eISSN: 2213-3712

REVISTA DE GESTÃO EM SISTEMAS DE SAÚDE – RGSS
HEALTH SYSTEMS MANAGEMENT JOURNAL – HSMJ

Data de recebimento: 25/8/2018 – Data de Aceite: 6/6/2019

https://doi.org/10.5585/RGSS.v8i2.14139

Segurança da informação e a área da saúde: a convergência dos temas e a intensidade das publicações científicas

Information security and healthcare: the convergence of themes and the intensity of scientific publications

Cristiana Fernandes de Muÿlder[1]

Jeferson Gonçalves de Oliveira[2]

Cássio Luís Batista[3]

Rodrigo Moreno Marques[4]

Resumo

Entende-se que a segurança da informação é um problema crítico na área da saúde pois está relacionada a sistemas de informação que contém dados críticos de pacientes e seus tratamentos. Neste contexto, buscou-se responder à questão de pesquisa: Quais são os principais frameworks de segurança da informação utilizados na área de saúde? O objetivo deste artigo consiste em revisar sistematicamente artigos que abordam estudos sobre a segurança da informação na saúde e identificar os principais frameworks e focos de discussão de segurança da informação citados na literatura. Como resultado, observa-se que somente 16 estudos citaram *frameworks* com enfoque na gestão da segurança da informação. Destes, somente 12 citaram a norma ISO/IEC 27799 e a norma HIPAA, específicas para a área de saúde. Conclui-se, assim, que poucos estudos foram produzidos nos últimos 10 anos, deixando uma lacuna no contexto de países em desenvolvimento ou hospitais de pequeno porte.

Palavras-chave Segurança Computacional. Administração em Saúde. Privacidade. Revisão. Dano ao paciente.

Abstract

It is understood that information security is a critical problem in the health area, because it is related to an information system that is based on the evolution of patients and their treatments. In this context, we sought to answer the research question: What are the main information security frameworks in the health area? The review article consists of a systematic review of data on information security and the main discussion boards and information security in the literature. As a result, the frameworks are seen to fit into the information structure. Of these, only 12 cited ISO / IEC 27799 and a HIPAA standard, specific to a health area. It is concluded, therefore, that the studies have been carried out in the last 10 years, leaving a gap in the context of developing countries or in small hospitals.

Keywords: Computer Security. Health Administration. Privacy. Review. Patient Harm.

1 Doutora em Economia Aplicada, Universidade FUMEC – FUMEC. Belo Horizonte, Minas Gerais – Brasil.
ORCID: https://orcid.org/0000-0002-0813-0999
cristiana.muylder@fumec.br

2 Mestre em Sistemas de Informação e Gestão do Conhecimento, Universidade FUMEC – FUMEC. Belo Horizonte, Minas Gerais – Brasil.
ORCID: https://orcid.org/0000-0003-4936-5820
jeferson.oliveirabh@gmail.com

3 Mestre em Engenharia Elétrica, Universidade FUMEC – FUMEC. Belo Horizonte, Minas Gerais – Brasil.
ORCID: https://orcid.org/0000-0002-0278-2232
batista@fumec.br

4 Doutor em Ciência da Informação, Universidade FUMEC – FUMEC. Belo Horizonte, Minas Gerais – Brasil.
ORCID: https://orcid.org/000-0002-6320-4874
rodrigo.marques@fumec.edu.br

1 Introdução

Com o desenvolvimento tecnológico e melhoria na utilização dos recursos da Internet, comunicação móvel, computação em nuvem, percebe-se que ocorre uma verdadeira explosão de informação em todas as áreas de conhecimento. Paralelamente, na área da saúde, essa mudança de paradigma permitiu reduzir obstáculos para a oferta de serviços mais personalizados aos pacientes, que podem acessar informações médicas e componentes de seus prontuários pela internet (Meingast, Roosta & Sastry, 2006).

Entretanto, tecnologias novas normalmente implicam em dificuldades de proteção, e as violações na segurança de informações na saúde têm um impacto significativo nos pacientes e nas organizações de saúde (Warren, 2005). Relatórios da indústria indicam que o número de incidentes de segurança em organização de saúde tem aumentado. A Symantec mostra que a indústria da saúde contabiliza 36% do total de incidentes de segurança no Reino Unido. Em 44%, a indústria da saúde continuava a ser o setor responsável pela maior porcentagem de divulgação indevida de dados (He & Johnson, 2017).

Em 13 de maio de 2017, *hackers* começaram a espalhar um *ransomware*[5] computadores de todo o mundo. De acordo com a Europol, mais de 200.000 computadores em 150 países foram vítimas do ataque cibernético que envolvia a requisição de resgate de 300 dólares para devolver o controle sobre os arquivos criptografados. No Reino Unido, o ataque cibernético afetou os sistemas de tecnologia de informação dos hospitais do Serviço Nacional de Saúde, resultando em operações canceladas, hospitais sendo colocados no status de transferência e os documentos como os registros de pacientes ficando indisponíveis na Inglaterra e na Escócia (Mattei, 2017).

Assim, organizações de saúde têm sido afetadas por ameaças e roubos de dados de segurança (Appari & Johnson, 2010; Tritilanunt & Tongsrisomboon, 2014). Dessa forma, proteger as informações do paciente se torna uma questão primordial para a prestação de serviços de cuidados de saúde (Fernando & Dawson, 2009). Para isso, é necessário regulamentar a segurança da informação para garantir a privacidade e confidencialidade do paciente.

Diante desse cenário, este trabalho objetiva apresentar uma revisão sistemática da literatura que permita responder à pergunta: quais são os principais frameworks de segurança da informação citados nos trabalhos para a área de saúde? A partir da análise dos trabalhos indexados sobre segurança da informação na saúde buscou-se: i) identificar os principais frameworks de segurança da informação que estão sendo utilizadas na área da saúde; ii) identificar o principal foco dos estudos em relação à segurança da informação.

2 Referencial teórico

A seção de referencial teórico aborda a segurança cibernética na saúde e os *frameworks* de segurança da informação na saúde.

