Abordagens sobre computação na nuvem: uma breve revisão sobre segurança e privacidade aplicada a e-saúde no contexto do Programa Conecte SUS e Rede Nacional de Dados em Saúde (RNDS)

Approaches to cloud computing: a brief review of security and privacy applied to e-health in the context of the Connect SUS Program and the National Health Data Network (RNDS)

DOI:10.34117/bjdv7n4-127

Recebimento dos originais: 07/03/2021
Aceitação para publicação: 06/04/2021

Luís Rafaeli Coutinho
Prefeitura Municipal de Florianópolis – SC – Distrito Sanitário Continente.
Prefeitura Municipal de Porto Belo – SC – Secretaria Municipal de Saúde de Porto Belo – SC.
E-mail:luisrafaelli29@gmailcom

Henrique Pereira Oliveira d'Eça Neves
USJ - Centro Universitário Municipal de São José/ADS
São José - Santa Catarina
Faculdade SENAC Palhoça
Palhoça – Santa Catarina
E-mail: prof.hike.neves@gmail.com

Lecian Cardoso Lopes
FURB - Universidade Regional de Blumenau
Blumenau - Santa Catarina
E-mail: lecianlopes@gmail.com

RESUMO

No presente artigo, apresentamos uma breve revisão da literatura para e-saúde em ambiente de armazenamento na nuvem. Foram selecionados artigos nas fontes da Medline e Google Scholar, objetivando encontrar informações recentes sobre esta tecnologia emergente para os serviços de saúde. Com relevância à segurança e privacidade de dados em diferentes estudos de computação em nuvem abordaram este tema. Armazenar informações como prontuários eletrônicos e dados relacionados à saúde na nuvem, requerer precauções para garantir a segurança e confidencialidade. Os provedores deste serviço devem garantir que os mecanismos de segurança estejam em vigor para evitar acesso não autorizado e violações de dados. O conhecimento na área de e-saúde e do Programa Conecte SUS também são abordados na sua essência quanto as necessidades de tratamentos na proteção dos dados. A LGPD é apresentada como um marco inovador na questão da conduta e cuidados que as empresas, profissionais e usuários devem ter na utilização dos sistemas e aplicativos em nuvem. Ademais, tópicos importantes da Rede Nacional de Dados em Saúde, ressaltam que os pacientes devem ser mantidos informados sobre como seus dados de saúde devem ser armazenados e gerenciados. O bom senso, o consentimento, a análise da importância na manutenção de dados específicos

relativizados à proteção das informações e penalidades impostas no caso de uso indevido são aqui analisadas.

Palavras-Chave: e-Saúde, LGPD, Nuvem, RNDS, Segurança

ABSTRACT

In this article, we present a brief review of the literature for e-health in a cloud storage environment. Articles were selected mainly by Medline and Google Scholar sources. Aiming to search for recent information about this emerging technology for health services. With relevance to data security and privacy that different cloud computing studies have addressed. Storing confidential information such as electronic medical records and health information in the cloud means that precautions must be taken to ensure the security and confidentiality of the data. Cloud service providers must ensure that all security mechanisms are in place to prevent unauthorized access and data breaches. Knowledge in the e-health area and the Connect SUS Program are also addressed in their essence and treatment needs in data security. The LGPD is presented as an innovative landmark in the question of the conduct and care that companies, professionals and users must have when using cloud systems and applications. As well as, important topics from the National Health Data Network. Patients should be kept informed about how their health data should be stored and managed. Common sense, consent, analysis of the importance of maintaining specific data related to the protection of information and penalties imposed in case of misuse.

Keywords: e-Health, LGPD, Cloud, RNDS, Security

1 INTRODUÇÃO

Os dados de saúde estão avançando em termos de quantidade e complexidade. As técnicas de geração de banco de dados tradicionais e de mineração de dados, necessitam de adequações quanto ao armazenamento, processamento e análise dos dados da área da saúde. Ferramentas inovadoras são necessárias para lidar com estes dados em tempo hábil (YOUSSEF, 2014).

De acordo com definição do National Institute of Standards and Technology (NIST) dos EUA, a computação em nuvem é "um modelo que pode ser distribuído, provisionado rapidamente e com recursos de computação configuráveis como servidores, armazenamento, aplicativos, redes e outros serviços" (MELL; GRANCE, 2009).

O compartilhamento de dados na nuvem está tornando-se vital para as organizações e usuários sociais. Os benefícios incluem maior produtividade e melhor gerenciamento de tempo, por exemplo, no uso de ferramentas colaborativas como o Google Docs. Com os usuários, os benefícios do compartilhamento de dados são claros, por exemplo, o Facebook, que permite compartilhar fotos e vídeos, além de compartilhar informações do dia-a-dia. Em relação aos prestadores de cuidados de saúde, estes estão migrando

rapidamente para a nuvem e os benefícios do compartilhamento também são evidentes, visto que, esta prática permite armazenar e compartilhar registros eletrônicos e, portanto, remover a dependência geográfica entre prestador de cuidados de saúde e paciente (THILAKANATHAN et al, 2014).

Porém, uma vez que uma das vantagens mais significativas da computação em nuvem é a sua enorme capacidade de armazenamento de dados, ela é suscetível a muitos ataques de privacidade e segurança. Como resultado, muitos hospitais e organizações de saúde estão relutantes em adotar a tecnologia "Cloud". Vale ressaltar que, alta acessibilidade, disponibilidade e confiabilidade podem tornar a computação em nuvem uma solução para problemas de interoperabilidade na área de saúde. O novo paradigma, para a prestação de serviços de saúde, foi adotado por países como EUA, Canadá, Reino Unido,

Coréia do Sul e União Europeia (ABBAS; KHAN, 2014).

