Revista Gestão.Org, v. 13, Edição Especial, 2015. p. 396-401
ISSN 1679-1827
http://www.revista.ufpe.br/gestaoorg

A Importância da Segurança da Informação no Ambiente Digital Para a Saúde

The Importance of Information Security in The Environment Digital Health

Gisele Martins Sá Alves[1], Márcia Valéria Rocha de Souza[1], Plinio Manoel Oliveira Silva[1]

[1]Centro de Estudo e Sistemas Avançados do Recife, CESAR, Brasil

Correspondência: Gisele Martins Sá Alves, Endereço: Rua Blone, 220 Cais do Apolo, Bairro do Recife CEP 50.030-390, Recife, PE Brasil. E-mail: gisinha87@gmail.com

Recebido: 14 de outubro de 2015 Aceito: 26 de março de 2016 Publicado: 09 de maio de 2016

Resumo

A utilização dos recursos de tecnologia para comunicação e informação tem sido fortemente aplicados em diferentes setores econômicos e sociais. O setor de saúde também foi um dos contemplados. As informações, antes armazenadas apenas em papéis, hoje são disponibilizadas de maneira digital. Este formato impactou positivamente para a divulgação e compartilhamento desses dados com a finalidade de informatizar o processo de gerência de saúde, principalmente entre as organizações mundiais como a WHO. Para que essa interação fosse realizada, surgiu a necessidade de uma padronização na comunicação dos dados de saúde entre sistemas interoperáveis. E graças a isso, alguns padrões/ protocolos foram criados e adotados para diferentes setores de saúde. Porém, observando que as informações de saúde pudessem ser expostas, adulteradas e corrompidas, foi destacada a importância da segurança na comunicação e no compartilhamento dos dados entre os sistemas de saúde. A não preocupação poderia acarretar danos irreversíveis aos usuários finais do sistema por se tratar de informações pertinentes, principalmente, de pacientes. Como consequência desta preocupação, tecnologias de segurança foram surgindo. Neste artigo serão apresentados alguns dos protocolos utilizados mundialmente para troca de informações e as principais tecnologias de segurança digital, sua utilização e importância para os sistemas interoperáveis de saúde.

Palavras-chave: eHealth; Segurança da Informação; Padrão de Comunicação; HL7; FHIR.

Abstract

The use of advances in technology resources for communication and information has been strongly applied in different economic and social sectors. The health sector was also one of contemplated. The information before stored only on paper, are now available in digital form. This format impacted positively to the dissemination and sharing of such data in order to computerize the health management process, especially among the world organizations such as the WHO. For this interaction was held, the need for standardization in communication of health data between interoperable systems. And because of this, some standards / protocols have been created and adopted to different health sectors. However, noting that health information could be exposed, adulterated and corrupted, was highlighted the importance of security in communication and data sharing between health systems. Not to worry could cause irreversible damage to end users of the system because it is relevant information, mainly from patients. As a result of this concern, several security technologies have emerged. This article will present some of the protocols used worldwide to exchange information and key digital security technologies, their use and importance for interoperable health systems.

Keywords: eHealth; Information Security; Communication Standard; HL7, FHIR.

1. Introdução

O avanço e o surgimento de novos recursos tecnológicos trouxeram inúmeras possibilidades para a aplicação da tecnologia em diferentes setores econômicos e sociais, entre eles destacaremos neste trabalho o do setor da saúde.

Um exemplo de como o avanço tecnológico atingiu essa área foi a criação do eHealth, onde segundo a World Health Organization - WHO (2015), a sua definição é todo e qualquer uso das tecnologias de comunicação e informação para a saúde.

As unidades de saúde trabalham com parceiros a nível global, regional e nacional para promover e fortalecer a utilização de tecnologias de informação e comunicação no desenvolvimento da saúde, a partir de aplicações no campo da governança global World Health Organization - WHO (2015). Ferreira e Lopes (2013) afirmam que dados são processados gerando informações que serão analisadas com o objetivo de aumentar o conhecimento específico dos negócios em saúde, porém, este conhecimento torna-se útil quando apoia decisões, sejam elas em relação ao diagnóstico ou plano terapêutico de um paciente ou em relação à gestão do estabelecimento ou do sistema de saúde.