2.1 Segurança cibernética na saúde

Langer (2017) define os atores relacionados à segurança de computadores e, de forma mais genérica da Internet (incluindo a Internet de Todas as Coisas[6]), os quais denomina como *Cast* ou, elenco, incluindo o *Black Hat* (agentes humanos que procuram obter controle sobre computadores ou dispositivos de outras pessoas para usuários com fins nefastos) e os sumarizam em grupos, os quais são aplicados no campo da segurança cibernética na saúde: ataques criptográficos, crime cibernético, ataques de negação de serviços, *injection exploits*, *malware* e exploração da segurança web (Langer, 2017).

Assim, para assegurar o armazenamento e a gerência de acesso aos S-RES, vários requisitos de segurança da informação devem ser levados em consideração: armazenagem dos registros eletrônicos de saúde (RES), possibilitando velocidade e a segurança no acesso aos recursos; proteção contra código malicioso; proteção

5 Tipo de software nocivo que restringe o acesso ao sistema infectado bloqueando-o por meio criptográfico. Posteriormente, solicita um pagamento para que o acesso possa ser restabelecido. Caso não ocorra, os arquivos podem ser perdidos.

6 Internet de Todas as Coisas é o termo utilizado para a rede de objetos físicos ou "coisas" incorporadas em produtos eletrônicos, softwares, sensores e conectividade para habilitar objetos a trocar dados com o fabricante, o operador e/ou outros dispositivos conectados.

ao acesso, sendo permitido somente ao usuário autorizado; dispositivos móveis devem fazer acesso seguro e eficiente à infraestrutura de saúde; sistemas de proteção online (firewalls, antivírus e dispositivos de filtragem de conteúdo) devem ser agregados na proteção de informação de saúde e atividades criminais na Internet visto que, qualquer falha de segurança é uma porta para o vazamento de informação (Chiuchisan, Balan, Geman, Chiuchisan, & Gordin, 2017).

Apesar da regulamentação de segurança, o profissional da saúde também é identificado como o elemento que traz mais vulnerabilidade para a segurança da informação de uma organização. A cultura de segurança de informação é reconhecida como a forma de influenciar o usuário a adotar os controles e políticas de segurança da informação nas organizações (Hassan & Ismail, 2016).

Com todos esses requisitos, o uso de um sistema de gerenciamento de segurança da informação é necessário para medir e gerenciar os processos de segurança da informação de forma estruturada para garantir uma abordagem coordenada e pouco fragmentada.

2.2 Ferramentas para o gerenciamento da segurança da informação

Atualmente, há varias padronizações, ferramentas, frameworks e recomendações de melhores práticas para gerência e manutenção de serviços de Tecnologia da Informação que são aplicados a vários segmentos de negócio. O padrão ISO/IEC 27001 é reconhecido internacionalmente por prover uma especificação para o gerenciamento de sistemas de segurança (ISO 27001, 2005). Já o padrão ISO/IEC 27002 dá suporte para a implementação de controles de segurança especificados na ISO/IEC 27001 (ISO 27002, 2005) e inclusive é citado para esse fim na própria norma.

Nos Estados Unidos, em 1996, foi criado o ato da Portabilidade do Seguro de Saúde e Prestação de Contas (*Health Insurance Portability & Accountability Act* – HIPAA). O HIPAA (EEUU, 1996) foi criado inicialmente para a portabilidade, privacidade e segurança da informação de saúde pessoal (*Protect Health Information* - PHI) que até então era principalmente registrada em fichas de papel. Em 2009 e 2013, a regulamentação passou por atualizações para cobrir melhor a transmissão eletrônica do PHI ou (ePHI). Este ato fez com que as organizações de saúde reavaliassem as questões que envolvem a privacidade e a segurança da informação em saúde.

Segundo Drevin, Kruger, Bell e Steyn (2017) o HIPAA é a legislação mais conhecida sobre a segurança e privacidade da informação na saúde. Nota-se que o HIPAA inclui cláusulas de proteção de direitos do usuário dos serviços de saúde como, por exemplo: ter acesso e obter cópia dos seus registros em saúde; corrigir ou complementar suas informações; receber uma notificação que apresenta como a informação em saúde pode ser usada e compartilhada; ser consultado sobre a possibilidade de que suas informações sejam usadas ou compartilhadas para certos propósitos, tais como marketing; obter relatórios que informem quando e porque a informação em saúde foi compartilhada para certos propósitos; registrar uma reclamação com o provedor do serviço de saúde, seguradora de saúde e/ou Governo dos EEUU se os direitos são negados ou a informação em saúde não foi protegida.

A regra de segurança da HIPAA (EEUU, 1996) e a *Health Information Technology for Economic and Clinical Health*, conhecido como HITECH (EEUU, 2009), são um passo em direção a padrões que assegurem a segurança e a integridade das informações dos pacientes armazenadas ou transmitidas eletronicamente. Da mesma forma, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) também recebeu Assentimento Real no Canadá em 13 de abril de 2000 (Canada, 2000).

O HIPAA foi melhorado em 2009, por meio do *American Recovery and Reinvestment Act* -ARRA (EEUU, 2009). Este ato impactou significativamente o desenvolvimento das tecnologias de informação em saúde, particularmente os Sistemas de Registros Eletrônicos de Saúde. O ARRA apresenta cinco objetivos: melhorar a qualidade médica, a segurança do paciente, a eficiência do tratamento de saúde e a redução das disparidades na saúde; engajar os pacientes e familiares; melhorar a coordenação do tratamento; assegurar a adequada privacidade e segurança da informação de saúde pessoal; beneficiar a população e a saúde pública (Hoyt & Yoshihashi, 2014).

Já no cenário internacional, de acordo com Orel & Bernik (2013), existia uma opinião geral que havia uma necessidade de mais especificidade na área de segurança da informação de saúde do que para outros domínios de informação. Em 2008 surgiu a ISO/IEC 27799 como um novo padrão específico para a área de saúde. A ISO/IEC 27799: 2008 (Informática em saúde - Gestão da segurança da informação na saúde usando ISO/IEC 27002) foi desenvolvida especificamente para ajudar as organizações de saúde a interpretar a padrão ISO/IEC 27002 e fornece diretrizes adicionais que não são explicitamente discutidas na norma ISO/IEC 27001, justamente por ser uma norma genérica (Tyali & Pottas, 2010).

Sendo assim, pela natureza sensível das informações na área de saúde, existem requisitos especiais que devem ser cumpridos para garantir a confidencialidade, a integridade e a disponibilidade de informações pessoais de saúde (ISO 27799, 2008). Dessa forma, entende-se que os padrões são imperativos para garantir benefícios aos pacientes e aos profissionais de saúde (Orel & Bernik; 2013).

