DOI: 10.5748/18CONTECSI/COM/HEA/6762

BLOCKCHAIN IN HEALTHCARE FOR MEDICAL DATA SHARING: A PROPOSAL OF A DATA GOVERNANCE FRAMEWORK TO COMPLY WITH LAWS AND REGULATIONS.

Geraldo Santos Júnior - UNIVERSIDADE DE SÃO PAULO - Orcid: https://orcid.org/0000-0002-6214-7660

Daniel Cordeiro - UNIVERSIDADE DE SÃO PAULO - Orcid: https://orcid.org/0000-0003-4971-7355

Violeta Sun - USP - Orcid: https://orcid.org/0000-0003-1739-5312

This study sought to analyze the use of Blockchain for medical data sharing, which meets the laws and regulations in the healthcare. Analysis of legal aspects of the use of Blockchain for medical data sharing through a data governance framework. In this work an exploratory qualitative study was carried out (Gil, 2002). The analysis of the study was carried out through a data governance framework, raised by a Systematic Literature Review (SLR) of the literature, using data sources from academic literatures following Kitchenham (2007). (i) Aspects to be considered in the use of Blockchain for medical data sharing; (ii) governance recommendations on the use of Blockchain for medical data sharing; (iii) technical recommendations on the use of Blockchain for medical data sharing. (i) List of recommendations on the use of Blockchain for medical data sharing, which complies with laws and regulations in the healthcare; (ii) Systematic Literature Review (SLR), aiming to identify data governance frameworks. Benefits for an organization in adopting an application for medical data sharing.

Keywords: blockchain, medical data sharing, medical data, data governance, framework

APLICAÇÃO DE BLOCKCHAIN NA ÁREA DA SAÚDE PARA COMPARTILHAMENTO DE DADOS DE PACIENTES: PROPOSTA DE USO DE UM FRAMEWORK DE GOVERNANÇA DE DADOS PARA ATENDER AS LEIS E NORMAS DA ÁREA DA SAÚDE.

Esse estudo buscou analisar o uso de Blockchain para o compartilhamento de dados de pacientes, considerando leis e normas que regem a área de saúde Utilização de um framework de Governança de Dados para analisar aspectos legais no uso de Blockchain para compartilhamento de dados de pacientes. Foi realizado um estudo exploratório, qualitativo sobre o uso do Blockchain na área da Saúde, buscando um framework de Governança de Dados que atenda às necessidades da área. Foi realizada uma revisão sistemática da literatura sobre o tema para levantar publicações já realizadas sobre o tema. (i) Aspectos a serem considerados no uso de Blockchain para compartilhamento de dados de pacientes; (ii) recomendações de modelo de governança de dados no uso de Blockchain para compartilhamento de dados de pacientes; (iii) recomendações de técnicas no uso de Blockchain para compartilhamento de dados de pacientes. Recomendações no uso de aplicação de um framework de Governança de Dados ao se considerar a utilização de Blockchain para compartilhamento de dados de pacientes,para que leis e normas da área da saúde sejam atendidas; (ii) Revisão da literatura, com o objetivo de identificar frameworks de governança de dados. Utilização de um modelo de Governança de Dados para atender as necessidades de segurança da informação no compartilhamento de dados de pacientes, utilizando o Blockchain.

Palavras-chave: blockchain, compartilhamento de dados de pacientes, dados de pacientes, governança de dados, framework

Blockchain in healthcare for medical data sharing: a proposal of a Data Governance framework to comply with laws and regulations Aplicação de Blockchain na área da saúde para compartilhamento de dados de pacientes: proposta de uso de um framework de Governança de Dados para atender as leis e normas da área da saúde

The success obtained with the application of Blockchain in areas such as finance, encouraged the investigation of its applications in healthcare. An important application is the use of this technology to create distributed and decentralized systems for medical data sharing. This use faces privacy and data security issues as patient data is protected by law. As it deals with data properties, the use of a data governance framework can be useful to consider legal aspects of the use of Blockchain in order to comply with laws and regulations applied to healthcare data.

Blockchain, medical data sharing, medical data, data governance, framework.

O sucesso obtido com a aplicação do Blockchain em áreas como finanças, incentivou a investigação de suas aplicações na área da saúde. Uma aplicação importante é o uso dessa tecnologia para a criação de sistemas distribuídos e descentralizados para o compartilhamento de dados de pacientes. Este uso enfrenta questões de privacidade e segurança de dados, uma vez que os dados de pacientes são protegidos pela lei. Por se tratar de propriedades de dados, objeto da área de governança de dados, o uso de um framework de governança de dados pode ser utilizado para considerar os aspectos legais sobre o uso de Blockchain nesse contexto. Este trabalho analisa por meio de um framework de governança de dados como o uso de Blockchain para o compartilhamento de dados de pacientes pode ser explorado de forma a atender leis e normas da área da saúde.

Blockchain, compartilhamento de dados de pacientes, dados de pacientes, governança de dados, framework.

INTRODUÇÃO

O *Blockchain* é uma lista ordenada de registros ligados entre si através de uma cadeia em blocos (Wang et al., 2019). Ele é conhecido e explorado em diversas áreas como cartórios, educação e finanças. No contexto de saúde, o *Blockchain* pode viabilizar o compartilhamento de dados de pacientes, garantindo autenticidade, integridade, privacidade e proveniência de dados (Weiss et al., 2017). No cenário brasileiro, o Ministério da Saúde apresentou um projeto de transformação digital da saúde que utiliza o *Blockchain* como parte da solução, pois garante a segurança, tem um bom desempenho, permite um controle de acesso seguro e possibilita escalabilidade (Ministério da Saúde, 2020). A área da saúde é regida por uma série de normas e leis que devem ser seguidas no tratamento de dados de pacientes. O *Blockchain* pode atender a essas necessidades regulamentares e viabilizar o compartilhamento de dados entre instituições.

Conceitos fundamentais

Governança refere-se à organização de normas, regras e princípios, a fim de se ter padrões de comportamento público, com o objetivo de se obter regularidades comportamentais (Nye e Donahue, 2000). Dessa forma, podem-se estabelecer formas de administrar problemas e interesses em comum entre pessoas e entidades. A governança envolve tanto os regimentos formais, quanto informais, no interesse de pessoas e organizações. Quando se trata de uma empresa, os assuntos referentes a uma organização são tratados dentro do pilar de governança corporativa. Nesse contexto, a definição de métodos, papéis, responsabilidades e processos relacionados ao uso de dados possui fundamental importância dentro de organizações, principalmente quando se faz uso de dados sensíveis, como no caso da área da saúde, que trata de dados de pacientes. Esses aspectos de governança são abordados pela área de Governança de Dados (GD) que tem como objetivo o estabelecimento de métodos, responsabilidades e processos. Esses objetivos são estabelecidos para que se tenha padronização, proteção na integração e armazenamento de dados corporativos (Olavsrud, 2021). GD atua tanto o contexto de dados internos, que são gerados dentro da organização, quanto o de dados externos, que são incorporados por dados gerados por sistemas fora da organização. Também estão contidos no escopo da GD as políticas, normas, diretrizes e processos internos de uma organização.