Diante da possibilidade das agências mundiais de saúde manipularem digitalmente as informações nos diversos setores, fez-se necessário a criação de padrões de comunicação mundial para facilitar a comunicação entre os sistemas interoperáveis de saúde. Através destes padrões, foi possível viabilizar a troca de informações entre as organizações mundiais facilitando a compreensão das mesmas.

Mendes et al. (2009), informou que políticas de padrões de informação e informática em saúde estão em discussão em países como Inglaterra, Austrália, Canadá e Estados Unidos. Entre os serviços que estes países oferecem estão: a implantação de padrões como identificação única para cidadãos e prestadores de serviço e intercâmbio eletrônico de informação, regras nacionais para a informatização da saúde, adoção de políticas nacionais para uso dos padrões de informação em saúde. No Brasil a Agência de Saúde Suplementar (ANS) estabeleceu o TISS como padrão para Troca de Informações em Saúde Suplementar.

Para Petry et al. (2006), dentre os principais padrões internacionais está o HL7, projetado para enviar mensagens englobando todo domínio de saúde e apresentam um nível de interoperabilidade semântica, onde os sistemas são capazes de compartilharem informações compreendidas através da definição de conceitos de domínio. Meingast et al. (2006) afirma que é recomendável que o uso dessas mesmas tecnologias, utilizadas para melhorar a qualidade da prestação de cuidados de saúde, garantam a privacidade e a segurança do usuário de saúde. As informações dos pacientes também estão sujeitas a ataques que podem ferir a integridade dos dados, já que está disponível por via eletrônica. Por isso o acesso aos dados, armazenamento e integridade são os principais desafios enfrentados pela indústria.

No entanto, Sharma et al. (2001) diz que o avanço tecnológico na área de saúde trouxe para o setor novos desafios em segurança e privacidade dos dados. Confirmando o posicionamento de Meingast et al. (2006) quando informou que garantir a privacidade e integridade dessas informações é fundamental, visto que a manipulação delas implica em questões de princípios éticos, médicos e socais.

Neste artigo serão analisadas questões de confiabilidade, privacidade e segurança no compartilhamento de dados entre os sistemas de saúde. O objetivo da pesquisa é realizar um levantamento das soluções existentes de segurança digital utilizadas na indústria. Na segunda seção será descrita a importância da utilização dos recursos digitais em saúde e os modelos e protocolos de comunicação para o setor. Na terceira seção serão discutidas questões de segurança digital e sua utilização no sistema de saúde. Na quarta seção abordaremos as principais soluções existentes para segurança digital que fornecem uma base aceitável no contexto de eHealth. Na quinta seção serão apresentadas sugestões para desenvolvimento no setor e por fim, na sexta seção, apresentaremos as conclusões deste trabalho.

2. Utilização dos recursos digitais em saúde

2.1. E-Health

Inevitavelmente os setores de saúde aderiram aos avanços tecnológicos investindo em tecnologia e comunicação integrando-as nos seus modelos de negócios.

O WHO define eHealth como a utilização de tecnologias da informação e comunicação para fins de saúde. Estas tecnologias estão sendo aperfeiçoadas para melhorar o fluxo de informações por meios eletrônicos com o objetivo de prestar serviços de saúde e gestão do sistema de saúde. O principal objetivo é que essas mudanças possam ser refletidas à todos cidadãos com igualdade e cuidados de alta qualidade, principalmente em ações humanitárias na área de saúde pública a nível global. O reflexo dessas mudanças está nos inúmeros sistemas que atendem o setor de saúde como, por exemplo, os que têm como objetivo melhorar a qualidade do atendimento do paciente ou sistemas que podem identificar epidemias, surtos em tempo real.

As principais agências das nações unidas para a saúde e telecomunicações, respectivamente, a World Health Organization (WHO) e a União Internacional das Telecomunicações (UTI), reconheceram a importância da colaboração para a saúde nas resoluções dos seus órgãos diretos e incentiva os países a desenvolverem estratégicas nacionais de eHealth. Dentre elas, para assegurar a qualidade e segurança, há investimento em interoperabilidade e política de privacidade e segurança da informação. Para alcançar o objetivo, são

desenvolvidas ferramentas que atendam as necessidades das agências mundiais de saúde. Piette et al. (2012) comentam que as ferramentas de eHealth são projetadas para melhorar a vigilância da saúde, gestão de sistemas de saúde, educação em saúde e de tomada de decisão clínica, e apoiar mudanças de comportamento relacionadas com as prioridade de saúde pública e gestão de doença. Dentre elas estão os padrões de mensagem entre sistemas interoperáveis.

