CIGIA
I CONFERÊNCIA INTERNACIONAL
DE GESTÃO DA INFORMAÇÃO E ARQUIVOS

OpenEHR como solução para o Regulamento Geral de Proteção de Dados

Mariana Leite-Sousa

Healthy Systems - HLTSYS, Portugal, msousa@hltsys.pt

Olívia Pestana

Faculty of Arts of the University of Porto, Portugal, opestana@letras.up.pt

Duarte Ferreira

Faculty of Engineering of the University of Porto, dferreira@fe.up.pt

Cátia Santos-Pereira

Healthy Systems - HLTSYS, Portugal, catiapereira@hltsys.pt

Ricardo Cruz-Correia

CINTESIS, Portugal, rcorreia@med.up.pt

Resumo

Introdução: As preocupações relacionadas com a privacidade e proteção de dados pessoais resultaram em reformas da legislação existente na UE. O Regulamento Geral de Proteção de Dados visa reformar as medidas existentes sobre o tema da proteção de dados pessoais dos cidadãos da União Europeia, com forte incidência nos direitos e liberdades das pessoas no estabelecimento de regras para o processamento de dados pessoais. O OpenEHR é uma norma que incorpora muitos princípios de interoperabilidade e segurança de software para registos eletrónicos de saúde.

Objetivo: Este trabalho tem como objetivo compreender até que ponto a norma openEHR pode ser considerada uma solução para os requisitos necessários ao RGPD.

Métodos: Foi feito uma lista de requisitos para um SIS compatível com o RGPD e uma identificação das funcionalidades openEHR. Os requisitos foram categorizados e comparados com as funcionalidades.

Resultados: Os requisitos identificados para os sistemas foram combinados com as funcionalidades openEHR, o que resultou em 15 requisitos combinados com o

openEHR. Todas as funcionalidades identificadas coincidem em pelo menos um requisito.

Discussão: O openEHR é uma solução para o desenvolvimento de um SIS que reforça a privacidade e proteção de dados pessoais, garantindo que estes sejam contemplados no desenvolvimento do sistema. As instituições podem garantir que o seu SIS seja compatível com o RGPD, salvaguardando a qualidade dos dados médicos e, como resultado, a prestação dos cuidados de saúde.

Palavras-chave: RGPD, openEHR, proteção de dados, SIS

1. Introdução

1.1. Privacidade e proteção de dados nos registos dos pacientes

As atividades do setor de saúde são extremamente dependentes de informação, sendo o registo clínico um dos elementos cruciais para os cuidados de saúde (Slee et al, 2000). Os registos clínicos contêm, de forma completa e exata, informações relacionadas com o historial médico, diagnóstico, tratamentos, prescrições médicas, entre outros dados. De certa forma, este pode ser encarado como um histórico da nossa vida. A informação médica assume assim um cariz extremamente sensível, sendo considerada um dos tipos mais confidenciais de informação pessoal.

As tecnologias de informação (TI) e os Sistemas de Informação de Saúde (SIS) surgiram como ferramentas importantes para suportar as necessidades organizacionais das instituições de saúde, sendo responsáveis por processar os dados de saúde. Compreendendo os efeitos da disseminação das TI numa era orientada pelos dados (Yamamoto, 2016), é importante perceber o seu impacto no tratamento e proteção dos dados pessoais. Os SIS proporcionam um ambiente integrado, onde a informação é facilmente partilhada e acedida, mas é cada vez mais importante que a privacidade seja pensada no desenho dos sistemas que são implementados.

Considerando a privacidade como direito fundamental dos cidadãos, a proteção dos dados pessoais dos pacientes trata-se de uma obrigação, fundamentada pela legislação que tem sido desenvolvida ao longo dos anos.