Na literatura é possível encontrar algumas definições para o termo GD. Segundo Khatri e Brown (2010), GD trata aspectos relacionados "a quem tem o direito decisório e é responsável pela tomada de decisão da organização sobre os ativos de dados". Para Ladley (2012), GD atua na "organização e implementação de políticas, procedimentos, estrutura, papéis e responsabilidades que delineiam e reforçam regras de comprometimento, direitos decisórios e prestação de contas para garantir o gerenciamento apropriado dos ativos de dados". Segundo Thomas (2006), GD é um "quadro organizacional, regras, decisões certas e responsabilidades das pessoas e dos sistemas de informação quanto ao desempenho de processos relacionados à informação". Segundo Wende e Otto (2007), GD consiste na "especificação do modelo para os direitos de decisões e responsabilidades para encorajar o comportamento desejável no uso de dados". De acordo com o *The Data Governance Institute* (2015), GD é "um sistema de direitos de decisão e responsabilidades para processos relacionados à informação, executado de acordo com modelos acordados que

descrevem quem pode realizar quais ações com quais informações, e quando, em que circunstâncias, usando quais métodos". Este trabalho adotará a definição atribuída pelo instituto, que foi escolhida, considerando os aspectos abordados na definição, como "direitos de decisão e responsabilidades", "quando e quais ações relacionadas a informações serão tomadas", "circunstâncias e métodos relacionados ao uso de informações" são pontos fundamentais nessa pesquisa, além da relevância e conceituação do Instituto.

METODOLOGIA

Neste trabalho foi realizado um estudo exploratório qualitativo (Gil, 2002). Esse estudo buscou analisar o uso de *Blockchain* para o compartilhamento de dados de pacientes. O compartilhamento deve atender as leis e normas da área da saúde. A análise do estudo foi feita utilizando um *framework* de GD. Inicialmente foi realizada uma Revisão Sistemática (RS) da literatura utilizando-se fontes de dados de literaturas acadêmicas seguindo Kitchenham (2007), de frameworks de governança de dados. Na sequência, foi realizado um levantamento de leis e normas que regem a área da saúde e feita uma seleção de diretrizes relacionadas ao compartilhamento de dados de pacientes. A partir dessas diretrizes, foram definidos fatores relacionados ao uso de *Blockchain* para compartilhamento de dados de pacientes. Para analisar os fatores levantados, foi utilizado um dos *frameworks* de GD levantados. Por fim, foi proposta uma lista de recomendações no uso de *Blockchain* para compartilhamento de dados de pacientes, que considera as principais leis e normas que regem a área da saúde.

Planejamento

Este trabalho explora aspectos legais relacionados à segurança de dados no uso da tecnologia no compartilhamento de dados e dá sequência ao estudo anterior de Santos et al. (2020), onde foi explorado o potencial uso de *Blockchain* na área da saúde, seus benefícios e desafios. Foi realizada uma RS da literatura, com o objetivo de identificar frameworks de governança de dados, nas bibliotecas digitais: *ACM Digital Library (ACM)*, *Institute of Electrical and Electronics Engineers (IEEE)* e *Scopus*. Esta RS teve como objetivo identificar frameworks utilizados para governança de dados para obter: (i) um panorama dos frameworks de governança de dados; (ii) propósitos e objetivos de uso; (iii) *framework* adequado às necessidades de s segurança e privacidade no uso de *Blockchain* para compartilhamento de dados de pacientes. Nesta RS foram aplicados os seguintes critérios:

Critérios de inclusão:

- Trabalhos publicados e disponíveis integralmente em bases de dados científicas;
- Trabalhos publicados entre janeiro de 2009 e dezembro de 2020;
- Trabalhos que apresentassem frameworks de governança de dados.

Critérios de exclusão:

- Trabalhos que não estivessem disponíveis em versões eletrônicas para acesso;
- Trabalhos que apresentassem frameworks de maturidade de governança de dados.

Condução

O termo de busca utilizado foi "*((framework) AND ("data governance" OR "governança de dados"))".* Foram coletados 76 artigos nas fontes de dados. Desses, 20 artigos foram filtrados pelos critérios de inclusão e exclusão. Por fim, foram selecionados 4 trabalhos: Khatri et. al. (2010); Barata et. al. (2015); Reis et. al. (2018) e; Abraham et. al. (2019).

RESULTADOS

Framework de governança de dados é uma estrutura lógica para classificar, organizar e comunicar atividades complexas envolvidas na tomada de decisões e ação sobre os dados corporativos (Topi et al., 2014). Neste trabalho, o *framework* será utilizado para avaliar os fatores relacionados à segurança/privacidade no uso de *Blockchain* para compartilhamento de dados de pacientes. Os frameworks referentes à maturidade da GD dentro de uma organização não foram listados, por não ser objeto de estudo deste trabalho. A seguir serão apresentados os frameworks de GD identificados na RS.

1. DAMA DMBOK

Proposto pela *Data Management Association* (DAMA), o *Data Management Body of Knowledge* (DMBOK) trata o gerenciamento de dados propondo melhores práticas, métodos e padrões (Cupoli et, al., 2014). DMBOK, conhecido como "corpo de conhecimento" foi desenvolvido em 2009 e é difundido mundialmente. No DMBOK são apresentados dez processos considerados essenciais no gerenciamento de dados:

- *Governança de dados:* autoridade e controle, envolvendo cumprimento, monitoramento e planejamento da gestão de dados;
- *Gerenciamento de arquitetura de dados:* definição estruturada por meio de desenhos técnicos sobre o uso dos dados organizacionais;
- *Desenvolvimento dos dados:* desenvolvimento e implementação, além de manutenção das necessidades de uso de dados na organização;
- Gerenciamento de operações de dados: planejamento, controle, gestão do uso dos dados, envolvendo a geração, retenção e remoção dos dados;
- *Gerenciamento de segurança de dados:* desenvolvimento de políticas e procedimentos que garantam medidas de controles e restrição no uso de dados de forma segura;
- *Gerenciamento de dados mestre e referência:* planejamento, implementação e controle do uso de dados mestres e referências;
- *Gerenciamento de Data Warehousing e Business Intelligence:* planejamento, implementação e controle no uso de dados na tomada de decisão de dados internos;
- *Gerenciamento da documentação e conteúdo:* planejamento, implantação e controle de atividades referentes à gestão de dados provenientes de registros eletrônicos e físicos;
- *Gerenciamento de metadados:* planejamento, implementação e controle de práticas que auxiliem na qualidade e integração do uso de metadados na organização;
- *Gerenciamento de qualidade de dados:* implementação de técnicas para medir, controlar, aprimorar e garantir a qualidade dos dados para uso da organização.

2. *Framework* conceitual para GD

Proposto por Abraham, Schneider e Brocke, este framework (Figura 1) é organizado nos escopos: *Organizacional*, *Dado* e *Domínio*.

Figura 1

Framework conceitual para GD. Adaptado de Abraham et al. (2019).

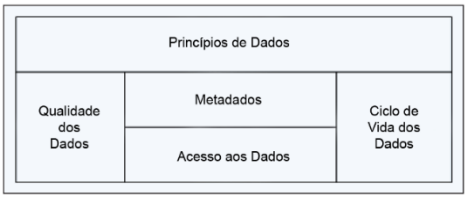
- *Antecedentes*: consiste nos fatores externos e internos que precedem ou preveem a adoção de práticas de governança de dados;
- *Escopo organizacional*: representa a abrangência da governança de dados. O escopo organizacional é dividido em: (i) intraorganizacional; (ii) interorganizacional;
- *Escopo de dado*: compreende todo tipo de fato na forma de texto, número, imagem, som ou vídeo;
- *Escopo de domínio*: esse escopo classifica os domínios de decisão de dados a partir do trabalho proposto por Khatri e Brown (2010). O autor deste modelo propõe os seguintes domínios: (i) qualidade de dados; (ii) segurança de dados; (iii) arquitetura de dados; (iv) ciclo de vida dos dados; (v) metadados; (vi) armazenamento e infraestrutura de dados;
- *Mecanismos de governança*: consistem em estruturas formais que conectam negócios, TI e funções de gerenciamento de dados e processos para tomada de decisão;
- *Consequências*: refere-se a resultados da governança de dados. No modelo são atribuídos e categorizados dois tipos de consequências da GD: (i) efeitos intermediários de desempenho; (ii) gerenciamento de risco.

