação lá registrada, aspectos que podem ser agravados pelas condições de saúde do paciente.[20] Essa compreensão sobre a informação de sua própria saúde pode ter consequências também na decisão de liberar ou restringir o seu acesso a profissionais da assistência em saúde. Já sob o ponto de vista dos profissionais de saúde, existe o receio de que esse acesso pelos pacientes possa levar a confusões e preocupações desnecessárias, levando consequentemente a um aumento de carga de trabalho para esclarecer essas dúvidas e tranquilizar seus clientes.[23] A solução para esse problema, segundo estudo de *Pearce* e *Bainbridge*,[19] é desenvolver mecanismos para apresentar a informação de modo que possa ser facilmente compreendida pelos pacientes. Pacientes acreditam que, com acesso aos seus próprios registros de saúde, poderão compreender melhor suas questões de saúde e preparar-se melhor para as consultas com profissionais.[23]

Este estudo avaliou a experiência do desenvolvimento e implantação do sistema nacional de prontuários da Austrália segundo o arcabouço de privacidade informacional de *Beke, Eggers* e *Verhoef.*[10] A utilização de um arcabouço conceitual de privacidade permitiu avaliar, por meio das manifestações relacionadas à privacidade registradas em artigos científicos, os diversos aspectos envolvidos na iniciativa de implantação desse sistema. Como se pode observar na tabela, até então nenhum trabalho publicado contemplou todos os aspectos da privacidade considerados nesse arcabouço. Efetivamente, diversos desses artigos não tinham como foco questões relacionadas à privacidade, mas mencionavam alguns desses aspectos como parte de seus estudos.

Claramente, este estudo tem limitações. A primeira é que artigos publicados após a data de realização do levantamento não foram incluídos na análise. A segunda é que, por ser um estudo de caso, com foco em um único país, e por adotar uma abordagem exploratória e qualitativa para a análise, os resultados apresentados não podem ser generalizados. Outra limitação é que a adoção de um arcabouço conceitual de privacidade informacional, apesar de ajudar a direcionar a análise das questões de privacidade, deixa de abordar outros aspectos que podem ser relevantes nessa discussão, como as controvérsias éticas envolvidas na propriedade da informação clínica sobre um paciente. Mesmo assim, são estabelecidos parâmetros que podem ser utilizados em futuros estudos, sejam esses exploratórios de sistemas em outros países, comparativos entre sistemas de diferentes países ou de aprofundamento de questões específicas referentes à privacidade de sistemas compartilhados de prontuários eletrônicos.

Por outro lado, o estudo permite derivar algumas conclusões e diretrizes. A experiência australiana mostra que a implantação de um sistema nacional de prontuário eletrônico, seja controlado ou seja fiscalizado pelo governo, deixa sempre muitos aspectos relacionados à privacidade em aberto ou indefinidas, e tal indefinição pode ser elemento crucial impeditivo da aceitação do sistema pela população. É preciso que haja um posicionamento explícito e claro, por parte de um governo que pretenda implantar iniciativa semelhante, sobre a garantia da confidencialidade dos dados e sobre quais são os usos secundários que poderão ser feitos dessa informação. Incertezas em relação a esses aspectos pode comprometer o sucesso da iniciativa, apesar dos potenciais benefícios reconhecidos por todos os usuários (pacientes e familiares) e provedores de serviços de assistência à saúde.

Ter um sistema de prontuário eletrônico controlado pelo paciente, em nível nacional, além do potencial benefício à assistência prestada aos pacientes, pode ainda ser um instrumento efetivo de empoderamento do cidadão, que passa a ter o conhecimento e o controle dos registros de informação sobre sua saúde e a possibilidade de complementá-los pessoalmente. Para que tal empoderamento seja efetivo, entretanto, é essencial que as condições de literacia em saúde da população como um todo sejam ampliadas. Assim como muitas outras iniciativas, para alcançar o pleno potencial de um sistema nacional de prontuário eletrônico controlado pelo paciente, é necessário investir na educação da população. Apenas desse modo será possível garantir que o cidadão tenha a clara compreensão do que significam os dados registrados em seus prontuários, o valor de suas anotações pessoais complementares e o impacto das restrições de acesso a parte de seus documentos de saúde.

