Como proteger informações do prontuário eletrônico do paciente: proposta de mecanismos

Odirlei Antonio Magnagnagno
Doutor em Administração pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS) – RS – Brasil. Encarregado do Setor de Tecnologia da Informação do Centro Universitário Assis Gurgacz (FAG) - Brasil. Professor do Centro de Ensino Superior de Cascavel - Dom Bosco, do Centro Universitário e do Instituto Assis Gurgacz – FAG - Cascavel, PR – Brasil.
http://lattes.cnpq.br/0950715470018900
E-mail: odirlei@fag.edu.br

Edimara Mezzomo Luciano
Pós-Doutorado pela London School of Economics and Political Science (LSE) - Grã-Bretanha. Doutora em Administração pela Universidade Federal do Rio Grande do Sul (UFRGS) - RS - Brasil. Professora e pesquisadora da Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS) - Porto Alegre, RS – Brasil.
http://lattes.cnpq.br/2607532326321244
E-mail: eluciano@pucrs.br

Rafael Mendes Lübeck
Pós-Doutorado pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS) – RS - Brasil.
Doutor em Administração pela Pontifícia Universidade Católica do Rio Grande do Sul (PUC-RS) - Brasil.
http://lattes.cnpq.br/5688248930763665
E-mail: rafael.lubeck@gmail.com

Data de submissão: 30/09/2019. Data de aceite: 03/04/2020. Data de publicação: 27/04/2021

RESUMO

O objetivo do artigo foi identificar mecanismos que possam contribuir para preservar a privacidade das informações do paciente contidas no prontuário eletrônico. A estratégia de pesquisa foi exploratória-descritiva, utilizando-se de Análise de Documentos e Estudo de Caso. Um conjunto de 20 documentos relativos a leis, manuais e normas foi analisado e dois estudos de caso foram conduzidos em hospitais, precedidos por um estudo de caso piloto. Os casos foram estudados por meio de entrevistas semiestruturadas, análise de documentos internos e observação. Em uma das etapas da pesquisa tem-se a identificação e análise de documentos regulatórios e normativos. E como resultado final, a identificação dos mecanismos que os hospitais pesquisados utilizam para a privacidade da informação. Os mecanismos mais utilizados são os de processos em relação à salvaguarda e os de relacionamento em relação à conscientização dos colaboradores. Como contribuição, o artigo mostra a necessidade do fortalecimento da discussão da temática para a academia, bem como uma relação de documentos e principalmente uma relação de mecanismos que podem contribuir para a proteção das informações na área da saúde.

Palavras-chave: Privacidade da informação. Prontuário eletrônico do paciente. Mecanismos de proteção da privacidade. Instituição de saúde. Segurança da informação.

How to protect information from the Patient's electronic medical record: proposed mechanisms

ABSTRACT

The purpose of this article is to identify mechanisms that may contribute to preserving the privacy of patient information contained in the electronic medical record. The research strategy is exploratory-descriptive, using Document Analysis and Case Study. A set of 20 documents, related to laws, manuals and standards, was analyzed and conducted case studies in two hospitals, preceded by a pilot case study. The cases were studied through semi-structured interviews, analysis of internal documents and occasional observation. In one of the stages of the research we have identification and analysis of regulatory and normative documents. And as a final result, the identification of the mechanisms that the hospitals surveyed use for information privacy. The most used mechanisms are those of processes in relation to the safeguard and those of relationship in relation to the awareness of the collaborators. As contribution, the article shows the need to strengthen the discussion of the theme for the academy. As well, a list of documents and mainly a list of mechanisms that can contribute to the protection of the information in the health area.

Keywords: *Information privacy. Electronic patient record. Privacy protection mechanisms. Health institution. Information security.*

Cómo proteger la información de la historia clínica electrónica dei paciente: mecanismos propuestos

RESUMEN

El objetivo del artículo fue identificar los mecanismos que pueden contribuir a preservar la privacidad de la información del paciente, contenida en la histo ria clínica electrónica. La estrategia de in vestigación fue exploratoria-descr iptiva, utilizando Análisis de Documentos y Estudio de Caso. Se analizó nn conjunto de 20 documen tos rela cionados con leyes, manuales y estándares , y se realizaron dos estudios de caso en hospitales, precedidos por un estudio de caso piloto. Los casos se estudiaron mediante entrevistas semiestructuradas, análisis de documentos internos y observación. En una de las etapas de investigación, existe la identificación y el análisis de documentos normativos y normativos. Y como resultado final, la identificación de los mecanismos que utilizan los hospitales investigados para la privacidad de la información. Los mecanismos más utilizados son los relacionados con los procesos de protección y los relacionados con la conciencia de los empleados. Como contribución, el artículo muestra la necesidad de fortalecer la discusión del tema para la academia. Además, una lista de documentos y principalmente una lista de mecanismos que pueden contribuir a la protección de la información en el área de la salud.

Palabras clave: *Privacidad de la información. Mecanismos electrónicos de registro depacientes para la protección de la privacidad. Institución de salud. Seguridad de la información.*

INTRODUÇÃO

As organizações têm se preocupado com a adoção de tecnologias da informação (TI), com a intenção de gerenciar seus dados e entregar melhores resultados aos seus *stakeholders*. A medida que aumenta a quantidade de informações coletadas, armazenadas e transmitidas, aumenta proporcionalmente A preocupação com a privacidade dos dados dos indivíduos (LEE *et al.,* 2019). Os hospitais públicos e privados, assim como clínicas e postos de saúde, são obrigados por lei a manter seguros os documentos que contenham os registros de informação do paciente (GOLDIM FRANCISCONI, 2005). Esse registro é realizando em um prontuário e, de acordo com a Resolução Nº 7, de 24 de novembro de 2016 do Ministério da Saúde, as informações relativas à atenção básica deverão ser realizadas por meio de prontuários eletrônicos do paciente (MS, 2016).

No ambiente hospitalar também há grande preocupação com a privacidade das informações, pois as informações relacionadas aos pacientes são de extrema intimidade, envolvendo aspectos a respeito da saúde do indivíduo. Porém, uma informação que deveria estar sendo protegida pode estar sendo utilizada sem que se saiba a finalidade, onde, como e por qual indivíduo ou organização. A proteção da informação do prontuário do paciente se torna mais importante, visto que as informações do paciente estão entre os tipos de informações passíveis de proteção devido a suas características (ACQUISTI GROSSKLAGS, 2007).

O prontuário eletrônico do paciente pode conter informações valiosas com dados de saúde da população (ARAUJO, PIRES e BANDIERA-PAIVA, 2014). Por isso, a privacidade, ou em outras palavras o sigilo das informações do prontuário dos pacientes, adquire importância ainda maior, porque trata-se de proteger as informações para análises de dados sobre a saúde da população (ALBUQUERQUE; JUNIOR; SANTOS). As informações coletadas nos prontuários podem indicar a proliferação de uma nova doença ou mesmo a disseminação de um vírus novo no país ou região (RABELO; BENTES PINTO, 2018; PAVÃO *et al.*, 2017).

Para minimizar o risco à violação da privacidade de um paciente, Francisconi e Goldim (1998) propõem que a equipe de saúde tenha como base a política de informações, sempre pensando quem necessita saber, o quê, para quê, e de quem são as informações. Portanto os riscos à violação da privacidade do paciente têm relação com o sigilo das informações do prontuário eletrônico. Torna-se importante, para manter essas informações sob sigilo, o comportamento dos profissionais que acessam essas informações constantemente. Esses indivíduos podem apresentar diferentes atitudes em relação às políticas e mecanismos de privacidade de um hospital, devido ao comportamento de cada sujeito ser por vezes desigual dentro de um mesmo grupo (LUCIANO *et al.*, 2011).