3. Governança de Domínio de Decisões de Dados

O modelo proposto por Khatri e Brown é baseado nos seguintes domínios da GD: Princípios de Dados; Qualidade dos Dados; Metadados; Acesso aos Dados; Ciclo de Vida dos Dados. Esses domínios estão representados na Figura 2.

Figura 2

Domínios de decisão para governança de dados. Adaptado de Khatri e Brown (2010).



- *Princípios de Dados*: esclarecer o papel dos dados como um ativo e na definição de papéis e responsabilidades das partes envolvidas em todo o uso de dados;

- *Qualidade dos Dados*: tratar e definir requisitos para qualidade dos dados, considerando responsabilidades e potenciais usos;
- *Metadados*: definir e especificar a semântica e conteúdo dos dados de forma que os dados se tornem claros para os usuários da organização;
- *Acesso aos Dados*: estabelecer e implantar os requisitos para o acesso e uso dos dados na organização;
- *Ciclo de Vida dos Dados*: tratar e definir o gerenciamento do ciclo de vida dos dados, envolvendo captura, retenção, arquivamento e exclusão dos dados.

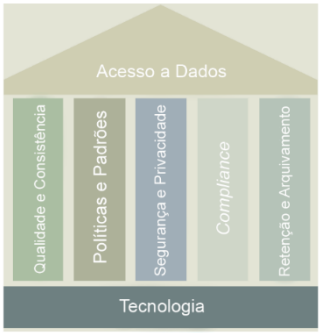
Este framework faz uso de questionamentos para atingir seu objetivo. Por meio de questões estratégicas relacionadas à GD, o modelo propõe funções potenciais e responsabilidades. As questões são agrupadas segundo os domínios da GD.

4. *Framework* Notre Dame

O framework de GD de Notre Dame tem duas bases como pontos fundamentais do modelo: acesso a dados e tecnologia. Além disso, o modelo possui cinco pilares entre as bases, que se trata de disciplinas da própria GD: qualidade e consistência; políticas e padrões; segurança e privacidade; *compliance*; retenção e arquivamento (Chapple, 2013). O *framework* é apresentado na Figura 3 com as bases separadas pelos pilares citados.

Figura 3

Framework de Governança de Dados de Notre Dame. Adaptado de Chapple (2013).



- *Acesso a dados*: o objetivo final claro do modelo é o acesso a dados. No modelo proposto, esse ponto recomenda possibilitar a todos aqueles que, por sua vez, necessitam de fato terem o acesso aos dados;
- *Tecnologia*: para o modelo, a tecnologia é uma ferramenta fundamental, porém a tecnologia não possui um fim em si mesmo. A tecnologia se torna como um meio que possibilita que os processos de negócio aconteçam e objetivo final seja atingido;
- *Qualidade e consistência*: esse pilar refere-se a garantias de que os dados que são utilizados partem de uma fonte confiável. Nesse pilar, questões relacionadas a garantias de que a interpretação dos dados seja feita de maneira confiável também são tratadas;
- *Políticas e padrões*: esse pilar trata as questões relacionadas às documentações necessárias. Nesse pilar são tratadas as questões de políticas de padronização;
- *Segurança e privacidade*: nesse pilar são tratadas as questões relacionadas à segurança e privacidade no tratamento dos dados, e questões de implementação de medidas que aumentem e garantam a segurança e privacidade dos dados;

- *Compliance*: esse pilar trata a adesão de leis e regulamentações que envolvem o armazenamento e processamento de dados dentro da organização. Essas diretrizes também estão relacionadas com a transmissão de dados com terceiros;
- *Retenção e arquivamento*: esse pilar trata questões de preservação de dados de forma eficaz e eficiente. O uso futuro na análise de informações pode ser beneficiado pela preservação de forma eficiente dos dados.

Análise de normas e diretrizes sobre privacidade e segurança de dados

O objetivo proposto foi selecionar documentos regulatórios e normas que poderiam afetar diretamente o uso do *Blockchain*, com questões de segurança e privacidade de dados de pacientes. Foi selecionado quatorze normas (enumeradas de CD01-CD14), descritas a seguir. O trabalho de Magnagnagno (2015) realizou o levantamento de mecanismos de privacidade de dados de pacientes na área da saúde, a partir de documentos regulatórios e normas. Neste trabalho, revisitamos os resultados para avaliar e ampliar a lista com normas que tangem o compartilhamento de dados de pacientes. A partir dessa nova seleção foi realizado um filtro de quais poderiam ser afetados pelo uso de *Blockchain*. A partir dessa lista de mecanismos, foram estudados os seus respectivos documentos regulatórios. Novas normas, como LGPD, foram incluídas por tratarem do manejo de dados sensíveis.

Quadro 1

Normas a serem consideradas no uso de Blockchain para o compartilhamento de dados de pacientes.

Código	Norma	Resumo	Autor
CD01	Norma ABNT NBR ISO/IEC 27001	Norma de definição e estabelecimento de requisitos de um sistema de gestão da segurança da informação, para uma organização.	Associação Brasileira de Normas Técnicas (2005)
CD02	Troca de Informações na Saúde Suplementar	Padrão obrigatório para intercâmbio de dados eletrônicos de saúde de usuários de planos de saúde entre agentes de saúde suplementar.	Agência Nacional em Saúde Suplementar (2020)
CD03	Resolução CFM Nº 1.821/2007	Resolução de normas técnicas sobre a digitalização e uso de sistemas de informação para uso de dados de pacientes.	Conselho Federal de Medicina (2007)
CD04	Código Penal	Código de regulação penal para definição de penas por atos considerados ilegais cometidos pelo cidadão.	Brasil (1940)
CD05	Código de ética da IMIA	Código de ética para profissionais de informática na saúde, com definição de princípios de conduta profissional.	International Medical Informatics Association (2003)
CD06	*Health Insurance Portability and Accountability Act*	Lei de portabilidade e responsabilidade de seguro saúde, com definições de regras nacionais para proteção de dados de saúde.	Centers for Medicare & Medicaid Services (2018)
CD07	ISO/TC 215	Comitê técnico para tratar do uso de informática na área da saúde, facilitando o	International Organization for

		intercâmbio e uso de dados de saúde.	Standardization (2017)
CD08	NBR ISO/IEC 27002	Norma para definição de práticas de gestão de segurança da informação para organizações, considerando o risco de segurança da informação.	Associação Brasileira de Normas Técnicas (2013)
CD09	Marco Civil da Internet	Lei de regulação do uso da internet no Brasil, com definição de princípios, papéis e garantias.	Brasil (2014)
CD10	Projeto de Lei de Assinaturas Digitais	Projeto de lei para definição de emissão de certificados digitais para pessoas físicas e jurídicas em um contexto digital.	Brasil (2002)
CD11	Manual Brasileiro de Acreditação Hospitalar	Manual para promover e garantir a implantação de um processo de avaliação de qualidade dos serviços de saúde, garantindo melhoria contínua.	Ministério da Saúde (2002)
CD12	Manual de Acreditação da JCI	Manual para avaliação para garantia de qualidade de forma periódica e voluntária, com definições de padrões requeridos.	Joint Commission International (2014)
CD13	*Personal Information Protection and Electronic Documents Act*	Lei de regulação da privacidade da informação, com definição de princípios a serem seguidos com boas práticas e obrigações legais.	Office of the Privacy Commissioner of Canada (2002)
CD14	Lei Geral de Proteção de Dados Pessoais	Lei para regulação de tratamentos de dados pessoais, inclusive no contexto digital, para pessoa física e pessoa jurídica.	Brasil. (2018)

Fatores no uso de *Blockchain* para compartilhamento de dados de pacientes

No Quadro 2 são apresentados os aspectos considerados nas normas selecionadas que serão utilizados como base para a análise neste trabalho.