3 Metodologia

O presente estudo baseia-se no modelo de revisão sistemática da literatura (RSL) proposto por Kitchenham (2004) que basicamente divide-se em três etapas: o planejamento da revisão, a condução da revisão e a análise dos resultados.

3.1 Planejamento da revisão sistemática

Na fase de planejamento foi estabelecido o protocolo para a execução da RSL que seguiu as seguintes etapas:

a. Descrição dos objetivos: tem como objetivo primário identificar os principais frameworks de segurança da informação apontados nos estudos e a distribuição dos mesmos pelas seguintes categorias: confidencialidade, integridade e disponibilidade.
b. Elaboração da questão de pesquisa: o presente estudo considerou as seguintes questões para subsidiar o processo de busca:

   i) Questão de pesquisa 01: Quais são os principais frameworks de segurança da informação utilizados na área de saúde descritos na literatura?

   ii) Questão de pesquisa 02: Quais são os principais focos dos estudos em relação à segurança da informação?
c. Com relação à estratégia de busca, o presente estudo baseia-se nos seguintes critérios:

   i) Seleção das bases para a pesquisa: segundo o protocolo, é recomendável a pesquisa em pelo menos 3 bases de qualidade e as selecionadas para o trabalho foram: *Web of Science*, *Scopus* e *Ebsco*. Essas três bases possuem um alto padrão de qualidade pois incluem milhares de revistas acadêmicas revisadas por pares e publicadas em todo o mundo. Além disso, também possuem um viés multidisciplinar necessário para o tema deste trabalho.

   ii) Elaboração da string de pesquisa: foi elaborada uma *string* que continha as palavras "informação", "segurança" e "saúde". Esses termos foram traduzidos para a língua inglesa e resultou no seguinte: ("*information*" *and* "*security*" *and* ("*healthcare*" *or* "*health care*")).
d. Adoção de critérios para inclusão e exclusão de trabalhos:

   i) Para inclusão dos estudos: as publicações devem estar disponíveis na Web, especificamente nas bases selecionadas, na língua inglesa, abordando estudos sobre segurança da informação na área de saúde e respondendo a qualquer uma das questões de pesquisa. Além disso, os artigos devem ter a sua data de publicação a partir de 2008, ano que as principais normas de segurança da informação já estavam consolidadas no mercado.

   ii) Estudo não incluídos: trabalhos duplicados, que não abordam o tema necessário, não respondam a nenhuma das questões de pesquisa ou possuem o ano de publicação anterior ao ano de 2008.

3.2 Condução da revisão sistemática

Na fase de condução da RSL foram executados os seguintes passos: a *string* de busca foi executada nas bases selecionadas; os estudos primários foram identificados

e selecionados de acordo com os critérios de inclusão e exclusão; os trabalhos foram avaliados seguindo os critérios de qualidade estabelecidos durante o planejamento da revisão.

3.2.1 Processo para recuperação dos estudos primários

Após a recuperação dos estudos primários por meio da *string* de busca, os trabalhos foram organizados na ferramenta ENDNOTE X7 para facilitar a separação e o rastreamento de cada uma das fases e critérios de inclusão/exclusão.

Sendo assim, foram encontrados 123 estudos após a busca inicial nas bases. Com a remoção dos trabalhos que não eram artigos científicos (capítulos de livros, textos técnicos e etc.), restaram 97 estudos. Após a remoção dos duplicados, obteve-se um total de 60 trabalhos. Destes, 8 não estavam disponíveis gratuitamente na Web e não puderam ser recuperados. Dos 52 artigos restantes, todos foram selecionados após a leitura dos resumos. Sendo assim, essa fase terminou com a seleção de 52 trabalhos conforme mostrado na Figura 1.

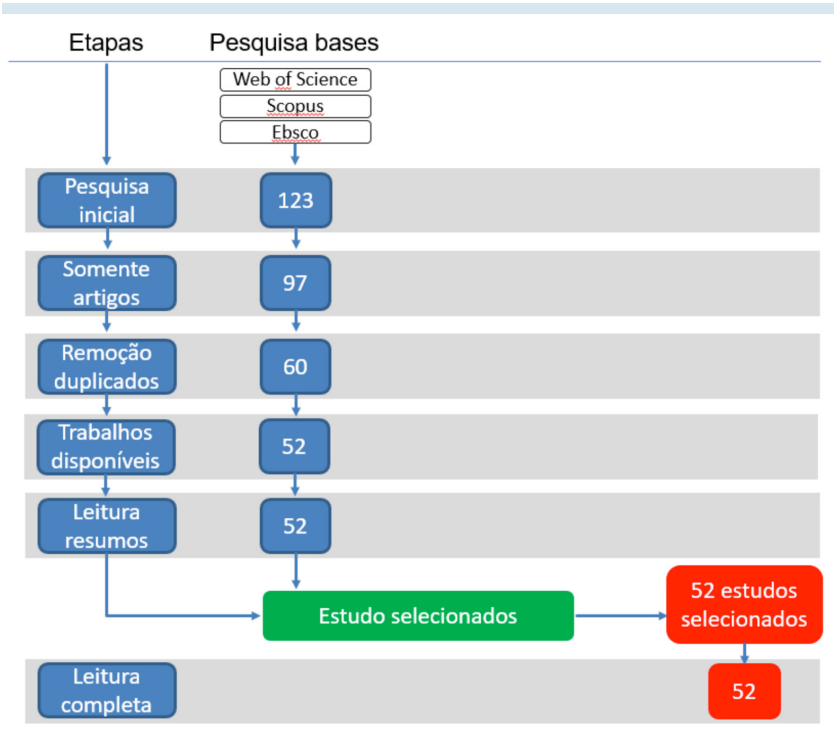

Figura 1: Processo de recuperação e pré-seleção
Fonte: Elaborado pelos autores.

3.2.2 Processo de seleção dos estudos

Após as fases de recuperação e pré-seleção, os artigos foram analisados por meio de uma leitura completa do seu conteúdo. Marconi e Lakatos (2003) citam que uma avaliação mais detalhada se faz necessária para garantir a qualidade dos estudos selecionados. Assim, os 52 trabalhos selecionados na fase anterior foram analisados e todos foram mantidos.

