U.PORTO

FEUP FACULDADE DE ENGENHARIA
UNIVERSIDADE DO PORTO

2017

Mestrado em Ciência da Informação

OpenEHR como solução para o Regulamento Geral de Proteção de Dados na área da saúde.

MARIANA LEITE SOUSA

UNIDADES ORGÂNICAS E ENVOLVIDAS

FACULDADE DE ENGENHARIA

FACULDADE DE LETRAS

Sumário

Agradecimentos

Quero agradecer a todos aqueles que me apoiaram no desenvolvimento deste trabalho, quer pelos recursos que me forneceram, quer pela paciência que sempre tiveram.

À minha orientadora, Olívia Pestana, pelo incentivo, pela confiança, pela exigência e pela força.

Ao Ricardo Cruz Correia pela oportunidade, pelo desafio e pelos ensinamentos.

Aos meus pais, Paula Leite e António Sousa, por tudo.

Abreviações e Acrónimos

CNPD	Comissão Nacional de Proteção de Dados
OCDE	Organização para a Cooperação e Desenvolvimento Económico
RES	Registo Eletrónico de Saúde
RGPD	Regulamento Geral de Proteção de Dados
SI	Sistema de Informação
SIS	Sistema de Informação de Saúde
TI	Tecnologia de Informação
UE	União Europeia

Resumo

O desenvolvimento das tecnologias alterou profundamente os processos das instituições de saúde, adquirindo um grande impacto na forma de processar a informação (a sua recolha, acesso, utilização e partilha).

A preocupação com a privacidade e proteção dos dados pessoais culminou em reformas das legislações existentes. O Regulamento Geral de Proteção de Dados visa reformular as medidas existentes em matéria de proteção de dados pessoais de cidadãos da União Europeia, com forte incidência nos direitos e liberdades das pessoas e no estabelecimento de regras para o tratamento de dados pessoais. As instituições cujos serviços prestados assentem no tratamento de dados pessoais necessitam de reformular as suas políticas e procedimentos, com forte incidência para a adaptação dos sistemas (que suportam o tratamento de dados) aos requerimentos do RGPD.

Este trabalho tem como objetivo principal perceber se a norma openEHR (que promove a interoperabilidade dos sistemas de RES) pode ser considerada uma solução para os requisitos necessários para um SIS estar em conformidade com o RGPD.

Foi então elaborada uma lista de requisitos para um SIS em conformidade com o RGPD e foi também feito um levantamento das especificações do openEHR (como cumprimento dos objetivos secundários), que produziram respetivamente 61 requisitos para SIS em conformidade com o RGPD e 8 especificações do openEHR.

Como resultado final, foi feita a correspondência entre os requisitos do sistema e as especificações openEHR, que resultou em 15 requisitos correspondidos. Conclui-se também que todas as especificações openEHR conseguem responder pelo menos a um requisito.

O openEHR apresenta-se assim como solução para o desenvolvimento de SIS que reforcem a privacidade e proteção dos dados pessoais, garantindo que estas são pensadas e implementadas desde o desenvolvimento dos sistemas. Desta forma, as instituições garantem a conformidade dos seus SIS com o RGPD mantendo a qualidade dos dados de saúde e, consequentemente, da prestação de cuidados.

Palavras -Chave: openEHR, Regulamento Geral de Proteção de Dados, Proteção de Dados Pessoais, Sistemas de Informação

Abstract

The evolution of technologies changed completely the health institutions procedures, with major impact in how they process their information (collection, access, use, and sharing of the data).

The concerns about privacy and personal data protection result in reforms of the existing legislation. The General Data Protection Regulation aims to reform the existing measures on the topic of personal data protection of the European Union citizens, with a strong input on the rights and freedoms of people and in the establishment of rules for the processing of personal data. The institutions which services lean on the processing of personal data need to revise their policies and procedures, with a strong input in the adaptation of their systems (that support data processing) to the requirements of the GDPR.

This work aims to understand if the openEHR standard (that promotes interoperability of EHR systems) can be considered a solution for the requirements needed for a HIS compliant with GDPR.

A list of requirements for a HIS compliant with GDPR and an identification of openEHR functionalities were made (as secondary goals), that result in 61 requirements for a HIS compliant with GDPR and 8 openEHR functionalities.

As a final result, the requirements identified for the systems were matched with the openEHR functionalities, which result in 15 requirements matched with openEHR. All the functionalities identified matched at least one requirement.

OpenEHR is a solution for the development of HIS that reinforce privacy and personal data protection, ensuring that they are contemplated in the system development. The institutions can secure that their HIS are compliant with GDPR while safeguarding the medical data quality and, as a result, the healthcare delivery.

Keewords: openEHR, General Data Protection Regulation, Personal Data Protection, Information Systems

1. Introdução

O setor da saúde dispõe de uma vasta riqueza informacional. Os profissionais de saúde, desde médicos e enfermeiros aos mais variados técnicos, lidam todos os dias com um grande volume de informação, sendo que as atividades que desempenham estão intimamente dependentes dessa informação, nomeadamente da sua disponibilidade e do acesso à mesma e da forma como é tratada, gerida e disponibilizada.

Essencialmente, a informação médica é um recurso com bastante valor para os profissionais, sendo essencial para a garantia de qualidade da prestação de cuidados (Bacelar e Correia, 2015).

Os registos clínicos constituem um dos elementos mais importantes para os cuidados de saúde, uma vez que contêm de forma completa e exata informações relacionadas com o historial médico, diagnóstico, tratamentos, prescrições médicas, entre outros dados.

Atendendo à vasta riqueza informacional da área da saúde, rapidamente se despontou a preocupação com a forma como a informação é organizada e, mais importante, com a facilidade em obter a informação adequada ao desempenho de determinada tarefa.

As tecnologias de informação e os sistemas de informação de saúde surgem assim como ferramentas capazes de suportar as necessidades organizacionais de hospitais e sectores hospitalares. O desenvolvimento das tecnologias facilita o processo de recolha e processamento de dados de saúde, o que levanta novas preocupações relacionadas com a sensibilidade da informação tratada pelos sistemas.

Com a oportunidade e benefícios que acompanham o desenvolvimento das TIC crescem novos riscos, particularmente para a privacidade e proteção dos dados dos indivíduos (Horvitz e Mulligan, 2015). Os sistemas de informação de saúde processam dados de cariz extremamente sensível, na medida em que contêm informação pessoal e privada. Um registo clinico pode conter informação banal, como o peso, a altura, a pressão arterial de determinado paciente, mas pode também conter informação sobre a fertilidade, aborto, problemas emocionais e cuidados psiquiátricos, comportamento sexual, doenças sexualmente transmissíveis, entre outros (Rindfleisch, 1997), informação que, uma vez divulgada, pode ter consequências negativas na vida do sujeito.