Os avanços na tecnologia da informação apontam grande progresso de tecnologias de saúde em vários domínios (KOTZ et al, 2015). No entanto, essas novas tecnologias também fizeram dados de saúde não só muito maiores, mas também muito mais difíceis de manusear e processar (UR REHMAN et al e LIU et al, 2016).

2 METODOLOGIA

De modo restrito, consideramos pesquisa a busca sistemática de respostas a indagações e soluções tecnológicas às necessidades da vida diária, entendendo ciência como a atividade restrita a pesquisa de novos conhecimentos e ampliação do entendimento daqueles já existentes. Entendemos tecnologia como o desenvolvimento e análise de novos materiais, equipamentos e métodos de execução de determinadas tarefas (WAINER, 2006).

Este estudo trata-se de uma revisão bibliográfica. Para a análise e estudo de sistemas de registros eletrônicos de saúde baseados na enumeração em nuvem, revisamos artigos, pesquisas em segurança e problemas de privacidade, que diferentes estudos de computação em nuvem usam para o desenvolvimento em plataformas "Cloud". Continuam este estudo verificamos conceitos de e-saúde, a lei LGPD, o Programa Conecte SUS e a RNDS. A literatura relacionada foi obtida principalmente por fontes da Medline e Google Scholar. Foram selecionados em torno de 40 artigos. Muitas publicações mostram a viabilidade de implementações da computação em nuvem. Eles foram analisados e revisados na busca de informações que favoreçam sua aplicabilidade

aos serviços de saúde. Os artigos apresentam as vantagens, mas também os cuidados que as soluções baseadas em nuvem podem e devem fornecer aos sistemas e-saúde em geral e aos seus usuários.

3 RESULTADOS E DISCUSSÃO

A capacidade de acessar universalmente todas as informações de saúde do paciente em tempo hábil é de extrema importância. Portanto, um alto nível de integração de dados, interoperabilidade e compartilhamento de dados entre diferentes profissionais da área de saúde são necessários. Principalmente em instituições que pretendem oferecer cuidados de saúde de alta qualidade aos pacientes atendidos (YOUSSEF, 2014).

Os requisitos de armazenamento e disponibilidade contínua de dados de e-saúde favorecem o uso da computação em nuvem para prestação de serviços. A computação em nuvem está emergindo como uma promessa, um novo paradigma para a computação e está chamando a atenção tanto da academia como da indústria. Ela está mostrando grande potencial para melhorar a colaboração entre diferentes organizações de saúde no cumprimento dos requisitos comuns como a agilidade, rentabilidade e disponibilidade. Além disso, a migração de registros de saúde do paciente para o armazenamento em nuvem alivia os provedores de saúde das tarefas de gerenciamento de infraestrutura (ABBAS; KHAN, 2014).

A vantagem do custo da computação em nuvem não é apenas relacionada ao armazenamento. O fato da não necessidade de adquirir uma infraestrutura de hardware e software adequada a atender os requisitos necessários à disponibilização dos dados e informações, com segurança, consumindo menos energia, onde os usuários desta tecnologia, também reduzirão a emissões de carbono. Pesquisas sugerem que as tecnologias de informação e comunicação (TIC) já são responsáveis por 2% das emissões globais de carbono e que sua participação relativa poderá aumentar ainda mais (HU; BAI, 2014).

3.1 NECESSIDADES E REQUISITOS PARA A PRIVACIDADE DA E-SAÚDE NA NUVEM

Os provedores de serviços em nuvem devem implantar sistemas de autenticação que assegurem a privacidade da informação do paciente. Os governos devem exigir que os prestadores de serviços “Cloud” atendam os requisitos de privacidade necessários para garantir a integridade dos dados do paciente. A implantação de um quadro legal ajudará

a realizar um ambiente seguro. Políticas de privacidade foram legisladas em vários países para regular e preservar a privacidade dos registros de pacientes. Como exemplo, a Lei de Portabilidade e Responsabilidade do Seguro de Saúde que regula a privacidade da informática em saúde e a segurança dos dados dos pacientes nos EUA (HIPAA).

É importante enfatizar que estas políticas dependem de cada país. De acordo com a lei espanhola 41/2002, um Registro Eletrônico de Saúde (RES) é definido como uma documentação, que contém informações sobre a clínica evolução do paciente durante sua assistência no processo de saúde. Nesta lei, o uso dos RES são definidos, exigindo pessoal médico para manter a privacidade dos pacientes. A lei espanhola trata esse tipo de informação como "especialmente protegida". Este tipo de nomenclatura está definido na Lei 15/1999 com o objetivo de proteger a privacidade do paciente. O consentimento do paciente é necessário para gerenciar e acessar esses dados, exceto no caso de uma emergência em que a vida do paciente está em risco. Lembrando que as informações contidas no RES, incluindo prontuários são de exclusividade do paciente. (RODRIGUES et al, 2013).

No Brasil, passou a ser garantida pela Lei Orgânica nº 8.080 em 1990,

incorporando em seu artigo 6º a adição, tanto do desenvolvimento científico, quanto tecnológico. Desde então, é evidente a busca pela qualidade da atenção à saúde no país por meio dessas tecnologias (ROTTA; BRAGA; DOS SANTOS 2020).