4 Resultados

O presente estudo elaborou uma revisão sistemática da literatura baseada no protocolo proposto por Kitchenham (2004) e após o processo de seleção final dos estudos chegou a um total de 52 trabalhos. Nestes, observa-se uma concentração de estudos nos anos de 2012, 2013 e 2017 conforme a Figura 2.

A distribuição dos artigos pelas bases pesquisadas mostra que, dos 52 estudos selecionados, 48 deles foram encontrados na base *Scopus* (Figura 3). A base *Web of Science* totalizou 31 artigos e a base *Ebsco* somente 14 trabalhos. A soma total resulta em mais de 52 artigos porque muitos deles foram encontrados em mais de uma base e foram removidos posteriormente.

Os 52 artigos selecionados são descritos e categorizados, no Quadro 1, em ordem cronológica:

Com relação ao enfoque dos trabalhos selecionados, nota-se que 12 artigos estão voltados para um aspecto mais completo de segurança na Governança de Tecnologia da Informação. A maioria desses estudos abordam frameworks (ou normas) mais abrangentes. Já o enfoque no "profissional de saúde", discutido em 10 trabalhos, mostra como os estudos na área de segurança da informação em saúde têm sido direcionados para disseminação da cultura de segurança para os profissionais da área, sendo que os mesmos são considerados uma

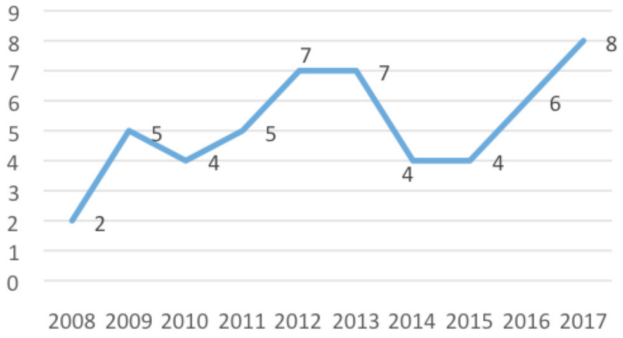

Figura 2: Distribuição dos 52 estudos por ano de publicação
Fonte: Dados da pesquisa.

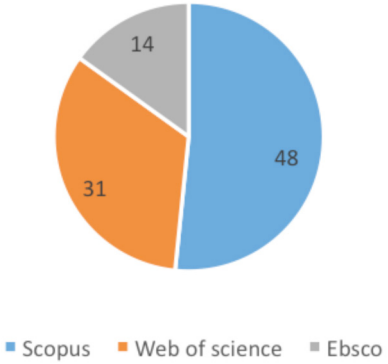

Figura 3: Distribuição dos 52 estudos por base de pesquisa
Fonte**:** Dados da pesquisa.

parte crítica do processo. A segurança da infraestrutura de redes foi discutida em 6 trabalhos e controle de acesso em 4. Apenas 3 trabalhos abordaram o uso de recursos de criptografia de dados e outros 2 trabalhos sobre investimentos em segurança também foram encontrados e devem ser mencionados.

Em relação aos trabalhos que citam normas ou frameworks, observa-se abaixo a classificação, no Quadro 2.

Nota-se que a norma ISO/IEC 27001 é citada em 11 estudos e a ISO/IEC 27002 é citada em 7 estudos. As normas HIPAA (com 8 citações) e ISO/IEC 27799 (com 5 citações), específicas para a saúde, aparecem na terceira e quarta colocação em relação ao número de artigos. Os *Frameworks* de alguns países como África do Sul, China e Canadá aparecem em artigos isolados. Observa-se, também, que normas criadas para o desenvolvimento de sistemas de informação, como o ISO/IEC 15026 e o

Nº	REFERÊNCIA	FOCO DO ESTUDO
1	Chi, Jones & Zhao (2008)	Controle de acesso
2	Gottberg & Pisa (2008)	Governança da segurança
3	Bava, Cacciari, Sossa, Zotti & Zangrando (2009)	Governança da segurança
4	Gleni, Maple & Yue (2009)	Criptografia de dados
5	Nemati & Church (2009)	Profissional de saúde
6	Söderström, Åhlfeldt & Eriksson (2009)	Governança da segurança
7	Sumner (2009)	Profissional de saúde
8	Ferreira (2010)	Controle de acesso
9	Narayana Samy, Ahmad & Ismail (2010)	Governança da segurança
10	Tyali & Pottas (2010)	Governança da segurança
11	Williams (2010)	Redes sociais
12	Adesina (2011)	Criptografia de dados
13	Kimura, Kobayashi, Yoshikawa & Ishihara (2011)	Controle de acesso
14	Krens, Spruit & Urbanus-Van Laar (2011)	Profissional de saúde
15	Ribas, Francisco, Yamamoto & Burattini (2011)	Governança da segurança
16	Zineddine (2011)	Governança da segurança
17	He & Johnson (2012)	Notações
18	Khansa, Cook, James & Bruyaka (2012)	Investimento em segurança
19	Liu, Chung, Chen, & Wang (2012)	Infraestrutura de rede
20	Ribas, Burattini, Massad & Yamamoto (2012)	Governança da segurança
21	Stahl, Doherty, & Shaw (2012)	Política de segurança
22	Wang, Xiao & Rao (2012)	Ferramenta de buscas
23	Zafar & Sneha (2012)	Sistemas de informação
24	Alsalamah, Gray, Hilton & Alsalamah (2013)	Controle de acesso
25	Andreeva (2013)	Dispositivos de acesso
26	Hameed & Yuchoh (2013)	Criptografia de dados
27	Hassan, Ismail & Maarop (2013)	Profissional de saúde
28	Orel & Bernik (2013)	Governança da segurança
29	Son, Kim, Park, Cha, & Park (2013)	Dispositivos médicos
30	Van Deursen, Buchanan, & Duff (2013)	Profissional de saúde
31	Agaku, Adisa, Ayo-Yusuf & Connolly (2014)	Percepção do paciente

Quadro 1: O principal foco dos 52 estudos selecionados
Fonte: Dados da Pesquisa. (continua…)