1.2. Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados (RGPD), aprovado a 27 de Abril de 2016, constitui uma reforma à Diretiva de 95/46/CE, sendo relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

O RGPD visa a proteção dos dados pessoais dos residentes da UE, providenciando uma framework consolidada que guie a utilização dos dados pessoais nas mais diversas indústrias dentro da UE. Essencialmente, o novo regulamento vem criar um modelo que obriga as organizações a considerarem as questões relacionadas com a proteção e riscos de privacidade dos dados pessoais. Para esse efeito, foi necessária a reformulação e definição de conceitos, princípios de tratamento e direitos dos titulares, assim como de obrigações associadas.

O RGPD estabelece princípios de tratamento de dados pessoais que assentam na transparência do tratamento, limitação da finalidade, minimização dos dados, exatidão, limitação da conservação dos dados, integridade e confidencialidade do tratamento e responsabilidade comprovada por parte das organizações.

Define ainda uma série de direitos para os titulares dos dados: direito à transparência, direito a ser informado, direito de acesso, direito à retificação e apagamento, direito à limitação, direito à portabilidade, direito à oposição do tratamento e direito relativo a decisões individuais automatizadas.

As organizações, categorizadas como responsáveis pelo tratamento ou subcontratantes, têm ainda o dever de implementar medidas técnicas e organizativas que visem a segurança dos tratamentos e dos dados pessoais. Estas obrigações traduzem-se na realização de registos de atividades de tratamento, proteção de dados desde a conceção e por defeito (pseudonimização, minimização dos dados), realização de Avaliações de Impacto na Proteção de Dados (DPIA), registo e notificação de violações de dados nas instituições.

1.3. openEHR

O openEHR é uma norma que apresenta um conjunto de especificações para uma arquitetura de Registos Eletrónicos de Saúde (RES), fornecendo diretrizes e ferramentas livres que permitem "capturar o conhecimento clínico de uma forma estruturada, independentemente do software, permitindo assim a interoperabilidade semântica" (Bacelar-Silva et al, 2013). O principal objetivo centra-se em permitir a construção de sistemas de RES que possam comunicar-se entre si sem que haja perda do significado do conteúdo" (Bacelar e Correia, 2015).

A principal característica técnica da norma openEHR centra-se numa estrutura de modelação a dois níveis (ou Modelação Multinível), onde se verifica a "separação do conteúdo da forma como este é representado" (Bacelar e Correia, 2015). Especificando, a modelação a dois níveis separa: o Modelo de Informação, que corresponde ao modelo que é implementado ao nível do software e é constituído por um modelo de referência estável, contendo os "tipos de dados que podem ser utilizados para representar a informação, como por exemplo dados de texto, quantidade e data." (Bacelar e Correia, 2015); do Modelo de Conteúdo, que corresponde ao segundo nível e contém as definições formais de conteúdo clínico na forma de arquétipos e templates. Os conceitos clínicos são, desta forma, estruturados fora do software, o que permite que os sistemas RES sejam mais flexíveis e de mais fácil manutenção e longevidade (Leslie, 2008).

1.4. Objetivos

O objetivo deste trabalho é compreender de que forma a norma openEHR pode ser considerada uma solução para os requisitos exigidos pelo RGPD.

2. Métodos

2.1. Requisitos do Regulamento Geral de Proteção de Dados

Considerando o objetivo do trabalho, definiu-se a necessidade de primeiramente identificar quais os requisitos para um SIS estar em conformidade com o RGPD. Foi feita uma análise do regulamento, com o objetivo de fazer o levantamento de requisitos, com base nas diretrizes indicadas pela norma "Guide for developing systems requirements specifications". Analisaram-se todos os artigos do regulamento e foram traduzidos em requisitos aqueles que constituíam uma funcionalidade ou obrigação a ser cumprida pelas organizações para estarem em conformidade com o regulamento. Ao resultado obtido chamou-se "Lista de requisitos para um SIS em conformidade com o RGPD".

2.2. Funcionalidades dos sistemas openEHR

Numa segunda fase, foi necessário identificar os princípios do openEHR face às funcionalidades de um SIS, procedendo-se dessa forma à leitura do "openEHR Architecture Overview". As funcionalidades foram listadas com principal foco nas funcionalidades diretas que permite a um sistema. A resultado obtido chamou-se "Lista de funcionalidades de um sistema openEHR".