2.2 Padrões de Comunicação para saúde

Devido à importância e necessidade na troca de informações, foi necessário que houvesse uma padronização das mensagens enviadas entre os sistemas interoperáveis. Dentre os padrões estudados neste trabalho estão os padrões internacionais HL7, FHIR e o brasileiro TISS.

O HL7 foi desenvolvido pela Health Level Seven, uma organização sem fins lucrativos, com a finalidade de propor um modelo de informação que pudesse representar o ambiente de saúde. Segundo Petry et al. (2006), o HL7 definiu uma estrutura de mensagens que representam informações clínicas, administrativas e financeiras consideradas fundamentais em um ambiente hospitalar. Foi projetado para enviar mensagem englobando todo domínio de saúde. Sua missão é capacitar interoperabilidade de dados de saúde global através do desenvolvimento de normas e permitindo a sua adoção e implementação como referenciado no site HL7 (2015). Este conjunto de normas internacionais estão concentradas na camada 7 de aplicação, a mais elevada do modelo OSI. Conforme Tran et al. (2007), o propósito não é fornecer uma solução de rede, mas apoiar a funcionalidade "plug-and-play" ao integrar dois ou mais sistemas de computador em um, unificando o sistema de informação em saúde.

Segundo Bender e Sartipi (2013), o FHIR é a ultima e mais atualizada versão do HL7 até o momento e trouxe uma nova abordagem para troca de informações de saúde. Foi baseada na arquitetura Restfull e se tornou um padrão mais robusto evitando a necessidade de ferramentas complexas. Porém para Franz et al. (2015), abordagens baseadas em FHIR têm gerado preocupações relacionadas com a segurança a fim de garantir a autenticidade, autorização e a autoridade das informações.

O TISS, padrão para Troca de Informações em Saúde Suplementar, foi estabelecido pela Agência de Saúde Suplementar (ANS) e tem o objetivo de padronizar as trocas eletrônicas de informações administrativas e financeiras entre as operadoras e prestadoras de saúde. Entretanto, os autores Petry et al. (2006) apontaram algumas deficiências, como não disponibilizar acesso ao modelo formal de validação de dados e apesar de sua estrutura ser simplificada, há pouco interesse na sua disseminação. Todavia, o TISS permite a comunicação com outros sistemas de informação em saúde existentes por que ele utiliza padrões disponíveis pelos bancos de dados e sistemas da Agência e do Ministério da Saúde.

3. Segurança digital em e-health

Com o desenvolvimento dos protocolos de comunicação, surgiu uma grande preocupação com o tratamento dos dados, segurança das informações; preocupações a respeito da segurança dos dados de saúde dos indivíduos em ser acidentalmente exposto ou vazado partes não autorizadas segundo a EUROPEAN COMMISSION (2014). A mesma afirma ainda que é importante garantir a segurança adequada tais como a criptografia de dados do paciente, mecanismos de autenticação para mitigar os riscos de segurança e controle de acesso. Também deve fornecer um terreno fértil para futuros projetos de investigação e inovação garantindo que novas tecnologias possam surgir para resolver novos problemas de segurança. Em um levantamento realizado por Meingast et. al (2006), também foram apresentadas como soluções existentes com o objetivo de atender necessidades de privacidade e segurança em eHealth a aplicação de técnicas de criptografia, controle de acesso baseados em função e mecanismos de autenticação. Porém Anderson (2001), afirma que a segurança da informação não pode ser resumida apenas a medidas técnicas como, por exemplo, os modelos de controle de acesso, protocolos e criptografia. O autor toma como base diversos acontecimentos onde informações confidenciais tornaram-se públicas graças a falta de competência ou ética de seus responsáveis. Sharma et al. (2012) reforça apresentando a confiabilidade das pessoas como um dos fatores determinantes no levantamento de riscos em segurança da informação. Sharma et al. (2012) também apresenta a computação em nuvem, outra abordagem em crescimento na utilização de recursos digitais para saúde e enfatiza que nesse cenário já é possível observar novos desafios para segurança e afirma que os modelos tradicionais de segurança não podem ser inteiramente aplicados neste tipo de cenário.