32	Huang, Behara, & Goo (2014)	Investimento em segurança
33	Mahncke & Williams (2014)	Governança da segurança
34	Vorakulpipat, Siwamogsatham, & Kawtrakul (2014)	Segurança como serviço
35	Krishna, Subrahmanyam, Anjaneyulu & Kim (2015)	Gerenciamento de riscos
36	Chen & Fu (2015)	Dispositivos wireless
37	Papoutsi, Reed, Marston, Lewis, Majeed & Bell (2015)	Percepção do paciente
38	Patel, Beckjord, Moser, Hughes, & Hesse (2015)	Infraestrutura de rede
39	Chen, Lambright, & Abdelwahed (2016)	Infraestrutura de rede
40	Agbele, Oriogun, Seluwa, & Aruleba (2016)	Infraestrutura de rede
41	Ghazvini & Shukur (2016)	Profissional de saúde
42	Hassan & Ismail (2016)	Profissional de saúde
43	Sedlack (2016)	Profissional de saúde
44	Uwizeyemungu & Poba-Nzaou (2016)	Governança da segurança
45	Chiuchisan, Balan, Geman, Chiuchisan, & Gordi (2017)	Infraestrutura de rede
46	Drevin, Kruger, Bell & Steyn (2017)	Vocabulário
47	Ghazvini & Shukur (2017)	Profissional de saúde
48	Ghazvini & Shukur (2017b)	Profissional de saúde
49	He & Johnson (2017)	Profissional de TI
50	Langer (2017)	Governança da segurança
51	Mattei (2017)	Lições aprendidas
52	Naik, Singh, Samaddar (2017)	Infraestrutura de rede

(Continuação) Quadro 1: O principal foco dos 52 estudos selecionados
Fonte: Dados da Pesquisa.

SDLC são citadas em dois trabalhos onde são abordados aspectos de segurança para esse fim.

Dessa forma, levando-se em consideração somente os frameworks com enfoque de gestão da segurança da informação, é possível observar o seguinte cenário (Quadro 3):

Observa-se, então, que somente 16 estudos citaram frameworks com enfoque na gestão da segurança da informação. Destes, somente 12 citaram a norma ISO/IEC 27799 e a norma HIPAA, específicas para a área de saúde em 10 anos de pesquisa. Isso mostra que somente 31% do total de estudos selecionados citam algum *framework* de segurança da informação, e os 69% restantes abordam controles de forma isolada.

Por fim, somente 7 desses trabalhos demonstram resultados em estudos de casos feitos em hospitais que adotaram ou estavam em processo de adoção dessas normas.

5 Discussão

Os estudos sobre a segurança da informação na área de saúde abordam um tema extremamente crítico para a sociedade atual. Alguns episódios como os problemas causados pelo *ransomware WannaCry* instiga a necessidade de novos estudos acerca da governança de segurança da informação na área da saúde, em especial.

Gottberg & Pisa (2008) mostram uma dificuldade de implantação de sistemas de gerenciamento de segurança da informação justamente pelas especificidades da área de saúde. Khansa, Cook, James & Bruyaka (2012) corroboram com essa complexidade principalmente pela insegurança que as instituições de saúde demonstram principalmente em relação aos custos de implementação. Os investimentos para a implantação de um padrão devem ser considerados e podem ser um gargalo para a adoção dessas normas (Ribas, Burattini, Massad & Yamamoto, 2012).

A partir desses indícios, este estudo buscou apresentar os artigos publicados nos últimos 10 anos em relação ao tema, permitindo uma análise do cenário mundial tratado pelos meios acadêmicos. Por meio de uma revisão sistemática da literatura, observou-se que 12 estudos abordaram a governança da segurança, sob um aspecto mais abrangente de gestão. Outro ponto importante é que 10 trabalhos focam na capacitação dos profissionais de saúde, mostrando, assim, que existe uma preocupação com o fator "pessoas", ativo importante da segurança da informação. Com isso, observa-se um cenário onde existe um enfoque mais distribuído, englobando a cultura e o treinamento dos profissionais que utilizam a infraestrutura de TI.

Porém, esse estudo demonstra um cenário preocupante: somente 16 estudos citaram *frameworks* internacionalmente reconhecidos para a gestão da segurança da informação. Isso representa somente 33% do total de

FRAMEWORK CITADO	ENFOQUE	ABRANGÊNCIA	**REFERÊNCIAS**
ISO/IEC 27001	Segurança da informação	Internacional	Bava, Cacciari, Sossa, Zotti & Zangrando (2009); He & Johnson (2012); Narayana, Ahmad e Ismail (2010); Orel & Bernik (2013); Ribas, Francisco, Yamamoto & Burattini (2011); Ribas, Burattini, Massad & Yamamoto (2012); Son, Kim, Park, Cha, & Park (2013); Tyali & Pottas (2010); Vorakulpipat, Siwamogsatham & Kawtrakul (2014); Zineddine (2011)
ISO/IEC 27002	Segurança da informação	Internacional	Gottberg & Pisa (2008); He & Johnson (2012); Orel & Bernik (2013); Ribas, Francisco, Yamamoto & Burattini (2011); Ribas, Burattini, Massad & Yamamoto (2012); Söderström, Åhlfeldt & Eriksson (2009) Zineddine (2011)
ISO/IEC 27799	Segurança da informação na saúde	Internacional	Bava, Cacciari, Sossa, Zotti & Zangrando (2009); Gottberg & Pisa (2008); Narayana, Ahmad e Ismail (2010); Orel & Bernik (2013); Tyali & Pottas (2010)
ISO/IEC 15026	Engenharia de sistemas e software	Internacional	He & Johnson (2012)
Health Insurance Portability and Accountability (HIPAA)	Segurança da informação na saúde	Estados Unidos da América	He & Johnson (2012); Khansa, Cook, James & Bruyaka (2012); Langer (2017); Nemati & Church (2009); Orel & Bernik (2013); Sedlack (2016); Son, Kim, Park, Cha, & Park (2013); Zineddine (2011)
Promotion of Access to Information Act (PAIA)	Direito de acesso à informação	África do Sul	Drevin, Kruger, Bell & Steyn (2017)
Protection of Personal Information (POPI)	Segurança da informação pessoal	África do Sul	Drevin, Kruger, Bell & Steyn (2017)
GB/T22239	Segurança da informação	China	He & Johnson (2017)
IEC 60601	Certificação de dispositivos eletromédicos	Internacional	Son, Kim, Park, Cha, & Park (2013)
Software Development Life Cicle (SDLC)	Ciclo de vida de desenvolvimento de sistemas de informação	Internacional	Zafar & Sneha (2012)
Personal Information Protection and Electronic Documents (PIPEDA)	Segurança de informação pessoal	Canadá	Zineddine (2011)

Quadro 2: Os principais frameworks identificados nos 52 estudos selecionados
Fonte: Dados da Pesquisa.

trabalhos selecionados e mostra que, em 10 anos, poucas pesquisas foram feitas sobre o tema. Outro resultado importante, diz respeito às normas específicas para a área da saúde. Somente 13 trabalhos citam as normas ISO/IEC 27799 e HIPAA, representando somente 25% dos estudos selecionados. Dessa forma, nota-se, especificamente na área de saúde, um retrato de escassez no meio acadêmico sobre a segurança da informação. A grande maioria dos estudos abordam controles de forma isolada e não possuem um enfoque completo de gestão, e, somente 7 estudos demonstram aplicação empírica em estudos de casos feitos em hospitais.