As questões relacionadas com a privacidade e a proteção dos dados pessoais voltam a ser preocupações primárias para as instituições responsáveis pelo tratamento de um número de dados pessoais elevado. Apesar de num ambiente hospitalar se priorizar a facilidade de acesso a um grande número de dados de saúde como garantia da qualidade da prestação de cuidados, a privacidade e segurança da informação médica não pode ser descuidada, uma vez que pode ter consequências consideráveis para a vida pessoal dos pacientes (Sociedade Europeia de Radiologia, 2017).

Como resposta às problemáticas da privacidade e proteção de dados, foi aprovado em Abril de 2016 um novo Regulamento Geral de Proteção de Dados (RGPD), apesar de só ser aplicável a partir de 25 de Maio de 2018. O RGPD aplica-se a organizações em que as atividades se centram ou implicam o tratamento de dados pessoais de cidadãos da União Europeia. Com a aplicação do novo regulamento são requeridas novas responsabilidades às organizações, no que tange a privacidade e segurança dos dados pessoais.

Desta forma, torna-se necessário conhecer as regras do Regulamento, analisar as novas obrigações associadas aos responsáveis pelo tratamento dos dados, verificar o nível de cumprimento atual com as regulamentações impostas e definir estratégias para adotar as medidas necessárias.

A necessidade de se reformularem as políticas, processos de tratamento e procedimentos das organizações, em conformidade com a nova lei de proteção de dados, tem gerado uma grande consciencialização em todas as instituições dos diversos setores, públicos e privados (Correa, 2016).

As instituições têm de ser capazes, até Maio de 2018, de tomar as medidas necessárias para estar em conformidade com o RGPD, assim como têm de ser capazes de garantir os direitos dos titulares dos dados indicados no regulamento. O RGPD introduz novos conceitos que devem ser considerados, alterações a princípios e conceitos já existentes, e novos papéis associados aos agentes responsáveis pelo tratamento de dados pessoais e autoridades reguladoras.

O setor da saúde encontra-se bastante exposto às implicações do novo RGPD. É importante notar que os dados clínicos se encontram espalhados por um grande número de sistemas de informação com diversas funções (recolha de dados, armazenamento, comunicação e integração, vigilância e monitorização, análise de dados, entre outros), o que torna o tratamento de dados pessoais de uma organização de saúde um processo bastante complexo de ser analisado e reformulado.

O conceito de “proteção de dados pessoais desde a conceção e por defeito” desperta também a preocupação de serem elaborados sistemas que estejam em conformidade com o RGPD desde o primeiro momento, de forma a serem mitigados os riscos e cumpridas as boas práticas no âmbito da proteção de dados.

O OpenEHR é uma norma que apresenta um conjunto de especificações para uma arquitetura de Registos Eletrónicos de Saúde, fornecendo diretrizes e ferramentas livres que permitem “capturar o conhecimento clínico de uma forma estruturada, independentemente do software, permitindo assim a interoperabilidade semântica. O seu principal foco está em permitir a construção de sistemas de RES que possam comunicar-se entre si sem que haja perda de significado do conteúdo” (Bacelar e Correia, 2015). Na sua essência, o OpenEHR permite que continuem a existir inúmeros SIS, mas os dados clínicos do paciente podem ser partilhados para onde quer que ele venha a ser atendido, independentemente do seu suporte tecnológico. O OpenEHR apresenta também uma característica técnica importante, centrada na separação do conteúdo clínico da forma como ele é representado (Modelação a dois níveis ou Modelação Multinível).

Considerando a natureza do OpenEHR como norma para a arquitetura de sistemas de EHR, é da máxima relevância perceber até que ponto este pode ser considerado como solução para a garantia de conformidade dos SIS com a RGPD.

1.1 - Identificação da questão de investigação

As tecnologias utilizadas no sector da saúde são usadas para trabalho com informação médica pessoal de cariz extremamente sensível.

As instituições de saúde devem ter a proteção dos dados pessoais, pelos quais se ocupam, como prioridade, de forma a não pôr em risco privacidade dos seus pacientes e, consequentemente, a reputação das instituições e a confiança da população nos serviços e instituições de saúde.

No âmbito do RGPD, é essencial que os sistemas de saúde implementados e desenvolvidos consigam responder às exigências requeridas, de maneira a estarem em conformidade com o regulamento e, mais importante, conseguirem corresponder às questões de privacidade e proteção de dados dos pacientes que lhes são confiados.

Considerando a riqueza da arquitetura de um sistema de informação segundo a norma openEHR, torna-se importante perceber em que medida pode responder aos requisitos de um sistema de informação de saúde em conformidade com o RGPD.

1.2 – Objetivos

Este projeto tem como principal objetivo realizar a correspondência entre as especificações da norma OpenEHR e os requisitos de um SIS em conformidade com o RGPD.

Para alcançar este objetivo, foram definidos os seguintes objetivos secundários:

- Elaboração da lista de requisitos para um SIS em conformidade com o RGPD;
- Listagem das especificações e funcionalidades promovidas pela norma openEHR;
- Correspondência dos pontos identificados na norma openEHR com os requisitos listados para um SIS em conformidade com o RGPD.

2. Revisão da Literatura

2.1- Informação e Dados Pessoais na saúde

As atividades do setor de saúde são extremamente dependentes de informação. Um dos elementos mais cruciais para os cuidados de saúde é o registo clínico (Slee et al, 2000). O desenvolvimento das tecnologias de informação e comunicação nas últimas décadas originou uma mudança de paradigma no setor de saúde, traduzindo-se numa alteração da forma como as instituições recolhem, acedem e utilizam os dados (Virone, 2012), resultando num aumento do volume, diversidade e complexidade dos mesmos (Patil e Seshadri, 2014).

Com a inserção das tecnologias no setor da saúde, culminando no desenvolvimento de sistemas de informação e aplicações médicas, a possibilidade de melhorar o registo da informação de saúde resultou numa migração do papel para o formato eletrónico, originando o aparecimento dos registos eletrónicos de saúde (Slee et al, 2000).