Posteriormente ocorreu a criação de um processo de certificação de sistemas de registro eletrônico de saúde, com o estabelecimento dos requisitos obrigatórios e, acompanhando a legislação federal para documento eletrônico, reforçou a obrigatoriedade do uso de certificação digital (assinatura eletrônica) para a validade ética e jurídica de um Prontuário Eletrônico do Paciente (PEP) e RES. Um marco regulatório importante foi à publicação da Resolução CFM Nº 1821/2007. A estrutura de um prontuário, independentemente de ser eletrônico ou em papel, deve seguir as orientações e determinações da Resolução CFM Nº 1638/2002 que define o prontuário médico e torna obrigatória a criação da Comissão de Revisão de Prontuários nas instituições de saúde (SBIS, 2012).

A estratégia brasileira foi desenvolvida com base no pacote de ferramentas (toolkit), elaborado pela Organização Mundial da Saúde (OMS). Publicado em 2012, esse pacote de ferramentas define três componentes para implementação de uma Estratégia de Saúde Digital: um método para o desenvolvimento da visão nacional de e-Saúde, referentes aos respectivos planos de ação e quadro de monitorização (WHO, 2020).

A Resolução CIT nº 19/2017 aprova e torna público, o documento Estratégia e-Saúde para o Brasil, disponibilizado no sítio eletrônico: saude.gov.br/

Estratégia e-Saúde, que propõe uma visão de e-Saúde e descreve mecanismos contributivos para sua incorporação ao SUS até 2020.

O Decreto nº 9.637/2018 por sua vez institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295/1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666/1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

Em 2020, a Portaria nº 467/2020, dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional prevista no art. 3º da Lei nº 13.979, de 6 de fevereiro de 2020, decorrente da, até então, epidemia de COVID-19. Alguns conselhos de classe da área da saúde criar resoluções autorizando, em caráter emergencial, liberar o uso de ferramentas como Whatsapp para realização de teleconsulta. O que provavelmente não deve ser permitido pelos mesmos conselhos no período pós-pandemia por uma questão de segurança e privacidade dos dados envolvidos.

Em 2018, foi criada a Lei Geral de Proteção de Dados, que entrou em vigor em 2020, sendo um parâmetro na conduta, procedimentos, manipulação, armazenamento e cuidados nas informações pessoais, que será abordada em capítulo próprio no decorrer deste trabalho. Para a informatização da saúde, a integridade e confidencialidade são atributos fundamentais. A integridade significa preservar a precisão e consistência de dados no sistema de saúde, refere-se ao fato de que os RES não foram adulterados por uso não autorizado. A confidencialidade é definida pela Organização Internacional para Normalização (ISO) na ISO-17799 como "garantindo que a informação seja acessível apenas para aqueles autorizados a ter acesso" (YOUSSEF, 2014).

3.2 APLICAÇÕES DA COMPUTAÇÃO EM NUVEM

O modelo de computação em nuvem muda a infraestrutura da informática para provedores de serviços terceirizados que gerenciam os recursos de hardware e software com reduções significativas de custos. Uma plataforma que, além de armazenar volumes gigantescos dos dados de saúde, também serve como um gerenciamento estruturado dos dados em vários provedores de saúde. Desta forma os dados podem ser extraídos de

diferentes bancos de dados para tratamentos e outros fins analíticos. Normalmente, a nuvem consiste em elementos em camadas, como o armazenamento físico, a infraestrutura de serviços, os aplicativos e a comunicação à infraestrutura. Essa tecnologia é aplicada para compartilhamento, processamento e gerenciamento de dados de saúde. Além disso, a infraestrutura da nuvem e-saúde pode ser: (a) implementada internamente pelo profissional de saúde (privado), (b) mantida por alguma parte externa (pública), (c) mantida pelo prestador de cuidados de saúde e por uma parte externa juntos (híbrido), podendo assim ser categorizadas (ABBAS; KHAN, 2014).

Um novo tipo de serviço de computação em nuvem (nuvens da comunidade) também é promovido como outra adição possível. Em nuvens de comunidades tais serviços podem ser fornecidos (muitas vezes por uma organização) e consumidos por grupos de organizações em negócios ou profissões semelhantes às da organização fornecedora. Atualmente, há poucos exemplos para demonstrar a viabilidade dessa abordagem (SULTAN, 2014).

Os avanços na tecnologia móvel permitiram a dispositivos móveis, como smartphones e tablets, serem utilizados em uma variedade de aplicações dentro da área da saúde. Nos últimos anos, estes dispositivos começaram a se tornar abundantes em muitas aplicações de saúde. O motivo do crescente uso da computação móvel é a sua capacidade de fornecer uma ferramenta ao usuário quando e onde são necessárias, independentemente do movimento do usuário, portanto, com suporte de localização e independência (YOUSSEF, 2014).

Com o advento do monitoramento eletrônico de saúde remota, sistemas prometem revolucionar a saúde convencional. Métodos de cuidados integrando Internet of Things (IoT) aumentam ainda mais a inteligência, flexibilidade e interoperabilidade em nuvem. Nos últimos anos há um crescente interesse em sensores portáteis e hoje vários dispositivos estão disponíveis para cuidados de saúde pessoais, atividades físicas e consciência de atividade.

Estruturas seguras de armazenamento na nuvem foram, portanto, propostas para uso com registros médicos sensíveis. No entanto, proteger o processamento de dados na nuvem continua sendo um desafio, considerando a grande quantidade de aplicativos habilitados à IoT (HASSANALIERAGH et al, 2015 e HOSSAIN; MUHAMMAD, 2016).