Os mecanismos, na visão de Guldentops *et al.* (2004), podem ser de estrutura, processos e relacionamento. Os mecanismos de estrutura têm a responsabilidade de criar regras e papéis, os mecanismos de processos têm a função de implementar os sistemas de tomada de decisão e também gerenciar as práticas e procedimentos voltados à estratégia de TI, mecanismo de relacionamento é entendimento dos objetivos entre negócio e TI.

Contudo, é difícil para os hospitais saberem exatamente como garantir a privacidade das informações de uma maneira ìntegra, pois o Brasil não conta com uma lei federal específica. A regulamentação tem se estabelecido por demandas e instâncias específicas. O setor de saúde conta com uma regulamentação ainda limitada, fragmentada e instável sobre o tema (VENTURA COELI, 2018). Um dos meios utilizados são as orientações de políticas de segurança e a criação de normas que orientem os colaboradores de uma instituição de saúde quanto à privacidade de informação. Os códigos de ética médica e de enfermagem são um exemplo de documentos normativos que tratam das questões legais e éticas da profissão.

O cumprimento das orientações, regulamentos e regras de segurança de informação por parte dos profissionais é o fator de fortalecimento da segurança da informação (BULGURCU *et al.*, 2010). Porém, se os profissionais não conseguirem entender algum item da política de segurança da informação ou fizerem juízo de valor e considerá-las não aplicáveis ao seu trabalho, podem não cumprir as determinações, tornando os esforços para criá-las frágeis ou mesmo inócuos (COSTA; PORTELA, 2018; DA VEIGA ELOFF, 2010). Trata-se de não apenas criar as normas, mas sim identificar e aplicar mecanismos efetivos para a segurança das informações do prontuário do paciente, o que nem sempre ocorre nas instituições de saúde (BULGURCU *et al.*, 2010 DA VEIGA ELOFF, 2010).

Este artigo dedica-se ao estudo da privacidade das informações, focando nas informações constantes no prontuário eletrônico dos pacientes em instituições de saúde. O objetivo deste estudo é identificar os mecanismos que podem contribuir para preservar a privacidade das informações registradas no prontuário eletrônico do paciente. Para tanto recorre a duas abordagens metodológicas, quais sejam: a análise de documentos regulatórios e normativos e o estudo de caso em duas instituições de saúde referência no país. Utilizando-se esse ferramental para a investigação pretendeu-se identificar estruturas, processos e relacionamentos do cotidiano dos hospitais que contribuem com a proteção das informações do prontuário dos pacientes.

REFERENCIAL TEÓRICO

O prontuário médico é um documento que tem a finalidade de registrar e armazenar as informações a respeito do tratamento, ou seja, os eventos clínicos que foram prestados aos pacientes. Além dessa finalidade, ele também é importante, pois serve como um meio de comunicação entre os profissionais, uma vez que fornece informações para o cuidado do paciente independentemente do meio em que está o documento, ou seja, em papel ou meio eletrônico (MASSAD *et al.,* 2003).

O prontuário eletrônico "é um meio físico, um repositório onde todas as informações de saúde, clínicas e administrativas, ao longo da vida de um indivíduo estão armazenadas" (MASSAD *et al.*, 2003, p. 6). Porém, segundo o mesmo autor, a migração do prontuário em papel para o eletrônico tem trazido diversas mudanças para os profissionais, clientes e gestores. Uma dessas mudanças é a maneira de armazenamento e consulta dessas informações, já que no meio eletrônico elas ficarão em base de dados, sendo acessadas através de uma interface de aplicação. Além das facilidades de armazenamento, as novas tecnologias da informação possibilitam que os dados sejam também processados, transmitidos e publicados, viabilizando as trocas eletrônicas de informações, muitas vezes do interesse do médico e do próprio paciente (ABRAHÃO, 2003), afetando exatamente a segurança e a privacidade dessas informações.

No cenário de informatização da área de saúde, o registro eletrônico é importante porque permite o armazenamento e o compartilhamento seguro das informações de um paciente (CAMPARA *et al.* 2013). No entanto, o uso indevido dessa ferramenta pode colocar a segurança da informação e a confiabilidade da informação do paciente em risco, caso a instituição de saúde não esteja preparada para lidar com a privacidade das informações dos pacientes (COSTA, 2003).

Antes de tratar sobre o que é a privacidade de informações, é preciso entender o que é o conceito geral de privacidade que, originalmente, deriva da palavra latina privo ou *privatus.* O significado dessas palavras remete a privar que diz respeito ao íntimo do indivíduo, relacionando ao estilo de vida, ao anonimato e ao sigilo (LEIKO-LILLPI *et al.*, 2001). A privacidade tem o seu conceito mostrado sobre dois aspectos, sendo que o primeiro foca no controle que a pessoa exerce sobre o acesso de outros a si mesmo, e o segundo define a privacidade como uma condição ou estado de intimidade (LOCH, 2003).

Grande parte da literatura disserta com base no primeiro aspecto. Cita-se por exemplo Faden e Beauchamp (1986), que descrevem a privacidade como um pedido positivo de uma pessoa a um *status* de dignidade pessoal ou a um tipo de liberdade que tem a escolha a respeito de informações ou acontecimentos pessoais que deseja revelar ou não e qual o momento para isso. Já para Alderman e Kennedy (1995), a privacidade é um direito de cada pessoa, e ela abrange desde a intimidade necessária para o pensamento crítico, permitindo que o indivíduo mantenha em segredo fatos sobre si mesmo, até a garantia de independência para formar a família de acordo com valores próprios, com direito de sentir-se em segurança no próprio lar. A privacidade é observada como o receio da pessoa em perder o controle do uso e a proliferação das informações pessoais, pois quanto menor é a privacidade, menor é o controle sobre a utilização das informações pessoais (ROSE, 2006).

A privacidade da informação é a reivindicação de pessoas, grupos ou instituições em determinar por si próprios em que momento, qual o meio e a quantidade de informações sobre si mesmos serão comunicadas aos outros (WESTIN, 1967). Anderson e Moore (2006) entendem que a privacidade pessoal está em constante desmoronamento com os avanços da TI, o que tem afetado o relacionamento tanto de pessoas como de profissionais. Isso ocorre devido ao grande crescimento dos riscos de quebra de privacidade, que pode acontecer de diversas formas, como por exemplo, a espionagem por meio eletrônico.

Com o avanço da tecnologia da informação, as informações estão tendo um valor cada vez maior, sendo consideradas uma mercadoria de troca, pois elas têm se destacado cada vez mais na vida pessoal e nas organizações (YANAGUIBASHI *et al*., 2017). Ao se tratar de privacidade dentro da TI, ela pode ser caracterizada como o risco de alimentar as empresas com informações das pessoas e os benefícios que isso gera ao indivíduo (BRAGANÇA *et al.,* 2010). Esse risco à privacidade da informação surge devido ao grande volume de dados gerados pela organização. Outro aspecto importante está relacionado à forma como as organizações atuam em relação à atitude de seus funcionários pelo cumprimento das políticas de segurança da informação. D'Arcy e Hovav (2009) explicam que programas de conscientização, monitoramento, conhecimento das políticas de segurança e a percepção de sanções formais diminuem a intenção de abusos na área de segurança da informação.