Warren (2011) apresenta em seu estudo a confidencialidade, integridade e disponibilidade dos dados, como atributos de segurança da informação essenciais para eHealth, fatores como segurança física, riscos e privacidade para os pacientes foram determinantes para o levantamento do que seria fundamental no setor. O autor ainda justifica os atributos citados anteriormente apresentando o fato do setor de saúde lidar com informações extremamente sensíveis e individuais, onde qualquer vazamento de informação prejudicaria a privacidade do paciente ou um eventual diagnóstico errado causado por algum dado acidentalmente modificado. O resultado

poderia causar sérios danos, possivelmente irreversíveis, ao paciente final envolvido e até mesmo à equipe médica responsável.

Lidar com segurança digital para a área de saúde está além da comunicação privada e troca de informações de forma segura, pessoas estão diretamente envolvidas, e assim a garantia de segurança no setor não apenas preserva a privacidade e individualidade, acima de tudo contribui em resguardar a vida dos envolvidos.

Existe uma grande preocupação no acesso, armazenamento e análise dos dados em ambientes multiusuários, então algumas técnicas são utilizadas para garantir que haja segurança. Em redes convencionais, mensagem de autenticidade, integridade, e confidencialidade é geralmente obtido pelos mecanismos de segurança, como SSH, SSL e o Auth porque o padrão de tráfego dominante é a comunicação end-to-end.

De acordo com Karlof et al. (2004), um protocolo de segurança da camada de enlace poderá satisfazer pelo menos três propriedades básicas de segurança como o controle de acesso, integridade de mensagem e confidencialidade mensagem. No controle de acesso o protocolo de camada de ligação evita a não autorizada participação na rede e deverá ser capaz de detectar as mensagens não autorizadas e rejeitá-las. Intimamente relacionada com mensagem de autenticidade, a integridade é a modificação de uma mensagem de um remetente autorizado enquanto ela está em trânsito, o receptor deve ser capaz de detectar este adulteração. A confidencialidade é a preservação das informações, por meio de criptografia, de pessoas não autorizadas. A criptografia deve não só permitir a recuperação da mensagem, mas também evitar que adversários interceptem as informações. Em seu trabalho, Meingast et al. (2006) afirmaram também que a criptografia pode ser utilizada para garantir a segurança dos dados.

4. Soluções existentes para segurança digital

A garantia de integridade e privacidade das informações em saúde é indispensável. A seguir apresentaremos mecanismos de segurança digital que unidos atendem de forma bastante aceitável as necessidades em segurança para a troca de informações entre sistemas interoperáveis de saúde.

Controle de Acesso é um dos recursos que podem evitar o alcance não autorizado à informações privadas. É através dele, via autenticação de usuário, que poder ser solicitado palavras-chave, que se podem agregar recursos como Sistemas Biométricos, Cartões Inteligentes ou Assinaturas Digitais. Martins et al (2005) afirma que é preciso atender ao princípio de menor privilégio e todo pedido de acesso deve ser documentado.

Assinatura digital consiste em um conjunto de dados criptografados, associados a um documento do qual são uma função através de mecanismos de certificação, essa abordagem garante a autenticidade do documento associado, mas não a sua confidencialidade. Portanto a necessidade da utilização de mecanismos de autenticação, juntamente com assinatura digital tornam-se uma abordagem bastante aceitável para Gandini et al.(2001).

Funções de Hashing ou checagem tem o objetivo de garantir a integridade das informações. Garante a integridade através de comparação entre os resultados da origem com os divulgados, explica Ferro (2003).

Protocolos de comunicação segura, todas as abordagens citadas anteriormente podem trafegar seus dados utilizando protocolos de comunicação seguros como, por exemplo, o SSL.

Mecanismo Honeypot consiste em propositalmente simular falhas de segurança, fazendo um invasor pensar que esteja de fato explorando uma vulnerabilidade do sistema, essa abordagem acaba se tornando uma espécie de armadilha para os invasores segundo Krawetz (2004), mas é importante lembra que essa abordagem não oferece nenhum tipo de segurança e não deve ser utilizada com o objetivo de substituir algum dos mecanismos apresentados anteriormente.

O quadro abaixo apresenta a relação entre atributos de segurança essenciais em eHealth e tecnologias aplicadas a segurança da informação apresentadas anteriormente.

