JHI JOURNAL OF HEALTH INFORMATICS

Regulação de segurança da informação eletrônica em saúde: visão geral

Safety regulation of health electronic information: an overview

Regulación de la seguridad de la información electrónica de salud: una visión general

Plinio de Sá Leitão-Júnior[1], Fábio Nogueira de Lucena[1], Renata Dutra Braga[1], Ricardo Alfredo Quintano Neira[2]

Descritores: Segurança Computacional; Regulação e Fiscalização em Saúde; Confidencialidade

RESUMO

Objetivo: Classificar os aspectos reguladores necessários ao atendimento das exigências legais de segurança de dados em Sistemas de Registro Eletrônico de Saúde (S-RES). **Método:** Estudo de revisão narrativa e qualitativo. Uma busca sistemática por artigos científicos foi realizada, seguida por pesquisa e análise de referências sobre regulamentação. **Resultados:** Cinco documentos reguladores foram selecionados, assim como as referências que estes usaram, para a produção de um dígrafo de citações. Os documentos foram avaliados sobre sua importância e contribuição. Uma categorização para seus conteúdos foi proposta. **Conclusão.** Os documentos reguladores são classificados como: (i) especificações técnicas que orientam o emprego do objeto a que se destina; (ii) regras, tais como: leis, projetos de lei, medidas provisórias, resoluções de conselhos federais de saúde, decretos e portarias; (iii) critérios de qualidade para S-RES; e (iv) políticas de gestão.

Keywords: Computer Security; Health Care Coordination and Monitoring; Confidentiality

ABSTRACT

Objective: To classify the norms required to meeting the legal requirements of data security in Electronic Health Record Systems (EHR-S). **Method:** Narrative and qualitative review of studies. A systematic search was conducted for scientific papers, followed by research and analysis of references about regulation. **Results:** Five regulatory documents were selected, and their references used for the production of a corresponding digraph. The documents were evaluated on their importance and contribution. An categorization for their content was proposed. **Conclusion:** Regulatory documents were classified as: (i) technical specification that guide the use of the object to which it refers; (ii) rule, such as law, bill, provisional measure of federal health advice resolutions, decree and order; (iii) quality criteria for EHR-S; and (iv) management policy.

Descriptores: Seguridad Computacional; Regulación y Fiscalización en Salud; Confidencialidad

RESUMEN

Objetivo: Clasificar los aspectos reguladores necesarios para cumplir con los requisitos legales de seguridad de los datos en el Sistemas de Registro de Salud Electrónicos (S-RES). **Método:** Estudio del revisión narrativa y cualitativa. Una búsqueda sistemática del artículos científicos fue realizado, seguido de la investigación y el análisis de las referencias sobre regulación. **Resultados:** Se seleccionaron cinco documentos normativos, y estas referencias utilizadas para la producción de un dígrafo. Los documentos fueron evaluados por su importancia y contribución. Se propuso una clasificación de su contenido. **Conclusión:** El documentos normativos se clasifican en: (i) las especificaciones técnicas que guían el uso del objeto al que se refiere; (ii) las reglas, como las leyes, proyectos de ley, las medidas provisionales, las resoluciones del asesoramiento federales de salud, decretos y portarias; (iii) los criterios de calidad para la S-RES; y (iv) las políticas de gestión.

[1] Especialista em Informática em Saúde, Universidade Aberta do Brasil - UAB/ Universidade Federal de São Paulo - UNIFESP, São Paulo (SP), Brasil.
[2] Mestrado em Informática em Saúde e orientador do Curso de Especialização em Informática em Saúde, Universidade Aberta do Brasil - UAB/ Universidade Federal de São Paulo - UNIFESP, São Paulo (SP), Brasil.

Autor Coorespondente: **Plinio de Sá Leitão-Júnior**
e-mail: **plinio@inf.ufg.br**

Artigo recebido: **17/04/2015**
Aprovado: **01/04/2016**

INTRODUÇÃO

O uso de sistemas de informação (SI) é uma realidade em vários campos do conhecimento. Há avanços importantes em algumas áreas, tais como o sistema bancário, o sistema de votação eletrônica e o sistema de declaração de ajuste de renda. As motivações para os avanços podem ser a inserção de interesses financeiros, que sobrepõem os desafios inerentes, a sazonalidade do processo, ou a relativa simplicidade de perfis de agentes operadores para a interoperação de sistemas.

Diferentemente das áreas supracitadas, na área da saúde o emprego de sistemas de informação possui desafios importantes, que dificultam à sua evolução para acompanhar as necessidades da sociedade[1-2]. A saúde em si possui heterogeneidade espacial, temporal, social, administrativa, financeira e tecnológica. Alinhar todas essas perspectivas é, no mínimo, uma missão não trivial, sobretudo quando se busca evoluir dentro do contexto da atenção à saúde do cidadão. A informação em saúde é um bem da sociedade e deveria ter a prioridade necessária, considerando interesses coletivos.

Sistema de informação em saúde (SIS) é definido como um conjunto de componentes inter-relacionados que coletam, processam, armazenam e distribuem a informação para apoiar o processo de tomada de decisão e auxiliar no controle das organizações de saúde[1]. O SIS objetiva, em geral, melhorar a atenção à saúde individual ou coletiva, pelo ganho de eficiência e eficácia no registro, recuperação e manipulação das informações sobre a saúde[1]. Sistema de registros eletrônicos de saúde (S-RES) constitui a denominação comumente usada para o SIS que suporta o emprego dos registros eletrônicos de saúde (RES).