Conclui-se, então, que esse cenário de complexidade, aliado a escassez de estudos científicos, pode tornar a área

	REFERÊNCIA / FRAMEWORK ABORDADO	ISO/IEC 27001	ISO/IEC 27002	ISO/IEC 27799	HIPAA
1	Bava, Cacciari, Sossa, Zotti & Zangrando (2009)	x	-	x	-
2	He & Johnson (2012)	x	x	-	x
3	Gottberg & Pisa (2008)	-	x	x	
4	Khansa, Cook, James & Bruyaka (2012)	-	-	-	x
5	Langer (2017)	-	-	-	x
6	Narayana, Ahmad e Ismail (2010)	x	-	x	-
7	Nemati & Church (2009)	-	-	-	x
8	Orel & Bernik (2013)	x	x	x	x
9	Ribas, Francisco, Yamamoto & Burattini (2011)	x	x	-	-
10	Ribas, Burattini, Massad & Yamamoto (2012)	x	x	-	-
11	Sedlack (2016)	-	-	-	x
12	Son, Kim, Park, Cha, & Park (2013)	x	-	-	x
13	Söderström, Åhlfeldt & Eriksson (2009)		x	-	-
14	Tyali & Pottas (2010);	x	-	x	-
15	Vorakulpipat, Siwamogsatham & Kawtrakul (2014)	x	-	-	-
16	Zineddine (2011)	x	x	-	x

Quadro 3: Os artigos que abordam os frameworks de segurança da informação

Fonte: Dados da Pesquisa.

de saúde suscetível a incidentes de segurança da informação, como ocorreu recentemente. Pouca pesquisa foi produzida nos últimos 10 anos, e isso evidencia, inclusive, a falta de validação empírica dessas implementações. Além disso, os trabalhos selecionados foram feitos, em sua maioria, em países desenvolvidos ou em grandes hospitais, deixando uma lacuna no contexto de países em desenvolvimento ou hospitais de pequeno porte - fato também observado por Vorakulpipat, Siwamogsatham & Kawtrakul (2014).

O presente trabalho não buscou esgotar a discussão e contou ainda, como limitação, a possível subjetividade presente em uma das fases de seleção a RSL (inerente ao método) referente a escolha das bases de artigos acessadas. Como trabalho futuro, pretende-se descrever os frameworks aplicados a partir de pesquisa de campo em hospitais ou centros de saúde brasileiros.

Referências

Adesina, Ademola O., Agbele, Kehinde K., Februarie, Ronald, Abidoye, Ademola P., & Nyongesa, Henry O.. (2011). Ensuring the security and privacy of information in mobile health-care communication systems. *South African Journal of Science*, *107*(9-10), 27-33. Retrieved March 25, 2018, from http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S0038-23532011000500012&lng=en&tlng=en.

Abbas, H., Maennel, O., & Assar, S. (2017). Security and privacy issues in cloud computing. https://doi.org/10.1007/s12243-017-0578-3

Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2013). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal of the American Medical Informatics Association*, *21*(2), 374-378. https://doi.org/10.1136/amiajnl-2013-002079

Agbele, K. K., Oriogun, P. K., Seluwa, A. G., & Aruleba, K. D. (2015, November). Towards a model for enhancing ICT4 development and information security in healthcare system. In *Technology and Society (ISTAS), 2015 IEEE International Symposium on* (pp. 1-6). IEEE. https://doi.org/10.1109/ISTAS.2015.7439404

Alsalamah, S., Gray, W. A., Hilton, J. C., & Alsalamah, H. (2013). Information security requirements in patient-centred healthcare supporting systems. http://dx.doi.org/10.3233/978-1-61499-289-9-812

Andreeva, E. (2013). Information security of healthcare systems: using a biometric approach. *Modelling in Medicine and Biology X*, *17*, 109.

Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management*, *6*(4), 279-314.

Bava, M., Cacciari, D., Sossa, E., Zotti, D., & Zangrando, R. (2009, July). Information security risk assessment in healthcare: the experience of an Italian Paediatric Hospital. In *Computational Intelligence, Communication Systems and Networks, 2009. CICSYN'09. First International Conference on*(pp. 321-326). IEEE. http://dx.doi.org/10.1109/CICSYN.2009.14

CANADÁ. The Personal Information Protection and Electronic Documents Act (PIPEDA) 2000. Retrieved March 25, 2018, from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Chen, Q., Lambright, J., & Abdelwahed, S. (2016, June). Towards Autonomic Security Management of Healthcare Information Systems. In *Connected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on* (pp. 113-118). IEEE. http://dx.doi.org/10.1109/CHASE.2016.58

Chi, H., Jones, E. L., & Zhao, L. (2008, December). Implementation of a security access control model for inter-organizational healthcare information systems. In *Asia-Pacific Services Computing Conference, 2008. APSCC'08. IEEE* (pp. 692-696). IEEE. http://dx.doi.org/10.1109/APSCC.2008.256

Chiuchisan, I., Balan, D. G., Geman, O., Chiuchisan, I., & Gordin, I. (2017, June). A security approach for health care information systems. In *E-Health and Bioengineering Conference (EHB), 2017* (pp. 721-724). IEEE. http://dx.doi.org/10.1109/EHB.2017.7995525

Drevin, L., Kruger, H., Bell, A. M., & Steyn, T. (2017, May). A Linguistic Approach to Information Security Awareness Education in a Healthcare Environment. In *IFIP World Conference on Information Security Education* (pp. 87-97). Springer, Cham. https://doi.org/10.1007/978-3-319-58553-6_8

EEUU. Health Insurance Portability and Accountability Act of 1996. Retrieved March 25, 2018, from https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

EEUU. American Recovery and Reinvestment Act. 2009. Retrieved March 25, 2018, from http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=111_cong_bills&docid=f:h1enr.pdf

EEUU. DEPARTMENT OF HEALTH AND HUMAN SERVICES et al. HITECH Act enforcement interim final rule. US Department of, 2009. Retrieved March 25, 2018, from https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html

Fatima, S. I., & Auti, R. A. (2017). Multi-Level Privacy-Preserving Patient Self-Controllable algorithm Healthcare in Cloud. *INTERNATIONAL JOURNAL*, *2*(9).