Indispensável à prestação de cuidados, o RES contém uma extensão de dados que corresponde a informação pessoal acerca de determinada pessoa, tais como “dados demográficos, historial médico, medicação e alergias, estado de imunizações, resultados de testes de laboratório, imagens de radiologia, sinais vitais, informações de características físicas, como idade e peso e mesmo informações de faturação.” (Odoemenam, 2011). A Diretiva de 2012 do Parlamento Europeu e do Conselho, relativa ao exercício dos direitos dos doentes em matéria de cuidados de saúde transfronteiriços, define ainda que registo clínico como “conjunto de documentos com todo o tipo de dados, avaliações e informações sobre a situação e a evolução clínica de um doente ao longo do processo de prestação de cuidados de saúde” (Comissão Europeia, 2012), o que pode remeter para informação pessoal e administrativa. Um RES pode ainda conter informações acerca dos familiares dos pacientes, como doenças diagnosticadas na família.

É notável que o setor da saúde lida com informação extremamente pessoal e privada, muitas vezes apenas partilhada em confidência com os profissionais de saúde (Wilkowska e Ziefle, 2012).

O dever da confidencialidade na Medicina está inerente ao Juramento de Hipócrates, datado de 1771, onde se salienta que um profissional de saúde guardará e respeitará o segredo que lhe foi confiado, até após a morte do paciente (Juramento Hipócrates, 1983).

Desta forma, a salvaguarda da privacidade dos pacientes é uma preocupação primária. Os dados clínicos que compõem um RES são uma ferramenta importantíssima para a qualidade da prestação de cuidados, mas devem ser compreendidos os possíveis danos para um titular dos dados caso não sejam asseguradas medidas que visem a sua proteção.

Essencialmente, é necessário compreender a importância de não pôr em risco o princípio sobre o qual os RES foram desenvolvidos: a confiança dos pacientes (Goldstein, 2014).

2.2. Privacidade e Proteção de Dados Pessoais

O conceito de privacidade foi amplamente definido por Samuel Warren e Louis Brandeis no seu trabalho “O Direito da Privacidade”, publicado pela Harvard Law Review em 1890, como “*the right to be left alone*”, vulgarmente traduzido como o direito de ser deixado em paz. Esta definição, clara e concisa, acarreta uma dimensão pessoal e social que perdura até aos dias de hoje, tendo adquirido significados adicionais ao longo do tempo.

A privacidade é vista como um direito universal inerente a qualquer ser humano, constatando-se que “ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra ou reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.” (Assembleia Geral das Nações Unidas, 1948).

Os princípios do conceito de privacidade estão assentes na sociedade, tendo existido sempre uma preocupação com as garantias de privacidade de liberdade. Contudo, atualmente, a privacidade é mais que isolamento ou tranquilidade em relação às informações pessoais de alguém.

O desenvolvimento das tecnologias, a globalização e o aparecimento da internet alteraram profundamente a sociedade em que vivemos (Comissão Europeia, 2010). Atualmente, a salvaguarda do direito à privacidade não depende apenas da vontade da pessoa expor, de que maneira for, a sua vida pessoal. Ao verificarmos uma mudança de paradigma que digitalizou e redefiniu a nossa sociedade e os nossos comportamentos, os procedimentos das instituições, dos negócios, da prestação de serviços e dos agentes governamentais

também se alteraram, abrindo espaço para novas oportunidades fortemente apoiadas na inclusão e exploração das tecnologias.

Reconhecendo a riqueza da informação como recurso, esta ganha uma importância preponderante no novo milénio, sendo que essa importância aumenta à medida que se vai desenvolvendo tecnologia capaz de extrair a sua utilidade.

A crescente evolução tecnológica teve um papel crucial no processo de modernização do setor de saúde(Gaudino 2010), que, através do desenvolvimento de sistemas de informação de saúde e outros tipos de tecnologias, desenvolveram ferramentas capazes de suportar as necessidades organizacionais dos hospitais e setores hospitalares.

Haux (2006) aponta que a importância e necessidade de se desenvolverem SIS está assente em fatores como a migração do papel para o formato digital (RES), no que tange o tratamento e armazenamento de dados, assim como o forte aumento de informação e dados no sector de saúde, a centralização dos SIS, o uso dos dados clínicos inseridos nos SIS para fins como o planeamento dos cuidados de saúde e investigação científica, para além dos fins administrativos e prestação de cuidados, a importância de gerir a informação médica de forma estratégica e as alterações relacionadas com os tipos de dados a serem processados (por exemplo, a inclusão de imagens para além de dados alfanuméricos). Os sistemas de informação assumiram assim um papel de grande relevância no setor da saúde, contribuindo para a sua modernização.

Considerando a natureza sensível da saúde e o aumento exponencial do volume de dados nas instituições, como resultado da influência das tecnologias médicas e dos SIS e o seu papel nos processos de recolha, tratamento, utilização e armazenamento de dados, é importante perceber em que medida o direito à privacidade das pessoas pode ser afetado.

A informação médica é considerada como sendo um dos tipos mais confidenciais de informação pessoal, sendo considerada propriedade da pessoa para a qual remete (Mountford et al., 2016). Dessa forma, é relevante compreender o conceito de dados pessoais, a sua abrangência e a sua importância na saúde, de forma a compreendermos quais as implicações da proteção de dados pessoais na privacidade.

Segundo a Diretiva de 95/46/CE, entende-se **dados pessoais** como “qualquer informação relativa a uma pessoa singular identificada ou identificável (“pessoa em causa”); é considerado identificável todo aquele que possa ser identificado, direta ou indiretamente, no-

meadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social" (Parlamento Europeu, 1995). A riqueza da informação médica, estruturada e depositada num RES, está assente na recolha deste tipo de dados. Com o princípio de que quanto mais detalhada a informação acerca de um indivíduo ou grupo de indivíduos, mais apropriado o tratamento a ser oferecido, o RES pode ser encarado como um histórico da nossa vida, composto por informações que caracterizam o nosso estado de saúde, os nossos atributos e defeitos físicos, o nosso comportamento, o nosso estilo de vida (ex. uso de tabaco ou álcool), o nosso histórico familiar (Donaldson e Lohr, 1994).

Neste âmbito, a privacidade no contexto da saúde corresponde ao "direito e desejo da pessoa controlar a divulgação da informação pessoal de saúde" (Rindfleisch, 1997).