2.3. Combinação dos requisitos com as funcionalidades

Uma vez elaborada a "Lista de requisitos de um SIS em conformidade com o RGPD" e a "Lista de funcionalidades de um sistema openEHR", foi elaborada uma tabela final com o objetivo de corresponder os requisitos identificados com as especificações openEHR.

Definiu-se que uma especificação openEHR poderia corresponder a mais do que um requisito de um SIS em conformidade com o RGPD. A correspondência foi então feita através da análise dos objetivos dos requisitos identificados e, posteriormente, da compreensão das funcionalidades identificadas. Se as funcionalidades openEHR cumprem o objetivo do requisito de uma forma direta, ou seja, se a simples utilização da arquitetura openEHR permite que determinado requisito seja cumprido, então é assinalada a correspondência.

2.4. Limitações

O caso de estudo desenvolvido apresentou algumas limitações. O facto do openEHR referir uma arquitetura de sistemas de RES limita uma maior correspondência face aos requisitos identificados, uma vez que o RGPD tem uma incidência forte nos processos organizacionais como um todo, em todo o tipo de indústrias e organizações.

Outra limitação apontada assenta no facto das organizações ainda se encontram em processo de reestruturação, havendo um foco maior na interpretação, compreensão e visão geral do RGPD face à sua implementação.

É também notada a falta de estudos semelhantes ao realizado no âmbito das tecnologias em conformidade com o RGPD. Mais concretamente, não foi encontrada literatura referente a reformas ou implementações de sistemas de informação de forma a obter conformidade com a RGPD. As soluções tecnológicas que são encontradas direcionam-se a fins comerciais, não existindo qualquer tipo de estudo ou análise da implementação efetuado, limitando a hipótese de comparação.

3. Resultados

3.1. Lista de requisitos

Foram identificados os seguintes requisitos referentes a um SIS em conformidade com o RGPD:

- Limitação do tratamento de dados pessoais
- Minimização dos dados pessoais
- Exatidão dos dados pessoais
- Prazos para limitação da conservação
- Limitação da conservação
- Integridade e confidencialidade
- Responsabilidade
- Demonstração de responsabilidade
- Consentimento Explícito
- Consentimento explícito do titular dos dados
- Registo do consentimento
- Capacidade de titular dos dados retirar consentimento
- Características do consentimento obtido
- Licitude do tratamento após retirar consentimento.
- Interesse legítimo do tratamento
- Informação acerca do interesse legítimo
- Objeção dos titulares dos dados ao interesse legítimo

- Comunicação e informação fornecida aos titulares dos dados
- Meios para a prestação de informações aos titulares dos dados
- Verificação da identidade dos titulares dos dados.
- Prazo para resposta ao pedido do titular dos dados
- Formato da resposta ao pedido de informação do titular dos dados
- Notificações de informação/privacidade
- Momento da notificação de informação/privacidade (dados pessoais obtidos diretamente)
- Período de notificação da informação ao titular dos dados
- Notificação ao titular dos dados de novos tratamentos
- Acesso dos titulares dos dados aos dados pessoais
- Formulário de resposta para pedidos do titular dos dados
- Confirmação de tratamento de dados pessoais
- Informações que titular dos dados tem direito a aceder
- Resposta ao pedido de acesso do titular dos dados
- Acesso direto do titular aos dados pessoais
- Retificação dos dados pessoais, por parte do titular dos dados
- Portabilidade dos dados pessoais dos titulares dos dados
- Portabilidade dos dados pessoais entre responsáveis pelo tratamento
- Interoperabilidade dos formatos e sistemas
- Objeção ao tratamento dos dados pessoais por parte do titular dos dados
- Apagamento dos dados pessoais a pedido do titular dos dados
- Comunicação com outras entidades responsáveis pelo tratamento de dados ou subcontratantes.
- Limitação do tratamento dos dados pessoais a pedido do titular dos dados
- Limitação do tratamento
- Notificação da anulação da limitação do tratamento dos dados pessoais.