S-RES é qualquer sistema que capture, armazene, apresente, transmita ou imprima informação identificada em saúde[3-4]. Informação identificada em saúde é aquela atinente à atenção e gestão da saúde, que pode levar à identificação do cidadão. Segundo a Resolução 1821 do Conselho Federal de Medicina (CFM), toda informação em saúde identificada individualmente necessita de proteção em sua confidencialidade, por ser princípio basilar do exercício da medicina; ainda, os dados do prontuário pertencem ao paciente e só podem ser divulgados com sua autorização ou a de seu responsável, ou por dever legal ou justa causa[5].

Questão a investigar

Sobre informação em saúde, pode-se observar muitos aspectos interessantes a investigar: interoperabilidade e seus modelos de implementação; segurança e confidencialidade de dados no Prontuário Eletrônico do Paciente (PEP); padrões e terminologias em uma especialidade de saúde; requisitos de software para às demandas do Sistema Único de Saúde (SUS); etc. Várias perspectivas podem ser aplicadas para explorar quaisquer desses aspectos, tais como: (i) conhecer e/ou elaborar critérios e regulamentações para o seu emprego; e (ii) aplicar e/ou propor estratégias e modelos viáveis para a sua implantação. Ambas perspectivas perpassam pela consciência dos problemas e dificuldades para se estabelecer melhorias no uso da informação em saúde.

A linha escolhida para esta pesquisa refere-se à segurança dos dados na atenção à saúde, incluindo apenas um dos seus objetivos, a confidencialidade. Segundo a Constituição Brasileira, Artigo 5º, "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"[6]. Qualquer informação recolhida com base em razões clínicas é considerada confidencial, incluindo resultados de diagnósticos, tratamentos propostos e estágios de doenças.

Os três objetivos fundamentais de segurança para registros eletrônicos de saúde são confidencialidade, integridade e disponibilidade[7]. De acordo com *International Organization for Standardization / Working Groups Drafts* (ISO/WD) 13606-4[8], que descreve uma metodologia para especificar os privilégios necessários para o acesso a registros eletrônicos de saúde: (i) *confidencialidade* refere-se ao processo que garante que as informações sejam acessíveis somente por pessoas autorizadas; (ii) *integridade* refere-se ao dever de garantir que as informações sejam precisas, para garantir a segurança do paciente; e (iii) *disponibilidade* refere-se à propriedade de ser acessível e utilizável sob demanda por entidade autorizada.

Em geral, credibilidade implica na preocupação com as questões éticas de sigilo e confidencialidade, bem como a violação legal que é intrínseca aos registros médicos. Além de potenciais implicações legais, danos à saúde do cidadão podem surgir quando não ocorrer o atendimento aos objetivos de segurança.

Uma indagação pertinente é: como avaliar se um sistema é adequado aos requisitos referentes à segurança de RES? Para respondê-la é necessário haver direcionamentos reguladores, que sejam capazes de nortear o desenvolvimento e a auditoria de S-RES quanto à sua segurança. Portanto, o conhecimento e o cumprimento de leis, resoluções, e quaisquer documentos com impacto regulador, de forma direta ou indireta, são mandatórios para preservar os direitos e promover a saúde do cidadão.

A pergunta desta pesquisa é: qual o conjunto de regulações, vigentes no Brasil, são pertinentes à segurança de dados e aplica-se a S-RES? Neste texto, dar-se-á aos termos "regulamentação" e "regulação" o mesmo significado: redação e publicação de regras ou regulamentos.

O propósito deste estudo é classificar os aspectos reguladores necessários ao atendimento das exigências legais de segurança de dados em S-RES. A meta é alcançar um conjunto de elementos capazes de nortear o desenvolvimento e a avaliação de objetivos de segurança. Não se pretende responder amplamente à questão de pesquisa, mas sistematizar e estruturar o conhecimento obtido, sendo uma contribuição para a melhoria de qualidade de S-RES. A contribuição para a comunidade científica é centrada nos estudos secundários produzidos, onde várias perspectivas serão tratadas sobre o objeto em apreciação.

Organização do artigo

A Seção 2 classifica o estudo e apresenta o método empregado para seleção dos aspectos reguladores (documentos). Os documentos selecionados para o estudo,

de acordo com os critérios estabelecidos, são apresentados na Seção 3. A Seção 4 discute os resultados obtidos, analisando os seus conteúdos segundo uma categorização proposta. As conclusões estão na Seção 5, reunindo as ideias principais abordadas no texto. Os agradecimentos e bibliografia estão nas Seções 6 e 7, respectivamente.

MÉTODO

Inicialmente, é pertinente classificar o método utilizado neste estudo: (a) quanto à natureza: pesquisa aplicada, que objetiva gerar conhecimento para aplicação prática dirigida à solução de problemas específicos; (b) quanto à abordagem: pesquisa qualitativa; (c) quanto ao objetivo: pesquisa explicativa, para tornar o objeto em estudo inteligível e justificar seus motivos; (d) quanto ao procedimento técnico: pesquisa bibliográfica; (e) quanto à sistematização: revisão narrativa, que é apropriada para descrever a história ou desenvolvimento de um problema e seu gerenciamento. O método é composto por duas fases: busca por artigos científicos; e busca e análise de referências concernentes à regulamentação.