Quadro 2

Aspectos considerados para análise das normas selecionadas.

Fator	Normas
Acesso de dados pelo paciente	CD13, CD14
Anonimato dos dados	CD05, CD14
Armazenamento dos dados	CD07
Autorização no compartilhamento de dados	CD03, CD04, CD05, CD14
Confidencialidade dos dados	CD12
Estrutura e conteúdo dos dados a serem compartilhados	CD02, CD03, CD05
Integridade dos dados	CD05, CD11, CD12
Perda de dados	CD12
Privacidade de cada campo dos dados	CD5, CD12, CD14
Requisitos e riscos na definição de perfis de usuários	CD01, CD03, CD06, CD10, CD12, CD13
Requisitos e riscos no compartilhamento de dados	CD01, CD03, CD06, CD07, CD08, CD09, CD11, CD14

Requisitos e riscos SGSI	CD01, CD08
Solicitação de remoção de dados pelo paciente	CD14
Trilha de auditoria	CD06

Análise de fatores levantados sob a perspectiva de framework de GD

A RS mostra a existência de múltiplos frameworks que auxiliam a implementação de GD. Este trabalho utilizará o framework de *Notre Dame como base para a análise das normas* devido a: (i) conhecimento e aceitação da comunidade de governança (Reis et al., 2018); (ii) foco e alvo final do framework, que é o acesso aos dados a quem necessita alinhado ao acesso aos dados pelo paciente, sendo o paciente o real dono do dado, que é o objetivo do modelo alvo do compartilhamento de dados de paciente; (iii) uso da tecnologia para atingir o foco e alvo do framework. Cada um dos fatores apresentados será analisado segundo o *framework* de GD de *Notre Dame.* Para isso, os fatores foram relacionados com os pilares do framework, segundo similaridade. Dessa forma, cada fator será analisado, segundo seu escopo, dentro de cada pilar do *framework*. No Quadro 3 é apresentada a relação entre os fatores identificados neste trabalho e os pilares do *framework* escolhido.

Quadro 3

Fatores identificados e Pilares do framework de governança de dados de Notre Dame.

Fator/Pilar	**Qualidade e consistência**	**Políticas e padrões**	**Segurança e privacidade**	***Compliance***	**Retenção e arquivamento**
A) Acesso	x	x			
B) Anonimato		x	x	x	x
C) Armazenamento	x	x	x	x	x
D) Autorização		x	x	x	x
E) Confidencialidade		x	x	x	
F) Estrutura e conteúdo				x	x
G) Integridade	x		x		
H) Perda de dados	x		x		
I) Privacidade de		x	x	x	
J) Perfis de usuários		x	x	x	
K) Compartilhamento		x	x	x	
L) SGSI		x	x	x	
M) Remoção	x		x	x	x
N) Auditoria	x	x	x	x	x

A) Acesso de dados pelo paciente: Esse fator será analisado segundo os pilares de "Qualidade e consistência" e "Políticas e padrões". Ao considerar o primeiro pilar, um paciente deve acessar dados que são confiáveis e que tenham a sua integridade garantida. Ao considerar o segundo pilar, a aplicação deverá seguir as diretrizes proporcionadas por leis e normas no contexto de dados de pacientes, incluindo os requisitos definidos pelo Sistema de Gestão de Segurança da Informação (SGSI) da organização. A ausência dessa funcionalidade requer que o paciente, caso deseje ter acesso a um exame/laudo, tenha que solicitar à organização. Dessa forma o problema de acesso aos dados pelo paciente ainda persiste e não é resolvido de forma integral.

B) Anonimato dos dados: Esse fator será analisado segundo os pilares de "Políticas e padrões", "Segurança e privacidade", "*Compliance*" e "Retenção e arquivamento". Ao considerar o primeiro pilar, a aplicação deverá seguir as diretrizes, incluindo os requisitos propostos pelo SGSI, sobre o armazenamento de dados de pacientes. Com relação ao segundo pilar, a aplicação deverá implementar controles e práticas para garantir a segurança e privacidade dos dados do paciente. Ao considerar o terceiro pilar, a aplicação deverá seguir as leis e normas referentes ao armazenamento de dados de pacientes. Ao considerar o terceiro pilar, a aplicação deverá garantir a preservação dos dados para que possa ser utilizado na geração de informações futuras. Os dados armazenados no banco de dados da aplicação devem ser armazenados de forma anônima, sem que seja possível identificar o paciente de forma direta. No armazenamento das informações médicas, a identificação do paciente deve ser preservada sempre que possível. Os dados do paciente são protegidos, inclusive em caso de vazamento de dados. Caso parte dos dados seja objeto de vazamento de dados, não será possível identificar as informações pessoais dos pacientes.

C) Armazenamento dos dados: Esse fator será analisado segundo cada um dos cinco pilares do modelo: "Qualidade e consistência", "Políticas e padrões", "Segurança e privacidade", "*Compliance*" e "Retenção e arquivamento". Ao considerar o primeiro pilar, o armazenamento dos dados deverá ser feito de forma com que a integridade do mesmo seja mantida. Nesse aspecto, realizar o armazenamento de valores *hash* na cadeia de *Blockchain* da aplicação é uma solução viável. A configuração proposta tem benefícios no contexto de privacidade e segurança. Caso aconteça algum acesso indevido e os dados gravados na cadeia sejam objeto de vazamento, nenhum dado sensível será exposto. Caso algum dado da cadeia de *Blockchain* da aplicação seja alterado, o conteúdo original não sofrerá alteração. Com relação ao segundo pilar, o armazenamento de dados também deverá considerar as políticas e padrões recomendados para o armazenamento de dados de paciente. Além disso, ao considerar o quarto pilar, tem-se que a escolha da forma como será armazenado poderá implicar em um não cumprimento de uma regulamentação, o que implicará em sanções penais para os envolvidos. Por isso, o armazenamento deverá seguir as leis, normas e regulamentações impostas pelo governo. Ao considerar o terceiro pilar, o armazenamento dos dados do paciente deverá ser feito considerando que se trata de dados sensíveis. A segurança e privacidade dos dados deverão ser priorizadas, implementando controles e práticas necessárias para que a segurança e privacidade dos dados do paciente sejam garantidas. Em relação ao último pilar, o armazenamento eficaz e eficiente dos dados pode ser utilizado futuramente na análise de informações para processos de melhoria contínua da organização, aprimorando o atendimento prestado ao paciente.