- Proteção de dados desde conceção
- Proteção de dados por defeito
- Registo de políticas de proteção de dados pessoais
- Registo das atividades do tratamento de dados pessoais
- Formato dos registos do tratamento dos dados pessoais
- Disponibilização dos registos de tratamento dos dados pessoais
- Desenvolvimento de procedimentos de notificação de violações de dados
- Controlo de acesso
- Registo de violações de dados pessoais
- Descrição da violação de dados pessoais para envio à autoridade reguladora
- Prazo para notificação de violação de dados pessoais
- Preservação de registos de DPIA
- Consulta de DPIA
- Envolvimento do Encarregado de Proteção de Dados
- Conformidade com códigos de conduta
- Conformidade com processos de certificação
- Transferência de dados para países terceiros ou organizações internacionais
- Garantias das transferências de dados pessoais

3.2. Lista de funcionalidades

Foram consideradas as seguintes funcionalidades openEHR:

Modelação Multinível: Promove a separação do modelo de referência, implementado em software, do modelo de conteúdo, definido através de arquétipos e templates. O resultado deste tipo de modelação é a separação e independência da estrutura do software do seu conteúdo, o que permite SIS flexíveis, interoperáveis e com grande escalabilidade. Todos os SIS suportam a mesma estrutura de dados.

Separação da informação clínica e demográfica: A separação do conteúdo do registo clínico da informação identificável demográfica ocorre através da existência de um repositório para os RES e outro para a informação demográfica. Esta separação

permite que a identidade do titular dos dados seja preservada em caso de violação de dados de um RES (informações em diferentes repositórios obriga a que sejam comprometidos dois servidores). Esta especificidade garante o anonimato do titular dos dados face à informação contida no seu RES.

Camada de Serviços: Atuando sobre o modelo de referência e sobre o modelo de arquétipos, permite definir a interface que o utilizador irá utilizar no sistema, criando vistas que irão possibilitar a consulta de dados. A camada de serviços assume um papel importante na disponibilização dos dados e na possibilidade da sua consulta, permitindo a criação de vistas seguras e intuitivas.

Controlo de versões (Versionamento e Indelebilidade e Assinatura digital): as alterações feitas pelos utilizadores (criação de novos registos, eliminação, modificação e transferência de registos, etc) não se realiza ao nível do Item/Registo, mas sim ao nível do repositório como um todo, ou seja, nenhuma versão é apagada ou modificada; todas as alterações requeridas são implementadas fisicamente como novas versões que são criadas e adicionadas ao repositório. Isto garante aos sistemas uma característica de indelebilidade (nenhuma informação pode ser apagada).

Permite ainda conter uma assinatura digital. Num sistema de versionamento, assinatura dos dados atua como uma verificação da integridade, uma medida de autenticação e também uma medida de não-repúdio.

Controlo de Acesso (Lista de controlo de acesso e controlo de acesso às configurações de acesso): O RES do openEHR permite a definição de uma lista de controlo de acesso, onde são indicados indivíduos identificados e respetivas categorias.

O openEHR permite ainda que seja definido um gate-keeper responsável pelo controlo das configurações de acesso do registo. Este determina quem pode fazer alterações à lista de controlo de acesso, sendo normalmente o próprio paciente ou um parente ou tutor legal (caso o registo pertença a uma criança menor ou um paciente incapaz). todas as alterações são mantidas no audit trail.

Audit trailing: todas as alterações feitas, a todos os níveis, no RES, são registadas no audit trail com dados relativos à identidade do utilizador, selo temporal, razão (das alterações realizadas), assinatura digital e informações da versão relevantes.

