Ontologia de privacidade em prontuário eletrônico de saúde

Marcio Silva Cruz (CTI) marcio.cruz@cti.gov.br
Dr. Ferrucio de Franco Rosa (CTI) ferrucio.rosa@cti.gov.br

Resumo

Este trabalho apresenta uma modelagem conceitual visando a preservação da privacidade dos dados de saúde dos pacientes. Busca-se identificar, formalizar e relacionar conceitos importantes, além de apresentar abordagens ontológicas com a utilização de um ou mais recursos para apoiar a preservação da privacidade em Prontuários Eletrônicos de Saúde. Este trabalho destina-se a ser útil para pesquisadores que buscam desenvolver métodos e técnicas sistemáticas voltadas à proteção e privacidade de dados altamente sensíveis.

Palavras-chave: Dados de Saúde; EHR; Privacidade; Prontuário Eletrônico; Ontologia.

1. Introdução

Atualmente, observa-se uma crescente demanda por sistemas críticos capazes de processar dados pessoais de pacientes e outros dados relacionados à saúde. Esse aumento decorre do avanço das tecnologias de monitoramento individualizado de cada paciente que permitem a coleta contínua de parâmetros fisiológicos como temperatura corporal, pressão arterial e frequência cardíaca.

EHR (*Electronic Health Record* - Registro Eletrônico de Saúde), ou prontuário eletrônico de saúde, refere-se às informações de saúde armazenadas digitalmente sobre a vida de uma pessoa com o objetivo de apoiar a continuidade dos cuidados, educação e pesquisa, e garantir a confidencialidade em todos os momentos (GAJANAYAKE et al., 2014). Contudo, a privacidade é uma questão crítica e central no tratamento dos dados sensíveis contidos nos sistemas que lidam com registros eletrônicos de dados de saúde, e aprimorar a privacidade desses dados, ao mesmo tempo que viabilize a pesquisa na área de saúde, é um desafio de pesquisa e desenvolvimento, especialmente a partir das perspectivas do paciente e do sistema de saúde.

A modelagem conceitual de privacidade em EHR revela-se essencial para o desenvolvimento de métodos e técnicas sistemáticas de proteção de infraestruturas críticas. Propor um modelo conceitual apoiado por uma ontologia, visando a privacidade dos dados em EHR, é o desafio de pesquisa abordado neste trabalho.

Apresenta-se a Ontologia de privacidade em prontuário eletrônico de saúde. O modelo conceitual proposto visa identificar, formalizar e relacionar conceitos e termos importantes como, usuário, dados de saúde, paciente, profissional de saúde e seus relacionamentos, os quais são formalizados por meio de uma ontologia de domínio em formato OWL.

O restante deste artigo está organizado da seguinte maneira: a Seção 2 apresenta o resumo de um mapeamento da literatura visando a identificar, analisar e classificar soluções baseadas em ontologias de privacidade em EHR; a Seção 3 descreve uma síntese da construção da ontologia; a Seção 4 apresenta uma visão geral da ontologia de domínio; e a Seção 5 considerações finais.

2. Síntese dos trabalhos analisados

Embora estudos revelem o impacto positivo da implantação de EHRs, a sua implementação é bastante desafiadora devido à complexidade na interoperabilidade e por envolver vários aspectos técnicos, questões sociais e organizacionais. Além do mais, existem outras questões relacionadas ao seu compartilhamento, como problemas de segurança e atribuição de responsabilidades e direitos entre os diversos atores (BEARD et al., 2012).

Um mapeamento da literatura foi conduzido, visando identificar soluções baseadas em ontologias com a utilização de um ou mais recursos para apoiar a preservação da privacidade em dados eletrônicos de saúde (CRUZ; ROSA, 2024). Na análise foram apresentados 14 artigos considerando os seguintes aspectos: (i) Domínio: Ontologia; Interoperabilidade; Politica Padrão de Privacidade; e Política de Controle de Acesso. (ii) Técnicas: ABE - *Attribute-Based Encryption*; OPM - *Open Provenance Model*; ABAC - *Attribute-Based Access Control*; RBAC - *Role Based Access Control*; XACML - *Extensible Access Control Markup Language*; BPMN - *Business Process Model and Notation*; *Machine Learning*; e *Cloud*. Este mapeamento da literatura apontou métodos, modelos, ferramentas e áreas de atuação que fundamentaram o desenvolvimento da Ontologia de Privacidade em Prontuário Eletrônico de Saúde.