Fernando, J. I., & Dawson, L. L. (2009). The health information system security threat lifecycle: An informatics theory. *International Journal of Medical Informatics*, *78*(12), 815-826.

Ferreira, A., Antunes, L., Chadwick, D., & Correia, R. (2010). Grounding information security in healthcare. *International Journal of Medical Informatics*, *79*(4), 268-283. https://doi.org/10.1016/j.ijmedinf.2010.01.009

Gbadeyan, A., Butakov, S., & Aghili, S. (2017). IT governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider. *Annals of Telecommunications*, *72*(5-6), 347-357. https://doi.org/10.1007/s12243-017-0568-5

Ghazvini, A., & Shukur, Z. (2016). Awareness Training Transfer and Information Security Content Development for Healthcare Industry. *INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS*, *7*(5), 361-370.

Ghazvini, A., & Shukur, Z. (2017, November). Review of information security guidelines for awareness training program in healthcare industry. In *Electrical Engineering and Informatics (ICEEI), 2017 6th International Conference on* (pp. 1-6). IEEE. https://doi.org/10.1109/ICEEI.2017.8312399

Ghazvini, A., & Shukur, Z. A Framework for an Effective Information Security Awareness Program in Healthcare.

Gleni, S., Maple, C., & Yue, Y. (2009, April). Security issues of a biometrics health care information system: the case of the NHS. In *Computing, Engineering and Information, 2009. ICC'09. International Conference on* (pp. 279-284). IEEE. https://doi.org/10.1109/ICC.2009.64

Gottberg, H.; Pisa, I. T.; Leão, B. (2008) Dealing with the Complexities when Implementing Information Security Practices in Healthcare Organizations. In: *HEALTHINF (1).* (pp. 205-208).

Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., & Müller, G. (2011). Aspects of privacy for electronic health records. *International journal of medical informatics*, *80*(2), e26-e31. https://doi.org/10.1016/j.ijmedinf.2010.10.001

Hameed, S. A., & Yuchoh, H. (2012, November). Toward Managing Security Cost for Healthcare Information. In *Advanced Computer Science Applications and Technologies (ACSAT), 2012 International Conference on* (pp. 414-418). IEEE. https://doi.org/10.1109/ACSAT.2012.75

Hassan, N. H., & Ismail, Z. (2016). INFORMATION SECURITY CULTURE IN HEALTHCARE INFORMATICS: A PRELIMINARY INVESTIGATION. *Journal of Theoretical & Applied Information Technology*, *88*(2).

Hassan, N. H., Ismail, Z., & Maarop, N. (2013, November). A conceptual model for knowledge sharing towards information security culture in healthcare organization. In *Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on* (pp. 516-520). IEEE. https://doi.org/10.1109/ICRIIS.2013.6716762

He, Y., & Johnson, C. (2017). Challenges of information security incident learning: An industrial case study in a Chinese healthcare organization. *Informatics for Health and Social Care*, *42*(4), 393-408. https://doi.org/10.1080/17538157.2016.1255629

He, Y., & Johnson, C. W. (2012). Generic security cases for information system security in healthcare systems. http://dx.doi.org/10.1049/cp.2012.1507

Hoyt, R. E., & Yoshihashi, A. K. (2014). *Health informatics: practical guide for healthcare and information technology professionals*. Lulu. com.

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: An economic analysis. *Decision Support Systems*, *61*, 1-11. https://doi.org/10.1016/j.dss.2013.10.011

ISO/TC 215 Health informatics. Retrieved March 25, 2018, from https://www.iso.org/committee/54960.html.

ISO 27001. Information Technology, Security Techniques, Information Security Management Systems, Requirements, *International Organization for Standardization ISO*, Geneve, 2005.

ISO 27002. Information Technology, Security Techniques, Code of Practice for Information Security Management, *International Organization for Standardization ISO*, Geneve, 2005.

ISO 27799. Information security management in health using ISO/IEC 27002, *International Organization for Standardization ISO*, Geneve, 2008.

Khansa, L., Cook, D. F., James, T., & Bruyaka, O. (2012). Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *computers & security*, *31*(6), 750-770. https://doi.org/10.1016/j.cose.2012.06.007

Kimura, E., Kobayashi, S., Yoshikawa, T., & Ishihara, K. (2011, July). A framework for an authorization system with spatial reasoning capacity to improve risk management and information security in healthcare. In *Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on* (pp. 587-591). IEEE. https://doi.org/10.1109/SAINT.2011.109

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(2004), 1-26.

Krens, R., Spruit, M. R., & Urbanus-van Laar, N. (2011, January). Information Security in Health Care-Evaluation with Health Professionals. In *HEALTHINF* (pp. 61-69).

Krishna, B. C., Subrahmanyam, K., Anjaneyulu, S. S. N., & Kim, T. H. (2015). A novel Dr. KSM approach for information security and risk management in health care systems. *International Journal of Bio-Science and Bio-Technology*, *7*(4), 11-16. http://dx.doi.org/10.1155/2015/852173

Langer, S. G. (2017). Cyber-Security Issues in Healthcare Information Technology. *Journal of digital imaging*, *30*(1), 117-125. https://doi.org/10.1007/s10278-016-9913-x

Liu, C. H., Chung, Y. F., Chen, T. S., & Wang, S. D. (2012). The enhancement of security in healthcare information systems. *Journal of medical systems*, *36*(3), 1673-1688. https://doi.org/10.1007/s10916-010-9628-3

Mahncke, R. J., & Williams, P. A. (2014). Developing and Validating a Healthcare Information Security Governance Framework.