3.3. Combinação dos requisitos com as funcionalidades

A seguinte tabela apresenta a correspondência entre as especificações openEHR e os requisitos de um SIS em conformidade com o RGPD:

RGPD \ OpenEHR	Controlo de Acesso - lista de	Controlo de Acesso - controlo do processo à	Controlo versões - assinatura digital	controlo de versões-	Separação informação clínica	Camada de Serviços	Audit Trailing	Modelação Multinível
PRINTRAT2- Minimização dos dados pessoais					✓			
PRINTRAT5- Limitação da conservação dos dados pessoais					✓			
PRINTRAT6- Integridade e confidencialidade	✓	✓	✓	✓			✓	
COMINF3- Verificação da identidade dos titulares dos dados					✓			
ACESS1- Acesso dos titulares dos dados aos dados pessoais	✓	✓						✓
ACESS3- Confirmação do tratamento dos dados pessoais				✓			✓	
ACESS6- Acesso direto do titular dos dados	✓	✓				✓		
PORTAB1- Portabilidade dos dados pessoais dos titulares dos dados								✓
PORTAB2- Portabilidade dos dados pessoais entre responsáveis pelo tratamento								✓
PORTAB3- Interoperabilidade dos formatos e sistemas						✓		✓

PROT1- Proteção de dados pessoais desde a conceção					✓			
PROT2- Proteção de dados por defeito	✓	✓	✓		✓			
REG1- Registo das atividades do tratamento de dados pessoais							✓	
REG3- Disponibilização dos registos de tratamento dos dados pessoais							✓	
TRANSF1- Transferências de dados para países terceiros ou organizações internacionais								✓
Total de correspondências	4	4	2	2	5	2	4	5

Face à funcionalidade **lista de controlo de acesso** foram correspondidos os seguintes requisitos:

- *Integridade e confidencialidade* - a lista de controlo de acesso garante a manutenção da privacidade do paciente ao liberar o acesso aos devidos utilizadores.
- *Acesso dos titulares dos dados* - A inclusão do titular dos dados na lista de controlo garante a possibilidade do mesmo poder aceder aos dados, o que garante a possibilidade deste obter uma cópia. Se o titular dos dados não estiver presente na lista de controlo, não é permitido o acesso e o posterior fornecimento da cópia.
- *Acesso direto dos titulares dos dados aos dados pessoais* - A lista de controlo de acesso permite definir que o titular dos dados tem direito de aceder diretamente aos seus dados pessoais. O SIS apenas permite o acesso do titular dos dados se este tiver identificado na lista de controlo de acesso, caso contrário o acesso é negado.
- *Proteção dos dados por defeito* - a lista de controlo de acesso permite assegurar que os dados pessoais são tratados apenas para as finalidades específicas para as quais foram recolhidos no que tange a acessibilidade dos mesmos. Ao predefinir os indivíduos que podem aceder aos dados, delimita-se a possibilidade de ocorrerem acessos que

não são pertinentes ao tratamento dos dados definido, salvaguardando-se a sua privacidade. Do ponto de vista da disponibilização dos dados sem intervenção humana a um indeterminado número de pessoas, a lista de controlo de acesso garante a restrição e limitação do acesso aos dados pessoais, impedindo que ocorram tratamentos indesejados.

O **controlo de acesso** às configurações responde aos seguintes requisitos:

- *Integridade e confidencialidade* - permite que seja determinado o indivíduo que pode modificar as configurações do controlo de acesso, contribuindo para que o acesso aos dados seja legítimo e justificado.
- *Acesso dos titulares dos dados*_- o titular dos dados, ao efetuar o controlo sobre as configurações do controlo da lista de acesso, permite definir quem poderá ter acesso aos seus dados pessoais, de forma a providenciar a cópia dos mesmos.
- *Acesso direto dos titulares dos dados aos dados pessoais* **-** o controlo das configurações da lista controlo de acesso, ao permitir a definição de um *gate keeper*, permite que o titular dos dados seja identificado como tal, sendo-lhe garantido o acesso aos dados.
- *Proteção dos dados por defeito* - o controlo das configurações da lista de controlo de acesso permite que a lista de acessos definida para determinado RES seja compatível, em termos de acessibilidade, com o tratamento dos dados pessoais assegurando a integridade do tratamento.