3. Construindo ontologia de privacidade EHR

O projeto de uma ontologia é um processo iterativo para determinar o escopo e definir os conceitos (classes), propriedades, instâncias, axiomas e restrições. De acordo com sua generalidade, ontologias podem ser classificas em ontologia de alto-nível, domínio, tarefa ou aplicação. A ontologia de domínio descreve os conceitos explícitos de um domínio especifico do conhecimento e seus relacionamentos, sendo observado em seu uso a padronização de conceitos, termos e definições, bem como a facilidade do compartilhamento de conhecimento e auxilio na análise das informações (GUARINO,1998).

Este artigo apresenta uma modelagem conceitual apoiada por uma ontologia de domínio e a implementação foi feita em OWL (*Web Ontology Language) (W3C* OWL *WORKING GROUP*, 2012). Ontologias baseadas em OWL possuem recursos ricos para definir inequivocamente relações e hierarquias complexas. A Figura 3.1 apresenta a hierarquia das principais classes e instâncias da ontologia de privacidade em EHR.

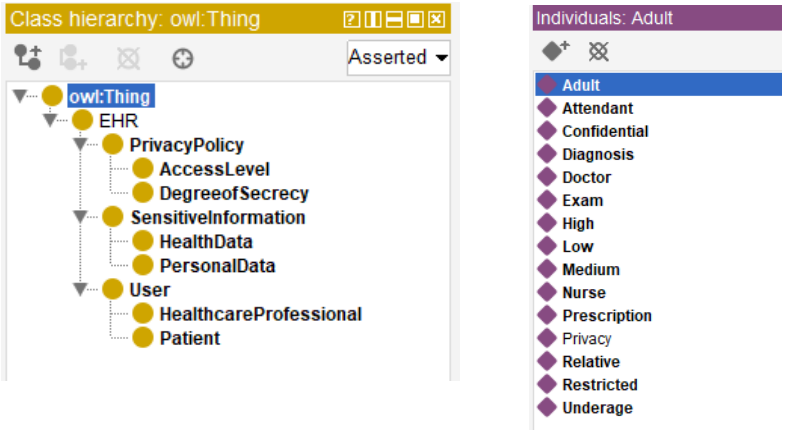

Figura 3.1 – Classes e instâncias da ontologia EHR

4. Ontologia de domínio: estrutura das classes

Nesta seção, apresenta-se uma visão geral das classes que irão compor a ontologia proposta. Na definição das classes utiiza-se uma abordagem Top-Down, onde os termos mais gerais são formulados primeiramente, permitindo que termos mais especializados sejam utilizados como Subclasses. Para representação na ontologia, cada expressão ou termo possui uma instância. A Classe *EHR* é a versão eletrônica dos dados de saúde ou histórico médico de uma pessoa. A Classe *HeathData* (Dados de saúde), representa todas as informações de saúde física ou mental, de uma pessoa, coletadas a qualquer tempo. Esses dados de saúde podem ser acessados por profissionais de saúde (*Healthcare professional*), durante um tratamento médico ou pesquisa médica, dependendo do concentimento ou autorização dada pelo paciente (*Patient*) com relação a privacidade de seus dados; os quais possuem nível de acesso (*AccessLevel*), conforme o grau de sigilo (*DegreeofSecrecy*) desses dados. Uma visão geral da proposta inicial da ontologia, contendo as principais classes e instâncias é apresentada na Figura 4.1.