D) Autorização no compartilhamento de dados: Esse fator será analisado segundo os pilares de "Políticas e padrões", "Segurança e privacidade", "*Compliance*" e "Retenção e arquivamento". Ao considerar o primeiro pilar, na implementação de uma funcionalidade de autorização e revogação de compartilhamento de dados de pacientes, as diretrizes definidas por políticas e padrões deverão ser seguidas. O não cumprimento de alguma regulamentação pode implicar em um estado de não conformidade com órgãos reguladores, ferindo o terceiro pilar. Nesse aspecto tratam-se questões de autorização e revogação de acesso aos dados do paciente. O paciente pode autorizar quem ele gostaria que tivesse acesso aos seus dados, seja uma organização, ou uma pessoa física. Ao

considerar o segundo pilar, a implementação de controles e práticas que aumentem a segurança e a privacidade dos dados do paciente no compartilhamento de seus dados deverá ser priorizada, por se tratar de dados sensíveis. Além da segurança e privacidade, o armazenamento de dados que foram recebidos pós-compartilhamento poderá beneficiar uma organização, consolidando informações na prestação de futuros atendimentos médicos, segundo o quarto pilar do framework. Na autorização de compartilhamento de dados, também deve ser previsto situações em que o paciente não tenha consciência de realizar a autorização e revogação. Por isso, essa funcionalidade deve prever que o paciente também indique uma ou mais pessoas de sua confiança para realizar e revogar o compartilhamento de seus dados. Permitir que o paciente possa conceder/revogar o acesso aos seus dados está diretamente ligado ao objetivo dele se tornar o real dono do dado.

E) Confidencialidade dos dados: Esse fator será analisado segundo os pilares de "Políticas e padrões", "Segurança e privacidade" e "*Compliance*". Ao considerar o primeiro pilar, a confidencialidade dos dados do paciente deverá ser garantida respeitando as políticas e padrões do contexto inserido. Assim como as questões referentes ao terceiro pilar do modelo, o cumprimento de diretrizes definidas por meio de leis e normas deverá ser seguido, para que haja conformidade por parte da aplicação, segundo as regulamentações do meio. Por se tratar de dados sensíveis, a escolha de uso de anonimato de dados como um padrão transmite segurança tanto para as organizações parceiras quanto para os pacientes. Questões de segurança e privacidade são relacionadas ao segundo pilar do framework. Nesse sentido, a segurança e privacidade deverá ser adequada aos dados sensíveis do paciente, aumentando a confidencialidade dos dados. O desconforto de pacientes e organizações no compartilhamento de dados é mitigado, potencializando o reuso dos dados e sucesso do uso da aplicação. A aplicação também segue os padrões de segurança contidos na documentação do *Hyperledger Fabric (*Hyperledger, 2020).

F) Estrutura e conteúdo dos dados a serem compartilhados: Esse fator será analisado segundo os pilares "*Compliance*" e "Retenção e arquivamento". Segundo o primeiro pilar, a estrutura e conteúdo dos dados que serão compartilhados não poderão ferir nenhuma regulamentação definida por órgãos reguladores. Uma configuração em que a escolha de quais dados serão compartilhados está em maior sinergia com o objetivo maior do paciente se tornar o real dono do dado, podendo escolher com quem e o que será compartilhado. Ao considerar o segundo pilar do framework, uma organização que receberá os dados poderá implementar práticas eficazes e eficientes no reuso dos dados.

G) Integridade dos dados: Esse fator será analisado segundo os pilares de "Qualidade e consistência" e "Segurança e privacidade". O primeiro pilar destacado do framework trata questões desse fator. A garantia de que os dados foram gerados em uma fonte confiável e de que a integridade dos dados é mantida são requisitos fundamentais. A integridade dos dados do paciente é fundamental para que o dado possa ser reutilizado. Todos os benefícios citados sobre o reuso de dados só serão possíveis se os dados compartilhados tiverem sua integridade garantida. Além disso, a segundo pilar do framework trata questões de segurança e privacidade, relacionadas às implementações que podem ser feitas para que a segurança e privacidade dos dados possam ser garantidas. Nesse sentido, o uso de uma função *hash* criptográfica pode ser usada para verificar a integridade dos dados do paciente. Caso alguma alteração tenha acontecido nos dados do paciente, o valor gerado

pela função será diferente do anterior. Assim, bastará aplicar a função e verificar se o valor gerado pela função será o mesmo; caso o valor seja diferente, indicará que os dados foram alterados.

H) Perda de dados: Esse fator será analisado segundo os pilares de "Qualidade e consistência" e "Segurança e privacidade". Em caso de perda de dados local pelo parceiro, há uma possibilidade de recuperação de dados com integridade. Considerando o primeiro pilar do framework, a integridade é um fator fundamental para que a recuperação do dado seja eficaz. Todo parceiro terá, além do sistema hospitalar, um banco de dados, utilizando armazenamento de dados em nuvem pública. Toda informação também é armazenada em um banco de dados da própria aplicação, facilitando a recuperação de dados em caso de perda de dados. Os dados têm diversas cópias, que podem ser utilizadas em caso de perda de dados em algum dos bancos de dados. Ao considerar o segundo pilar, a implementação de controles e práticas é fundamental para a segurança e privacidade dos dados.

I) Privacidade de cada campo dos dados: Esse fator será analisado segundo os pilares "Políticas e padrões", "Segurança e privacidade" e "*Compliance*". Ao considerar o primeiro pilar do framework, a implementação de padrões, como por exemplo, o uso de estrutura organizacional garante uma maior governança dos dados. A privacidade de cada campo é tratada de forma escalonada, em geral. Cada funcionário terá acesso apenas aos dados do seu setor e serviço prestado. Ao considerar o segundo pilar, esse maior controle, segundo a especialidade de atuação aumenta a segurança e privacidade dos dados do paciente. Por exemplo, o setor de recepção tem acesso aos dados cadastrais e agenda. O setor de enfermagem tem acesso à agenda do dia, atendimentos realizados, triagem e evolução, de forma que os enfermeiros terão acesso somente aos dados de pacientes atendidos por eles. O setor médico terá acesso à agenda do dia, pacientes, triagem, consulta e evolução, que tenha prestado atendimento segundo a sua especialidade. Ao considerar o terceiro pilar, o cumprimento de leis e normas do uso de dados sensíveis é assegurado.

J) Requisitos e riscos na definição de perfis de usuários: Esse fator será analisado segundo os pilares de "Políticas e padrões", "Segurança e privacidade" e "*Compliance*". Sendo dados sensíveis, o acesso aos dados deve ser concedido apenas aos funcionários que de fato devem ter acesso aos dados. Considerando o primeiro pilar, a definição de políticas de acesso, com base na estrutura organizacional auxilia na implementação de padrões de controle. Ao considerar o segundo pilar, a implementação de controles e práticas garantem a segurança e privacidade dos dados. As informações pertencentes ao grupo de médicos poderão ser configuradas para que apenas esse grupo tenha acesso aos dados. Semelhantemente, em áreas como enfermaria, apenas os enfermeiros que tiveram contato com o paciente terão acesso aos dados do paciente. Ao considerar o terceiro pilar, o cumprimento de leis e normas sobre o uso de dados sensíveis, é garantido.

K) Requisitos e riscos no compartilhamento de dados: Esse fator será analisado segundo os pilares "Políticas e padrões", "Segurança e privacidade" e "*Compliance*". Ao considerar o primeiro pilar, no compartilhamento de dados de pacientes é fundamental a adequação das diretrizes propostas por políticas a serem adotadas. A adequação às regulamentações está relacionada à conformidade das leis e normas, considerando o terceiro pilar. Ao considerar o segundo pilar, os principais requisitos e riscos no

compartilhamento de dados de pacientes se concentram nos temas: segurança, compartilhamento, privacidade e segurança. Para mitigar riscos relacionados à privacidade e segurança no compartilhamento de dados de pacientes, o compartilhamento poderá ser feito somente pelo dono, escolhendo o que e com quem será compartilhado. Assim como mencionado, outras ferramentas como uso de ponteiros e função *hash* criptográfica pode ser utilizado para que o compartilhamento de dados possa acontecer de forma segura.