A especificação **controlo de versões** responde aos requisitos:

- *Integridade e confidencialidade* - a assinatura digital assegura a autenticação, não repúdio e integridade dos RES, funcionando como medida importante de segurança e de integridade dos dados pessoais (e respetivo tratamento).
- *Proteção dos dados por defeito* - a assinatura digital permite que seja salvaguardado o acesso e disponibilização da informação, funcionando como medida de segurança dos dados pessoais e do tratamento.

O **controlo de versões (versionamento)** assegura aos SIS uma característica de indelebilidade, garantindo que nenhuma informação é apagada. Esta funcionalidade responde aos seguintes requisitos:

- *Integridade e confidencialidade* - A indelebilidade dos RES obtida através da consecutiva criação de novas versões constitui uma medida importante contra a perda, destruição ou danificação acidental dos dados contidos no RES, garantindo informação confiável e íntegra em todos os momentos do tratamento.
- *Confirmação de tratamento de dados pessoais* - Através do versionamento dos registos, é possível identificar o utilizador que procedeu a alterações, data e hora e razão das ações realizadas ao RES, possibilitando a confirmação de tratamento para com os titulares dos dados.

A **separação do RES da informação demográfica** responde aos seguintes requisitos:

- *Minimização dos dados* - permite que os dados sejam limitados à finalidade do tratamento, na medida em que a utilização de dados pessoais demográficos é minimizada (apenas é utilizado o RES para a prestação de cuidados, enquanto os dados demográficos são armazenados em repositório próprio).
- *Limitação da conservação dos dados pessoais*_- a identidade do titular dos dados está automaticamente preservada a partir do momento em que a informação clínica e a informação demográfica são separadas. Dessa forma, enquanto os dados clínicos forem conservados para o tratamento, os dados pessoais demográficos apenas são relacionados ao RES através de um identificador externo.
- *Verificação da identidade do titular dos dados* - o RES associado a um paciente é único e, através de um identificador, é associado à informação demográfica do respetivo titular dos dados. Desta forma, caso exista a necessidade de identificar o titular dos dados face à informação clínica, basta relacioná-lo ao identificador que o liga ao RES.
- *Proteção dos dados desde a conceção* - permite que o titular dos dados clínicos seja pseudo-anonimizado, uma vez que o seu RES é separado da informação demográfica identificável e apenas são relacionadas através de um identificador externo.
- *Proteção de dados por defeito*_- garante que, no momento da prestação de cuidados, apenas sejam consideradas os dados pessoais de saúde, salvaguardando a informação demográfica.

A **camada de serviços** responde aos seguintes requisitos:

- *Acesso direto do titular dos dados aos dados pessoais* - a camada de serviços, através do Virtual EHR API e do EHR Service, cria uma vista que permite ao titular dos dados consultar do seu RES.
- *Interoperabilidade dos formatos e sistemas* - permite que se criem diferentes interfaces, nos diferentes sistemas que compõem o ambiente hospitalar, utilizando os mesmos dados. Quando são definidas as diferentes vistas que permitem a consulta dos dados do RES, o registo mantém a sua unicidade e mesma estrutura, garantindo a interoperabilidade.

A especificação **Audit Trail** responde aos seguintes requisitos:

- *Integridade e confidencialidade* - garante o registo de logs de acesso, identidades dos utilizadores e tempo e duração da ação, assegurando a integridade.
- *Confirmação do tratamento de dados pessoais* - Com o audit trail, e considerando a rastreabilidade que permite, é possível perceber se estão a ser efetuadas quaisquer tipos de ações no RES do titular dos dados, sendo possível confirmar essa informação.
- *Registo das atividades de tratamento dos dados pessoais*_– o audit trail regista todas as informações relacionadas com ações executadas no RES.
- *Disponibilização dos registos de tratamento dos dados pessoais* – através da rastreabilidade que permite, o audit trail possibilita criar um registo do tratamento dos dados passível de ser disponibilizado à autoridade de controlo.
- *Registo das violações de dados pessoais* – permite fornecer um registo das violações de dados pessoais que se verificaram, na medida em que regista acessos não autorizadas e ações indevidas para com os dados pessoais.