Busca por artigos científicos

As bases de dados usadas na busca são **BVS** (Biblioteca Virtual de Saúde) e **PubMed**, disponíveis em www.bireme.br/php/index.php e www.ncbi.nlm.nih.gov/pubmed, respectivamente.

Os descritores de busca baseiam-se na *Medical Subject Headings* (MeSh) da *National Library of Medicine* (NLM), onde foram identificados os seguintes *MeSH Headings*: *Confidentiality* e *Computer Security*. Algumas buscas nas referidas bases de dados foram realizadas com várias combinações dos *entry terms* de ambos os *MeSH Headings*. Foi selecionada a seguinte *string* de busca, pois a mesma levava a documentos mais próximos do esperado:

("confidentiality" OR "confidential information" OR "computer security" OR "data protection" OR "information protection") AND ("brazil" OR "brasil")

Os critérios de inclusão selecionados são: **(I1)** artigos publicados a partir de 2009, período que é justificado pela busca de estudos que abordem aspectos atuais e sejam contemporâneos em relação às mudanças de regulação; **(I2)** artigos que mencionam o emprego e/ou importância dos elementos reguladores sobre segurança e confidencialidade; **(I3)** artigos que exploram padrões para os dados em saúde; **(I4)** artigos que exploram aspectos legais de acesso à informação em saúde. Os critérios de exclusão escolhidos são: **(E1)** artigos que valorizam segurança e/ou confidencialidade de dados em saúde, mas cujo foco principal é a análise de alguma morbidade; **(E2)** artigos sobre aspectos éticos, comportamentais ou de qualidade para a saúde; **(E3)** artigos que não possuem texto disponível; **(E4)** artigos que não são escritos em língua portuguesa ou inglesa.

Busca e análise de referências sobre regulamentação

Esta fase está dividida em três estágios: (i) coleta preliminar de documentos; (ii) expansão do conjunto de documentos; (iii) apreciação do conjunto final de documentos.

No estágio "coleta preliminar de documentos", foram selecionadas as referências reguladoras: (i) citadas nos artigos científicos obtidos na fase anterior; ou (ii) obtidas de forma *ad hoc*, de acordo com a experiência dos autores desta pesquisa. No estágio "expansão do conjunto de documentos", os documentos obtidos no precedente estágio serão empregados como semente para a obtenção de novos documentos. Cada semente é analisada e são extraídas citações a outras referências reguladoras, as quais serão incorporadas ao conjunto final de documentos reguladores. No estágio "apreciação do conjunto final de documentos reguladores", ocorre a análise dos documentos selecionados segundo uma classificação de conteúdo proposta (categorização). Uma discussão é levada em curso para avaliar a cobertura dos documentos em relação às categorias da classificação.

RESULTADOS

Ao aplicar a *string* de busca nas referidas bases de dados, 39 artigos foram encontrados no PubMed, enquanto que 43 na BVS.

A *string* de busca foi aplicada em ambas as bases de dados, em seguida, a seleção dos artigos obedeceu a aplicação do Critério de Inclusão I1. Foram obtidos os resultados: PubMed – 39 artigos encontrados; BVS – 43

Tabela 1 – Artigos selecionados, após aplicar os critérios de inclusão e de exclusão.

Autores e Ano	Título do Artigo
[Figueiredo e Motta, 2013][9]	SocialRAD: an infrastructure for a secure, cooperative, asynchronous teleradiology system
[Kobayashi et al., 2009][10]	Proposal for DICOM Multiframe Medical Image Integrity and Authenticity
[Kobayashi et al., 2009a][11]	Providing Integrity and Authenticity in DICOM Images: A Novel Approach
[Maruo e Maruo, 2012][12]	Digital signature of electronic dental records
[Pêgo-Fernandes e Werebe, 2010][13]	Electronic medical files for patients: some steps towards the future
[Pereira et al., 2013][14]	A mapping of Information Security in Health Information Systems in Latin America and Brazil
[Rezende et al., 2010)][15]	Ética e telessaúde: reflexões para uma prática segura
[Skelton-Macedo et al., 2012][16]	Teleodontologia: valores agregados para o clínico/especialista
[Spinardi-Panes et al., 2013][17]	Aspectos éticos e legais na prática da telessaúde em fonoaudiologia
[Tase et al., 2013][18]	Identificação do paciente nas organizações de saúde: uma reflexão emergente
[Valente et al., 2010][19]	Vital Signs Remote Monitoring Through Multipoint Videoconferencing
[Vasconcellos-Silva et al., 2009][20]	As novas tecnologias de autocuidado e os riscos do autodiagnostico pela Internet
[Ventura, 2013][21]	Lei de acesso à informação, privacidade e a pesquisa em saúde
[Wangenheim, 2013][22]	Assinatura digital de laudos médicos: um assunto ainda não resolvido

artigos encontrados. Após o emprego dos demais critérios de inclusão e de exclusão, assim como a eliminação das duplicações em ambas as bases, restaram 14 artigos.

Os artigos selecionados estão apresentados na Tabela 1, ordenados pelo autor. A primeira coluna apresenta os autores e o ano do artigo; a segunda coluna apresenta o título do artigo.

Coleta preliminar de documentos

No primeiro estágio da busca e análise de referências sobre regulamentação, ocorreu a coleta preliminar de documentos regulamentadores citados nos artigos científicos, que estão listados na Tabela 1, obtendo-se a Tabela 2. A primeira coluna da Tabela 2 refere-se aos autores e ano do artigo, enquanto que a segunda apresenta os documentos regulamentadores referenciados.