3.3 ISCUSSÃO DE TÓPICOS REVISADOS NOS ARTIGOS

Para médicos e outros profissionais da área da saúde, o uso de soluções mais seguras, consiste em que elas sejam úteis e adequadas dentro do seu fluxo de trabalho clínico. Ações de tecnologia da informação em saúde apresentam muitos problemas exigentes para os usuários se autenticarem com os sistemas. Novos mecanismos de autenticação que trabalhem com smartphones, tablets, desktops, e laptops possuem relevância (KOTZ et al, 2015).

A adoção da tecnologia da computação em nuvem é mais do que um projeto de grande escala. Portanto, a complexidade do sistema será um critério fundamental ao decidir pela sua adoção. Além disso, os sistemas de informação hospitalar, como o Sistema de Imagem e Comunicação (PACS), o Sistema de Informação Hospitalar (HIS) e o Sistema de Informação Radiológica (RIS) são únicos por natureza. Migrar esses sistemas para a plataforma de computação em nuvem também será um fator crítico que estas organizações precisam considerar (LIAN; YEN; WANG, 2014).

Na revisão bibliográfica em questão, foi possível encontrar uma série de trabalhos de pesquisa em redes de sensores sem fio WSN (Wireless Sensor Networks) para aplicações médicas. Na verdade, a enorme quantidade de dados gerados e recolhidos por redes de sensores médicos apresentam vários desafios que as arquiteturas existentes ainda não podem resolver de forma mais eficiente com relação à segurança (LOUNIS et al, 2016). Devido à terceirização de dados, o servidor em nuvem não pode ser totalmente confiável para fornecer serviço de controle de acesso a dados, o que significa que os métodos de controle de acesso existentes ao servidor não são mais aplicáveis para sistemas de armazenamento em nuvem, exigindo o uso de outras técnicas para privacidade destes dados (YANG et al, 2013).

A crescente necessidade do cuidado remoto dos pacientes em casa combinada com a crescente popularidade de dispositivos móveis devido a sua natureza onipresente resultando em muitos aplicativos desenvolvidos para permitir a saúde móvel. A “Cloud”, em combinação com tecnologias móveis, permitiu que os médicos convenientemente monitorassem e avaliassem a saúde do paciente enquanto o paciente está no conforto de sua própria casa (HOSSAIN; MUHAMMAD, 2016).

Isso exige compartilhamento de informações de saúde entre equipes de saúde, como médicos e enfermeiros, a fim de fornecer melhor cuidados e de forma mais segura aos pacientes. No entanto, o compartilhamento de informações de saúde pode introduzir

problemas de privacidade e de segurança que podem muitas vezes entrar em conflito com a própria legislação (CHEN; YANG; SHIH, 2014).

3.4 MECANISMOS DE SEGURANÇA E CONTROLE DE PRIVACIDADE

Alguns dos problemas de segurança que devem ser considerados pelos provedores de serviços “Cloud” e seus clientes no cuidado às informações de saúde são: o acesso baseado em função, mecanismos de segurança de rede, criptografia de dados, assinaturas digitais e monitoramento de acesso. Além disso, para garantir a segurança das informações e cumprir as políticas de privacidade, o provedor de serviços em nuvem deve ser compatível com várias certificações e requisitos de terceiros. Como SAS70 Type II, PCI DSS Level 1, ISO 27001 e à Lei Federal de Gestão da Segurança da Informação (FISMA) por exemplo (RODRIGUES et al, 2013).

A confidencialidade e a integridade podem ser alcançadas através de técnicas de controle de acesso por autenticação, e criptografia. A autenticação é um efetivo método para proteger os dados. Técnicas com uma identidade baseada em sistema de criptografia (IBE) no controle de acesso de RES são bem difundidas (UR REHMAN, 2016).

A criptografia baseada em atributo (ABE) é um dos sistemas de criptografia mais usados na computação para o armazenamento de dados de saúde em nuvem. Alguns autores sugerem um modelo de nuvem híbrida que contém controles de acesso e técnicas de proteção de segurança como uma solução confiável (HU; BAI, 2014). A criptografia baseada em atributos (ABE) tem sido usada para projetar sistemas de compartilhamento do PEP. No entanto, as soluções existentes não conseguem alcançar vários aspectos importantes e objetivos de segurança. Um sistema de ABE multi-autoridade com texto cifrado, com responsabilidade do usuário e aplicado para projetar um sistema de compartilhamento do PEP, pode contribuir com uma segurança maior dos dados (XHAFA et al, 2015). É essencial que os esquemas ABE obtenham a revogação de atributos, pois os atributos dos usuários podem ser alterados com frequência (WANG et al, 2018).

O controle de acesso aos dados é uma maneira eficaz de garantir segurança de dados na nuvem. Uma política de texto cifrado com criptografia baseada em atributos (CP-ABE) é uma técnica promissora neste controle. No entanto, devido à ineficiência de decodificação e revogação, os esquemas CP-ABE existentes não podem ser aplicados diretamente para construir um esquema de controle de acesso aos dados para sistemas de armazenamento em nuvem multi-autorais, onde os usuários podem possuir atributos de

múltiplas autoridades. Uma proposta para um controle de acesso para armazenamento em nuvem multi-autoridade (DAC-MACS), com um esquema de controle de acesso a dados eficaz e seguro com decodificação e revogação apresentou boas possibilidades em estudo (YANG et al, 2013).

Uma proposta de novo modelo de privacidade acessível e autorizado pelo paciente com controle de privacidade multinível e preservando esquemas de autenticação cooperativa (PSMPA), aplicando três níveis diferentes de requisitos de segurança e privacidade na computação em nuvem, deve ser pensado. Distribuída em dispositivos móveis (sistema proposto) com aplicações em saúde, ilustraram que o PSMPA pode resistir a vários tipos de ataques maliciosos e superar esquemas anteriores em termos de armazenamento, computação e sobrecarga de comunicação. Após prova formal de segurança e avaliações de eficiência (ZHOU et al, 2015).