Referências bibliográficas

1. Galvao MCB, Ricarte ILM. Prontuário do Paciente. Rio de Janeiro: Guanabara-Koogan; 2012. p. 322.

2. Tharmalingam S, Hagens S, Zelmer J. The value of connected health information: Perceptions of electronic health record users in Canada. BMC Med Inform Decis Mak [Internet]. 2016 [access: 2020/08/15];16(1):1–9. Available from: http://dx.doi.org/10.1186/s12911-016-0330-3

3. Essén A, Scandurra I, Gerrits R, Humphrey G, Johansen MA, Kiergegaard P, et al. Patient access to electronic health records: Differences across ten countries. Heal Policy Technol [Internet]. 2018 [access: 2020/08/15];7(1):44–56. Available from: http://dx.doi.org/10.1016/j.hlpt.2017.11.003

4. Fragidis LL, Chatzoglou PD. Implementation of a nationwide electronic health record (EHR): The international experience in 13 countries. Int J Health Care Qual Assur. 2018;31(2):116–30.

5. Solove DJ. Conceptualizing privacy. Calif Law Rev. 2002;90(4):1087–155.

6. Warren S, Brandeis LD. The Right to Privacy. Harv Law Rev. 1890;4(5):1–22.

7. Kokolakis S. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Comput Secur [Internet]. 2017 [access: 2020/08/15];64:122–34. Available from: http://dx.doi.org/10.1016/j.cose.2015.07.002

8. Lee D. Facebook sued by top prosecutor over Cambridge Analytica. BBC News [Internet]. 2018 [acceso: 26/03/2020]; Available from: https://www.bbc.com/news/technology-46627133

9. O'Sullivan D. Facebook reveals bug exposed 6.8 million users' photos. CNN International Edition [Internet]. 2018 [access: 2020/08/15]; Available from: https://edition.cnn.com/2018/12/14/tech/facebook-private-photos-exposed-bug/index.html

10. Beke FT, Eggers F, Verhoef PC. Consumer Informational Privacy: Current Knowledge and Research Directions. Found Trends® Mark [Internet]. 2018 [access: 2020/08/15];11(1):1–71. Available from: http://www.nowpublishers.com/article/Details/MKT-057

11. Gritzalis S, Lambrinoudakis C, Lekkas D, Deftereos S. Technical guidelines for enhancing privacy and data protection in modern electronic medical environments. IEEE Trans Inf Technol Biomed [Internet]. 2005 [access: 2020/08/15];(3):413–23. Available from: http://www.ncbi.nlm.nih.gov/pubmed/16167696

12. Yüksel B, Küpçü A, Özkasap Ö. Research issues for privacy and security of electronic health services. Futur Gener Comput Syst [Internet]. 2017 [access: 2020/08/15];68:1–13. Available from: http://dx.doi.org/10.1016/j.future.2016.08.011

13. Australian Government. Australian Digital Health Agency. My Health Record [Internet]. 2018 [access: 2020/08/15]. Available from: https://www.myhealthrecord.gov.au/

14. Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. Inf Syst Res. 2006;17(1):61–80.

15. Wohlin C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. Proc 18th Int Conf Eval Assess Softw Eng - EASE '14 [Internet]. 2014 [access: 2018/09/17]:1–10. Available from: http://dl.acm.org/citation.cfm?doid=2601248.2601268

16. Nøhr C, Parv L, Kink P, Cummings E, Almond H, Nørgaard JR, et al. Nationwide citizen access to their health data: Analysing and comparing experiences in Denmark, Estonia and Australia. BMC Health Serv Res. 2017;17(1):1–11.