Sobre os dados na Tabela 2, observam-se duas classes de documentos: de caráter geral e de escopo restrito à saúde. A análise focará nos documentos pertinentes à saúde, tendo o cuidado de considerar os aspectos norteadores dos documentos de caráter geral. Sobre os documentos coletados pertinentes à saúde, seus conteúdos podem ser agrupados em: (G1) prática médica no sentido amplo; (G2) telemedicina, telessaúde, práticas à distância e uso da Internet; (G3) legitimidade e segurança de RES.

Os documentos do Grupo G1, tal como o Código de Ética Médica, não foram abordados neste trabalho, pois representam orientações abrangentes sobre a prática médica. Os documentos do Grupo G2 são aqueles focados no exercício da telemedicina, psicologia à distância, telessaúde em fonoaudiologia, etc., e estão fora do escopo deste trabalho, pois não tratam especificamente do objeto em estudo. Vale ressaltar que, apesar dos potenciais benefícios à atenção, educação e pesquisa em saúde, no Brasil não se discute a teleconsulta, a qual já está presente em outros países.

O Grupo G3 inclui documentos pertinentes à presente pesquisa. Basicamente, são resoluções elaboradas por entidades de classe na área da saúde, ou documentos construídos em parceria com estas. As resoluções são atos normativos emanados dos plenários do Conselho Federal de Medicina (CFM), e de alguns dos Conselhos Regionais de Medicina, que regulam temas de competência privativa dessas entidades em suas áreas de alcance. Os documentos desse grupo estão referenciados por:

- Pêgo-Fernandes e Werebe[13] mencionam a importância de resoluções CFM sobre a legitimidade de RES, sem pontuar em alguma dessas resoluções;
- Rezende et al.[15] mencionam a Resolução CFM 1639[23] de 2002, que trata sobre o uso de sistemas informatizados para a guarda e manuseio do prontuário médico, que foi revogada pela Resolução CFM 1821/2007[5]; e o Manual de Certificação para S-RES[24], uma iniciativa do CFM e da Sociedade Brasileira de Informática em saúde (SBIS), que é destinada a S-RES que capturem, armazenem, apresentem, transmitam ou imprimam informações identificadas em saúde.

Assim, a partir de busca sistemática de artigos científicos, dois documentos foram selecionados: **(D1)** Resolução CFM 1821/2007[5]; e **(D2)** Manual de Certificação para S-RES[24] promovido pelo CFM e pela SBIS.

De acordo com o método descrito na Seção 2, a coleta preliminar de documentos sobre regulamentação prevê, em seu segundo estágio, a obtenção de referências por busca *ad hoc*, ou seja, significa a incorporação de documentos por algum método não sistemático. Nesse contexto, foram inseridas cinco referências: **(D3)** Resolução do Conselho Federal de Odontologia (CFO) 91/2009[25], que aprova as normas técnicas concernentes à digitalização, uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, quanto aos Requisitos de Segurança em Documentos Eletrônicos em Saúde; **(D4)** Projeto de Lei do Senado 474/2008[26], que altera as Leis nos 8.080, de 19 de setembro de 1990, e 9.656, de 3 de junho de 1998, para dispor sobre a informatização dos serviços de saúde; **(D5**) Portaria 2073/2011[27] do Ministério da Saúde, que regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar; **(D6)** Lei 12.682/2012[28], que dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos, também conhecida como lei da digitalização; e **(D7)** Projeto de Lei do Senado 167/2014[29], que autoriza o

Tabela 2 – Documentos regulamentadores referenciados e padrões mencionados.

Autores e Ano	Documentos regulamentadores referenciados
[Maruo e Maruo, 2012][12]	Código de Processo Civil (autenticidade de documentos), Lei 11419/2006 (informatização de processo judicial)
[Pêgo-Fernandes e Werebe, 2010][13]	Resoluções CFM (genericamente, legitimidade de RES), Constituição brasileira, Código penal brasileiro e Código de ética médica (confidencialidade)
[Pereira et al., 2013][14]	ISO/IEC 27000 (sistemas de gestão de segurança da informação)
[Rezende et al., 2010)[15]	Constituição brasileira, Código penal brasileiro, Código de processo penal, Código civil brasileiro, Código de processo civil (confidencialidade), Código de ética médica (confidencialidade), Resolução CFM 1639/2002 (Revogada por CFM 1821/2007), Manual de Certificação para S-RES, ISO/IEC 17799/2005 (Código de prática para a gestão da segurança da informação), Resolução CREMESP 097/2001 (Uso da Internet), Resolução CMF 1643/2002 (Telemedicina), Resoluções CFP 002/1995, 003/2000, 006/2000 (Exercício da psicologia a distância).
[Spinardi-Panes et al., 2013][17]	Lei 6065/1981 (Confidencialidade), Resolução CFFa 427/2013 (Telessaúde em fonoaudiologia)
[Tase et al., 2013][18]	Lei 8069/1990 (impressões planares e digitais)
[Ventura, 2013][21]	Lei 12527/2011 (Acesso à informação), Lei 8080/1990 (Direito à saúde), Lei 12527/2011 (Acesso sem consentimento).
[Wangenheim, 2013][22]	Medida provisória/2200-2/2001 (certificação digital)

armazenamento eletrônico dos prontuários dos pacientes.