A Diretiva de 95/46/CE identifica certos tipos de dados pessoais como "categorias especiais" de dados, com base no facto do seu processamento ter um impacto mais profundo nos direitos de privacidade dos indivíduos. No artigo 8º número 1 da Diretiva de 95/46/CE, afirma-se que "os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convenções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e à vida sexual"(Parlamento Europeu, 1995). A estas categorias de dados pessoais sensíveis, deve ser garantido um nível de proteção mais significativo, como refere Rudgard na sua publicação "European Privacy – Law and practice for data protection professionals". No entanto, é importante salientar que o artigo 8º número 3 nomeia algumas exceções para o tratamento dos dados pessoais sensíveis, nomeadamente os dados pessoais de saúde, que são os dados relevantes para o presente trabalho. Desta forma, o número 1 do artigo 8º "não se aplica quando o tratamento dos dados for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou gestão de serviços de saúde e quando o tratamento desses dados for efetuado por um profissional de saúde obrigado ao segredo profissional pelo direito nacional ou regras estabelecidas pelos organismos nacionais competentes, ou por outra pessoa igualmente sujeita a uma obrigação de segredo equivalente" (Parlamento Europeu, 1995). O tratamento de dados de saúde pode também ser legitimado pelo consentimento explícito dado pelo titular dos dados, assim como em caso de necessidade de proteger interesses vitais da pessoa em causa ou de uma outra pessoa, se estiver física ou legalmente incapaz de dar o seu consentimento.

É possível inferir, desta forma que a proteção dos dados pessoais de saúde possibilita a proteção da privacidade dos indivíduos, sendo estes parte integrante da vida privada das pessoas.

Desta forma, aliada às preocupações face à privacidade dos indivíduos, a preocupação com a proteção dos dados pessoais de saúde emerge como temática importante a ser explorada.

2.3. Problemáticas associadas à privacidade da informação e dados de saúde

Compreendendo os efeitos da disseminação das TI numa era orientada pelos dados (Yamamoto, 2016) e a maneira como estas transformaram a escala e a forma como os dados pessoais são recolhidos, acedidos, utilizados e transferidos, é necessário compreender as problemáticas que expõem a privacidade e proteção dos dados dos indivíduos.

A informação sensível, uma vez exposta ou divulgada, não pode nunca mais voltar a ser secreta, o que implica que o dano causado ao indivíduo e o desrespeito pelo seu direito à privacidade nunca mais será reposto. E, atualmente, os avanços tecnológicos culminaram num panorama em que os dados de saúde dos pacientes confrontam novas ameaças em relação à sua privacidade e segurança (Nass e Levit, L. A. Gostin, 2009).

A procura por um ambiente de SIS integrado e com fácil acesso à informação, visando a melhoria da qualidade da prestação de cuidados, origina a que os dados pessoais de saúde sejam partilhados num ambiente multidisciplinar, onde são facilmente copiados e transferidos. No entanto, é importante notar que o acesso aos dados para a melhor prestação de cuidados não pode nunca pôr em causa os direitos fundamentais dos cidadãos.

Ao abrigo do segredo médico (sigilo), os pacientes vêm cumprido o direito à confidencialidade das informações que divulgam. O segredo profissional é interpretado como “a proibição de revelar factos ou eventos que tomaram conhecimento ou que foram divulgados confidencialmente durante a prática da atividade profissional” (Código Penal, 1995).

Neste âmbito, os direitos de privacidade e confidencialidade relacionam-se diretamente com o direito da proteção de dados pessoais. (Faria e Cordeiro, 2014).

A confiança do paciente no médico é essencial para a relação entre ambos e para o tratamento a ser efetuado. E a quebra dessa confiança por parte dos profissionais de saúde pode ter consequências graves na prestação de cuidados, para além dos danos na vida dos pacientes.

Paula Lobato Faria (2014), no seu artigo sobre a "Privacidade dos dados de saúde e o direito de confidencialidade", afirma que o "direito à confidencialidade é baseado nos direitos fundamentais de privacidade e na "autodeterminação da informação", que se relaciona com a proteção de dados pessoais (direito da proteção de dados)". Afirma, ainda, que à confidencialidade podemos atribuir um sentido negativo e positivo: deve ser garantida a não interferência e o segredo em relação à informação (através do sigilo médico), mas também devem ser garantidas ações e medidas práticas e proativas que assegurem a confidencialidade da informação (medidas de segurança, supervisão, controlo). (Faria e Cordeiro, 2014).

Já referimos a riqueza dos RES relativamente à informação sobre os pacientes, assim como já constatamos a sensibilidade dessa informação.

O tratamento dos dados de saúde, assim como o acesso e disseminação, deve ser ponderado, de maneira a não serem postas em causa as medidas de segurança e de privacidade e confidencialidade.

A partilha indevida de informação entre profissionais e o acesso por terceiros (nem sempre o profissional de saúde responsável pelo tratamento) (Silva, 2007), tem de ser devidamente controlado e impedido. Essencialmente, é importante notar que sem confidencialidade, os pacientes podem evitar os cuidados de saúde que necessitam ou ocultar informação importante no momento da prestação de cuidados, com receio que a confidencialidade dos seus dados pessoais não seja devidamente protegida (Agaku et al, 2014). A própria qualidade dos dados pode ser posta em causa, pois os profissionais de saúde podem não registar toda a informação no registo clínico, resultando na perda do valor informacional para a melhoria dos cuidados de saúde (Ben-Assuli, 2015).

No contexto tecnológico, a segurança dos SIS é difícil de assegurar, o que, aliado à crescente dependência das instituições para o desempenho das funções, pode aumentar a sua vulnerabilidade. As medidas de privacidade e segurança devem ser estabelecidas e reforçadas se quereremos verdadeiramente alcançar os benefícios da extensa utilização dos SIS e dos tratamentos eletrónicos de dados (Goldstein, 2014).

Neste momento, é importante perceber o impacto das tecnologias no tratamento dos dados pessoais. Os dados pessoais estão efetivamente seguros? As novas tecnologias inseridas nos ambientes hospitalares tratam os dados devidamente? Os responsáveis pelo tratamento dos dados estão consciencializados em relação às implicações das tecnologias na forma como estes são tratados? (Parlamento Europeu, 2012).

A empresa holandesa Gemalto, através da sua plataforma "Breach Level Index", emitiu um relatório anual relativo aos registos de violações de dados pessoais que ocorreram no ano de 2016, em todos os setores industriais. Concluiu que, no ano de 2016, 1 378 509 261 registos de dados pessoais foram violados, provenientes de 1792 incidentes, onde em 52,12%, o nível de comprometimento dos dados era desconhecido. Desse número de registos pessoais violados, apenas 4,2% se encontravam encriptados, garantindo que os dados pessoais se encontravam protegidos. Especificamente no setor da saúde, registou-se a maior percentagem de violações de dados, correspondendo a 27,5% de todos os incidentes registados (The Breach Level Index, 2016).