Soluções em Segurança	Privacidade	Integridade	Transmissão Segura de dados
Controle de Acesso	X		
Assinatura Digital	X		
Hashing		X	
Protocolos de Comunicação seguros			X

Quadro 1 – Relação entre atributos de segurança essenciais em eHealth e tecnologias aplicadas a segurança da informação.

5. Trabalhos futuros

Embora tenhamos observado alguns recursos que trouxeram avanços para segurança digital, contribuindo de maneira bastante significativa também no setor de saúde, acreditamos que as seguintes melhorias contribuiriam ainda mais para a evolução da troca de informações entre sistemas interoperáveis de saúde.

Definição de um único padrão de comunicação: Como foi observado, existem algumas iniciativas com o objetivo de contribuir para a melhoria da comunicação entre sistemas de saúde, projetos como o HL7, TISS e o openEHR trouxeram para o eHealth facilidades na comunicação entre sistemas. Infelizmente não existe uma regra sobre qual padrão utilizar, e as empresas que desenvolvem soluções em software ficam inteiramente livres, e alguns problemas acabam surgindo quando sistemas distintos necessitam realizar adaptações para realizar o compartilhamento dessas informações, gerando um esforço que poderia ser evitado se todos os desenvolvedores da área aplicassem o mesmo padrão.

Definição obrigatória para implementação dos padrões de comunicação: Padrões como HL7 FHIR recomendam a utilização de REST, mas não impedem que desenvolvedores utilizem outras abordagens, entidades como a WHO poderiam exigir a aplicação de um único padrão de implementação, contribuindo para uma política de desenvolvimento madura.

6. Conclusão

A tecnologia permitiu que o registro e o compartilhamento de informações realizado em formato eletrônico e digital, mas necessidades para a segurança dessas informações surgiram com a possibilidade da adulteração desses dados.

Neste artigo discutimos a importância da segurança digital para o setor de eHeatlh e foram apresentadas questões de privacidade, integridade, atributos essenciais para qualquer ferramenta de software interessada em lidar com informações de saúde. Apresentamos soluções existentes que atendem os atributos levantados e sugerimos soluções futuras para o amadurecimento do desenvolvimento digital dos sistemas de interoperabilidade para saúde.

Referências

ANDERSON, R. Why Information Security is Hard – An Economic Perspective. **Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual. IEEE**, v. 17, p. 358 365, 2001. Disponível em: <http://ieeexplore.ieee.org/xpl/freeabs_all.jsp%3Freload=true%26arnumber=991552>. Acessado em: 02 jul. 2015.

BENDER, D.; SARTIPO, K. HL7 FHIR: An Agile and RESTful Approach to Healthcare Information Exchange.

IEEE International Symposium on Computer-Based Medical Systems ,Porto, v.26, p.326 331 492, 2013.

Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6627810>. Acessado em: 10 jul.

2015.

EUROPEAN COMMISSION. Green paper on mobile Health ("mHealth"), **European Commission.** version 219 final, Brussels, 2014. Disponível em: <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=5147>. Acessado em: 12 jul 2015.

FERREIRA, D. P.; LOPES, P. R. L. Padrões de Normatização em Informática em Saúde. **Especialização em Informática em Saúde**, Cuiabá. Disponível em: <http://www.cee78is.org.br/Downloads/UAB-2013-Inform%C3%A1tica-em-Sa%C3%BAde-Padroes-em-IS.pdf>. Acessado em: 7 jul. 2015.

FERRO, W. R. Comércio eletrônico e a segurança da rede: uma visão tecnológica. **Seminários em Administração FEA - USP**, 2003. Disponível em:

<http://150.162.138.5/portal/sites/default/files/anexos/27416-27426-1-PB.pdf>. Acessado em: 11 jul 2015.

FRANZ, B.; SCHULER, A.; KRAUSS, O. Applying FHIR in an Integrated Health Monitoring System. **European Journal for Biomedical Informatics**, Prague, v. 11, p. 51 56, 2015. Disponível em: <http://www.ejbi.org/img/ejbi/2015/2/Franz_en.pdf>. Acessado em: 11 jul. 2015.

GANDINI, J. A. D.; SALOMÃO, D. P. S.; JACOB, C. A segurança dos documentos digitais. **Revista Jurídica, Ano 50**, n. 295, 2002. Disponıvel em <http://egov.ufsc.br/portal/sites/default/files/anexos/27250-27260-1-PB.pdf>. Acesso em: 12 jul 2015.

