# Aspectos legais do Prontuário Eletrônico do Paciente: Um Comparativo do Cenário Atual Frente a Resolução do CFM

Nélio Fernandes Borrozzino[1]; Ivan Torres Piza[2]

**Resumo:** Nos dias atuais, o Conselho Federal de Medicina define quais são as características legais do prontuário médico e do prontuário/registro eletrônico do paciente, inclusive publicando uma cartilha em conjunto com a Sociedade Brasileira de Informática em Saúde com essas descrições normativas inclusas. O objetivo do presente estudo foi analisar como o assunto é abordado nas publicações recentes em um comparativo com as resoluções brasileiras. Através de uma revisão bibliográfica da literatura, mediante critérios de inclusão e exclusão pré estabelecidos, 10 artigos foram abordados no presente estudo. Em linhas gerais, termos como Health Insurance Portability and Accountability Act (HIPAA), Health Level 7 (HL7) e outras preocupações frente a segurança das informações foram encontrados nas publicações elencadas. Semelhante ao Brasil, embora esses registros eletrônicos tragam uma segurança eficiente frente aos documentos em papel, existe certa atenção em aumentar e assegurar a privacidade do paciente.

**Palavras-chave**: Sistemas Computadorizados de Registros Médicos; Privacidade.

## Legal aspects of electronic patient record: A Comparison of current scenario front resolution of the Federal Council of Medicine

**Abstract**: Nowadays, the Federal Council of Medicine defines what are the legal characteristics of medical records and the medical records / electronic record of the patient, including publishing a booklet in conjunction with the Brazilian Society of Health Informatics with these regulations descriptions included. The aim of this study was to analyze how the issue is addressed in recent publications on a comparison with Brazilian resolutions. Through a literature review of the literature by criteria of inclusion and exclusion pre-established, 10 articles have been addressed in this study. In general, terms like Health Insurance Portability and Accountability Act (HIPAA), Health Level 7 (HL7) and other concerns facing the security of information was found in the listed publications. Similar to Brazil, although these electronic records bring forward an efficient security to paper documents, there is some attention to increase and ensure patient privacy.

**Keywords**: Computerized Medical Records Systems. Privacy.

## Aspectos jurídicos del registro electrónico del paciente: Un escenario comparativo actual con la resolución del CFM

**Resumén**: Hoy, el Consejo Federal de Medicina define cuáles son las características legales de las historias clínicas y los registros / registro electrónico médico del paciente, incluyendo la publicación de un folleto en conjunto con la Sociedad Brasileña de Informática de la Salud con estas regulaciones descripciones incluidos. El objetivo de este estudio fue analizar cómo el tema se aborda en publicaciones recientes en una comparación con las resoluciones brasileñas. A través de una revisión bibliográfica de la literatura por los criterios de inclusión y exclusión pre-establecidos, 10 artículos se han abordado en este estudio. En términos generales, términos tales como Health Insurance Portability and Accountability Act (HIPAA), Health Level 7 (HL7 y otros problemas que enfrenta la seguridad de la información se encuentran en las publicaciones que se indican. Al igual que en Brasil, aunque estos registros electrónicos que presente una seguridad eficaz de los documentos en papel, hay un poco de atención para aumentar y garantizar la privacidad del paciente.

**Palabras-clave**: Computerized Medical Records Systems. Privacy.

## INTRODUÇÃO

O prontuário médico é definido pelo Conselho Federal de Medicina (CFM), mediante a resolução nº 1.638/2002, publicada em 9 de agosto de 2002, como um "documento único composto pelo conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo" (BRASIL, 2002).Entretanto, os arquivos médicos se tornam volu-

[1]Enfermeiro Coordenador na Empresa Informar Saúde (GRUPO BEM). Especialista em Informática em Saúde pela Universidade Federal de São Paulo. Graduando em Direito pela Faculdade Municipal de São Bernardo do Campo. **Email**: neliofb@gmail.com
[2]Professor Livre-Docente - Departamento de Informática em Saúde, Escola Paulista de Medicina, UNIFESP. **Email**: ivanpisa@unifesp.br

mosos com o passar dos anos e exigem a disposição de um grande local físico nos estabelecimentos de saúde. Nesse sentido, essa problemática, envolvendo o espaço físico para o armazenamento dessas informações, foi uma grande justificativa para o desenvolvimento de novas tecnologias para guardar e transferir dados em saúde. Trata-se então de informações continuas de determinada pessoa, contendo seus dados pessoais, registros médicos (contemplando não apenas textos com evoluções médicas, mas também imagens e resultados de exames), entre outras informações, tomando esse documento com uma grande importância no tratamento do paciente, em sua segurança e na própria comunicação entre a equipe multidisciplinar(BRASIL, 2002; 2007).