Considerando o aumento de violações de dados que se têm vindo a registar na área da saúde nos últimos anos (Horvitz e Mulligan, 2015), sustentados por relatórios[1] como o "Breach Level Index", é cada vez mais importante que a tecnologia implementada no setor da saúde seja desenhada desde o início "como sendo capaz de estar em conformidade com os requisitos de privacidade e de segurança" (Gaudino, 2010). Desta forma, a privacidade tem de ser considerada desde o momento inicial, do ponto de vista tecnológico, no desenho e conceção dos sistemas de informação que são desenvolvidos.

As instituições devem ter como prioridade a privacidade e proteção de dados de maneira a não perder a confiança dos seus pacientes (Walker et al., 2017). As TI devem ser desenvolvidas e implementadas com vista a suportar a prestação de cuidados, mas devem também garantir a proteção dos dados pessoais que suportam. A utilidade das tecnologias na saúde é consensual, mas o problema reside na importância ética que a tecnologia assume. A principal preocupação em relação às questões da privacidade reside na dimensão em que a informação pode ser associada ou ligada a uma pessoa em particular e, considerando que as tecnologias suportam os processos de recolha, tratamento e armazenamento dos dados, é necessário garantir a defesa dos direitos fundamentais, percebendo que o

[1] Outros exemplos são o "2016 Data Breach Investigations Report" da Verizon e o "Data Breach QuickView Report" da Risk Based Security

direito à privacidade assume novos contornos, à medida que as TI também se vão expandindo (Silva, 2007).

Considerando a privacidade como direito fundamental, o Código Penal Português (1995) estabelece dois tipos de crimes contra a privacidade: a violação de privacidade, entendido como a divulgação não consentida de factos relativos à vida privada ou doença séria de uma pessoa (a menos que tal ação seja feita por um interesse público legítimo e relevante) e a divulgação do segredo a que tiveram acesso por meio da profissão que desempenham. A proteção da privacidade e dos dados pessoais dos pacientes por parte dos profissionais de saúde e pelas próprias instituições trata-se assim de uma obrigação, fundamentada pela legislação que tem sido desenvolvida ao longo dos anos.

2.4. Legislação de proteção de dados na área da saúde

Declaração Universal dos Direitos Humanos

A legislação e diretrizes concebidas com o objetivo de proteger os direitos dos indivíduos têm a sua base na Declaração Universal dos Direitos Humanos, redigida em 1948 pela Assembleia Geral das Nações Unidas. Com o objetivo essencial de proteção dos direitos e liberdades do Homem, a Declaração Universal dos Direitos do Homem, contém ainda provisões relativas ao direito à não intromissão na sua vida privada e vida familiar, demonstrada no artigo 12º "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção de lei" (Assembleia Geral das Nações Unidas, 1948).

Convenção Europeia dos Direitos do Homem

Em 1950, realiza-se a Convenção Europeia dos Direitos do Homem, com o principal objetivo de assegurar em cada jurisdição a garantia coletiva dos direitos e liberdades enunciados na Declaração Universal dos Direitos Humanos.

O artigo 8º, número 1, referente ao respeito pela vida privada e familiar, volta a indicar o "direito de um indivíduo ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". No entanto, o número 2 do mesmo artigo indica que "não pode haver

ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros." (Convenção Europeia dos Direitos do Homem, 1979), o que indica que, apesar do direito à privacidade ser um direito fundamental, a interferência justificada naquilo que é considerado informação pessoal pode ser fundamentado por um interesse legítimo. A necessidade de perceber o balanço entre privacidade e interferência justificada constitui um tema recorrente nas leis de proteção dos dados (Rudgard, 2012).

Diretrizes OCDE

Entre 1960 e 1980, vários países europeus implementaram legislação que visava controlar o uso de informação pessoal pelas grandes empresas e agências governamentais. Estas ações demonstram uma forte consciencialização da Europa para com as preocupações morais da privacidade, sendo que a proteção dos dados pessoais foi desde cedo incorporada como direito constitucional.

Em 1980, sob iniciativa da Organização para a Cooperação e Desenvolvimento Económico (OCDE) e do Conselho Europeu, foram desenvolvidas as "Diretrizes da OCDE para a proteção da privacidade e dos fluxos transfronteiriços de dados pessoais", que visavam definir políticas a ser aplicadas em relação ao tratamento de dados pessoais, não apenas no contexto europeu, mas em relação a todos os países membros da OCDE. O principal objetivo do documento elaborado era encontrar um equilíbrio entre a proteção da privacidade e dos direitos e liberdades dos indivíduos sem constituir barreiras às ações comerciais, permitindo um fluxo de dados entre as barreiras transfronteiriças (Rudgard, 2012).

Essencialmente, as Diretrizes da OCDE eram compostas por uma séria de princípios básicos a ser aplicados ao responsável pelo tratamento dos dados pessoais, no que tange o tratamento dos dados. Constavam essencialmente os princípios de limitação de recolha, qualidade dos dados, especificação do propósito, limitação do uso dos dados, salvaguardas de segurança, transparência, participação dos indivíduos e responsabilidade.

É possível notar uma crescente preocupação não apenas com o estabelecimento da privacidade e proteção dos dados como direito dos indivíduos, mas com o papel que as

instituições e organizações desempenham na garantia do cumprimento desses direitos, nomeadamente em relação ao tratamento que dão aos dados pessoais.

Convenção 108 do Conselho da Europa

O crescimento das TI na década de 60 elevou a necessidade de serem adotadas regras mais específicas para garantir a proteção dos dados pessoais.

Em 1981 foi aberta a assinatura da Convenção para a proteção das pessoas relativamente ao tratamento automatizado de dados pessoais, com o objetivo de assegurar "para cada indivíduo, independentemente da sua nacionalidade ou residência, respeito pelos seus direitos e liberdades fundamentais, em particular o direito à privacidade, em relação ao tratamento automático dos seus dados pessoais" (Conselho da Europa, 1981).

Esta constituiu a primeira abordagem à utilização de informação pessoal de forma computorizada e à responsabilidade de salvaguarda respetiva. Neste sentido, visa proteger as pessoas contra abusos que possam ser associados à recolha e tratamento de dados pessoais, respeitando o tratamento de dados leal e lícito.