L) Requisitos e riscos SGSI: Esse fator será analisado segundo os pilares de "Políticas e padrões", "Segurança e privacidade" e "*Compliance*". Ao considerar o primeiro pilar, os requisitos definidos pelo SGSI podem variar para cada organização. Esses requisitos podem ser alterados conforme o tipo da organização (hospital, clínica, laboratório, etc.). Assim, apenas cada SGSI apontará quais os requisitos que a aplicação deverá preencher, para cada organização. Ao considerar o segundo pilar, a implementação de controles e práticas que aumentam a segurança e privacidade dos dados do paciente está ligado ao cumprimento requisitos impostos pelas leis e normas da área. Assim, a cobertura e nível de *compliance* da aplicação dentro da organização aumentarão, considerando o terceiro pilar.

M) Solicitação de remoção de dados pelo paciente: Esse fator será analisado segundo os pilares "Qualidade e consistência", "Segurança e privacidade", "*Compliance*" e "Retenção e arquivamento". Ao considerar o terceiro pilar, o paciente, garantido pela LGPD, poderá, a qualquer momento, solicitar que seus dados sejam removidos da aplicação, questões de segurança e privacidade, que estão relacionadas ao segundo pilar destacado. A remoção de dados implicará todos os locais que fazem uso dos dados daquele paciente. Ao considerar o primeiro e o último pilar, uma aplicação deverá realizar as remoções em todos os locais em que os dados daquele paciente são armazenados e, armazenar um dado diretamente na cadeia do *Blockchain*, implicará no não cumprimento da regulamentação. Para que os dados do paciente possam ser removidos, na cadeia de *Blockchain* deverão ser armazenados apenas valores de referência para os dados originais. Caso um paciente solicite que seus dados sejam apagados, a remoção será possível.

N) Trilha de auditoria: Esse fator será analisado segundo cada um dos cinco pilares do modelo: "Qualidade e consistência", "Políticas e padrões", "Segurança e privacidade", "*Compliance*" e "Retenção e arquivamento". Ao considerar o primeiro pilar, é necessário que se tenha uma trilha de auditoria da origem dos dados. A integridade dos dados precisa ser auditável, de forma que a integridade dos dados possa ser verificada. Ao considerar o segundo pilar, políticas e padrões devem ser implementados de forma a garantir a governança dos dados. Ao considerar o terceiro pilar, os controles e implementações realizadas na aplicação de forma a garantir e potencializar a segurança e privacidade dos dados do paciente deve ser auditável. As ações de autorização e revogação de compartilhamento de dados de pacientes são registradas pela aplicação. Para cada uma dessas ações também é gerado um valor *hash* que é armazenado no *Blockchain* da aplicação. Todas as ações relacionadas ao compartilhamento de dados de pacientes possuem uma trilha de auditoria, garantindo a conformidade com as leis e regulamentações, considerando o quarto pilar. Além disso, a configuração de perfis faz com que os funcionários de uma organização só tenham acesso aos dados que eles de fato precisam ter acesso. Todas as anotações e inclusões de dados são registradas e passíveis de auditoria. Ao considerar o quinto pilar, a retenção e arquivamento dos dados deverão ser

claros e transparentes. O armazenamento incorreto e indevido dos dados poderá ser passível de controle de auditoria futura.

Recomendações para o uso de *Blockchain* para compartilhamento de dados

Este trabalho se propõe a levantar uma série de recomendações a serem consideradas no desenvolvimento de uma aplicação com uso de *Blockchain* para compartilhamento de dados de pacientes. Essas recomendações consistem em direcionamentos na implementação de uma aplicação de *Blockchain*, que atendam normas e diretrizes da área da saúde. Por meio do framework de governança de dados de *Notre Dame*, os aspectos levantados foram analisados. A seguir, serão apresentadas recomendações, para o compartilhamento de dados de pacientes, sob o ponto de vista do framework de governança de dados de *Notre Dame*:

1. Acesso de dados pelo paciente: o paciente deve ter acesso aos seus dados pessoais, cadastrais, consultas, prontuário eletrônico, imagens, vídeos, laudos, entre outras informações, relacionadas a ele. Esse acesso pode ser realizado por meio da internet, utilizando um computador pessoal ou telefone celular. Isso facilita a leitura de algumas informações, como visualização de imagens em uma tela de um computador. Essa flexibilização permite que o paciente tenha acesso em qualquer lugar, desde que tenha acesso a um aparelho celular ou computador pessoal, com acesso à internet. Assim, o paciente tem a facilidade de ter acesso as suas informações sem a necessidade de se deslocar até uma organização de forma presencial.

2. Anonimato dos dados: o armazenamento dos dados do paciente deverá seguir o padrão de manter o anonimato dos dados do paciente por padrão. Assim, todos os dados que puderem ser armazenados sem que a identificação direta do paciente seja extremamente necessária, deverão ser armazenados de forma anônima. Essa configuração transmite confiabilidade no uso da aplicação para o paciente e para a organização. Assim, em casos de vazamento de dados, alguns cenários são mitigados a chance de vazamento de dados pessoais e identificação direta do paciente.

3. Armazenamento dos dados: os dados que serão armazenados na cadeia do *Blockchain* da aplicação devem ser referência para os dados originais. Assim, em caso de alteração de dados na cadeia, os dados originais são preservados, ainda que para que isso seja realizado seja necessário um custo computacional alto, dificultando a viabilidade da alteração. No contexto de segurança, caso haja o vazamento de dados, apenas valores *hash* seriam vazados, mantendo e preservando a segurança dos dados dos pacientes.

4. Autorização no compartilhamento de dados: o paciente deve ser responsável pela autorização e revogação de acesso aos seus dados médicos. Dessa forma, caso uma organização queira ter acesso, o paciente deverá autorizar, além de escolher quais informações ele deseja compartilhar com a organização. A autorização e revogação de acesso aos dados do paciente deverá ser realizada por meio de interfaces que facilitem a usabilidade das funcionalidades, neste processo. Dessa forma, assim como na consulta aos dados, o paciente pode conceder e revogar acesso aos seus dados por meio da internet. Além do paciente, a funcionalidade também deverá prever cenários em que o paciente não tenha condições físicas e psicológicas de realizar a concessão e revogação. Assim, o

paciente poderá cadastrar um usuário de sua confiança, que poderá conceder e revogar acesso aos seus dados médicos.

5. Confidencialidade dos dados: o tema de confidencialidade dos dados também é abordado, uma vez que se trata de uso de dados de pacientes, que são dados sensíveis. Para que a confidencialidade dos dados seja mantida, algumas técnicas podem ser aplicadas. Dessa forma, a criptografia dos dados que serão armazenados deve ser aplicada, para uma maior segurança. O uso de função *hash* criptográfica pode ser aplicado na criptografia dos dados do paciente. Além disso, a segurança na forma como os funcionários da organização acessa os dados também pode ser aprimorada. Assim, o uso de assinatura digital também deverá ser incorporado pela aplicação para compartilhamento de dados de pacientes.