Com a inovação e a tecnologia, consequentemente, o prontuário médico atinge um âmbito diferenciado e em 23 de novembro de 2007 ocorre a publicação pelo CFM da resolução nº 1.821/07, que aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde (BRASIL, 2002). A utilização da tecnologia atrelada à área da saúde contribuem de forma positiva aos cidadãos com um aumento significativo da qualidade desses serviços, fundamentalmente quando o assunto é prontuário eletrônico do paciente, considerado como a principal ferramenta de tecnologia da informação e comunicação em saúde (TICS) que o profissional médico trabalhará em suas rotinas diárias. (BRASIL, 2002; PINTO, 2006)

Um assunto importante disposto em ambas resoluções, no Art. 1º da resolução CFM nº 1.638/2002 ao citar o caráter sigiloso do documento e no Art. 3º e 4º da resolução CFM nº 1.821/07 que estabelece os níveis de garantia de segurança 1 (NGS1) e 2 (NGS2), é a privacidade, o sigilo e a segurança das informações do prontuário eletrônico do paciente(BRASIL, 2002; 2007). Em âmbito nacional, segundo a Constituição Federal vigente de 1988, o art. 5º, inciso X dispõe que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação", direito subjetivo fundamental pelo qual tais níveis de garantia de segurança asseguram a individualidade e as informações sigilosas do paciente (BRASIL, 1988). Outra característica em estabelecer os níveis de garantia de segurança é justamente eliminar a utilização do prontuário em papel. Instituições que desejam abandonar o prontuário médico em papel e utilizar apenas um serviço de Registro Médico Eletrônico (RES) devem possuir os critérios do NGS2, enquanto os critérios do NGS1 não estinguem a necessidade de impressão e a sua utilização (BRASIL, 2007; CFM/SBIS, 2012).

Segundo a Sociedade Brasileira de Informática em Saúde (SBIS) e o CFM, o Prontuário Eletrônico do Paciente (PEP)/RES deve possuir requisitos mínimos e obrigatórios em vários aspectos e, em nível de segurança, devem abranger o NGS1, cumprindo uma série de requisitos de segurança, tais como o controle da versão do software utilizado, controle de acesso, disponibilidade, autenticação, comunicação remota, auditoria e documentação, e em um nível mais elevado de segurança, o NGS2, deve cumprir todos os requisitos já dispostos no primeiro nível, acrescentando a utilização de certificados digitais ICP-Brasil nos processos de assinatura e autenticação (CFM/SBIS, 2012).

A ICP-Brasil é a infraestrutura de Chaves Públicas Brasileira, criada em 24 de agosto de 2001 através da Medida Provisória 2.200-2. Nela são estabelecidos os critérios que servem de base para os serviços de assinatura, não-repúdio, identificação e sigilo. Com esse padrão, há a possibilidade de migração dos prontuários em papel para o meio eletrônico sem o prejuízo legal dos documentos e consequente aumento da segurança do RES mediante a certificados digitais (BRASIL, 2001).

Frente ao aspecto de segurança às informações do paciente e utilização de certificados e requisitos para aumentar a segurança do PEP/RES, o objetivo do presente estudo foi analisar como o assunto é abordado nas publicações recentes em um comparativo com a resolução CFM nº 1821/2007 e as diretrizes expostas pela SBIS e CFM.

## METODOLOGIA

Trata-se de uma revisão bibliográfica da literatura de caráter quantitativo e qualitativo. Para a análise dos artigos encontrados foram utilizados os seguintes critérios de inclusão: idiomas em português ou inglês; artigos completos; e ano de publicação após 2010.

Um importante critério de exclusão foi o texto do artigo não abordar a temática principal do presente estudo, ou seja, não abordar os aspectos legais relacionados à privacidade do paciente em prontuários/registros médicos eletrônicos.

Como conduta inicial, foi realizada uma busca por temas similares em três bases eletrônicas em saúde através de três descritores cadastrados no Descritores em Ciências da Saúde (DECS): Sistemas Computadorizados de Registros Médicos e Privacidade, com os seguintes resultados: MedLine (46 artigos), Scielo (0 artigos) e Lilacs (1 artigos), entre o período de 01 de julho de 2014 a 15 de agosto de 2014.