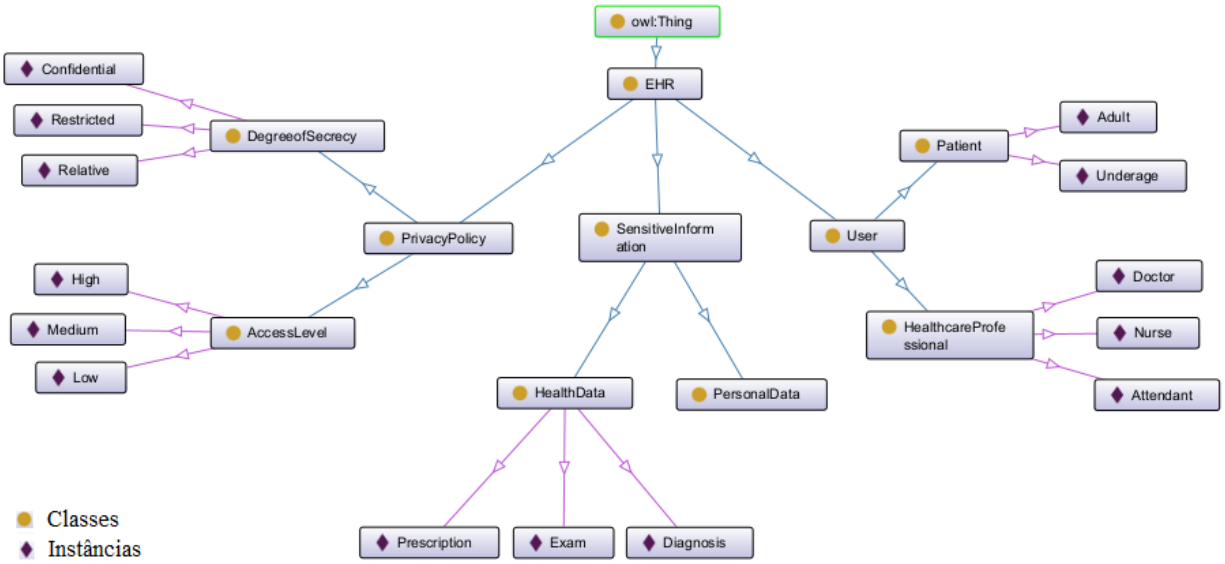

Figura 4.1 – Principais Classes e instâncias da Ontologia de privacidade em EHR

O núcleo da ontologia contém os principais conceitos do domínio específico, permitindo assim a estruturação e compreensão dos conceitos relacionados. As propriedades das classes permitem a definição da relação entre conceitos. A Tabela 4.1 apresenta a estratégia de relacionamento, com as propriedades destacadas em vermelho; conceitualmente as classes são descritas nos parágrafos seguintes.

EHR	Tem	Política de Privacidade	contém	Grau de Sigilo
				Nível de acesso
	Tem	Informação Sensível	é um	Dado de Saúde
			é um	Dado Pessoal
	Tem	Usuário	é um	Paciente
			é um	Profissional de Saúde

Tabela 4.1 – Representação das Propriedades das Classes

Política de Privacidade: Conjunto de princípios, diretrizes e práticas que regulam a coleta, o uso, o armazenamento e o compartilhamento de dados pessoais, com o objetivo de assegurar transparência e conformidade com normas legais e éticas de proteção de dados. Define responsabilidades e direitos dos agentes de tratamento e dos titulares (BRASIL, 2018).

Informação Sensível: Dado que, se divulgado ou acessado indevidamente, pode causar dano, discriminação ou violação de direitos fundamentais à pessoa natural. Inclui origem racial, convicção religiosa, opinião política, dado genético, biométrico, de saúde ou vida sexual (BRASIL, 2018).

Usuário: Sujeito que interage com um sistema, serviço ou aplicação digital, fornecendo ou acessando informações, podendo ser titular de dados, operador ou controlador, conforme o papel assumido no tratamento (BRASIL, 2018).

Grau de Sigilo: Nível de restrição aplicado à informação de acordo com sua criticidade e potencial de impacto em caso de divulgação não autorizada. Classifica-se em restrito, confidencial e relativo (BRASIL, 2012).

Nível de Acesso: Permissão atribuída a um agente ou perfil para visualizar, modificar ou excluir informações conforme o grau de sigilo e a função desempenhada. Implementa o princípio do menor privilégio e controle de acesso baseado em papéis (NIST, 2020).

Dado de Saúde: Informação relacionada ao estado físico ou mental de uma pessoa natural, incluindo histórico médico, resultados de exames, diagnósticos, tratamentos e dados genéticos ou biométricos associados à saúde (BRASIL, 2018).

Dado Pessoal: Informação relacionada a pessoa natural identificada ou identificável, direta ou indiretamente, por meio de um identificador como nome, CPF, dados de localização, identificadores eletrônicos ou outros fatores específicos (BRASIL, 2018).

Paciente: Pessoa que recebe atendimento, tratamento, cuidado ou serviço de saúde, seja em instituição pública ou privada, mantendo relação de confiança e confidencialidade com os profissionais de saúde (SAITO et al., 2013).

Profissional de Saúde: Pessoa legalmente habilitada e/ou registrada em conselho de classe para exercer atividades técnicas, assistenciais ou de pesquisa em saúde, comprometida com princípios éticos, sigilo profissional e proteção de dados sensíveis de pacientes. (WORLD HEALTH ORGANIZATION – WHO, 2023).

4.1. Estratégia de Privacidade

A partir do mapeamento conceitual, uma estratégia de privacidade dos dados de saúde em EHRs é proposta. A Figura 4.2 apresenta a instância Médico, da Classe *Healthcare professional* (Profissional de Saúde); as instâncias Alto, Médio e Baixo, da Classe *AccessLevel* (Nível de Acesso); e as instâncias Exame, Diagnóstico e Prescrição, da Classe *HeathData* (Dados de saúde). Em nossa proposta o nível de acesso para um médico é alto, permitindo o acesso a todos os dados de saúde. No entanto, em um outro cenário, o nível de acesso para um atendente seria baixo para acessar exames e diagnósticos.