6. Estrutura e conteúdo dos dados a serem compartilhados: os dados não devem ser compartilhados de forma direta. Assim como foi citado anteriormente, os dados que serão compartilhados com os parceiros serão valores *hash*, que são ponteiros de referência para cada objeto (consulta, exame, imagem, prontuário, etc.). Cada valor *hash* é uma referência a um objeto específico, que será concedido acesso pelo paciente para leitura dos dados. O compartilhamento de dados é feito potencializando a segurança e privacidade dos pacientes, sendo que os dados que são compartilhados são apenas valores de referência. Outro ponto importante é o tipo de *Blockchain* que será escolhido. São conhecidos dois tipos de *Blockchain*: *Permissioned* e *Permissionless*. Ao considerar o contexto de dados de pacientes, a volumetria de dados a ser compartilhado em uma rede, envolvendo exames, prontuários, etc. é alta. Quando se tem a necessidade de processamento de um alto número de transações, ter um tipo de *Blockchain* que consome muita energia em seu processo de consenso não é recomendado (Ferreira, 2017). Ao fazer uso de um *Permissioned Blockchain*, a aplicação terá um menor custo envolvendo o processo de consenso, além de assegurar a garantia de que as transações entre os participantes ocorrerão de forma segura. Nesse tipo de *Blockchain*, o processo de criação de um consenso permite a criação de uma assinatura digital, que poderá ser verificada pelos envolvidos no processo (Ferreira, 2017).

7. Integridade dos dados: o uso de uma função *hash* para geração do valor *hash*, para cada objeto (exame, prontuário, laudo, imagem, etc.), que será armazenado na cadeia do *Blockchain* da aplicação, auxilia na verificação de integridade dos dados. Esse tipo de configuração permite a validação dos dados originais. Assim, qualquer alteração dos dados originais implica na alteração do valor *hash* gerado. Dessa forma, os dados originais são protegidos e passíveis de verificação de alteração, para confirmar a integridade.

8. Perda de dados: um cenário passível de acontecer é a perda de dados por uma organização parceira. Caso uma organização tenha algum tipo de problema em sua infraestrutura local, a aplicação, por ter uma cópia de todos os dados, deverá ser capaz de prover o acesso a esses dados pela organização novamente. Assim, tem-se a mitigação de um ponto único de falha no armazenamento de dados dos pacientes. Isso acontece porque a aplicação será responsável pelo armazenamento dos dados, enquanto cada parceiro terá uma cópia dos dados.

9. Privacidade de cada campo dos dados: para manter, garantir e potencializar a privacidade dos dados dos pacientes, o paciente deverá escolher quais dados ele gostaria de compartilhar. Essa possibilidade de escolher o quê e com quem será compartilhado é uma

das características de o paciente se tornar o real dono do dado. Dessa forma, apenas os dados escolhidos pelo paciente serão compartilhados, segundo sua autorização. A definição de permissão de quais dados serão visualizados por cada funcionário dentro da organização será descrita no próximo item.

10. Requisitos e riscos na definição de perfis de usuários: de forma complementar ao item anterior, outro fator importante é a governança de acesso e visualização do dado dentro da organização. Quando uma organização recebe um prontuário, uma imagem ou um laudo de outra organização, a definição de quem poderá ter acesso deverá acontecer segundo a estrutura organizacional da instituição que recebeu os dados. Para que a organização possa dar sequência ao tratamento e cuidado do paciente, os funcionários só visualizarão os dados pertinentes ao seu setor, especialidade e histórico de tratamento prestado. Um funcionário só terá acesso aos dados de um paciente se já prestou atendimento a esse paciente ou caso esse paciente seja atendido pelo funcionário durante a jornada de atendimento e cuidado, dentro da organização. Se um paciente passar pelo setor de enfermagem de um hospital, apenas os funcionários que estavam na escala do dia do atendimento, ou que tiveram interação com o paciente terão acesso aos dados do paciente.

11. Requisitos e riscos no compartilhamento de dados: todas as funcionalidades devem considerar o fato de serem dados sensíveis e, por isso, deverão ser tratados considerando a privacidade e segurança dos dados do paciente. Além disso, recomenda-se o conceito do paciente como real dono dos dados, podendo escolher quando, com quem e o quais dados serão compartilhados. Assim, o compartilhamento se dá quando um paciente autoriza o acesso aos seus dados. A visualização dos dados pelos funcionários da organização acontece segundo a estrutura organizacional da instituição. Os dados são armazenados no banco de dados pela aplicação e os valores *hash* de cada objeto é armazenado na cadeia de *Blockchain* da aplicação.

12. Requisitos e riscos SGSI: uma aplicação de *Blockchain* para o compartilhamento de dados de pacientes não incorpora um SGSI. Dessa forma, se trata de um aspecto externo, que varia para cada organização. Assim, cada organização pode ter o seu SGSI, que atuará na definição de como os dados de pacientes serão utilizados. Portanto, a aplicação de *Blockchain* deve analisar os requisitos propostos pelo SGSI da organização para se adequar e estar em conformidade com o proposto.

13. Solicitação de remoção de dados pelo paciente: assim como previsto por direito para cada paciente, a aplicação de *Blockchain* para compartilhamento de dados de pacientes deverá prever a funcionalidade de remoção dos dados, caso um paciente solicite. Esse cenário tem relação no tipo de configuração e escolha de quais dados serão armazenados na cadeia de *Blockchain* da aplicação, tendo em vista que os dados gravados na cadeia de *Blockchain* não podem ser apagados. Assim, a aplicação deverá armazenar na cadeia de *Blockchain* os valores *hash* referentes a cada objeto (exame, imagem, etc.). Caso um paciente solicite a remoção dos dados pela organização, os dados poderão ser removidos.

14. Trilha de auditoria: a aplicação de *Blockchain* para compartilhamento de dados de pacientes deverá fazer registro de todas as ações realizadas pelo paciente e pelas organizações parceiras. O registro de alteração, inserção e exclusão de dados deverá ser gravado no banco de dados da aplicação. Além disso, os dados relacionados à autorização

e revogação de acesso no compartilhamento de dados também deverá ser armazenado. A aplicação terá uma trilha de auditoria das ações realizadas e das partes envolvidas.

Quadro 4

Quadro resumo das recomendações, segundo os fatores levantados.

Agrupamento	Fator	Recomendação
Governança	Autorização no compartilhamento	Paciente (e próximos, que o paciente autorizar) concede o acesso aos dados.
	Privacidade de cada campo dos dados	O paciente escolhe quais dados ele gostaria no compartilhamento de seus dados.
	Requisitos e riscos na definição de perfis	Governança de acesso ao dado segundo a estrutura organizacional da instituição.
	Requisitos e riscos no compartilhamento	Paciente como real dono dos dados autoriza o que e com quem será compartilhado.
	Requisitos e riscos SGSI	Cada organização pode ter o seu SGSI, que atuará na definição do uso dos dados.
	Trilha de Auditoria	Registro de todas as ações realizadas pelo paciente e pelas organizações parceiras.
Técnico	Acesso de dados pelo paciente	Paciente possui acesso aos dados a qualquer momento.
	Anonimato dos dados	Armazenamento de dados de forma anônima sempre que possível.
	Armazenamento dos dados	Armazenamento de referência para os dados reais na cadeia do *Blockchain.*
	Confidencialidade dos dados	Uso de criptografia para armazenamento dos dados dos pacientes.
	Estrutura e conteúdo dos dados	Os dados que serão compartilhados com os parceiros serão ponteiros para cada objeto.
	Integridade dos dados	Possibilidade de verificação de integridade, devido ao uso de função criptográfica *hash.*
	Paciente solicita remoção dos dados	Funcionalidade de remoção dos dados, caso um paciente solicite.
	Perda de dados	A aplicação, por ter uma cópia dos dados, é capaz de fornecer os dados em caso de perda.