Um jeito de coibir abusos é deixar claro que o colaborador será severamente punido caso detectado, pois a severidade da punição e a certeza da detecção - do não cumprimento das normas de segurança da informação - são fatores significativos sobre as intenções de comportamento na área de segurança da informação. Entretanto a existência e a visibilidade de mecanismos de detecção provavelmente sejam mais importantes que a severidade da sanção imposta (HERATH RAO, 2009).

Já o estudo de Bulgurcu *et al*. (2010) concluiu que as crenças de caráter normativo têm maior efeito que a intenção de cumprimento, quando comparadas à severidade das sanções. Entende-se que os funcionários serão mais propensos a seguir as políticas de segurança se percebem que há uma probabilidade alta de serem pegos no ato da violação das políticas de segurança. Mecanismos de proteção são a maneira de se manter a informação sob sigilo, uma vez que a vida cotidiana está cada vez mais *on-line* e as informações dos indivíduos mais disponíveis para as organizações. Tal situação tem aumentado a preocupação com a privacidade de informações tanto para as pessoas, comunidade científica e organizações, incluídas as instituições de saúde (MARTORELL *et al*., 2016).

As instruções a respeito de segurança da informação podem estar contidas nas políticas de segurança, que têm a função de dar suporte, auxiliar no planejamento de implantação de sistemas, sobre como deve agir cada integrante da equipe de assistência médica e como será abordada a política de segurança.

Contudo, a decorrência da vulnerabilidade vem do funcionário que não segue a política de segurança da informação (BULGURCU *et al.,* 2010). A vulnerabilidade é a possibilidade de um incidente indesejado ocorrer caso não haja medidas para evitá-lo (VANCE *et al.,* 2012). Com isso, "cada organização deve estabelecer quais políticas serão utilizadas, tendo como base suas necessidades, requisitos legais, cultura interna e sistemas informatizados" (FERREIRA ARAÚJO, 2008, p. 34).

Todavia, mesmo com as políticas estabelecidas e com as boas práticas divulgadas para melhorar a segurança da informação de um hospital, se o usuário do sistema de informação não colaborar e não estiver consciente da necessidade de manter sigilosas as informações do prontuário do paciente, as chances de êxito se reduzem (BRAGANÇA *et al.*, 2010). A consciência em relação à informação segura é consequência do esforço das ações realizadas pelas organizações para qualificar a segurança da informação. Sensibilizar o usuário para o cumprimento e bom desempenho das políticas de segurança da informação é essencial para diminuir as ameaças à segurança da informação (SIPONEN, 2000).

As ameaças à segurança no setor da saúde compreendem: o uso não autorizado de recursos, alteração não autorizada de informações, divulgação não autorizada e a paralização do sistema de informação seja por ataques via internet, mau funcionamento dos equipamentos em decorrência de exclusão de arquivo ou de dados corrompidos, como também, a ausência de cópias de segurança e de um plano de recuperação de dados (WIN *et al*. 2006 MERCURI, 2004). Esse ataque ao sistema de informação e de rede pode ocorrer por meio de uma pessoa externa, que pode ser um ex-funcionário descontente, um paciente ou um *hacker*, com a intenção de simplesmente deixar o sistema inoperante ou ter acesso às informações de pacientes (APPARI JOHNSON, 2010).

Todos os participantes do processo de registro, armazenamento ou acesso à informação de um prontuário eletrônico tendem a saber o valor da informação e a importância de preservá-la. A informação é utilizada para a tomada de decisões na organização, podendo trazer prejuízos financeiros caso ocorra algum vazamento (LUCIANO KLEIN, 2014). Por isso, essa informação deve estar sempre protegida e controlada, não importando como est*á* sendo armazenada ou compartilhada.

A privacidade e a confidencialidade das informações têm grande impacto nas instituições de saúde, visto que o potencial risco de violação de um deles compromete o nível de confiança necessária nas relações sociais. Verificou-se que 72% da equipe de enfermagem havia utilizado indevidamente o sistema de informação para conhecer dados sobre pacientes que não estavam sob sua responsabilidade. Para grande parte dos respondente, a motivação do acesso havia sido a mera curiosidade (CURRAN CURRAN, 1991).

Outra maneira de quebra de privacidade ou confidencialidade são os comentários a respeito das informações dos pacientes, por profissionais de saúde, em qualquer ambiente hospitalar, de modo inapropriado, tais como elevadores, refeitórios e corredores. Nesses locais, pode haver pessoas estranhas e que não estejam ligadas ao atendimento do paciente que ouçam a conversa, obtendo assim informações inapropriadas a respeito da saúde e tratamento do paciente (GOLDIM FRANCISCONI, 2004 MONTENEGRO *et al.*, 2016).

Com a intenção de evitar esse tipo de situação, os profissionais de saúde possuem documentos regulatórios para tratar de aspectos éticos nas práticas profissionais. A criação desses documentos tem a finalidade de orientar, a partir de diretrizes, a atuação do profissional. Uma delas é o sigilo, sobre o qual Massad *et al.* (2003) indicam que o profissional de saúde é responsável pela integridade e pela guarda da informação na qual tem acesso ao registrar, manipular, digitar, armazenar ou processar as informações do paciente.

O vazamento de informações e a invasão da privacidade dos pacientes é uma questão de ética, que deve ser tratada com mais seriedade pelos profissionais da saúde, pois a ética é a ciência da moral e refere-se ao comportamento do indivíduo (PUPULIM SAWADA, 2002).

No entanto, o Brasil ainda precisa percorrer um longo caminho tanto no que diz respeito à coleta e armazenagem dessas informações quanto ao sigilo delas (LOTT; CIANCONI, 2018). Torna-se importante criar uma cultura na organização voltada à não divulgação das informações do paciente em situações nas quais disseminar essas informações não contribuam para a saúde do paciente ou para análises gerenciais. Além disso, o processamento dessas informações também carece de qualificação dos profissionais da saúde para o devido uso dos dados para que gerem informações efetivas para os órgãos gestores (GONÇALEZ; SANTANA; JORENTE; 2015).

PROCEDIMENTOS METODOLÓGICOS

A pesquisa foi realizada por meio de uma abordagem exploratória-descritiva com dados qualitativos. O estudo de caso múltiplo foi usado como estratégia de pesquisa. As técnicas de coleta de dados foram a análise de documentos, entrevistas e observações. A primeira técnica utilizada foi a Análise de Documentos Regulatórios e Normativos, que ocorreu pela análise de 17 referências bibliográficas pertinentes ao assunto da pesquisa. Por meio delas, foi possível identificar 20 documentos reguladores que poderiam ter algum mecanismo de proteção de privacidade da informação.

A segunda abordagem metodológica utilizada foi o Estudo de Caso. A realização dos Estudos de Caso teve importância para os propósitos deste estudo, devido a tornar possível identificar processos formais ou informais do cotidiano dos hospitais. Nos Estudos de Caso, utilizaram-se entrevistas, análise de documentos internos e também observação.