Expansão do conjunto de documentos

No estágio de expansão dos documentos inicialmente coletados, os quais são denominados documentos-semente, há a análise desses documentos e a extração de citações a outras referências reguladoras, que serão incorporadas para formar o conjunto final de documentos. A análise dos documentos do conjunto final levou ao dígrafo de citação exibido na Figura 1: cada nó é um documento e cada arco dirigido denota citação entre documentos, onde a ponta da seta indica o documento citado. Os Documentos D1 a D7 estão postos em nós retangulares, identificados por CFM_1821, Cert_SRES, CFO_61, PLS_474, Portaria_2073, Lei_12682 e PLS_167, respectivamente. A identificação dos nós segue o padrão *xxxx_nnnn*, onde: (i) *xxxx* refere-se à natureza do documento, tais como ABNT_ISO e MP para norma ISO traduzida pela ABNT e medida provisória, respectivamente; e (ii) *nnnn* denota o número identificador do documento sem mencionar o ano de publicação. A Figura 1 está dividida em duas partes: em 1(a) há os documentos reguladores em que há citação entre si, e em 1(b) estão os demais documentos reguladores.

DISCUSSÃO

A questão principal deste trabalho – qual o conjunto de regulações, vigentes no Brasil, são pertinentes à segurança de dados e aplica-se a S-RES? – pode ser solucionada a partir do conteúdo da Figura 1. Vale ressaltar que este trabalho não objetiva esclarecer, pedagogicamente, os elementos pertinentes à segurança de dados eletrônicos em saúde, mas localizar e comentar sobre os documentos que tratam sobre a resposta da questão de pesquisa.

A Figura 1 revela várias categorias pertinentes à resolução da questão: (i) documentos compostos por especificações técnicas que orientam o emprego do objeto a que se destina, tal como ABNT/ISO 18308[4] sobre requisitos clínicos e técnicos para uma arquitetura de RES; (ii) documentos que definem e aprovam regras que devem ser seguidas, tais como: leis, projetos de lei, medidas provisórias, resoluções de conselhos federais de saúde, decretos e portarias; (iii) documentos que orientam a adoção de critérios de qualidade, tal como o Manual de Certificação para S-RES[24]; e (iv) documentos que definem políticas de gestão, tal como a Política Nacional de Informação e Informática em Saúde (PNIIS)[30].

Sobre documentos reguladores, vale ressaltar que, segundo o Código de Defesa do Consumidor[31], em seu Artigo 39º, "é vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: ... VIII - colocar, no mercado de consumo, qualquer produto ou serviço em desacordo com as normas expedidas pelos órgãos oficiais competentes ou, se normas específicas não existirem, pela Associação Brasileira de Normas Técnicas ou outra entidade credenciada pelo Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro)". Dessa forma, na ausência de normas específicas capazes de regular os objetivos de segurança para S-RES, deve-se buscar norma expedida pela ABNT ou outra entidade credenciada ao Conmetro.

Dentre as resoluções CFM que tratam sobre registro eletrônico de saúde, a Resolução CFM 1821 está vigente e orienta sobre a eliminação do prontuário em papel, incluindo suas questões sobre segurança e privacidade[5]. A maturidade dessa resolução sofreu influência importante do convênio de cooperação técnica entre o CFM e a Sociedade Brasileira de Informática em Saúde (SBIS), que produziu o Manual de Certificação para S-RES[24] sobre o processo de certificação de sistemas informatizados em saúde. A evolução dessa parceria resultou na citação mútua entre o manual e a resolução, que estão identificados na Figura 1 por CFM_1821 e Cert_SRES, respectivamente. Em 2004, foi construída a primeira versão do Manual de Requisitos de Segurança, Conteúdo e Funcionalidades para Sistemas de Registro Eletrônico em Saúde (RES), que sofreu modificações até a sua última Versão 4.1, concluída em 2013.

O Manual de Certificação para S-RES é um documento que fundamenta-se explicitamente em especificações técnicas, e representa o recurso transmissor de concretude à implantação de resoluções CFM, que tratam sobre o fator eletrônico do registro de saúde[24]. A Tabela 3 apresenta um resumo dos documentos utilizados pelo manual, e está dividida em três colunas: resoluções CFM, especificações técnicas ISO/ABNT e documentos com força de lei.

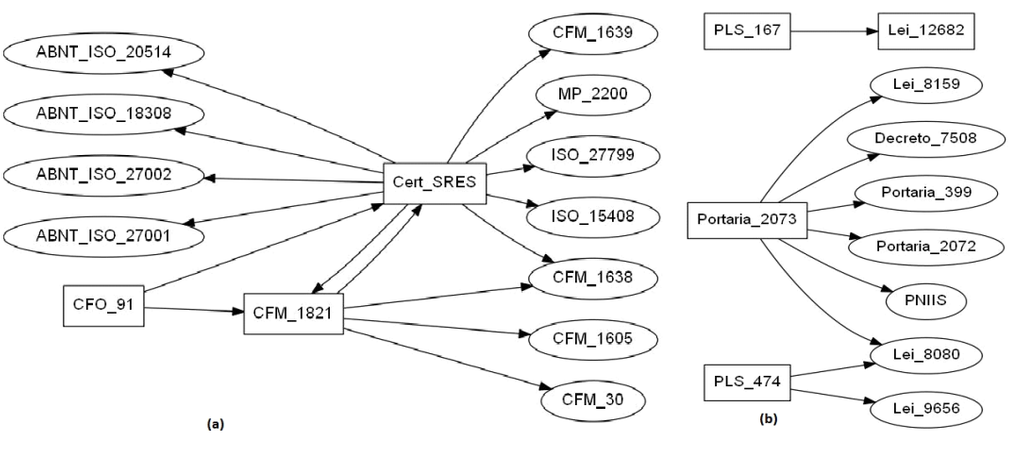

Figura 1 – Dígrafo de citação entre documentos: (a) com citação entre si; (b) sem citação entre si.