3.5 APLICATIVOS e-SAÚDE

As tecnologias permitem às informações de saúde estarem acessíveis a todos. Sabendo encontrá-las é possível utilizar aplicativos que expõem informações sobre determinados conhecimentos, outros com o objetivo de esclarecer ou acompanhar tratamentos e também proporcionar bem-estar. Estes aplicativos fazem uso de tecnologias computacionais e são executados em diferentes plataformas, com a Web, computadores pessoais ou dispositivos móveis. Porém, na maioria das vezes necessitando estar conectados à internet para o trânsito das informações manipuladas (E-SAÚDE, 2020).

O Serviço Único de Saúde (SUS) no Brasil, que presta atenção básica aos cidadãos brasileiros ganhou uma versão eletrônica o e-SUS AB há alguns anos, possibilitando a coleta de informações dos pacientes atendidos, alimentando uma base de dados. As informações nele armazenadas estão disponíveis para os gestores municipais prepararem estratégias de saúde a serem aplicadas à população (ALBUQUERQUE, 2017 e SILVA, 2019), durante um tratamento em outra cidade, sem perda de informações dos procedimentos anteriores.

Os aplicativos apresentados abordam principalmente a coleta e armazenamento de informações dos pacientes, permitindo acompanhar seus tratamentos a qualquer hora e local, dando aos gestores municipais e estaduais a possibilidade de aplicarem estratégias para mantenimento da saúde da população (MACHADO, 2011).

Em contrapartida existem aplicativos, de uso pessoal, focados em proporcionar o bem-estar, informar sobre casos de saúde ou apresentar as possibilidades de diagnósticos

frente aos sinais e sintomas informados. Há restrições às informações trabalhadas pelos aplicativos de uso pessoal, onde o aplicativo não pode diagnosticar enfermidades ou indicar procedimentos terapêuticos ou procedimentos diagnósticos, pois isto é um ato médico (CFM, 2011). Seus resultados resumem-se em indicar possíveis diagnósticos ou indicar um profissional da saúde.

Todos esses aplicativos fazem uso da rede computacional, seja local ou a internet para o fluxo de informação. Estas informações podem ser armazenadas em servidores locais ou em nuvem. Exigindo um custo que varia com os tipos de aplicativos a utilizar, o volume de dados a armazenar e o fluxo de dados e usuários existentes. No armazenamento em nuvem a preocupação com o mantenimento e segurança dos equipamentos e softwares envolvidos, fica a cargo da provedora do serviço, que busca sempre oferecer o melhor serviço a seus clientes (AUGUSTO, 2019).

Diferentes tipos de serviços são oferecidos em nuvem e as principais empresas envolvidas com eles, são: Dropbox, Google, Amazon, Microsoft e Apple. Além de prover o serviço de armazenagem eles disponibilizam funcionalidades empresariais como o compartilhamento de arquivos ou via edição de textos, planilhas eletrônicas e apresentações (GONÇALVES, 2016).

O documento Estratégia e-Saúde para o Brasil estabeleceu nove ações pilares da Estratégia de Saúde Digital brasileira, baseado no Pacote de Ferramentas da (OMS) Fonte: Brasil (2021a).

1) Reduzir a fragmentação das iniciativas de estratégia da Saúde Digital no SUS e aprimorar a governança da estratégia;

2) Fortalecer a intersetorialidade de governança de estratégia da Saúde Digital;

3) Elaborar o marco legal de estratégia da Saúde Digital no País;

4) Definir e implantar uma arquitetura para a Estratégia da Saúde Digital;

5) Definir e implantar os sistemas e serviços de Estratégia da Saúde Digital;

6) Disponibilizar serviços de infraestrutura computacional;

7) Criar arquitetura de referência para sustentação dos serviços de infraestrutura;

8) Criar a certificação em estratégia da Saúde Digital para trabalhadores do SUS;

9) Promover a facilitação do acesso à informação em saúde para a população (BRASIL, 2021a; ROTTA; BRAGA; DOS SANTOS 2020a).

Para que fossem contempladas as partes dois e três das etapas indicadas no Pacote de Ferramentas, propôs-se o Plano de Ação, o Monitoramento e a Avaliação (PAM&A)

da Estratégia de Saúde Digital para o Brasil 2019-2023 (Brasil, 2021b, ROTTA; BRAGA; DOS SANTOS 2020a).

A aplicação de serviços em nuvem para o e-Saúde gera preocupações quanto à segurança dos dados, principalmente por envolver o prontuário médico de um paciente. Possuindo um sigilo inviolável onde a resolução CFM nº 1997/2012 afirma "que o conteúdo do prontuário, lavrado pelo médico e pertencente ao paciente, é um documento amparado pelo sigilo profissional" (CFM, 2011). Dispor tais informações e documentos em ambiente de nuvem apresenta riscos e incertezas, mesmo com os provedores garantindo a segurança dos mesmos e os amparos legais regidos pela Lei Geral de Proteção de Dados - LGPD (BRASIL, 2018; GONÇALVES, 2016; AUGUSTO, 2019).

4 LEI GERAL DE PROTEÇÃO DE DADOS – LGPD

A Lei Geral de Proteção de Dados, conhecida por LGPD, é um novo marco legal brasileiro de grande impacto, aplicada para instituições públicas e privadas. Trata da proteção dos dados pessoais em qualquer relação que os envolva, por qualquer meio, seja por pessoa natural ou jurídica, e tomou por base o Regulamento Europeu de Proteção de Dados Pessoais. (BRASIL, 2018; PINHEIRO, 2020).