Os Estudos de Caso foram realizados em dois grandes hospitais, um no Rio Grande do Sul e outro de São Paulo, ambos considerados hospitais de referência na utilização inovadora e intensiva de TI. A pedido dos hospitais, eles não serão nominados, mas identificados nesta pesquisa sob os codinomes de Hospital Gama e Hospital Beta, respectivamente. O Hospital Gama é público e um dos maiores do país, possuindo mais de 800 leitos, e no decorrer dos anos de 2017/2018 teve mais de 32 mil internações, cerca de 580 mil consultas, e mais de três milhões e cem mil exames, contando com aproximadamente 6 mil colaboradores. O Hospital Beta é particular e foi criado há mais de 94 anos, é referência nacional em diversas especialidades médicas, sendo considerado um dos mais importantes centros médicos do Brasil e da América Latina. Possui aproximadamente 460 leitos, cerca de 5 mil colaboradores e atende mais de 120 mil pacientes por ano, é considerado pioneiro na incorporação de novas tecnologias.

Para a realização dos Estudos de Caso, primeiramente foi aplicada uma entrevista semiestruturada, realizada com pessoas que possuem contato com a informação do paciente no prontuário eletrônico. A amostra foi de quatro pessoas no hospital Gama e cinco pessoas no Hospital Beta. Dentre essas pessoas estavam o gerente responsável pela área de TI ou de segurança da informação, pessoas que trabalham com a interface TI/usuário final e pessoas que contribuem para a formação das políticas de segurança da informação.

Ao término das entrevistas foi realizada análise de documentos internos, tais como regulamentos internos, práticas de privacidade de informações, sites e boas práticas. A terceira técnica utilizada foi a observação, realizada durante as visitas aos hospitais para as entrevistas e coleta de documentos, consultas ao site da instituição e conversas informais com colaboradores e clientes/pacientes. As características de cada entrevistado constam no quadro 1. A sigla EB se refere aos respondentes do Hospital Beta, e EG aos respondentes do Hospital Gama.

Quadro 1 − Dados dos respondentes dos casos estudados

Código	Gênero	Idade	Cargo	Experiência profissional/ Anos de empresa
EB1	F	41	Administrador de projetos na área de inovação	21/6
EB2	M	37	Gerente de infraestrutura	18/1
EB3	M	29	Analista de negócios	11/11
EB4	M	31	Administrador de projetos	10/8
EB5	M	36	Analista de suporte técnico pleno	18/7
EG1	M	38	Coordenador de TI	10/10
EG2	F	43	Chefe do setor de Segurança da Informação	17/15
EG3	F	49	Chefe do Setor de Sistemas Assistenciais	23/23
EG4	M	25	Analista de TI	5/5

Fonte: Dados da pesquisa.

Os estudos de caso foram precedidos de um caso piloto, objetivando validar o roteiro de entrevistas e identificar quais documentos poderiam ser coletados. A aplicação do teste piloto é importante, uma vez que é possível verificar problemas e dúvidas que não foram detectadas durante a elaboração do instrumento de coleta de dados (CHAGAS, 2000).

O caso piloto foi realizado com quatro colaboradores de um hospital de médio porte no Estado do Paraná. A média de tempo por entrevista do caso piloto foi de 20 minutos, aproximadamente. Além de garantir que as perguntas e observações realizadas fossem objetivas no sentido de medir as variáveis que se pretendia, o intuito do teste, conforme observa Gil (2002), foi desenvolver as habilidades e processos de aplicação. Após a utilização do roteiro para o caso piloto, verificou-se a necessidade de adequações, como a identificação das perguntas com numeração, assim como adequações de semânticas. Essas alterações foram realizadas, melhorando assim os instrumentos de coleta de dados para a aplicação nos demais Estudos de caso.

Para a análise dos dados foi utilizada a Análise de Conteúdo, seguindo especialmente as recomendações de Bardin (1977), pela qual primeiramente foram agrupados os dados transcritos das entrevistas para facilitar e melhorar os recursos durante a análise. Após a seleção dos documentos regulatórios e normativos, foi realizada uma análise de todos eles na íntegra, buscando identificar os possíveis mecanismos de proteção da privacidade. Após a análise de cada estudo de caso, foram unificados os mecanismos, gerando uma só informação. O quadro 2 apresenta um resumo de cada uma das abordagens metodológicas utilizadas e os objetivos de cada uma delas, juntamente com as suas técnicas de coleta de dados.

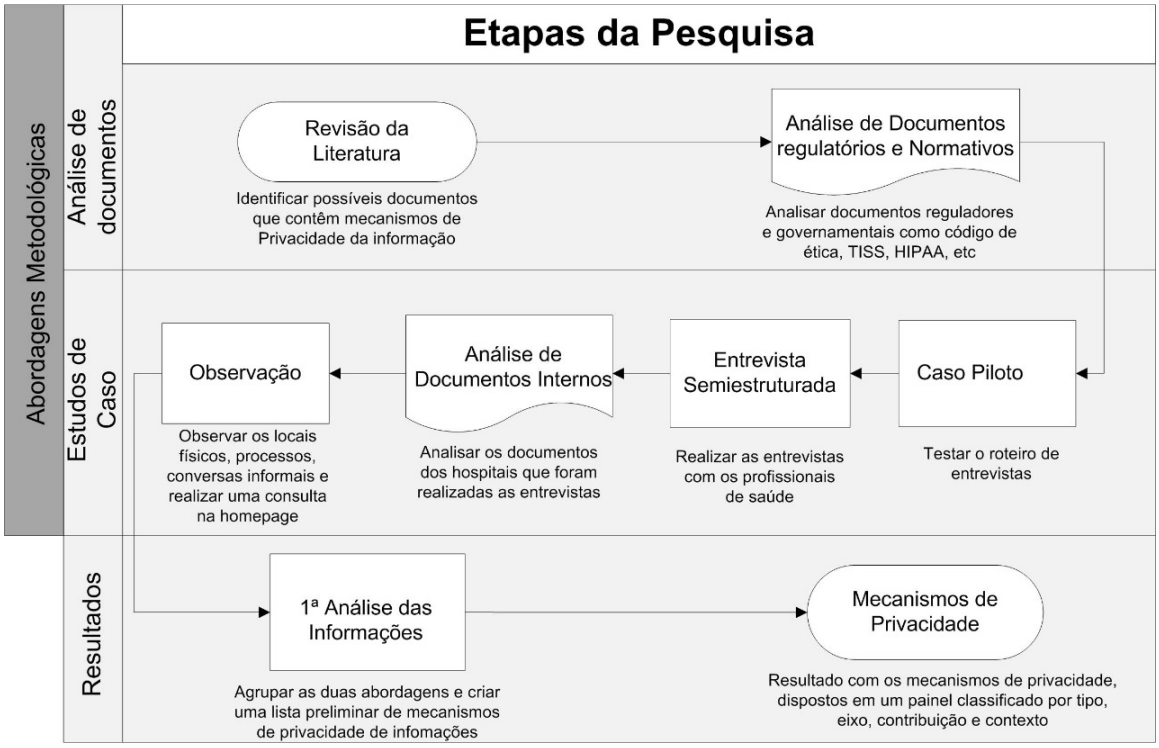
Para a validade do resultado e, principalmente, para se evitar a arbitrariedade, foi requisitado o auxílio de dois *experts*, um deles em segurança da informação e o outro em mecanismos, para realizar a classificação de cada um dos mecanismos conforme o seu tipo e também dentro do seu eixo de ação. A figura 1 apresenta um resumo de todas as etapas realizadas no estudo.