O Projeto de Lei do Senado 474 de 2008, identificado na Figura 1 por PLS_474, altera as Leis nos 8.080, de 19 de setembro de 1990, e 9.656, de 3 de junho de 1998, para dispor sobre a informatização dos serviços de saúde. Apesar de pouco citado, inclui aspectos pertinentes à segurança, tal como tornar obrigatório o cadastro nacional único no Sistema Único de Saúde (SUS) aos usuários e aos profissionais de saúde e de unidades de saúde, para a assinatura de documentos de saúde[26].

A Portaria 2073[27] de 2011 do Ministério da Saúde, que é identificada na Figura 1 por Portaria_2073, regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde, nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar. Essa portaria não lida diretamente com segurança de S-RES, mas possui definições importantes com impacto na segurança e na qualidade da assistência à saúde, tal como fundamentar a definição de uma arquitetura de informação nacional, independente de plataforma tecnológica de software ou hardware, para orientar o desenvolvimento de sistemas de informação em saúde. As especificações presentes nessa portaria são uma realidade nacional. Como exemplo, vale citar o edital da Rede Nacional de Ensino e Pesquisa (RNP) para a chamada de propostas para Programas de P&D Temáticos da RNP – 2014-2015 onde se cita: "O desenvolvimento de tecnologias móveis em saúde deve atender às recomendações da Portaria nº 2073/GM/MS de 31 de agosto de 2011 que regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde".

A Resolução do Conselho Federal de Odontologia (CFO) 91[25] de 2011, identificada na Figura 1 por CFO_91, aprova as normas técnicas concernentes à digitalização, uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, quanto aos Requisitos de Segurança em Documentos Eletrônicos em Saúde. Essa resolução é fortemente baseada na Resolução CFM 1821[5] e utiliza as definições de segurança construídas no Manual de Certificação para S-RES[24]. Somente o CFM e o CFO têm resolução que exige requisitos adicionais à certificação digital. Dessa forma, como não há nem por parte dos demais conselhos nem por intermédio de outras legislações nenhuma exigência adicional, para que uma instituição de saúde atenda perfeita e completamente a legislação brasileira sobre documentos eletrônicos, os demais profissionais de saúde devem utilizar também certificados digitais padrão ICP-Brasil para assinar suas anotações e registros no prontuário eletrônico[32].

A Lei 12.682 de 2012, identificada na Figura 1 por Lei_12682, também conhecida como lei da digitalização, é uma regulação genérica sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. No âmbito da saúde, cobre aspectos já previstos na Resolução CFM 1821/2007, tais como uso de certificado Padrão ICP-Brasil, indexação de documentos digitais e proteção contra acessos não autorizados, não havendo conflito entre a lei e o disposto anteriormente pela resolução CFM. Em adição, a lei não trata sobre o descarte de documentos originais que foram digitalizados[28].

O Projeto de Lei do Senado 167 de 2014, que é identificado na Figura 1 por PLS_167, trata sobre a autorização do armazenamento eletrônico dos prontuários dos pacientes[29]. Seu conteúdo modifica a Resolução CFM 1821/2007, no que se refere ao tempo mínimo para retenção de prontuários armazenados em meio eletrônico, óptico ou equivalente, fixando-o em 20 (vinte) anos.

Uma classificação para o conteúdo dos documentos reguladores é proposta (Tabela 4), revelando o suporte de conteúdo dos documentos reguladores. A classificação é composta por grupo e subgrupo: o primeiro define sete categorias de conteúdo para os documentos; o segundo delineia o assunto abordado dentro da categoria. A Tabela 4 apresenta a classificação sugerida e a análise dos documentos: "X" indica que o documento cobre o item de classificação da linha da tabela.

A classificação proposta é uma contribuição importante, visto que traduz de forma ortogonal o conteúdo dos documentos. A coluna Subgrupo da Tabela 4 representa uma compilação da composição dos documentos, e fornece as dimensões com que o aspecto

Tabela 3 – Resumo dos documentos utilizados pelo Manual de Certificação CFM/SBIS[24].

Resoluções CFM	Especificações técnicas ISO/ABNT	Leis
(a) define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde (CFM 1638, 2002); **(b)** revogada (CFM 1639, 2002); **(c)** autoriza a eliminação do prontuário em papel desde que o arquivo resultante do processo de digitalização seja assinado com um certificado digital padrão ICP-Brasil, bem como seja armazenado num sistema de gerenciamento eletrônico de documentos Resolução (resolução CFM 1821, 2007).	**(a)** diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização (ISO 17799, versão 2005); **(b)** definição, escopo e contexto de registro eletrônico de saúde (ISO 20514, versão 2005, tradução ABNT 2008); **(c)** requisitos para sistemas de gestão da segurança da informação (ISO 27001, versões 2005 e 2003; tradução ABNT 2013); **(d)** código de prática para controles de segurança da informação (ISO 27002, versões 2005 e 2003, tradução ABNT 2013); **(e)** gestão de segurança da informação em saúde, utilizando a norma ISO 27002 (ISO 27799, versão 2008); **(f)** processo e requisitos específicos para certificação de segurança de sistemas: parte 1: Introdução e modelo geral; parte 2: requisitos funcionais de segurança; e parte 3: Requisitos de garantia da segurança ISO 15408, versão 2009); **(g)** requisitos para uma arquitetura do registro eletrônico (ISO 18308, versão 2001, tradução ABNT 2013).	Institui a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências (medida provisória 2200, 2001).