A atual relação entre a proteção de dados pessoais e o consentimento de uso na área da saúde corresponde na observância do dever de garantir ao paciente a deliberação livre e, consequentemente, a revisão e a possibilidade de retirada da anuência a qualquer momento sem prejuízo algum, mediante a garantia de que o tráfego desses dados não implicará em danos de espécie alguma (SARLET; CALDEIRA, 2019).

5 PROGRAMA CONECTE SUS

O Plano de Monitoramento e Avaliação de Saúde Digital para o Brasil para 2020-2028 descreve a organização e governança das ações de Monitoramento e Avaliação, bem como o conjunto de atividades a serem executadas e os respectivos atores responsáveis. As ações propostas no Plano têm como objetivo central propiciar que o Plano de Ação se mantenha consistente e aderente à Visão de Saúde Digital (BRASIL, 2020a).

O Conecte SUS é um programa do Governo Federal para a implementação da Estratégia de Saúde Digital no País. Sua finalidade é apoiar a informatização e a integração dos estabelecimentos de saúde, viabilizando as trocas e acesso às informações de saúde dos cidadãos brasileiros para longitudinalidade do cuidado em saúde (ROTTA et al, ROTTA; BRAGA; DOS SANTOS 2020b). Foi instituído pela Portaria nº 1.434, de

28 de maio de 2020, voltado à informatização da atenção e à integração dos estabelecimentos públicos e privados do SUS (BRASIL, 2020b).

Várias iniciativas importantes aconteceram anteriormente, mas sem estratégia bem definida, o marco da Estratégia de Saúde Digital no Brasil iniciou com a proposição da Política Nacional de Informação e Informática em Saúde (PNIIS). A Estratégia de Saúde Digital para o Brasil foi uma ferramenta identificada e agregada às ações do SUS. A sua finalidade é propor a estruturação, organização e a governança do SUS, por meio de tecnologias, bem como o uso e a disponibilidade destas em prol do uso de dados e informações de forma segura, visando subsidiar a gestão em todos os níveis de atenção (ROTTA; BRAGA; DOS SANTOS 2020b).

O programa Conecte SUS é composto pela Rede Nacional de Dados em Saúde (RNDS) e pelo Programa de Apoio à Informatização e Qualificação dos Dados da APS (Informatiza APS). A RNDS é uma plataforma nacional de integração de dados em saúde, favorecendo o uso ético desses dados. Seu objetivo é promover a troca de informações entre os pontos da Rede de Atenção à Saúde (RAS), permitindo a transição e continuidade do cuidado nos setores de saúde, público e privado (BRASIL, 2020c).

6 REDE NACIONAL DE DADOS EM SAÚDE

É uma plataforma nacional de integração de dados em saúde, favorecendo o uso ético desses dados. Seu objetivo é promover a troca de informações entre os pontos da rede de atenção a saúde (RAS), permitindo a transição e continuidade do cuidado nos setores de saúde pública e privado (ROTTA; BRAGA; DOS SANTOS 2020a).

No Brasil, a Portaria 1.434, de 28 de maio de 2020, aprovada recentemente pelo Ministério da Saúde, foi criada para estabelecer normas para o uso de TIC. Essa Portaria, além de instituir o Programa Conecte SUS, altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a RNDS, e também dispõe sobre a adoção de padrões de interoperabilidade em saúde (Brasil, 2020).

O acesso à RNDS será realizado via Portal Conecte SUS, Aplicativo Conecte SUS, assim como por meio do Prontuário Eletrônico do Cidadão (PEC) do e-SUS APS e dos demais sistemas de prontuários eletrônicos, públicos e privados que se integrarem à RNDS (ROTTA; BRAGA; DOS SANTOS 2020b).

O acesso, tanto pelo Portal, quanto pelo Aplicativo Conecte SUS, será realizado por meio do CPF do cidadão gestor ou profissional de saúde, validado pela base de dados da

Receita Federal. Para realizar a identificação e autenticação, será necessário ter (ou criar) uma conta gov.br (Brasil, 2021d).

As informações disponibilizadas pela RNDS poderão ser utilizadas para os seguintes fins (ROTTA; BRAGA; DOS SANTOS 2020b):

I - clínicos e assistenciais;

II - epidemiológicos e de vigilância em saúde;

III - estatísticos e de pesquisas;

IV - de gestão;

V - regulatórios; e

VI - de subsídio à formulação, à execução, ao monitoramento e à avaliação das políticas de saúde.

A RNDS está divida em serviços informacionais e serviços tecnológicos. É alimentado por diferentes bases de dados fornecendo informações de saúde para diferentes consumidores e geradores dessas informações (União, Estados, municípios, estabelecimentos de saúde, farmácias, laboratórios, portal e aplicativo Conecte SUS). A infraestrutura da nuvem e-saúde na RNDS é do tipo hibrida (mantido por um prestador e por uma parte externa). Com relação aos serviços tecnológicos relacionados à segurança na RNDS podemos citar segundo ROTTA; BRAGA; DOS SANTOS 2020b :

- *Blockchain*: solução responsável por tratar questões de segurança, rastreabilidade, desempenho, acesso e escalabilidade do software (BRAGA e VORA et al, 2018).

- Serviço de elegibilidade: é utilizado para definir se o profissional de saúde está habilitado ou não a acessar os dados do cidadão, aplicando regras de vinculação do profissional com o estabelecimento de saúde, CPF, categoria profissional, certificação da instalação de prontuário eletrônico, entre outros.