Quadro 2 – Abordagem metodológica *versus* objetivos *versus* técnicas de coleta de dados

Abordagem Metodológica	Objetivos	Técnica de coleta de dados/Objetivo
Estudo de Caso	Identificar e classificar as práticas de privacidade das informações dos casos estudados	Entrevista semiestruturada, análise de documentos internos e observações, visando verificar como é o processo utilizado para proteger a informação
Análise de Documentos Regulatórios e Normativos	Identificar os documentos regulatórios e normativos que possam conter mecanismos de privacidade das informações	Verificar documentos regulatórios e normativos, com o objetivo de encontrar informações a respeito de práticas, sugestões e recomendações de privacidade da informação
Estudo de Caso + Análise de Documentos Regulatórios e Normativos	Classificar os mecanismos identificados nos documentos Regulatórios e Normativos e os mecanismos encontrados nos Estudos de Caso	Comparar e analisar os mecanismos encontrados em cada abordagem, classificando por tipo mecanismo (estrutura, processo ou relacionamento)
Estudo de Caso + Análise de Documentos Regulatórios e Normativos	Identificar os mecanismos que podem contribuir para preservar a privacidade das informações registradas no prontuário eletrônico do paciente	Agrupamento de todos os mecanismos identificados, qualificando por contexto e contribuição

Fonte: Os autores.

Figura 1 – Desenho de pesquisa



Fonte: Os autores.

Após a descrição dos procedimentos metodológicos, na próxima seção foram elencados os resultados do estudo, procedidos das discussões teórico-empíricas e considerações finais.

RESULTADOS

A Análise de Documentos iniciou pela identificação de quais documentos poderiam ser fonte de mecanismos de preservação da privacidade. A identificação destes documentos foi feita a partir de análise bibliográfica, bem como análise dos sites das associações de Medicina e Enfermagem nacionais e internacionais. O quadro 3 mostra os documentos que foram analisados.

Quadro 3 − Documentos Analisados

Código	Tipo de Documento
DE1	Norma ABNT NBR ISO/IEC 27001
DE2	TISS - Troca de Informação em Saúde Suplementar
DE3	Resolução CFM Nº 1.821
DE4	Código de Ética Médica – Brasil
DE5	Código de Ética dos Profissionais de Enfermagem
DE6	Constituição Federal
DE7	Código Civil (lei 10.406)
DE8	Código de Defesa do Consumidor (lei 8.078)
DE9	Código Penal (lei nº 2.848)
DE10	Código de Ética da IMIA para Profissionais de Informática em Saúde
DE11	Lei de Acesso à informação (lei nº 12.527)
DE12	Política Nacional de Informação e Informática em Saúde (PNIIS)
DE13	HIPAA - Health Insurance Portability and Accountability Act
DE14	ISO / TC 215
DE15	NBR ISO/IEC 27002
DE16	Marco Civil da internet
DE17	A Infraestrutura de Chaves Públicas ICP-Brasil MP Nº 2.200-2
DE18	Manual de Acreditação da ONA
DE19	Manual de Acreditação da Joint Commission International (JCI)
DE20	PIPEDA- "Personal Information Protection and Electronic Documents Act"

Fonte: Dados da pesquisa.

Os 20 documentos foram lidos e analisados detalhadamente. A cada menção de um mecanismo ele era tabulado, tanto o nome como a sua descrição. Neste processo, foram identificados 37 diferentes mecanismos. Igualmente, identificaram-se mecanismos a partir da análise dos resultados das entrevistas nos casos estudados, bem como os documentos coletados nos casos e a observação. No Hospital Beta foram identificados 36 mecanismos e no Hospital Gama 41 mecanismos, a partir das diferentes técnicas de coleta de dados. A lista de mecanismos proveniente da análise de documentos e a lista proveniente dos estudos de caso foram consolidadas, retirando-se as repetições. Assim, chegou-se a um conjunto de 50 mecanismos, levando em consideração que na abordagem de Análise dos Documentos Regulatórios e Normativos têm-se 20 citações possíveis e na Análise dos Estudos de Caso tem-se 14 citações possíveis, totalizando um total de 34 citações possíveis.

Para a análise final, primeiramente os mecanismos foram reclassificados, criando um novo código e alterando o nome original, para deixar o nome mais sucinto. Após essa adequação, os mecanismos foram agrupados em Mecanismos de Estrutura, Mecanismos de Processo e Mecanismos de Relacionamento, conforme conceito apresentado por Guldentops, Van Grembergen e De Haes (2004). Segundo os autores, os Mecanismos de Estrutura são responsáveis por criar regras e papéis, os Mecanismos de Processo gerenciam práticas voltadas a estratégia de TI e também têm a função de implementar os sistemas de tomadas de decisões, e os Mecanismos de Relacionamento são responsáveis pelo entendimento dos objetivos entre TI e negócios.

Após a classificação pelo tipo de mecanismos, foi realizada uma classificação conforme o seu eixo de ação, ou seja, vulnerabilidade (VN), salvaguarda (SG), detecção (DT), punição (PN) e conscientização (CN) (ALBRECHTSEN HOVDEN, 2009 BULGURCU *et al.*, 2010), marcando com um (X) em qual dos eixos o mecanismo melhor se enquadra.

Por fim, os mecanismos foram classificados em acordo com o requisitos de Segurança, , seguindo a classificação proposta por Luciano e Klein (2014), quais sejam: Confidencialidade (CONFD), Integridade (INT), Disponibilidade (DISP), Autenticidade (AUT), Confiabilidade (CONFB), Conformidade (CONFM) e Irrefutabilidade (IRR). Nas tabelas 1, 2, 3 ao lado do nome do mecanismo está a quantidade de vezes em que ele foi citado. Utilize-se a seguinte legenda para as tabelas seguintes: VN: vulnerabilidade SG: salvaguarda DT: detecção PN: punição CN: conscientização.

Tabela 1 − Mecanismos de Estrutura

n.	Mecanismos de Estrutura	VN	SG	DT	PN	CN	Requisito
1	Área de qualidade para controlar os documentos-2		X				CONFD
2	Comissão de Revisão de Prontuários-6		X				CONFM
3	Controle e armazenamento dos prontuários eletrônicos em um sistema especializado em GED-3	X					DISP
4	Estrutura física adequada para o gerenciamento do SI-17		X				DISP
5	Implantação e manutenção do Sistema de Gestão da Segurança da Informação-13		X				CONFD
6	Instalação de Antivírus, VPN e *firewall-12*		X				CONFD
7	Pessoa responsável pela Política de Segurança da Informação-10		X				CONFD
8	Proteções internas para a conexão de um novo *hardware* ou *software* na rede – 8		X				CONFD
9	Quantidade de profissionais dimensionados de acordo com a realidade da organização ou departamento-8		X				DISP

Fonte: Dados da pesquisa.