Diretiva 95/46/CE

Numa altura em que vários países europeus já haviam adotado leis nacionais acerca da proteção de dados, (Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, 2014), surge o principal instrumento jurídico da UE sobre a proteção de dados. A Diretiva de 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desse dados, constitui a primeira tentativa de harmonizar as leis de proteção de dados existentes até ao momento, fruto da diversidade de abordagens nacionais à legislação de proteção de dados (Rudgard, 2012). Esta diversidade ao nível das legislações constituía um obstáculo no funcionamento do mercado interno da UE. "Se os direitos fundamentais dos titulares dos dados, principalmente o direito à privacidade, não for salvaguardado ao nível da Comunidade, os fluxos transfronteiriços de dados podem ser impedidos" (Rudgard, 2012).

Desta forma, é apresentada uma estrutura comum a todos os estados-membro da UE, visando tornar equivalente o nível de proteção dos direitos e liberdades das pessoas no

que diz respeito ao tratamento de dados pessoais (Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, 2014). A Diretiva de 95/46/CE visava dar corpo aos princípios do direito à privacidade já consagrados na Convenção 108 e alargar a sua aplicação. No entanto, a Diretiva explora a possibilidade de adotar novos instrumentos de proteção, materializando-se no estabelecimento de autoridades de controlo independentes como meio de melhorar o cumprimento de regras sobre a proteção de dados.

Apesar dos esforços da Diretiva, puderam ainda ser registadas algumas diferenças significativas na forma como os Estados-Membro implementaram a Diretiva, dificultando o aproveitamento total dos seus benefícios.

O principal foco da Comissão Europeia tem sido a melhoria da implementação e aplicação da Diretiva, levando a sérias revisões nos anos seguintes que acabariam por resultar no presente RGPD.

Carta dos Direitos Fundamentais da União Europeia

A Carta dos Direitos Fundamentais da União Europeia foi proclamada em 2000, num esforço por parte da UE de colmatar as suas políticas, que poderiam afetar os direitos humanos, e também num esforço de aproximar os cidadãos da União (Agência dos Direitos Fundamentais da União Europeia e Conselho da Europa, 2014). Reconhecendo a necessidade de fortalecer a proteção dos direitos fundamentais dos seus cidadãos, face às mudanças na sociedade, progresso social e desenvolvimentos científicos e tecnológicos, a UE decidiu tornar os direitos dos cidadãos mais visíveis (Comissão Europeia, 2000).

A Carta inclui os princípios gerais definidos na Convenção Europeia dos Direitos Humanos, mas referencia especificamente a proteção dos dados pessoais, elevando-o expressamente a um direito da UE, como definido no artigo 8º, número 1 “Todos têm o direito à proteção de dados pessoais referentes a ele ou a ela”. O artigo 8º, número 2 especifica ainda que “Tais dados devem ser tratados de forma justa para um propósito específico e na base do consentimento da pessoa a quem dizem respeito ou outra base legítima definida por lei. Todos têm o direito de acesso aos dados que foram recolhidos (…) e o direito de ter esses dados retificados” (Comissão Europeia, 2000).

A Carta torna-se juridicamente vinculativa com a entrada em vigor do Tratado de Lisboa, em Dezembro de 2009.

2.5. Enquadramento do Regulamento Geral da Proteção de Dados[2]

O Regulamento Geral da 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.

A necessidade de existir uma reforma relativa à Diretiva em vigor provém dos fatores associados à evolução tecnológica e à globalização, que criaram novos desafios na matéria de proteção de dados, como já referido em seções anteriores.

As evoluções que se registaram exigiram um "quadro de proteção sólido e mais coerente na União Europeia, apoiado por uma aplicação mais rigorosa das regras" (Parlamento Europeu, 2016).

Assentando nessa base, o novo RGPD pretende aumentar a proteção dos dados pessoais dos residentes da União Europeia e providenciar uma *framework* consolidada que guie a utilização dos dados pessoais nas mais diversas indústrias dentro da UE, substituindo o rol de regulações e *frameworks* já existentes pelos diferentes países.

É importante salientar que, tratando-se de uma regulação da UE, o RGPD corresponde a um "ato legislativo vinculativo que se torna imediatamente aplicável em todos os seus elementos em todos os países membros." [3] Desta forma, todos os Estados Membros estão sob a encargo de implementar as obrigações apresentadas no RGPD.

O RGPD começou por ser delineado através de uma proposta emitida em Janeiro de 2012 pela Comissão Europeia, onde se propunha a redação de um regulamento geral que 1) visava a proteção dos indivíduos a respeito do tratamento dos seus dados pessoais e na livre circulação desses mesmos dados e 2) a proteção dos indivíduos a respeito do tratamento dos dados pessoais por parte das autoridades competentes, para propósitos de prevenção, investigação, deteção ou acusação de ofensas criminais ou execução de penalidades criminais, e a livre circulação desses mesmos dados (Comissão Europeia, 2012).

[2] As definições e conceitos da presente seção são fundamentados no Regulamento Geral de Proteção de Dados da União Europeia.

[3] http://europa.eu/european-union/eu-law/legal-acts_pt

O RGPD foi então aprovado em Abril de 2016, sendo aplicado a partir de 25 de Maio de 2018 (é dado um período de 2 anos para as organizações ajustarem os seus processos).

Os principais objetivos do regulamento são (Parlamento Europeu, 2016):

1. estabelecer regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados;
2. defender os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais.

O âmbito de aplicação do RGPD incide sobre todo o tipo de tratamentos de dados, em todo o tipo de industrias, onde os dados pessoais sejam "tratados por meios total ou parcialmente automatizados, bem como o tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados".

Relativamente à aplicação territorial do regulamento, este aplica-se ao tratamento de dados pessoais de titulares residentes no território da UE, quer o responsável pelo tratamento se situe no território da UE, quer o responsável pelo tratamento se situe fora da UE, mas o tratamento dos dados pessoais incida sobre pessoas singulares que pertençam à UE

Essencialmente, o novo regulamento vem criar um modelo que obriga as entidades e organizações a considerarem as questões relacionadas com a proteção e os riscos de privacidade dos dados pessoais. Para esse efeito, foi necessária a reformulação e definição de conceitos, assim como de obrigações associadas.