- Consentimento: inclui um termo para que o cidadão decida sobre autorizar ou não o compartilhamento dos seus dados de saúde. Trata-se, portanto, de uma manifestação livre (BRASIL, 2018);

- Certificado digital: responsável pela identificação unívoca e credenciamento de pessoas e estabelecimentos de saúde à RNDS, garantindo proteção às transações eletrônicas e outros serviços.

7 CONSIDERAÇÕES FINAIS

O ambiente em nuvem alivia as organizações de saúde das tarefas de gerenciamento de infraestrutura e também minimiza custos de desenvolvimento e manutenção

tecnológicos. Esta estrutura oferece um alto nível de integração, interoperabilidade, disponibilidade e compartilhamento de dados de saúde entre prestadores de cuidados de saúde, pacientes e praticantes. As precauções devem ser consideradas essencialmente com mecanismos de segurança e privacidade. A presente revisão mostra estudos crescentes e em desenvolvimento sobre a tecnologia de armazenamento em nuvem que devem ser aprimorados e otimizados.

Neste contexto a LGPD deve ser entendida como uma referência na conduta e tratamento de dados pessoais e sensíveis, nos vários setores do uso da informática, em especial nos serviços de saúde.

A Rede Nacional de Dados em Saúde e programa Conecte SUS por sua vez visam informatizar todas equipes de saúde com integração dos dados de saúde público e privado, qualificando esses dados em saúde. Melhorando a eficiência de intervenções e cuidados ao cidadão em todos os níveis de atenção.

A segurança e a privacidade estão emergindo como um novo desafio na informática no setor de saúde com o uso da tecnologia “Cloud”. Buscando a confidencialidade, o sigilo das informações pessoais, o armazenamento seguro de dados, a preservação da autenticidade e integridade das informações eletrônicas em saúde, assim como, de outros domínios comerciais.

REFERÊNCIAS

ABBAS, Assad; KHAN, Samee U. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. IEEE Journal of Biomedical and Health Informatics, v. 18, n. 4, p. 1431-1441, 2014.

ALBUQUERQUE, Saemmy Grasiely Estrela de et al. Buscando a qualidade da informação produzida pelo e-sus ab: influências, dificuldades e perspectivas dos gestores em saúde. 2017.AUGUSTO, Varella Walter. Implementação e migração para computação em nuvem. Editora Senac São Paulo, 2019.

AUGUSTO, Varella Walter. Implementação e migração para computação em nuvem. Editora Senac São Paulo, 2019.

BRAGA, Juliao et al. Blockchain to improve security, knowledge and collaboration inter-agent communication over restrict domains of the internet infrastructure. arXiv preprint arXiv:1805.05250, 2018.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF. 2018. Acessado em 5 mar. 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/ lei/L13709.htm.

Brasil. Ministério da Saúde. Secretaria-Executiva. Departamento de Informática do SUS. Estratégia de Saúde Digital para o Brasil 2020-2028 [recurso eletrônico] / Ministério da Saúde, Secretaria-Executiva, Departamento de Informática do SUS. – Brasília : Ministério da Saúde, 2020a.

BRASIL. MINISTÉRIO DA SAÚDE. Portaria 1.434, de 28 de maio de 2020b. Institui o Programa Conecte SUS e altera a Portaria de Consolidação nº 1/GM/MS, de 28 de setembro de 2017, para instituir a Rede Nacional de Dados em Saúde e dispor sobre a adoção de padrões de interoperabilidade em saúde. Acessado em 05 de mar. de 2021. Disponível em: http://www.in.gov.br/en/web/dou/-/portaria-n-1.434-de-28-de- -maio-de-2020-259143327.

BRASIL. MINISTÉRIO DA SAÚDE. Saúde Digital. Portal do Governo Brasileiro, 2021a. Acessado em 5 mar. 2021. Disponível em: <https://saudedigital.saude.gov.br/>.

BRASIL. MINISTÉRIO DA SAÚDE. Plano de Ação, Monitoramento e Avaliação (PAM&A) da Estratégia de Saúde Digital para o Brasil 2019-2023. Portal do Governo Brasileiro, 2021b. Acessado em 05 mar. 2021. Disponível em <https://saudedigital. saude.gov.br/a-estrategia-brasileira/>.

BRASIL. MINISTÉRIO DA SAÚDE. Rede Nacional de Dados em Saúde (RNDS). Portal do Governo Brasileiro, 2021c. Acessado em 5 mar. 2021. Disponível em: <https:// rnds.saude.gov.br/>.

BRASIL. MINISTÉRIO DA SAÚDE. Crie sua conta gov.br. Portal do Governo Brasileiro. Acessado em 5 março 2021d. Disponível em: https://sso.acesso.gov.br/login?client_ id=acesso.gov.br

CENTERS FOR DISEASE CONTROL AND PREVENTION et al. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. MMWR: Morbidity and mortality weekly report, v. 52, n. Suppl. 1, p. 1-17, 19, 2003.

CFM, Resolução CFM nº 1.627/2001, Conselho Federal de Medicina. 2001.

CFM, Resolução CFM nº 1997/2012, Conselho Federal de Medicina. 2012.

CFM; SBIS, Cartilha Sobre Prontuário Eletrônico - A Certificação de Sistemas de Registro Eletrônico de Saúde, segurança e confiabilidade para a informação do paciente. CFM e SBIS, 2012.

CHEN, Chin-Ling; YANG, Tsai-Tung; SHIH, Tzay-Farn. A secure medical data exchange protocol based on cloud environment. Journal of medical systems, v. 38, n. 9, p. 112, 2014.