Mediante a análise, 32 artigos foram excluídos devido a sua data de publicação ser inferior a 2010, 3 artigos por não possuírem o resumo e o texto completo para a avaliação e 2 por não abordarem a temática de legalidade à privacidade. Ao final da avaliação, 10 artigos foram elencados e validados para a inclusão no estudo.

## RESULTADOS E DISCUSSÃO

Após a análise dos resultados, foi organizado o Quadro 1, contendo um breve resumo dos artigos utilizados no estudo. De forma geral, os autores abordam o

Quadro 1: Distribuição de artigos localizados nas bases de dados LILACS (2010-2014) e MEDLINE (2010-2014), sobre a privacidade no uso de sistemas computadorizados de serviços médicos.

| Título do Artigo | Autores | Resultados |
|---|---|---|
| Analysis of the security and privacy requirements of cloud-based electronic health records systems. | RODRIGUES, J. J. et al. (2013) | Eficácias e problemáticas em utilizar registros médicos de saúde em nuvem. Citam ações governamentais: Health Insurance Portability e Accountability Act (HIPAA) dos EUA e as normas de segurança Health Level 7 (HL7). O armazenamento em nuvem traz benefícios que sobrepõe as desvantagens em relação à Segurança/Privacidade. |
| Storing and using health data in a virtual private cloud. | REGOLA, N.; CHAWLA, N. V. (2013) | Desafios ao se tratar de dados em saúde e tecnologia da informação. Explana sobre a HIPAA (EUA) e compara a segurança de armazenamento de registros médicos em servidores locais com a utilização de armazenamento em nuvem para aumentar a segurança. |
| Secure electronic exchange of pathology reports. | BJUGN, R.; BREVIG, T, (2012) | Enfatiza a importância em disponibilizar um prontuário com toda a história clínica (exames e consultas anteriores) da atenção primária, secundária e terciária em saúde, expondo essa importância para a equipe multiprofissional. Ao se tratar de segurança, o artigo aborda o aspecto legal de que as informações contidas no prontuário são de uso confidencial, sendo as instituições de saúde as principais responsáveis pelo cuidado dessas informações. Os autores demonstram um modelo de acesso eletrônico relacionados à patologias para conexão remota e compartilhamento entre empresas, garantindo segurança às informações desse modelo. |
| An event driven hybrid identity management approach to privacy enhanced e-health. | SÁNCHEZ-GUERRERO, R. et al. (2012) | O uso de certificado digital para garantir a segurança e privacidade em *E-health*. Ele traz um modelo novo de sistema de certificação que visa preencher as lacunas dos modelos tradicionais de certificados, os quais não cumprem todos os princípios/regras de privacidade. O artigo também aborda termos como Security Assertion Markup Language (SAML), Public Key Infrastructure (PKI) e Liberty Alliance (ID-FF). |
| A systematic review of re-identification attacks on health data. | EL EMAM, K. et al. (2011) | Aborda uma revisão de como as jurisdições permitem a divulgação de dados em saúde, sem o consentimento do paciente, informando que alguns métodos atuais de identificação não oferecem proteção suficiente ao usuário. Os autores relatam que pela falta de pesquisa na área, esse assunto (a falta de segurança) se torna delicado para uma conclusão definitiva. |
| A novel key management solution for reinforcing compliance with HIPAA privacy/security regulations. | LEE, C. D.; HO, K. I.; LEE, W. B. (2011) | O artigo trata que os registros médicos eletrônicos podem causar sérios problemas de segurança e privacidade ao paciente. Relaciona que essa preocupação está ligada ao HIPAA. Nesse assunto, os autores descrevem mecanismos criptográficos integrados para aumentar essa lacuna de segurança e privacidade. Com a utilização desses mecanismos, é possível aumentar a segurança e a privacidade de registros médicos eletrônicos. |
| Building a diabetes screening population data repository using electronic medical records. | TUAN W., J.; SHEEHY, A. M.; SMITH, M. A. (2011) | Iniciando com a problemática de que o avanço em saúde e o rápido crescimento dos registros médicos eletrônicos traz um complexo desafio aos pesquisadores com o fim de extrair, localizar e analisar informações para sua pesquisa. O artigo propõe a criação de um repositório para a pesquisa de triagem em diabetes. Em relação à segurança, os autores se preocuparam a seguir as diretrizes HIPAA. O sistema de repositório, seguindo os padrões HIPAA são eficientes na pesquisa de triagem em diabetes. Citam que pode ser utilizado nos demais assuntos e não apenas na patologia proposta em seu experimento. |
| Intelligent security and privacy solutions for enabling personalized telepathology. | BLOBEL, B. (2011) | Tratando-se de novos paradigmas em saúde, o estudo aborda aspectos fundamentais de segurança e privacidade para qualquer ambiente de e-health ou e-pathology. |
| An open, interoperable, and scalable prehospital information technology network architecture. | LANDMAN, A. B.; (2011) | Descreve como a tecnologia da informação pode garantir o rápido acesso as informações do paciente, o armazenamento de informações passadas e a intercomunicação dos setores em saúde. No âmbito da emergência, essa rede de comunicação deve abordar aspectos legais que são descritos no artigo, visando garantir a privacidade e a segurança das informações. |
| A methodology for the pseudonymization of medical data. | NEUBAUER, T.; HEURIX, J. (2011) | As informações em saúde estão susceptíveis a violações de privacidade e segurança, principalmente pelo interesse de seguros de saúde e empregadores. Visando a autonomia do paciente, o estudo analisa a utilização de autorizações permitidas pelo próprio paciente para acesso aos seus dados de saúde. O artigo começa com uma exploração detalhada dos mecanismos de proteção de privacidade existentes, como criptografia, anonimato e pseudônimo, além de fornecer um método que aumenta a segurança nas informações do paciente e estão de acordo com a HIPAA. |