17. Bidargaddi N, Kidd MR. Learning from development of a third-party patient-oriented application using Australia's national personal health records system [Internet]. 2017 [access: 2018/09/17]. Available from: https://arxiv.org/abs/1709.03577

18. Garrety K, McLoughlin I, Dalley A, Wilson R, Yu P. National electronic health record systems as "wicked projects": The Australian experience. Inf Polity. 2016;21(4):367–81.

19. Pearce C, Bainbridge M. A personally controlled electronic health record for Australia. J Am Med Informatics Assoc. 2014;21(4):707–13.

20. Hemsley B, McCarthy S, Adams N, Georgiou A, Hill S, Balandin S. Legal, ethical, and rights issues in the adoption and use of the "My Health Record" by people with communication disability in Australia. J Intellect Dev Disabil [Internet]. 2017 [access: 2018/09/17]:1–9. Available from: http://www.tandfonline.com/doi abs/10.3109/13668250.2017.1294249

21. Mendelson D, Wolf G. "My [Electronic] Health Record" – Cui Bono (for Whose Benefit)? J Law Med [Internet]. 2016 [access: 2018/09/17];24(2):283–96. Available from: https://ssrn.com/abstract=2881787

22. Hanna L, Gill SD, Newstead L, Hawkins M, Osborne RH. Patient perspectives on a personally controlled electronic health record used in regional Australia: 'I can be like my own doctor.' Heal Inf Manag J. 2017;46(1):42–8.

23. Kerai P, Wood P, Martin M. A pilot study on the views of elderly regional Australians of personally controlled electronic health records. Int J Med Inform [Internet]. 2014 [access: 2018/09/17];83(3):201–9. Available from: http://dx.doi.org/10.1016/j.ijmedinf.2013.12.001

24. Garrety K, McLoughlin I, Wilson R, Zelle G, Martin M. National electronic health records and the digital disruption of moral orders. Soc Sci Med [Internet]. 2014;101:70–7. Available from: http://dx.doi.org/10.1016/j.socscimed.2013.11.029

25. Bidargaddi N, Van Kasteren Y, Musiat P, Kidd MR. Developing a third-party analytics application using Australia's national personal health records system: Case study. J Med Internet Res. 2018;20(4):5.

26. Lehnbom EC, Brien JE, McLachlan AJ. Knowledge and attitudes regarding the personally controlled electronic health record: An Australian national survey. Intern Med J. 2014;44(4):406–9.

27. Carroll J, Butler-Henderson K. MyHealthRecord in Australian Primary Health Care: An Attitudinal Evaluation Study. J Med Syst. 2017;41(10):5.

28. Srur BL, Drew S. Challenges in designing a successful e-health system for Australia. In: 2012 International Symposium on Information Technologies in Medicine and Education [Internet]. Hokodate, Japan: Institute of Electrical and Electronics Engineers; 2012 [access: 2018/09/17]. p. 480–4. Available from: http://ieeexplore.ieee.org/document/6291347/

29. Andrews L, Gajanayake R, Sahama T. The Australian general public's perceptions of having a personally controlled electronic health record (PCEHR). Int J Med Inform [Internet]. 2014 [access: 2018/09/17];83(12):889–900. Available from: http://dx.doi.org/10.1016/j.ijmedinf.2014.08.002

30. van Kasteren Y, Maeder A, Williams PA, Damarell R. Consumer perspectives on My Health Record: A review. Stud Health Technol Inform. 2017;239:146–52.

31. Parsons BF, Ryder N. High uptake of shared electronic health records among HIV-infected patients at an Australian sexual health clinic. Sex Health. 2016;13(4):393–4.

32. Walsh L, Hemsley B, Allan M, Adams N, Balandin S, Georgiou A, et al. The E-health Literacy Demands of Australia's My Health Record: A Heuristic Evaluation of Usability. Perspect Heal Inf Manag [Internet]. 2017 [access: 2018/09/17];14(Fall):1–28. Available from: http://search.ebscohost.com/login.aspx?direct=true&db=cmedm&AN=29118683&site=ehost-live

Conflicto de intereses

El autor declara que no existe conflicto de intereses.