HEALTH LEVEL SEVEN INTERNATIONAL – Homepage, 2015. Disponível em: <http://www.hl7.org/>. Acessado em: 10 jul 2015.

KARLOF, C.; SASTRY, N.; WAGNER, D. TinySec: a link layer security architecture for wireless sensor networks. **2nd international conference on Embedded networked sensor systems**, Nova Iorque, p. 162-175, 2004. Disponível em: <http://dl.acm.org/citation.cfm?id=1031515>. Acessado em: 1 de ago. 2015.

KRAWETZ, N. Anti-honeypot technology. **Security & Privacy, IEEE 2.1 (2004)**, p. 76-79. Disponível em: <http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1264861>. Acessado em: 1 jul. 2015.

MARTINS, A. B.; SANTOS, C. A. S. Uma Metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **Revista de Gestão da Tecnologia e Sistema da Informação**, v. 2, n. 2, p. 121-136, 2005. Disponível em: <http://www.scielo.br/pdf/jistm/v2n2/02.pdf>. Acessado em: 14 jul 2015.

MEINGAST, M.; ROOSTA, T.; SASTRY, S. Security and Privacy Issues with Health Care Information Technology. **IEEE EMBS Annual International Conference,** Nova Iorque, v. 28, p. 5453 5458, 2006. Disponível em:

<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4463039&url=http%3A%2F%2Fieeexplore.ie

ee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4463039>. Acessado em: 20 jul. 2015.

MENDES, S. F.; WINTER, A. C.; WERNECK, H. F.; VIEIRA, L. E. S.; ROTZSCH, J. M. P.; DIAS, R. D. M.; UGULINO, W. C. Radar TISS - A Implantação do Padrão de Troca de Informação em Saúde Suplementar no Brasil. **Journal of Health Informatics**, v. 1, p. 61 67, 2009. Dispoível em: <http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/view/86/97>. Acessado em: 02 jul. 2015.

PETRY, K.; LOPES, P. M. A.; VON WANGENHEIN, A. Padrões para a Interoperabilidade na Saúde. **X Congresso Brasileiro de Informática em Saúde**, Florianópolis, v. 10, p. 1035 1039, 2006. Disponível em: <http://www.sbis.org.br/cbis/arquivos/961.pdf>. Acessado em: 2 ago. 2015.

PIETTE, J. D.; LUN, K. B.; MOURA, L. A.; FRASER, H. S. F.; MECHAEL, P. N.; POWELL, J.; KHOJA, S. R. Impacts of e-health on the outcomes of care in low- and middle-income countries: where do we go from here? **Bulletin of the World Health Organization**, v. 90, p. 365 372. Disponível em: <http://www.who.int/bulletin/volumes/90/5/11-099069/en/)>. Acessado em: 3 jul. 2015.

SHARMA, M; BAI, Y.; CHUNG, S.; DAI, L. Using Risk in Access Control for Cloud-Assisted eHealth. **International Conference on High Performance Computing and Communications**, Liverpool, v. 14, p. 1047 1052, 2012. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6332289>. Acessado em: 3 jul. 2015.

TRAN, T.; KIM, H.; CHO, H. A Development of HL7 Middleware for Medical Device Communication. **Software Engineering Research, Management & Applications, Busan**, v. 15, p. 485 492, 2007. Disponível em: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4296975>. Acessado em 1 jul. 2015.

WARREN, M. J. A Risk Analysis Model to Reduce Computer Security Risks among Healthcare Organizations. **Risk Management: An International Journal**, Perpetuity Press, v. 3, n. 1, p. 27 37, UK. 2000. Disponível em: <http://www.jstor.org/stable/3867742>. Acessado em: 10 jul. 2015.

WHO. World Health Organization. Suíça, 2015. eHealth Standardization and Interoperability. **World Health Organization.** WHA66.21. 2013. Disponível em: < http://apps.who.int/gb/ebwha/pdf_files/EB132/B132_R8-en.pdf >. Acessado em: 12 jul 2015.

WHO, World Health Organization. Suíça, 2015. Pacote de Ferramentas da Estratégia Nacional de eSaúde. Organização Mundial da Saúde e União Internacional das Telecomunicações. **World Health Organization.** 2012. Disponível em: <http://apps.who.int/iris/bitstream/10665/75211/13/9789248548468_por.pdf?ua=1 >. Acessado em: 12 jul 2015.