O RGPD define **dados pessoais** como "informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, número de identificação, dados de localização, identificadores por via eletrónica ou a um mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"; **tratamento de dados pessoais** corresponde a "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a com-

paração ou interconexão, a limitação, o apagamento ou destruição". Por esta definição presente no RGPD, podemos verificar que o conceito de tratamento de dados foi amplamente alargado, estando mais abrangente em relação às ações que podem ser realizadas no processamento de dados pessoais.

O **responsável pelo tratamento** é definido como "a pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais"; **subcontratante** entende-se como "pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes".

Dados relativos à saúde, definem-se como "dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde", estando englobados numa categoria especial de dados pessoais.

Percebendo os conceitos que foram reformulados e entendendo o conceito de tratamento, é necessário perceber que princípios foram estabelecidos em relação ao tratamento de dados pessoais, que introduzem alterações significativas.

Os princípios relativos ao tratamento de dados pessoais assentam em:

- → **licitude, lealdade e transparência** dos dados pessoais (em relação ao titular dos dados);
- → devem ser **limitados à finalidade** definida pelo responsável pelo tratamento (não podendo haver um tratamento posterior dos dados que seja incompatível ou diferente das finalidades definidas inicialmente);
- → os dados pessoais devem ser tratados segundo um princípio de **minimização dos dados** (ou seja, os dados devem ser adequados e limitados ao que é necessário em relação às finalidades para as quais são tratados);
- → os dados devem ser exatos e atualizados sempre que necessário, o que implica a adoção de medidas adequadas para que estes sejam apagados ou retificados sem demora e sem comprometer o tratamento, cumprindo assim o princípio de **exatidão**;

→ devem cumprir um **limite de conservação** (ou seja, devem ser conservados de forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados);

→ devem ser tratados de uma forma que assegura a sua segurança, impedindo o tratamento ilícito e a sua perda, destruição ou danificação acidental, sendo assegurada a sua **integridade e confidencialidade**.

→ Para assegurar o cumprimento dos princípios de tratamento de dados indicado, o responsável pelo tratamento tem o dever de demonstrar e comprovar **responsabilidade.**

O tratamento de dados pessoais deve ainda ser assente numa base legal que assegure que o tratamento dos dados é prosseguido de um **interesse legítimo**. Nesta medida, o tratamento lícito dos dados é considerado legítimo nas seguintes situações:

- quando o titular dos dados tiver dado o seu **consentimento** para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas;
- quando o tratamento for necessário para a execução de um contrato do qual o titular dos dados faz parte;
- quando o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento está sujeito;
- quando o tratamento for necessário ao exercício de funções de interesse público ou a exercício da autoridade pública;
- quando o tratamento for necessário para efeitos de interesse legítimo, exceto se prevalecerem os interesses e direitos e liberdades do titular que exijam a proteção dos dados.

No que tange o tratamento das categorias especiais de dados, nos quais são englobados os dados de saúde, é estritamente proibido o seu tratamento, salvo a verificação de uns dos seguintes pontos:

- se o titular dos dados tiver dado o seu consentimento explícito para o tratamento para uma ou mais finalidades específicas;
- se o tratamento for necessário para efeitos de cumprimento das obrigações e do exercício de direitos específicos do responsável pelo tratamento ou do titular dos

dados em matéria de legislação laboral, de segurança social e de proteção social;

- se o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular, no caso de o titular dos dados estar física ou legalmente incapacitado de dar o seu consentimento;
- se o tratamento for efetuado, no âmbito das suas atividades legítimas e mediante garantias adequadas, por uma fundação, associação ou qualquer outro organismo sem fins lucrativos e que prossiga fins políticos, filosóficos, religiosos ou sindicais, e desde que esse tratamento se refira exclusivamente aos membros ou antigos membros desse organismo (…) e que os dados pessoais não sejam divulgados a terceiros sem o consentimento dos seus titulares;
- se o tratamento se referir a dados pessoais que tenham sido manifestamente tornados públicos pelo seu titular;
- se o tratamento for necessário por motivos de interesse público importante (…) que deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção de dados pessoais e prever medidas adequadas e específicas que salvaguardem os direitos fundamentais e os interesses do titular os dados;
- se o tratamento for necessário para efeitos de medicina preventiva e do trabalho, para avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou Estados Membros ou por força de um contrato com um profissional de saúde;
- se o tratamento for necessário por motivos de interesse público no domínio da saúde, tais como a proteção contra ameaças transfronteiriças graves para a saúde ou para assegurar um elevado nível de qualidade e de segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos,
- se o tratamento for necessário para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos (…) deve ser proporcional ao objetivo visado, respeitar a essência do direito à proteção dos dados pessoais e prever medidas de segurança adequadas.

Em relação às condições aplicáveis ao consentimento, é importante perceber que este deve derivar de um ato deliberado e informado por parte dos titulares dos dados, não dando margem para dúvidas em relação à compreensão do tratamento a que os seus dados serão sujeitos (não se pode basear no silêncio ou inatividade por parte do titular dos dados ou caixas pré assinaladas). O consentimento deve também ser diferenciado de outros tipos de notificações ou acordos escritos, sendo apresentado de forma distinta. Deve ser permitido ao titular dos dados retirar o consentimento dado ao tratamento dos seus dados, incluindo através de métodos que utilizem a mesma forma de obter consentimento. O consentimento obtido por parte dos responsáveis pelo tratamento deve ser verificável e demonstrável. Desta forma, devem ser mantidos alguns tipos de registos de como e quando o consentimento foi obtido.

No que tange as condições aplicáveis ao consentimento de crianças (em relação a ofertas diretas de serviços da sociedade da informação), este apenas é considerado lícito se as crianças tiverem pelo menos 16 anos. No caso da criança ter menos de 16 anos, deve ser obtido o consentimento dos pais ou dos representantes legais. Esta medida destina-se a proteger os dados pessoais de determinada criança. No caso dos serviços oferecidos diretamente às crianças, os responsáveis pelo tratamento devem "assegurar que as suas notificações de privacidade estão escritas de forma clara e compreensível, capaz de ser compreendida por uma criança" (Information Comissioner Officer, 2016). O consentimento dos pais ou representantes legais apenas não é necessário para o tratamento dos dados de crianças para fins de prevenção ou serviços de aconselhamento oferecidos diretamente à criança.