Estratégias de privacidade podem variar de acordo com a política de acesso de cada organização. Ontologias podem contribuir neste contexto, pois são ferramentas de modelagem que possibilitam compartilhar, mesclar ou editar o conhecimento.

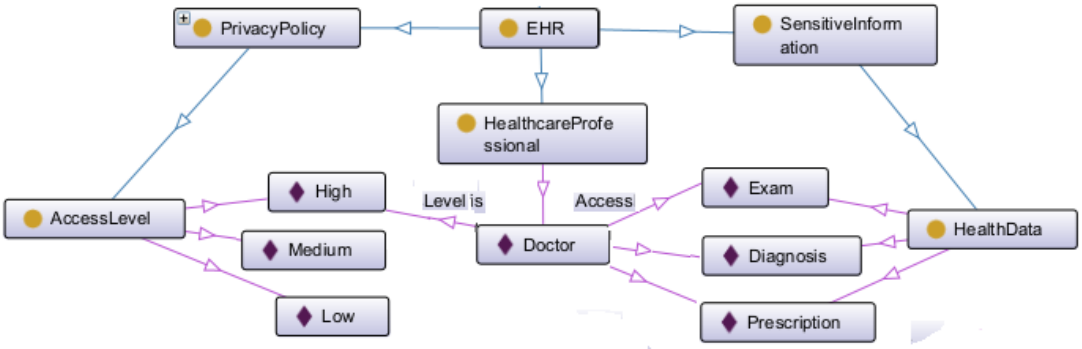

Figura 4.2 – Estratégia de privacidade dos dados de saúde

5. Considerações finais

Neste artigo, apresentou-se o projeto de pesquisa que aborda o desenvolvimento de uma ontologia de domínio destinada a preservação da privacidade em EHRs.

Apresentou-se o desenvolvimento dos conceitos principais e uma aplicação de mundo real, onde a ontologia é usada para fornecer parâmetros e termos formalizados para definir estratégias de privacidade. Este trabalho destina-se a ser útil para pesquisadores que buscam desenvolver métodos e processos sistemáticos, baseados em ontologia, voltados à proteção e preservação da privacidade das informações de prontuários eletrônicos de saúde.

Como trabalhos futuros, espera-se continuar expandindo a ontologia e melhorando sua expressividade, incorporando outros conceitos, relações, propriedades e indivíduos.

Referências

BEARD, L. et al. The challenges in making electronic health records accessible to patients. **Journal of the American Medical Informatics Association**, v. 19, n. 1, p. 116–120, 2012.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. Decreto nº 7.845, de 14 de novembro de 2012. **Regulamenta a Lei de Acesso à Informação** (Lei nº 12.527/2011). Brasília, 2012.

COSTA, J. F. R.; PORTELA, M. C. Percepciones de gestores, profesionales y usuarios acerca del registro electrónico de salud y de aspectos facilitadores y barreras para su implementación. **Cadernos de Saude Publica**, v. 34, n. 1, 2018.

CRUZ, M. S.; ROSA, F. F. Privacidade em prontuário eletrônico de saúde: uma abordagem ontológica. In: Seminário em Tecnologia da Informação do Programa de Capacitação Institucional (PCI) do CTI Renato Archer, 14., 2024, Campinas-SP: MCTI/CTI Renato Archer, 2024. p. 1-6. https://www.gov.br/cti/pt-br/publicacoes/producao-cientifica/seminario-pci/xiv_seminario_pci-2024.

GAJANAYAKE, R.; IANNELLA, R.; SAHAMA, T. Privacy oriented access control for electronic health records. **Electronic Journal of Health Informatics**, v. 8, n. 2, 2014.

GUARINO, N. Formal Ontology and Information Systems. **Formal Ontology in Information Systems: Proceedings of the 1st International Conference**, v. 46, n. June, p. 3–15, 1998.

JOINT TASK FORCE NIST. Security and Privacy Controls for Information Systems and Organizations. **NIST**

Special Publication, 465. https://doi.org/10.6028/NIST.SP.800-53r5, 2020.

SAITO, D. Y. T.; ZOBOLI, E. L. C. P.; SCHVEITZER, M. C.; MAEDA, S. T. User, client or patient? which term is more frequently used by nursing students? **Texto e Contexto Enfermagem**, v. 22, n. 1, p. 175–183, 2013.

W3C OWL WORKING GROUP. **W3C OWL Web Ontology Language**. Disponível em: <https://www.w3.org/TR/owl2-overview/>. Acesso em: 18 set. 2024.

WORLD HEALTH ORGANIZATION (WHO). **Health workforce**. Disponível em: < https://www.who.int/teams/health-workforce >. Acesso em: 26 mar. 2025.