contexto de segurança em algumas áreas de tecnologia da informação relacionada à saúde. Nota-se que alguns termos, como Health Insurance Portability and AccountabilityAct (HIPAA) e Health Level7 (HL7), surgem como temática, discussão ou diretriz em mais de um artigo, logo sua relevância será tratada na discussão desses resultados.

Os padrões HIPAA foram criados em 1996 pelo Departamento de Saúde e Serviços Humanos dos Estados Unidos da América (U.S. Departmentof Health andHuman Services), como um conjunto de normas nacionais para proteção de determinadas informações em saúde. Essas normas protegem de forma especifica as informações de saúde capazes de identificação, como: os dados pessoais, número de segurança social, data de nascimento e endereço, bem como informações em relação ao quadro de saúde e tratamento do paciente, seja no passado, na atualidade ou a serem realizados (HIPAA, 1996). Além delas, Rodrigues (2013) traça em seu artigo que existem outros padrões que podem ser utilizados,mesmo quando o serviço em foco é disponibilizado em nuvem, citando: SAS70 Type II, PCI DSS Level1, ISO 27001, e US Federal Information Security Management Act (FISMA). É exatamente com o uso de mecanismos correlacionados, segurança de rede, criptografia de dados, assinaturas digitais e o monitoramento de acesso, simultaneamente com certificações de segurança, que a segurança das informações se torna mais concreta.

No âmbito da pesquisa, considerando afrágil privacidade do paciente, Regola e Chawla (2013) elaboram um protótipo de infraestrutura em nuvem se preocupando também com as normas HIPAA e o compartilhamento de informações entre os pesquisadores, sem a violação da privacidade e da autonomia do paciente. Em contrapartida, El Emam (2011) traz uma pesquisa com a ausência de uma conclusão definitiva sobre a segurança do PEP em pesquisa. De fato para os autores, a divulgação de dados privados em saúde, sem o consentimento do paciente para a realização de pesquisas é um alerta real sobre o desrespeito à sua privacidade.

O uso dessas diretrizes, embora com algumas controvérsias, certamente traz maior segurança às informações em saúde, todavia não tornam os prontuários absolutamente seguros. Nesse sentido, Sánchez-Gerrero (2010) aborda o uso de certificados digitais para aumentar a segurança no uso de tecnologia das informações em saúde, visando preencher essas lacunas remanescentes dos certificados tradicionais. Como exemplo, o autor cita termos como Security AssertionMarkupLanguage (SAML), Public Key Infrastructure (PKI) e Liberty Alliance (ID-FF). O uso de certificados digitais, como preconizado pelo CFM na utilização da ICP-Brasil, se assemelha no grau de segurança relatado pelos autores, ademais, seguindo os preceitos vigentes na atualidade brasileira, que são tão complexos e engessados como a HIPAA, demonstrando uma preocupação compartilhada nesse quesito.

Um importante termo citado em grande parte dos artigos pesquisados foi o Health LevelSevenInternational (HL7). O HL7 foi fundado em 1987 para fornecer informações globais sobre troca, compartilhamento, integração e recuperação de informações em saúde com rigor cientifico e conhecimentos técnicos para prática ou gestão clínica. Preconizado pelo CFM no Brasil, os PEP/RES também precisam se enquadrar em resoluções e normas para uma sustentação adequada de sua qualidade e segurança. Semelhante aos padrões encontrados nos estudos supra citados, o próprio NGS1, mesmo sem a eliminação do documento em papel, traz diretrizes organizacionais e estruturais tão relevantes quanto as elencadas em outro país.