Tabela 4 – Classificação sugerida e a análise dos documentos reguladores.

Classificação		CFM	CFO	PLS	Portaria	Cert.	Lei	PLS
Grupo	Subgrupo	1821	91	474	2073	S-RES	12.682	167
Certificação digital	Cadastro SUS			X				
Certificação digital	CRM digital	X						
Certificação digital	Obrigatoriedade			X				
Certificação digital	Segurança			X				
Certificação S-RES	Categorias de certificação					X		
Certificação S-RES	Certificação CFM-SBIS	X	X			X		
Certificação S-RES	Processo e requisitos					X		
Certificação S-RES	Níveis de segurança					X		
Certificação S-RES	Papel do SUS			X				
Certificação S-RES	Princípios					X		
Comissões	Definição de comissões	X						
Padrões em saúde	Adoção ou recomendação				X	X		
Princípios para S-RES	Código aberto e padronização			X				
Princípios para S-RES	Definição conceitual					X		
Prontuário do paciente	Autorização de registro eletrônico	X		X				
Prontuário do paciente	Eliminação de registro em papel	X						X
Prontuário do paciente	Legalidade			X				X
Prontuário do paciente	Normas para ser digital	X					X	
Prontuário do paciente	Segurança em S-RES	X	X	X				
Retenção de prontuário	Prontuário eletrônico	X	X					X
Retenção de prontuário	Prontuário em papel	X	X					
Retenção de prontuário	Prontuário microfilmado	X	X					

eletrônico para os registros de saúde tem sido tratado. Essas dimensões, em sua totalidade, estão focadas, direta ou indiretamente, na preocupação sobre o cuidado para os dados: a segurança com que devem ser tratados; o respeito com o paciente; e as direções de uso para uma melhoria na atenção à saúde.

CONCLUSÕES

Este trabalho teve por base o cuidado com os dados digitais em saúde, especificamente a segurança dos sistemas de informação que manipulam o registro eletrônico de saúde. A motivação foi contribuir com a qualidade da informação em saúde, pois trata-se de um bem da sociedade e deve ser tratado com a atenção necessária, considerando interesses coletivos.

Um dígrafo de citação foi produzido para os documentos selecionados, em que se pôde perceber as suas referências mútuas e as fontes usadas para a construção dos seus conteúdos, a saber: (i) documentos compostos por especificações técnicas que orientam o emprego do objeto a que se destina; dois exemplos são: a norma ABNT ISO 18308[4] de 2004 sobre requisitos clínicos e técnicos para uma arquitetura do registro eletrônico de saúde, e a norma ISO 27799[33] de 2008 sobre a gestão da segurança da informação em saúde; (ii) documentos que definem e aprovam regras que devem ser seguidas, tais como: leis, projetos de lei, medidas provisórias, resoluções de conselhos federais de saúde, decretos e portarias; (iii) documentos que direcionam para o concreto a adoção de critérios de qualidade, tal como o Manual de Certificação para S-RES[24]; e (iv) documentos que definem políticas de gestão, tal como a política nacional de informática e informação em saúde[28].

Uma classificação para o conteúdo dos documentos reguladores foi concebida, constituindo-se em uma contribuição importante, visto que traduz de forma ortogonal o conteúdo dos documentos. As dimensões da classificação, em sua totalidade, estão focadas, direta ou indiretamente, na preocupação sobre o cuidado para os dados: a segurança com que devem ser tratados; o respeito com o paciente; e as direções de uso para uma melhoria na atenção à saúde.

REFERÊNCIAS

1. Marin HF. Sistemas de informação em saúde: considerações gerais. J.Health Inform. 2010;2(1):20-4.
2. Cavalcante RB, Brito MJM, Porto F. Sistema de informação: contribuições e desafios para o cotidiano de trabalho em unidades de terapia intensiva de Belo Horizonte. J. Health Inform. 2009;1(1):34-42.
3. Associação Brasileira de Normas Técnicas. ABNT/ISO. ABNT/ISO/TR 20514. Informática em saúde – Registro eletrônico de saúde – Definição, escopo e contexto. São Paulo: ABNT; 2008. 27p.
4. Associação Brasileira de Normas Técnicas. ABNT/ISO. ABNT ISO/TS 18308. Informática em saúde – Requisitos para uma arquitetura de RES. São Paulo: ABNT; 2013. 29p.
5. Conselho Federal de Medicina (CFM). Resolução CFM nº1821 de 23 de novembro de 2007. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Diário Oficial da União: Republica Federativa do Brasil. 2007 Nov 23; Seção I:252.
6. Brasil. Constituição, 1988. Constituição da República Federativa do Brasil. Brasília: Senado ;1988.
7. Haas S, Wohlgemuth S, Echizen I, Sonehara N, Müller G. Aspects of privacy for electronic health records. Int J Med Inform. 2011;80(2):26-31.
8. International Organization for Standardization (ISO). ISO/WD 13606-4, Health informatics – Electronic health record communication – Part 4: Security. Genebra:ISO; 2009. 30p.
9. Figueiredo JF, Motta GH. SocialRAD: an infrastructure for a secure, cooperative, asynchronous teleradiology system. Stud Health Technol Inform. 2013;192:778-82.
10. Kobayashi LOM, Furuie SS. Proposal for DICOM multiframe medical image integrity and authenticity. J Digit Imaging. 2009;22(1):71-83.
11. Kobayashi LO, Furuie SS, Barreto PS. Providing integrity and authenticity in DICOM images: a novel approach. IEEE Trans Inf Technol Biomed. 2009;13(4):582-9.