A **Modelação Multinível** responde aos seguintes requisitos:

- *Acesso do titular dos dados* –. a modelação de arquétipos, permite que estes sejam exportados e disponibilizados ao titular dos dados.
- *Portabilidade dos dados pessoais dos titulares dos dados* - esta especificação assegura a capacidade de extrair os dados requeridos num formato estruturado e de leitura automática. Os mesmos dados são lidos da mesma forma em diferentes sistemas e softwares.

- *Portabilidade dos dados pessoais entre responsáveis pelo tratamento* - qualquer sistema desenvolvido utilizando a arquitetura openEHR, mesmo pertencendo a diferentes fornecedores, consegue suportar os mesmos dados (modelados na forma de arquétipos e templates), assegurando a portabilidade entre fornecedores.
- *Interoperabilidade dos formatos e sistemas*_- a implementação no software do modelo de referência é comum aos SIS, enquanto a modelação dos arquétipos e templates permite a interoperabilidade semântica dos dados e, consequentemente, dos sistemas.
- *Transferência de dados pessoais para países terceiros ou organizações internacionais* - a Modelação Multinível permite a transferência através das características de portabilidade e interoperabilidade que lhe são associados devido à modelação do modelo de referência e dos arquétipos e templates.

4. Discussão

4.1. Geral

A arquitetura e especificações do openEHR atuam maioritariamente sobre requisitos que moldam a camada funcional do sistema ou que correspondem a indicações relativas às garantias de rastreabilidade e integridade e confidencialidade dos dados.

A proteção dos dados desde a conceção do SIS, a portabilidade e interoperabilidade dos dados e sistemas é garantida pela própria arquitetura do openEHR, assente na Modelação Multinível e na consequente separação da informação clínica da informação demográfica.

A integridade e confidencialidade dos dados pessoais, assim como medidas de segurança da informação que assentem em políticas de minimização e limitação do tratamento e rastreabilidade dos dados são maioritariamente respondidas pelas especificações de controlo de acesso, controlo de versões e audit trail.

A arquitetura openEHR constitui ainda uma ferramenta valiosa para o cumprimento de requisitos aos quais não responde diretamente. O controlo de versões e audit trail permitem alimentar os registos de informações relacionadas com o tratamento dos dados e possíveis violações de dados. Já os requisitos associados ao consentimento explícito podem ser cumpridos através da criação de arquétipos e templates.

O facto do openEHR corresponder a um conjunto de especificações de um sistema de RES constitui uma limitação à obtenção de mais correspondências para com os requisitos de um sistema conforme o RGPD. Todas as funcionalidades são centradas no RES, não abrangendo alguns processos organizacionais essenciais ao cumprimento do regulamento.

No entanto, é importante notar que as reformas organizacionais que devem ser conduzidas, com vista à conformidade com o RGPD, requerem uma atuação ao nível dos seus processos e serviços organizacionais, mas também especificamente ao nível dos seus sistemas, que maioritariamente suportam o tratamento dos dados pessoais.

5. Outras descobertas

5.1. Trabalhos futuros

Propõe-se a implementação da arquitetura openEHR e a verificação da resposta aos requisitos indicados nos resultados. Sugere-se ainda a exploração das especificações openEHR para o cumprimento de requisitos que não são respondidos de uma forma direta pela norma, mas que, com a sua implementação, as organizações possam utilizar as suas funcionalidades como ferramenta de suporte à realização de tarefas.