Maseti, O. S. (2008). A model for role-based security education, training and awareness in the South African healthcare environment.

Mattei, T. A. (2017). Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack. *World neurosurgery*, *104*, 972-974.

Meingast, M., Roosta, T., & Sastry, S. (2006, August). Security and privacy issues with health care information technology. In *2006 International Conference of the IEEE Engineering in Medicine and Biology Society* (pp. 5453-5458). IEEE.

Naik, B. B., Singh, D., Samaddar, A. B., & Lee, H. J. (2017, February). Security attacks on information centric networking for healthcare system. In *Advanced Communication Technology (ICACT), 2017 19th International Conference on*(pp. 436-441). IEEE. https://doi.org/10.23919/ICACT.2017.7890126

Narayana Samy, G., Ahmad, R., & Ismail, Z. (2010). Security threats categories in healthcare information systems. *Health informatics journal*, *16*(3), 201-209. https://doi.org/10.1177%2F1460458210377468

Nemati, H. R., & Church, M. (2009). A human centered framework for information security management: a healthcare perspective. *AMCIS 2009 Proceedings*, 591.

Orel, A., & Bernik, I. (2013). Implementing Healthcare Information Security: Standards Can Help. *Data and Knowledge for Medical Decision Support. B. Blobel, A. Hasman and J. Zvarova. Amsterdam, European Federation for Medical Informatics*, 195-199.

Papoutsi, C., Reed, J. E., Marston, C., Lewis, R., Majeed, A., & Bell, D. (2015). Patient and public views about the security and privacy of Electronic Health Records (EHRs) in the UK: results from a mixed methods study. *BMC medical informatics and decision making*, *15*(1), 86. https://doi.org/10.1186/s12911-015-0202-2

Patel, V., Beckjord, E., Moser, R. P., Hughes, P., & Hesse, B. W. (2015). The role of health care experience and consumer information efficacy in shaping privacy and security perceptions of medical records: national consumer survey results. *JMIR medical informatics*, *3*(2). https://dx.doi.org/10.2196%2Fmedinform.3238

PONEMON INSTITUTE. Data Breach: The Cloud Multiplier Effect. 2014. Retrieved March 25, 2018, from http://go.netskope.com/rs/665-KFP-612/images/Ponemon-DataBreach-CloudMultiplierEffect-June2014.pdf.

Ribas, C. E.; Burattini, M. N.; Massad, E.; Yamamoto, J. F. (2012). Information Security Management System-A Case Study in a Brazilian Healthcare Organization. In: *HEALTHINF*. (pp. 147-151).

Ribas, C. E., Francisco, A. J. F., Yamamoto, J. F., & Burattini, M. N. (2011). A New Approach to Information Security Assessment: a case study in a Brazilian healthcare organization.

Sahibudin, S., Sharifi, M., & Ayat, M. (2008, May). Combining ITIL, COBIT and ISO/IEC 27002 in order to design a comprehensive IT framework in organizations. In *Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on* (pp. 749-753). IEEE. https://doi.org/10.1109/AMS.2008.145

Sedlack, D. (2016). Understanding Cyber Security Perceptions Related to Information Risk in a Healthcare Setting.

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2017). Service resizing for quick DDoS mitigation in cloud computing environment. *Annals of Telecommunications*, *72*(5-6), 237-252. https://doi.org/10.1007/s1224

Söderström, E., Åhlfeldt, R. M., & Eriksson, N. (2009). Standards for information security and processes in healthcare. *Journal of Systems and Information Technology*, *11*(3), 295-308. https://doi.org/10.1108/13287260910983650

Son, J., Kim, S., Park, G., Cha, J., & Park, K. (2013). Security requirements for the medical information used by U-Healthcare medical equipment. *International Journal of Security and Its Applications*, *7*(1), 169-180.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal*, *22*(1), 77-94. https://doi.org/10.1111/j.1365-2575.2011.00378.x

Sumner, J., Liberman, A., Rotarius, T., Wan, T. T., & Eaglin, R. (2009). Health Care Communication Networks: Disseminating Employee Information for Hospital Security. *The health care manager*, *28*(4), 287-298. https://doi.org/10.1097/HCM.0b013e3181bdec73

Tipton, H. F. (2007). *Official (ISC) 2 guide to the ISSMP CBK*. CRC Press.

Tritilanunt, S., & Tongsrisomboon, A. (2014). Risk analysis and security management of IT information in hospital. *Int J Comput Inform Technol*, *4*(3), 1-9.

Tyali, S., & Pottas, D. (2011). Information Security Management Systems in the Healthcare Context. In *Proceedings of the South African Information Security Multi-Conference: Port Elizabeth, South Africa, 17-18 May 2010* (p. 177). Lulu. com.

Uwizeyemungu, S., & Poba-Nzaou, P. (2016). Security and Privacy Practices in Healthcare Information Systems: A Cluster Analysis of European Hospitals. In *ICISSP* (pp. 37-45).

Van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *computers & security*, *37*, 31-45. https://doi.org/10.1016/j.cose.2013.04.005

Vorakulpipat, C., Siwamogsatham, S., & Kawtrakul, A. (2014). An investigation of information security as a service practice: case study in healthcare. *International Journal of Computer Applications in Technology*, *49*(3-4), 365-371. https://doi.org/10.1504/IJCAT.2014.062372

Wang, J., Xiao, N., & Rao, H. R. (2012). An exploration of risk information search via a search engine: Queries and clicks in healthcare and information security. *Decision Support Systems*, *52*(2), 395-405. https://doi.org/10.1016/j.dss.2011.09.006

Warren, B. (2005). Identity theft prevention in the healthcare setting. *Journal of healthcare protection management: publication of the International Association for Hospital Security*, *21*(1), 101-111.

Williams, J. (2010, May). Social networking applications in health care: threats to the privacy and security of health information. In *Proceedings of the 2010 ICSE workshop on software engineering in health care* (pp. 39-49). ACM. https://doi.org/10.1145/1809085.1809091

Zafar, H., & Sneha, S. (2012). Ubiquitous Healthcare Information System: Toward Crossing the Security Chasm. *Communications of the Association for Information Systems*, *31*.

Zineddine, M. (2011, December). Automated healthcare information privacy and security: UAE case. In *Internet Technology and Secured Transactions (ICITST), 2011 International Conference for* (pp. 592-595). IEEE.