E-SAÚDE. E-Saúde – É de saúde que Entendemos mais, My Health Tecnologia, 2020, disponível em: https://esaudeapp.com.br, acesso em: 05 jul. 2020..

GONÇALVES, Glauber Dias et al. Trabalho colaborativo em serviços de armazenamento na nuvem: Uma análise do dropbox. In: XXXIV Brazilian Symposium on Computer Networks and Distributed Systems (SBRC). 2016.

HASSANALIERAGH, Moeen et al. Health monitoring and management using Internet-ofThings (IoT) sensing with cloud-based processing: Opportunities and challenges. In: 2015 IEEE International Conference on Services Computing. IEEE, 2015. p. 285-292.

HOSSAIN, M. Shamim; MUHAMMAD, Ghulam. Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Computer Networks, v. 101, p. 192-202, 2016.

HU, Yan; BAI, Guohua. A systematic literature review of cloud computing in eHealth. arXiv preprint arXiv:1412.2494, 2014.

KOTZ, David et al. Security for mobile and cloud frontiers in healthcare. Communications of the ACM, v. 58, n. 8, p. 21-23, 2015.

LIAN, Jiunn-Woei; YEN, David C.; WANG, Yen-Ting. An exploratory study to understand the critical factors affecting the decision to adopt cloud computing in Taiwan hospital. International Journal of Information Management, v. 34, n. 1, p. 28-36, 2014.

LIU, Zheli et al. Cloud-based electronic health record system supporting fuzzy keyword search. Soft Computing, v. 20, n. 8, p. 3243-3255, 2016.

LOUNIS, Ahmed et al. Healing on the cloud: Secure cloud architecture for medical wireless sensor networks. Future Generation Computer Systems, v. 55, p. 266-277, 2016.

MACHADO, Cristiani Vieira; LIMA, Luciana Dias; BAPTISTA, Tatiana Wargas de Farias. Princípios organizativos e instâncias de gestão do SUS. Qualificação dos Gestores do SUS, v. 2, p. 47-72, 2011.

MELL, Peter; GRANCE, Tim. The NIST Definition of cloud computing. v. 15, 10 jul. 2009. 2010.

ORGANIZAÇÃO MUNDIAL DA SAÚDE. Capacidades Humanas para a Saúde Telessaúde. Disponível em: <http://www.paho.org/bra/index.php?option=com_content&view=article&id=256&Itemid=373>. Acesso em: 06 jul. 2016.

PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD. Saraiva Educação SA, 2020.

RODRIGUES, Joel JPC et al. Analysis of the security and privacy requirements of cloudbased electronic health records systems. Journal of medical Internet research, v. 15, n. 8, p. e186, 2013.

ROTTA, Rejane Faria Ribeiro; BRAGA, Renata Dutra; DOS SANTOS, Silvana de Lima Vieira. Programa Nacional em Saúde Digital: Trajetória da Saúde Digital no Brasil, Universidade Federal de Goiás. Comissão de Governança de Informação em Saúde, 2020a.

ROTTA, Rejane Faria Ribeiro; BRAGA, Renata Dutra; DOS SANTOS, Silvana de Lima Vieira. Rede Nacional de Dados em Saúde: o que precisamos saber ?, Universidade Federal de Goiás. Comissão de Governança de Informação em Saúde, 2020b.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. civilistica. com: revista eletrônica de direito civil, v. 8, n. 1, p. 1-27, 2019.

SILVA, Francisco Anderson Mariano da et al. Avaliação do serviço (e-SUS–AB) na perspectiva dos gestores municipais de saúde da 7ª Região Paraibana. 2019.

THILAKANATHAN, Danan et al. A platform for secure monitoring and sharing of generic health data in the Cloud. Future Generation Computer Systems, v. 35, p. 102-113, 2014.

UR REHMAN, Muhammad Habib et al. Big data analytics in mobile and cloud computing environments. In: Innovative Research and Applications in Next-Generation High Performance Computing. IGI Global, 2016. p. 349-367.

VORA, Jayneel et al. Bheem: A blockchain-based framework for securing electronic health records. In: 2018 IEEE Globecom Workshops (GC Wkshps). IEEE, 2018. p. 1-6.

WAINER, J. et al. O que é pesquisa em informática em saúde?. RITA, v. 13, n. 1, p. 42-56, 2006.

WANG, Shangping et al. Efficiently revocable and searchable attribute-based encryption scheme for mobile cloud storage. IEEE Access, v. 6, p. 30444-30457, 2018.

WORLD HEALTH ORGANIZATION - WHO; INTERNATIONAL TELECOMMUNICATION UNION - ITU. National eHealth Strategy Toolkit. 2012.

Acessado em 10 jul. 2020. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_HEALTH. 05-2012-PDF-E.pdf.

XHAFA, Fatos et al. Privacy-aware attribute-based PHR sharing with user accountability in cloud computing. The Journal of Supercomputing, v. 71, n. 5, p. 1607-1619, 2015.

YANG, Kan et al. DAC-MACS: Effective data access control for multiauthority cloud storage systems. IEEE Transactions on Information Forensics and Security, v. 8, n. 11, p. 1790-1801, 2013.

YOUSSEF, Ahmed E. A framework for secure healthcare systems based on big data analytics in mobile cloud computing environments. Int J Ambient Syst Appl, v. 2, n. 2, p. 1-11, 2014.

ZHOU, Jun et al. PSMPA: Patient self-controllable and multi-level privacy-preserving cooperative authentication in distributedm-healthcare cloud computing system. IEEE transactions on parallel and distributed systems, v. 26, n. 6, p. 1693-1703, 2014.