CONCLUSÕES

Este trabalho elencou fatores relacionados a leis e normas e propõe recomendações a serem consideradas no desenvolvimento de uma aplicação que utilize *Blockchain* para compartilhamento de dados de pacientes. Ao seguir essas recomendações, a aplicação estará de acordo com as regulamentações legais. Assim, o uso de um *framework* de GD auxilia no compartilhamento de dados de forma a atender leis e normas da área da saúde. Considera-se que esse trabalho pode auxiliar gestores da área de tecnologia na definição de estratégias de investimento que utilizem o *Blockchain*. O acesso a dados gerados em outras instituições pode ser um diferencial competitivo para uma organização. Com o acesso a uma maior quantidade de dados de pacientes, uma organização poderá obter diversos benefícios, dentre eles: (i) oferecer um atendimento mais abrangente, com base no

histórico do paciente; (ii) redução de custos no reaproveitamento de exames; (iii) análise de tratamentos e prevenção de doenças a partir de uma maior base de dados de pacientes e; (iv) melhorias no atendimento prestado a partir da análise de dados de seus pacientes, identificando oportunidades de melhorias de processo.

RECOMENDAÇÕES

Muitos dos benefícios e oportunidades do uso de *Blockchain* para compartilhamento de dados de pacientes já são conhecidos. Sua adoção requer atenção a regulamentações legais e normas da área de saúde. O uso de um *framework* de GD pode auxiliar o processo de compartilhamento de dados de pacientes de forma a atender as leis e normas da área da saúde. Como trabalhos futuros, pretende-se analisar aplicações existentes que utilizem *Blockchain* utilizando o framework de GD apresentado, assim como desenvolver uma aplicação de *Blockchain* para compartilhamento de dados de pacientes utilizando as recomendações desse *framework.*

REFERÊNCIA BIBLIOGRÁFICA

Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. International Journal of Information Management, 49, (pp. 424-438).

Agência Nacional em Saúde Suplementar. (2020). Padrão TISS - organizacional. Disponível em: http://www.ans.gov.br/images/stories/Plano_de_saude_e_Operadoras/tiss/Padrao_tiss/tiss3/Padrao_TISS_Componente_Organizacional_202006.pdf. Acesso em: 01/08/2020.

Associação Brasileira de Normas Técnicas. (2005). Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos.

Associação Brasileira de Normas Técnicas. (2013). Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.

Barata, A. M., & Prado, E. P. V. (2015, May). Data Governance in Brazilian Organizations. In SBSI (pp. 267-272).

Brasil. (1940). Lei 2.848/1940. Código Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 28/07/2020.

Brasil. (2002). PL 7316/2002. Disciplina o uso de assinaturas eletrônicas e a prestação de serviços de certificação. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=96920. Acesso em: 28/07/2020.

Brasil. (2014). Lei 12.965/2014. Marco Civil da Internet. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28/07/2020.

Brasil. (2018). Lei 13.709/2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 28/07/2020.

Centers for Medicare & Medicaid Services. (2018). HIPAA Basics for Providers: Privacy, Security, and Breach Notification Rules. Washington, D.C.

Chapple, M. (2013). Speaking the same language: Building a data governance program for institutional impact. Educause Review, 48(6), 14-16.

Conselho Federal de Medicina. (2007). Resolução CFM No1.821/2007. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2007/1821. Acesso em: 01/08/2020.

Cupoli, P., Earley, S., & Henderson, D. (2014). Dama-dmbok2 framework. DAMA International.

Ferreira, J. (2017). Blockchain para Criação de Novos Modelos de Negócio e Seus Impactos na Indústria de Serviços Financeiros. Monografia. Universidade Federal de Pernambuco.

Gil, A. C. (2002). Como elaborar projetos de pesquisa (Vol. 4, p. 175). São Paulo: Atlas.

Hyperledger. (2020). A Blockchain Platform for the Enterprise. Disponível em: https://hyperledger-fabric.readthedocs.io/en/release-2.2/. Acesso em: 26/11/2020.

International Medical Informatics Association. (2003). O Código de Ética da IMIA para Profissionais de Informática em Saúde. Disponível em: https://www.imia-medinfo.org/new2/pubdocs/Portuguese_trans_Brasil.pdf. Acesso em: 01/08/2020.

International Organization for Standardization. (2017). International Organization for Standardization's (ISO) Technical Committee (TC) on health informatics. Chicago.

Joint Commission International. (2014). Padrões de Acreditação da Joint Commission International para Hospitais. Disponível em: https://www.jcrinc.com/-/media/deprecated-unorganized/imported-assets/jcr/default-folders/items/ebjcih14b_sample_pagespdf.pdf?db=web&hash=22513968F3BD3D7653E69A96EFAC5234. Acesso em: 28/07/2020.

Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM, 53(1), 148-152.

Kitchenham, B. (2007). Guidelines for Performing Systematic Literature Reviews in Software Engineering. Disponível em: https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf. Acesso em: 21/03/2020.

Ladley, J. (2012). Data Governance: How to Design, Deploy and Sustain an Effective Data Governance Program. The Morgan Kaufmann Series on Business Intelligence. Elsevier Science.

Magnagnagno, O. A. (2015). Mecanismos de proteção da privacidade das informações de prontuário eletrônico de pacientes de instituições de saúde (Master's thesis, Pontifícia Universidade Católica do Rio Grande do Sul).

Ministério da Saúde. (2002). Manual Brasileiro de Acreditação Hospitalar. Disponível em: http://bvsms.saude.gov.br/bvs/publicacoes/acreditacao_hospitalar.pdf. Acesso em: 28/07/2020.

Ministério da Saúde. (2020). Rede Nacional de Dados em Saúde. Disponível em: https://rnds.saude.gov.br/. Acesso em: 14/05/2021.

Nye, J., & Donahue, J. (Eds.). (2000). Governance in a Globalizing World. Washington, D.C.: Brookings Institution Press. Disponível em: http://www.jstor.org/stable/10.7864/j.ctvdf0j9t. Acesso em: 21/07/2021.

Office of the Privacy Commissioner of Canada. (2002). PIPEDA in brief. Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/. Acesso em: 28/07/2020.

Olavsrud, T. (2021). What is Data Governance: A Best Practices Framework for Managing Data Assets. Disponível em: https://www.cio.com/article/3521011/what-is-data-governance-a-best-practices-framework-for-managing-data-assets.html. Acesso em: 20/03/2021.

Reis, J. R., Viterbo, J., & Bernardini, F. (2018, May). A rationale for data governance as an approach to tackle recurrent drawbacks in open data portals. In Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age (pp. 1-9).

Santos Júnior, G., Cordeiro, D., & Sun, V. (2020). CONTECSI USP - International Conference on Information Systems and Technology Management - ISSN 2448-1041

The Data Governance Institute. (2015). Definitions of Data Governance. Disponível em: http://www.datagovernance.com/adg_data_governance_definition/. Acesso em: 27/03/2021.

Thomas, G. (2006). Alpha males and data disasters: the case for data governance. Brass Cannon Press.

Topi, H., & Tucker, A. (Eds.). (2014). Computing handbook: Information systems and information technology (Vol. 2). CRC Press.

Wang, Y., Zhang, A., Zhang, P., & Wang, H. (2019). Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain. IEEE Access, 7, 136704-136719.

Weiss, M., Botha, A., Herselman, M., & Loots, G. (2017, May). Blockchain as an enabler for public mHealth solutions in South Africa. In 2017 IST-Africa Week Conference (IST-Africa) (pp. 1-8). IEEE.

Wende, K., & Otto, B. (2007). A contingency approach to data governance. In Proceedings of 12th International Conference on Information Quality (pp. 163-176).