Tabela 2 − Mecanismos de Processo

n.	Mecanismos de Processo	VN	SG	DT	PN	CN	Requisito
10	Acesso do prontuário somente no momento da internação-4		X				CONFD
11	Acesso dos prontuários eletrônicos aos colaboradores da TI, somente àqueles com necessidades legitimas e relevantes-13		X				CONFD
12	Análise dos antecedentes de candidatos a empregos de cargos que têm acesso a informação sigilosa-2		X				INT
13	Análise regular da segurança dos Sistemas de Informação-7		X				CONFD
14	Anulação imediata dos acessos do empregado demitido-4		X				CONFD
15	Armazenamento de *logs* de acesso e *logs* de alterações realizadas no prontuário do paciente-9		X				CONFM
16	*Backup* estruturado das informações-8		X				DISP
17	Bloqueio de utilização de mídias de gravação (*pendrive*), acesso a repositórios na internet e e-mail externo-1			X			INT
18	Ciência da leitura dos termos de Segurança da Informação-3		X				CONFD
19	Coleta somente dados relevantes dos clientes/pacientes-3		X				INT
20	Criação de uma integração de *login* e senha válidos para todos os sistemas-2		X				IRR
21	Criptografia para o tráfego externo de informações-10		X				AUT
22	Cursos e treinamentos a distância obrigatórios com provas e avaliações de teste de conhecimento-5		X				CONFD

(Continua)

Tabela 2 – Mecanismos de Processo (Conclusão)

n.	Mecanismos de Processo	VN	SG	DT	PN	CN	Requisito
23	Definição de regras para transmissão de dados externos -7		X				INT
24	Determinação de máscara de senha e tempo máximo de troca de senha e bloqueio por muitas tentativas-11		X				CONFD
25	Divisão das funções dos colaboradores nos sistemas-4					X	INT
26	Identificação e autenticação dos usuários-19	X					CONFB
27	Inativação do sistema por tempo ocioso-4		X				CONFD
28	Liberação do acesso aos dados relevantes somente para pessoas devidamente autorizadas-12		X				CONFD
29	Monitoramento constantemente das atividades incomuns de processamento da informação-7		X				CONFM
30	Não utilização do celular, principalmente no beira leito-2		X				INT
31	Obrigatoriedade de assinatura do termo de conduta na contratação- 5		X				CONFB
32	Penalização com multa-1				X		CONFM
33	Planejamento das atividades, para executar as tarefas com segurança-8		X				DISP
34	Plano de contingência para desastres com informações-9		X				DISP
35	Política pública especifica para a privacidade da informação no Brasil-2		X				INT
36	Prevenção no posicionamento de computadores próximos a corredores-3		X				CONFD
37	Sanções adequadas para os que violam as políticas de privacidade-16				X		CONFM
38	*Software* de HIS adequado e de boa qualidade-7		X				CONFD
39	Treinamento constante para os colaboradores-16					X	CONFD
40	Utilização de nomes fictícios nas bases de testes e homologações-4		X				INT
41	Utilização do certificado digital nos prontuários eletrônicos-10		X				CONFB

Fonte: Dados da pesquisa.

Tabela 3 – Mecanismos de Relacionamento

n.	Mecanismos de Relacionamento	VN	SG	DT	PN	CN	Requisito
42	Criação e divulgação aos colaboradores da política de privacidade -13					X	CONFM
43	Disponibilização das políticas de Segurança da Informação aos clientes-1		X				INT
44	Divulgação dos meios de segurança de SI antes da implantação-4					X	INT
45	Envio de comunicados constantes aos colaboradores, orientando sobre a proteção da informação-16					X	CONFM
46	Instrução informal de médicos e enfermeiros a não divulgar casos -9		X				CONFM
47	Intranet para consulta dos documentos de políticas-9	X					DISP
48	Manutenção das informações dos clientes apenas o tempo necessário por lei-4		X				DISP
49	Prevenção para que os colaboradores não conversem com pacientes a respeito de diagnósticos em áreas públicas-6					X	CONFM
50	Valorização e premiação pelo cumprimento da Segurança da Informação-4		X				CONFD

Fonte: Dados da pesquisa.

Tabela 4 − Resumo do resultado por tipo de mecanismo

Tipo de mecanismos	Total	Requisitos						
		CONFD	INT	DISP	AUT	CONFB	CONFM	IRR
Estrutura	9	5	0	3	0	0	1	0
Processo	32	12	8	3	1	3	4	1
Relacionamento	9	1	2	2	0	0	4	0
TOTAL	50	18	10	8	1	3	9	1

*Legenda: CONFD–Confidencialidade INT–Integridade DISP–Disponibilidade AUT-Autenticidade CONFB – Confiabilidade CONFM – Conformidade IRR - Irrefutabilidade
Fonte: Elaborado pelos autores.

A tabela 4 apresenta um resultado resumido dos mecanismos identificados, fazendo um cruzamento com os requisitos em que foram classificados. Os mecanismos seguem a definição de Guldentops *et al.*, (2004) e os requisitos estão em acordo a proposição de Luciano e Klein (2014). Por fim, realizaram-se discussões teórico-empíricas trazendo as contribuições do estudo.

Devido ao crescimento contínuo da tecnologia, a privacidade na área hospitalar requer principalmente proteção de dados e integridade (SMITH, 1996). Os mecanismos encontrados durante a pesquisa são classificados em sua maioria no eixo de ação de salvaguarda, que é o cuidado com o perigo e, consequentemente, a proteção dos dados do paciente, desde o seu registro, acesso e armazenamento. Já a integridade é apontada no resultado da pesquisa como o segundo principal requisito, ficando atrás da confidencialidade. Esses dois requisitos estão associados porque não parece lógico proteger uma informação não íntegra. A confidencialidade teve um destaque muito grande nos resultados. Isso mostra que os hospitais procuram conscientizar os colaboradores e principalmente proteger as suas informações. Ademais, D'Arcy e Hovav (2009) reforçam que além de programas de conscientização, o conhecimento das políticas de segurança, a percepção de sanções formais e o monitoramento, diminuem a intenção de abusos na área de segurança da informação.

Porém, essa conscientização teve um número baixo em relação à salvaguarda, e isso não é uma evidência favorável, pois os hospitais tentam proteger as informações, entretanto esquecem que o fator humano pode influenciar a privacidade da informação. Conforme o entendimento de Bragança, Luciano e Testa (2010), o usuário do sistema de informação deve colaborar e estar consciente, pois caso contrário o sistema não terá êxito, podendo ocorrer uma vulnerabilidade. Bulgurcu *et al.* (2010) colaboram evidenciando que a decorrência da vulnerabilidade vem do funcionário que não segue a Política de Segurança da Informação.

O que se observa nos achados é uma preocupação grande com a conscientização em relação aos treinamentos e instruções dos colaboradores, classificados no tipo de Mecanismo de Relacionamento. Esse resultado é importante, pois demonstra que os hospitais mantêm as suas políticas de privacidade e se preocupam com a salvaguarda, por meio das normas. Bulgurcu *et al.* (2010) explicam que as crenças de caráter normativo têm maior efeito que a intenção de cumprimento, quando comparadas à severidade das sanções. Os funcionários serão mais propensos a seguir as políticas de segurança se percebem que há uma probabilidade alta de serem pegos no ato da violação dessas políticas.

Além da criação e manutenção de normas e políticas, os hospitais trabalham o fator comportamental do ser humano, por meio dos treinamentos e instruções, no sentido de prevenir e divulgar novos meios de segurança, para evitar possíveis problemas relacionados à segurança da informação. O comportamento pode originar possíveis violações na segurança da Informação e consequentemente provocar acréscimo de vulnerabilidade, que também ocorre por erro humano devido à sobrecarga de trabalho ou até mesmo por falta de atenção (LIGINLAL *et al*., 2009).

Após a análise dos mecanismos encontrados e classificados, uma questão que chamou a atenção é que, de maneira geral, os eixos de detecção e punição não tiveram grande destaque no resultado. Isso mostra que as ações dos hospitais não têm uma preocupação muito grande com detecção ou a punição. Esse resultado foi pouco expressivo, mesmo que Herath e Rao (2009) expliquem que a existência e a visibilidade de mecanismos de detecção provavelmente sejam mais importantes que a severidade da sanção imposta. Complementam que um jeito de coibir abusos é deixar claro que o colaborador será severamente punido caso detectado, pois a severidade da punição e a certeza da detecção do não cumprimento das normas de segurança da informação, são fatores significativos sobre as intenções de comportamento na área de Segurança da Informação.