Salienta-se ainda a relevância de, em trabalhos futuros, estender a lista de requisitos para um SIS em conformidade com o RGPD, e a conjugação da mesma com normas relevantes para o desenvolvimento de SIS seguros, tal como a ISO 27001- Gestão de Segurança de Informação.

6. Conclusão

Os resultados deste trabalho mostram o openEHR como abordagem promissora para o desenvolvimento de SIS em conformidade com o RGPD, servindo como um apoio importante para a investigação de soluções focadas no RGPD e na reforma dos SIS que suportam a complexidade do tratamento de dados pessoais na área da saúde.

Essencialmente, o openEHR apresenta-se como solução importante para as questões de privacidade e proteção dos dados impostas pelo RGPD às instituições, respondendo às necessidades funcionais dos SIS.

A utilização das TI tornou-se essencial à prática da prestação de cuidados médicos. O openEHR permite a existência de um ambiente hospitalar integrado e voltado para a prestação de cuidado de saúde contribuindo para o acesso a informação de qualidade. No entanto, pelas suas características, permite que a privacidade e proteção dos dados pessoais estejam asseguradas.

O investimento e a implementação de SIS não têm de ser vistos como adversos às políticas de privacidade e proteção dos dados. Se existir conformidade entre os SIS e as regras estabelecidas no RGPD, estes podem ser usados na sua plenitude.

7. Referências

1. Bacelar-Silva, Gustavo M, Hilton Cesar, Patricia Braga, e Rodney Guimaraes. 2013. "OpenEHR-Based Pervasive Health Information System for Primary Care: First Brazilian Experience for Public Care." Proceedings of the 26th IEEE International Symposium on Computer-Based Medical Systems U6 572–873. Acedido a 20 de outubro de 2017 em http://ieeexplore.ieee.org/document/6627881/

2. Bacelar, Gustavo, e Ricardo Correia. 2015. "As Bases Do openEHR," 1ª ed. Porto: Virtual Care. Acedido a 20 de outubro de 2017 em https://www.researchgate.net/publica-tion/282869250_As_Bases_do_openEHR

3. Beale, Thomas, e Sam Heard. 2007. "openEHR - Architecture Overview." The OpenEHR Foundation. Acedido a 20 de outubro de 2017 em http://www.openehr.org/releases/1.0.2/architecture/overview.pdf

4. Comissão Europeia. 2012. "Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation." COM (2012) 11 final: 1–119. Acedido a 20 de outubro de 2017 em http://eur-lex.europa.eu/legal-con-tent/EN/ALL/?uri=celex%3A52012PC0011

5. ICO Office. 2016. "Overview of the General Data Protection Regulation (GDPR)." https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/accountabi-lity-and-governance/.

6. IEEE (The Institute of Electrical and Electronics Engineers). 1998. IEE Guide for developing System Requirements Specifications. Acedido a 20 de outubro de 2017 em https://sites.google.com/a/mix.wvu.edu/csee480/ieee-std--1233---requirements-specification-1.

7. Parlamento Europeu. 2016. "Regulamento 2016/679 de 27 de Abril de 2016 relativo à pro-teção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) L119". Jornal Oficial das Comunidades Europeias. (59):1-88. Bruxelas. Acedido a 20 de outubro de 2017 em http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uri-serv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

8. SBIS (Sociedade Brasileira de Informática em Saúde). 2016. Manual de certificação para sistemas de Registro Eletrônico em Saúde. Acedido a 20 de outubro de 2017 em http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2016_v4-2.pdf

9. Slee, Vergil, Debora Slee e Joachim Schmidt.2000. The Endangered Medical Record. Minnesota: Tringa Press.

10. Yamamoto, R. 2016. "Large-Scale Health Information Database and Privacy Protection." Japan Medical Association Journal 59 (2–3): 91–109. Acedido a 20 de outubro de 201 em https://www.scopus.com/inward/record.uri?eid=2-s2.0-85013421213&partnerID=40&md5=c88c927d6c1951bbf7176acc1a77fb93.