12. Maruo IT, Maruo H. Digital signature of electronic dental records. Am J Orthod Dentofacial Orthop. 2012;141(5):662-5.
13. Pêgo-Fernandes PM, Werebe E. Electronic medical files for patients: some steps towards the future. São Paulo Med J. 2010;128(6):317-9.
14. Pereira SR, Fernandes JC, Labrada L, Bandiera-Paiva P. A mapping of information security in health information systems in Latin America and Brazil. Stud Health Technol Inform. 2013;190:123-5.
15. Rezende EJC, Melo MCB, Tavares EC, Santos AF, Souza C. Ética e telessaúde: reflexões para uma prática segura. Rev Panam Salud Publica. 2010;28(1):58-65.
16. Skelton-Macedo MC, Jacob CH, Ramos DLP, Cardoso RJA, Antoniazzi JH. Teleodontologia: valores agregados para o clínico/especialista. Rev Assoc Paul Cir Dent. 2012;66(2):95-9.
17. Spinardi-Panes AC, Lopes-Herrera SA, Maximino LP. Aspectos éticos e legais na prática da telessaúde em fonoaudiologia. Rev CEFAC. 2013;15(4):1040-3.
18. Tase TH, Lourenção DCA, Bianchini SM, Tronchin DMR. Identificação do paciente nas organizações de saúde: uma reflexão emergente. Rev Gaúcha Enferm. 2013;34(2):196-200.
19. Valente A, Pereira D, Almeida E, Matsunaga RH, Dos Santos I. Vital Signs Remote Monitoring Through Multipoint Videoconferencing. Conf Proc IEEE Eng Med Biol Soc. 2010; 2010:2176-9.
20. Vasconcellos-Silva PR, Castiel LD. As novas tecnologias de autocuidado e os riscos do autodiagnóstico pela Internet. Rev Panam Salud Publica. 2009;26(2):172-5.
21. Ventura M. Lei de acesso à informação, privacidade e a pesquisa em saúde. Cad Saúde Pública. 2013;29(4):636-8.
22. Wangenheim AV, Custódio RF, Martina JE, Giuliano IB, Andrade R. Assinatura digital de laudos médicos: um assunto ainda não resolvido. Rev Assoc Med Bras. 2013;59(3):209-12.
23. Conselho Federal de Medicina. Resolução CFM nº1639 de 10 de julho de 2002. Aprova as Normas Técnicas para o Uso de Sistemas Informatizados para a Guarda e Manuseio do Prontuário Médico e dispõe sobre o tempo de guarda dos prontuários, estabelece critérios para certificação dos sistemas de informação e dá outras providências. Diário Oficial da União: Republica Federativa do Brasil. 2002 Jul 10.
24. Sociedade Brasileira de Informática em Saúde (SBIS) e Conselho Federal de Medicina (CFM). Manual de Certificação para Sistemas de Registro Eletrônico em Saúde. Versão 4.1. Brasília. SBIS; 2013.
25. Conselho Federal de Odontologia (CFO). Resolução 91 de 20 de agosto de 2009. Aprova as normas técnicas concernentes à digitalização, uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, quanto aos Requisitos de Segurança em Documentos Eletrônicos em Saúde. Rio de Janeiro; 2009 Ago 20.
26. Brasil. Projeto de Lei do Senado 474 de 11 de dezembro de 2008. Altera as Leis nos 8.080, de 19 de setembro de 1990 e 9.656, de 3 de junho de 1998, para dispor sobre a informatização dos serviços de saúde. Brasília; 2008 Dez 11.
27. Brasil. Ministério da Saúde. Portaria 2073 de 31 de agosto de 2011. Regulamenta o uso de padrões de interoperabilidade e informação em saúde para sistemas de informação em saúde no âmbito do Sistema Único de Saúde nos níveis Municipal, Distrital, Estadual e Federal, e para os sistemas privados e do setor de saúde suplementar. Brasília. 2011 Ago 31.
28. Brasil. Presidência da República. Lei 12.682 de 9 de julho de 2012. Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos. Diário Oficial da União: Republica Federativa do Brasil. 2012 Jul 10; Seção 1:1.
29. Brasil. Projeto de Lei do Senado 167 de 7 de maio de 2014. Autoriza o armazenamento eletrônico dos prontuários dos pacientes. Brasília. 2014 Mai 7.
30. Brasil. Ministério da Saúde. Comitê de Informação em Informática em Saúde. Política nacional de informação e informática em saúde (PNIIS). 2013. 50p.
31. Brasil. Presidência da República. Lei 8078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: Republica Federativa do Brasil. 1990 Set 11.
32. Costa CGAC. CRM Digital. Sociedade Brasileira de Informática em Saúde – SBIS; 2012.
33. International Organization for Standardization (ISO). ISO/DIS 27799. Health informatics — Information security management in health using ISO/IEC 27002; Genebra:ISO; 2008. 58p.