De maneira geral o que se percebe é que a preocupação maior está nos processos e meios de instrução e treinamento para se evitar o vazamento das informações do prontuário eletrônico do paciente. A privacidade é observada como o receio da pessoa perder o controle do uso e a proliferação das informações pessoais, pois quanto menor é a privacidade, menor é o controle sobre a utilização das informações pessoais (ROSE, 2006).

Dos 50 mecanismos encontrados, nove são de estrutura, 32 de processo e nove de relacionamento, destacando–se com uma quantidade bem elevada dos mecanismos de processo em relação aos demais. Essa maior atenção dada a processos pode ter relação com o que Costa (2003) escreve: se caso a instituição de saúde, seja ela qual for, não estiver preparada, o uso indevido do prontuário eletrônico pode colocar a segurança e a confiabilidade da informação em risco.

Contudo, conforme mostra o resultado do estudo e resumido na tabela 1, o requisito de confiabilidade teve uma classificação pouco expressiva. Acredita-se que tal situação ocorra porque os colaboradores sabem o valor da informação contida no prontuário eletrônico. Isso vem ao encontro de outro requisito detectado nos resultados, a confidencialidade. A confidencialidade, ou seja, a proteção contra a divulgação não autorizada da informação sobressaiu no resultado final, porém o que é destacável é a relação desse requisito com o tipo de mecanismo de processo, ou seja, a grande maioria das ações relacionadas à privacidade e segurança das informações dos hospitais são os processos criados para garantir a confidencialidade da informação.

CONSIDERAÇÕES FINAIS

Em virtude das diferentes abordagens metodológicas e técnicas de coleta de dados para os 50 mecanismos identificados, acredita-se que eles possam ser aplicados em diferentes hospitais, porém, é necessário ressaltar que não necessariamente todos os mecanismos são aplicáveis a todos os contextos. Observa-se que dos 50 mecanismos identificados, 18 deles estão associados à confidencialidade, e desse total, 12 deles, foram classificados como mecanismos deprocessos. Portanto, os mecanismos mais utilizados são os de processo em relação à salvaguarda e os mecanismos de relacionamento em relação à conscientização dos colaboradores.

Com isso, conclui-se que, apesar de ser possível a aplicação de todos os mecanismos em hospitais, provavelmente os hospitais pequenos terão dificuldades em alguns mecanismos, que requerem recursos financeiros, assim como uma boa estrutura física e pessoal.

O que mais se destacou no resultado foram os mecanismos de processo, inclusive bem mais que os de estrutura, e isso mostra que os grandes hospitais têm a preocupação com processos internos seguros no manuseio do prontuário eletrônico.

Este estudo traz à tona alguns problemas vivenciados na rotina de instituições de saúde - como, por exemplo, o vazamento de informações e imagens não autorizadas de pacientes. A relevância dos problemas que isso representa para todos os envolvidos, como paciente, instituição e profissionais de saúde, indicou a necessidade do fortalecimento da discussão dessa temática para a academia.

Outra contribuição da pesquisa é exatamente para os hospitais, independentemente do seu tamanho. A primeira contribuição é mostrar em quais documentos regulatórios e normativos os hospitais podem se basear, para ter um comportamento mais seguro em relação à privacidade da informação. A segunda contribuição é mostrar a relação de mecanismos descobertos no decorrer de todas as abordagens metodológicas e técnicas de coleta de dados, que podem auxiliar os gestores e os responsáveis pela segurança da informação dos hospitais a proteger os seus dados e principalmente proteger as informações dos pacientes no prontuário eletrônico, pois se constatou que os hospitais possuem alguns mecanismos. Entretanto, isso ainda não é o suficiente, uma vez que existem ocorrências de incidentes com a informação e a privacidade do paciente.

Os principais limites da pesquisa, além daquelas que são inerentes às características de cada um dos métodos escolhidos, é que as entrevistas realizadas nos Estudos de Caso ocorreram somente com pessoal de TI. Embora não fosse o objetivo, foi o que acabou sendo possível, e se considerou que essa restrição da função dos respondentes não afetaria os objetivos do estudo.

Uma das propostas para as pesquisas futuras é identificar os fatores críticos de sucesso em cada mecanismo encontrado neste trabalho. Outra proposta é a replicação da pesquisa em hospitais de pequeno e médio porte visando a comparação entre os achados.

REFERÊNCIAS

ABRAHÃO, M. S. *A Segurança da Informação Digital na Saúde*. [S.l.]: Sociedade Beneficente Israelita Brasileira, 2003. Disponível em: http://www.einstein.br/biblioteca/artigos/131%20132.pdf. Acesso em: 30 Jun. 2019.

ACQUISTI, A.; GROSSKLAGS, J. Privacy and Rationality in Individual decision making. I*EEE Security & Privacy*, [*S.l.*], v.3, n.1, p. 26-33, jan/fev 2005.

ALBRECHTSEN, E.; HOVDEN, J. The information security digital divide between information security managers and users. *Computers & Security,* [*S.l.*], v. 28, n. 6, p. 476-490, 2009.

ALBUQUERQUE JUNIOR, A. E. SANTOS, E. M. A percepção da importância de Controles de segurança da informação em hospitais públicos brasileiros. *Revista Eletrônica de Comunicação, Informação & Inovação em Saúde,* [*S.l.*], v. 6, n. 2 p. 2-18, 2013.

ALDERMAN E.; KENNEDY C. *The Right to Privacy*. New York: Knopf, 1995.

ANDERSON, R.; MOORE T. The Economics of Information Security. *Science,* [*S.l.*], v. 314, n. 5799, p.610-613, October 27, 2006. DOI: http://dx.doi.org/10.1126/science.1130992.

APPARI. A.; JOHNSON, M. E. Information Security and Privacy in Healthcare: Current State of Research. I*nternational Journal of Internet and Enterprise Management,* [*S.l.*], v. 6, n. 4, p. 279-314, 2010.

ARAUJO, T. V.; PIRES S. R.; BANDIERA-PAIVA P. Adoção de padrões para Registro Eletrônico em Saúde no Brasil. *Revista Eletrônica de Comunicação, Informação & Inovação em Saúde*, [*S.l.*], v. 8, n. 4, p. 554-566, 2014. DOI:10.3395/reciis.v8i4.895.pt

BARDIN, L. *Análise de conteúdo.* Lisboa: Edições 70, 1977.

BRAGANÇA, C. E. B. A; LUCIANO, E. M.; TESTA, M. G. Segurança da Informação e privacidade de informações de pacientes de instituições de saúde: uma análise exploratória da privacidade percebida pelos profissionais. In: ENANPAD, 2010, Rio de Janeiro. *Anais* [...]. Rio de Janeiro:[*s.n*], 2010.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information Security Policy: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*,[*S.l.*], v. 34. n. 3, p. 523-548, September, 2010.

CAMPARA, M. *et al*. Implantação do Prontuário Eletrônico de Paciente. *Revista de Administração Hospitalar*, [*S.l.*], v.10, n.3, p. 61-74, setembro/dezembro, 2013.

CHAGAS, A. T. R. O Questionário na Pesquisa Científica. A*dministração On Line. Prática - Pesquisa – Ensino,* [*S.l*], v. 1, n.1, 2000.