## CONCLUSÃO

A preocupação com a segurança das informações é algo extremamente relevante em nossa atualidade e os artigos estudados corroboram com essa perspectiva, seja ela nacional ou internacional. Atualmente no Brasil, o próprio Conselho Federal de Medicina emite registros digitais aos médicos visando um melhor controle e uma maior segurança no uso de tecnologias em saúde, a qual os registros médicos eletrônicos se incluem. Os mecanismos e diretrizes norte-americanos apresentados no estudo são tão completos e detalhados quanto os preconizados pelas diretrizes brasileiras segundo o CFM e a SBIS.

Entretanto,a problemática em manter as informações sigilosas não se extinguem com o uso da tecnologia, mesmo ela se mostrando superior aos prontuários em papel. A própria análise dos artigos utilizados demonstra que se trata de um assunto em busca de constantes soluções. É evidente que, para um estudo mais aprofundado, há a necessidade em comparar os mecanismos aqui citados de forma minuciosa e especifica,algo que não foi tratado, pois o próprio objetivo desse trabalho teve o seu foco mais abrangente.

## REFERENCIAS

Bjugn R, Brevig T. Secure electronic exchange of pathology reports. Tidsskr. Nor Laegeforen. 2012 Oct 30;132(20).

Blobel B. Intelligent security and privacy solutions for enabling personalized telepathology. DiagnPathol. 2011 Mar 30;6 Suppl 1:S4.

Brasil. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado; 1988.

Brasil. Medida Provisória nº 2.200-2, de 24 de Agosto de 2001. Institui a Infraestrutura de Chaves Públicas Brasileira: ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências. Diário Oficial da União. 27 Ago 2001.

Brasil. Resolução nº 1.638/2002, de 09 de Agosto de 2002. Define prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde. Diário Oficial da União. Brasília, DF, 09 Ago. 2002.

Brasil. Resolução nº 1.821/07, de 23 de Novembro de 2007. Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde. Diário Oficial da União. Brasília, DF, 23 Nov. 2007.

Centers for Medicare and Medicaid Services.(1996). Health Insurance Portability Accountability Act of 1996 (HIPAA), [Online]. Available:", [online] Available: http://www.cms.hhs.gov/hipaageninfo.

Chien-Ding L; Ho K; Wei-Bin L, "A Novel Key Management Solution for Reinforcing Compliance With HIPAA Privacy/Security Regulations," Information Technology in Biomedicine, IEEE Transactions on. 2011 July; 15(4): 550-556.

Conselho Federal de Medicina (CFM) e Sociedade Brasileira de Informática em Saúde. Cartilha Sobre Prontuário Eletrônico – A certificação de sistemas de registro eletrônico em saúde. Editor Claudio Giulliano Alves da Costa. 2012.

El Emam K, Jonker E, Arbuckle L, Malin B. A systematic review of re-identification attacks on health data. PLoS One. 2011;6(12). HL7 International Inc. http://www.hl7.org

JPC Rodrigues J, de la Torre I, Fernández G, López--Coronado M. Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems J Med Internet Res 2013;15(8):e186.

Landman AB, Rokos IC, Burns K, Van Gelder CM, Fisher RM, Dunford JV, Cone DC, Bogucki S. An open, interoperable, and scalable prehospital information technology network architecture. PrehospEmerg Care. 2011 Apr - Jun;15(2):149-57.

Neubauer T, Heurix J. A methodology for the pseudonymization of medical data. Int J Med Inform. 2011 Mar;80(3):190-204.

Pinto VB. Prontuário eletrônico do paciente: documento técnico de informação e comunicação do domínio da saúde. Enc. Bibli: R. Eletr. Bibliotecon. Ci. Inf., Florianópolis. 1º Sem 2006; volume 21: pag. 34-48.

Regola N, Chawla NV.Storing and Using Health Data in a Virtual Private Cloud.J Med Internet Res 2013;15(3):e63.

Sánchez-Guerrero R; Almenárez F; Díaz-Sánchez D; Marín A; Arias P; Sanvido F. 2012. "An Event Driven Hybrid Identity Management Approach to Privacy Enhanced e-Health." Sensors 12, no. 5: 6129-6154.

Tuan WJ, Sheehy AM, Smith MA. Building a diabetes screening population data repository using electronic medical records. J Diabetes SciTechnol. 2011 May 1;5(3):514-22.

Página em branco