COSTA, C. G. A. Prontuário Eletrônico do Paciente: Legislação, Auditoria e Conectividade. In: Congresso Latino Americano de Serviços de Saúde, 8., 2003, [*S.l.*]. *Anais* [...]. [*S.l. :s.n.*], 2003.

COSTA, J. F. R. PORTELA, M. C. Percepções de gestores, profissionais e usuários acerca do registro eletrônico de saúde e de aspectos facilitadores e barreiras para a sua implementação. *Cadernos de Saúde Pública*, [*S.l.*], v. 34, n. 1, p. 1-14 , 2018.

CURRAN, M.; CURRAN, K.. The ethics of information. *Journal of Nursing Administration,* [*S.l.*], v. 21, n.1, p. 47-9, 1991.

D'ARCY, J.; HOVAV, A. Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics,* [*S.l.*], v. 89, p. 59-71, 2009.

DA VEIGA, A.; ELOFF, J. H. P. A framework and assessment instrument for information security culture. *Computers & Security*, [*S.l.*], v. 29, n. 2, p. 196-207, 2010.

ERMAKOVA, T. *et al.* Antecedents of Health Information Privacy Concerns. Procedia Computer Science, [S.l.], v. 63, p. 376-383, 2015. DOI: https://doi.org/10.1016/j.procs.2015.08.356.

FADEN R.R.; BEAUCHAMP T.L. *A history and theory of informed consent.* New York: Oxford Univ, 1986.

FERREIRA, F. N. F.; ARAÚJO, M.T. P*olíticas de Segurança da Informação* - Guia prático para elaboração e implementação. Rio de Janeiro: Ciência Moderna, 2008.

FRANCISCONI, C. F., GOLDIM, J.R. Aspectos bioéticos da confidencialidade e privacidade. *In*: COSTA, S.I.F.; OSELKA, G.; GARRAFA, V. (org.). *Iniciação à Bioética*. Brasília: Conselho Federal de Medicina, 1998. p.269-84.

GIL, A. C. *Como elaborar projetos de pesquisa*. 4. ed. São Paulo: Atlas, 2002.

GOLDIM, J. R.; FRANCISCONI, X. *Bioética Clínica.* [*S.l*], 2005. Disponível em: http://www.pucrs.br/bioetica/cont/carlos/bioeticaclinica.pdf. Acesso em: 25 jun. 2018.

GONÇALEZ, P. R. V. G.; SANTANA, R. C. G. S; JORENTE, M. J. V. Privacidade do usuário na atividade de busca: o caso do Arquivo Público do Estado de São Paulo. *Perspectivas em Ciência da Informação,*[*S.l.*], v.20, n.3, p.137-151, jul./set. 2015.

GULDENTOPS, E.; VAN-GREMBERGEN, W.; DE HAES, S. Control and governance maturity survey: establishing a reference benchmark and a self-assessment tool. I*nformation Systems Control Journal,* [*S.l.*], v. 6, p.32-35, 2004.

LEE, H. *et al*. Information privacy concerns and demographic characteristics: Data from a Korean media panel survey. *Government Information Quarterly,* [*S.l.*], v. 36, n. 2, 2019. DOI: https://doi.org/10.1016/j.giq.2019.01.002.

LEINO- KILPI, H. *et al*. Privacy: a review of the literature. *International Journal of Nursing Studies,* [*S.l.*], v. 38, n. 6, p. 663-671, 2001.

LIGINLAL, D.; SIM, I.; KHANSA, L. How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. *Computers & Security*, [*S.l.*], v. 28, p.215-228, 2009.

LOCH, J.A. *Confidencialidade:* natureza, características e limitações no contexto da relação clínica.[S.l.: s.n.], 2003.

LOTT, Y. M. CIANCONI, R. B. Vigilância e privacidade, no contexto do big data e dados pessoais: análise da produção da Ciência da Informação no Brasil. P*erspectivas em Ciência da Informação,* [*S.l.*], v.23, n.4, p.117-132, out./dez. 2018.

LUCIANO, E. M.; BRAGANÇA, C. E. B. de A.; TESTA, M. G. Privacidade de informações de pacientes de instituições de saúde: a percepção de profissionais da área de saúde. *Reuna,* Belo Horizonte, v. 16, p. 89-102, 2011.

LUCIANO, E. M.; KLEIN, R. H. – In. PRADO, E.P.V.; SOUZA C.A. (org.). *Fundamentos de Sistemas de Informação.* Rio de Janeiro: Elsevier, 2014. cap. 6, p. 93-110.

MARTORELL, L. B.; NASCIMENTO, W. F. do; GARRAFA, V. Redes sociais, privacidade, confidencialidade e ética: a exposição de imagens de pacientes no facebook. I*nterface-Comunicação, Saúde, Educação,*[*S.l.*], v. 20, n. 56, p. 13-23, 2016.

MASSAD, E., MARIN, H.F., AZEVEDO, R. S. *O Prontuário do Paciente na Assistência, Informação e Conhecimento Médico*. São Paulo: USP, 2003.

MERCURI, R.T. The HIPAA - potamus in Health Care Data Security. *Communications of the ACM,* [*S.l.*], v.47, n.7, 2004.

MONTENEGRO, L.C. *et al*. Problemas éticos na prática de profissionais de saúde em um hospital escola. *Avances en Enfermería,* [S.l.], v. 34, n. 3, p. 226, 2016.

PAVÃO, A. L. B. *et al*. The role of Brazilian National Health Information Systems in assessing the impact of Zika virus outbreak. *Revista da Sociedade Brasileira de Medicina Tropical*, [*S.l.*], v. 50, n. 4, p. 450-457, 2017.

PUPULIM, J. S. L.; SAWADA, N. O. O cuidado de enfermagem e a invasão de privacidade do doente: uma questão ético-moral. *Revista Latino-americana de Enfermagem*, [S.l.], v. 10, n.3, p. 483-488, 2002.

RABELO, C. R. O.; BENTES PINTO, V. Representação Temática da Informação no Prontuário do Paciente: um estudo sobre o uso da CID-10 nas Organizações de Saúde localizadas em Fortaleza-CE. R*evista de Saúde Digital e Tecnologias Educacionais,*[*S.l.*], v. 3, p. 114-131, 2018.

ROSE, E. A. An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management,* [*S.l.*], v. 43, 3, p. 322-335, 2006.

SIPONEN, M. A conceptual foundation for organizational information security awareness. Information *Management & Computer Security,* [*S.l.*], v.8, n.1, p. 31-41, 2000.

SMITH, M. Data protection, health care and the new European directive. *British Medical Journal,*[*S.l.*], v. 312, p. 197–198, 1996.

VANCE, A.; SIPONEN, M.; PAHNILA, S. Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information & Management,* [*S.l.*], 2012.

VENTURA, M.; COELI, C. M. Para além da privacidade: direito à informação na saúde, proteção de dados pessoais e governança. *Cadernos de Saúde Pública,*[*S.l.*], v. 34, p. e00106818, 2018.

WESTIN, A. F. *Privacy and Freedom*. New York: Atheneum, 1967.

WIN, K.T., SUSILO, W.; MU, Y. Personal Health Record Systems and Their Privacy Protection. *Journal of Medical Systems,* [*S.l.*], v.30, p. 309-315, 2006.

YANAGUIBASHI, E. A. *et al*. Prontuário Eletrônico do Paciente e certificação de software em saúde: Avanços que visam maior segurança dos dados médicos. *Revista Brasileira de Inovação Tecnológica em Saúde*, [*S.l.*], v. 7, n. 2, p. 2236-1103, 2017.