O RGPD definiu ainda uma série de **direitos para os titulares dos dados**, direitos esses que os fortalecem face à antiga Diretiva:

- **Direito à transparência** por parte dos responsáveis pelo tratamento, na medida em que devem ser fornecidas ao titular dos dados todas as informações a respeito do tratamento de forma concisa, transparente, inteligível e de fácil acesso, utilizando uma linguagem clara e simples. Estas informações são prestadas por escrito ou por outros meios, incluindo meios eletrónicos.
- **Direito a ser informado**, que engloba a obrigação de providenciar as informações transparentes por parte do responsável pelo tratamento, em relação ao tratamento dos dados pessoais que são fornecidos. Este direito engloba não só a obrigação de providenciar informação ao titular dos dados, mas também de

providenciar qualquer informação requerida pelo titular em relação ao tratamento dos dados a qualquer momento.

- **Direito de acesso** fornece ao titular dos dados a possibilidade de obter do responsável pelo tratamento a confirmação de que os seus dados pessoais são ou não objeto de tratamento e, caso estes estejam a ser processados, os titulares dos dados têm o direito de aceder aos seus dados pessoais e a informações tais como a finalidade do tratamento, a categoria dos dados pessoais em questão, os destinatários a quem os dados pessoais foram ou serão divulgados, o prazo previsto de conservação dos dados pessoais (no caso de não ser possível, os critérios para fixar este prazo), as informações disponíveis sobre a origem dos dados pessoais (caso os dados não tenham sido recolhidos junto do titular dos dados), existência de decisões automatizadas, incluindo a definição de perfis (nesses casos, devem ser fornecidas informações úteis à lógica subjacente). Na medida em que o titular dos dados tem também o direito de aceder às informações em relação a tratamento dos dados, deve-lhe ser apresentada a existência do direito de solicitar ao responsável pelo tratamento a retificação, apagamento ou a limitação do tratamento dos seus dados pessoais ou do direito de se opor ao tratamento, assim como do direito de apresentar reclamação a uma autoridade de controlo. Perante o exercício deste direito, o responsável pelo tratamento deve fornecer uma cópia do tratamento dos dados pessoais aos respetivos titulares dos dados. Caso o pedido seja feito eletronicamente, a informação deve ser providenciada num formato comum.
- **Direito à retificação** dos dados permite que os titulares dos dados retifiquem os dados pessoais sujeitos a tratamento, caso este se encontrem imprecisos ou incompletos.
- **Direito ao apagamento**, ou direito ao esquecimento, permite que os titulares dos dados requeiram o apagamento ou remoção dos dados pessoais em certas situações específicas (mais concretamente, no caso do tratamento dos dados não satisfazer os requisitos do RGPD).
- **Direito à limitação** do tratamento permite que o titular dos dados restrinja o tratamento dos dados, permitindo que o responsável pelo tratamento armazene os dados pessoais, mas não proceda a mais nenhum tipo de tratamento (quando o tratamento tiver sido limitado, os dados pessoais só podem voltar a ser objeto

de tratamento com o consentimento do titular ou para feitos de declaração, motivos de interesse público, exercício ou defesa de um direito num processo judicial ou defesa dos direitos de outra pessoa singular ou coletiva).

- **Direito à portabilidade** garante aos titulares dos dados a obtenção dos seus dados pessoais num formato estruturado e legível, passível de ser transferido diretamente para outro ambiente tecnológico, de forma segura e sem comprometer a sua usabilidade. Este direito só pode ser exercido sobre os dados que foram fornecidos pelo titular dos dados e apenas a dados que sejam processados por meios automáticos (não se aplica a registos em papel).
- **Direito de oposição/objeção** ao tratamento aplica-se em três tipos de situações: tratamento de dados para marketing direto, tratamento para propósitos de investigação/estatística científica/histórica, tratamento de dados assente no interesse legítimo ou a performance de uma função de interesse público. Os titulares dos dados têm então o direito de objetar o tratamento dos dados pessoais, cabendo depois ao responsável pelo tratamento a justificação da licitude do tratamento dos dados pessoais.
- **Direito relativo à decisões individuais automatizadas**, incluindo a definição de perfis, atribui o direito aos titulares de não serem sujeitos a decisões tomadas com base no tratamento automatizadas ou com base na definição de perfis que os possam afetar significativamente.

O RGPD resultou numa reformulação de conceitos, princípios e direitos dos titulares dos dados, com grandes implicações para as entidades e organizações. A implementação de certas medidas técnicas e organizativas torna-se essencial para conseguir responder obrigações impostas pelo regulamento.

O RGPD aponta medidas que promovem a responsabilidade das instituições e o cumprimento do regulamento, e espera-se que as instituições, ponham estas medidas em prática.

Primeiramente, é necessário compreender que as organizações responsáveis pelo tratamento têm a obrigação de demonstrar responsabilidade e conformidade com o RGPD. Desta forma, é necessária a implementação de medidas que permitam que os processos

da organização consigam responder a estas obrigações, tais como formação dos profissionais, auditorias internas das atividades de tratamento e revisão das políticas internas de privacidade da organização.

Torna-se necessário que seja mantida a documentação em relação às atividades de tratamento de dados pessoais levadas a cabo pela instituição. Os registos de tratamento devem conter informação associada ao tipo de dados que serão processados, o propósito de utilização dos dados, período de retenção dos dados e descrição das medidas de segurança técnicas e organizativas a ser tomadas. A documentação mencionada deve ser fornecida num contexto de auditoria ou sempre que seja requisitada pela autoridade reguladora.

As instituições têm também a obrigação de implementar medidas técnicas e organizativas que demonstrem a integração da proteção de dados nas suas atividades de tratamento desde o momento inicial. O conceito de “Proteção de dados desde a conceção” e “Proteção de dados por defeito” é desta forma introduzido, sendo uma das obrigações mais importantes do RGPD. A utilização de técnicas de pseudonimização e minimização dos dados torna-se fundamental para assegurar a privacidade dos titulares dos dados e, dessa forma, garantir um tratamento dos dados pessoais em conformidade com os requisitos do regulamento. Na sua essência, a proteção de dados desde a conceção e por defeito visa incutir nas entidades responsáveis pelo tratamento de dados pessoais um sentido de preocupação com os riscos associados à privacidade e proteção de dados dos indivíduos desde o início dos processos (novo produto, serviço, projeto), e não num sentido de reação a violações de dados ou quebras de privacidade dos titulares dos dados. A proteção dos dados pessoais deve ser endereça desde início e, por defeito, as instituições devem pôr em prática os mecanismos necessários para garantir que apenas são recolhidos, utilizados e conservados os dados necessários para a realização de uma determinada tarefa, e que apenas vão ser mantidos durante o período necessário ao cumprimento dessa tarefa (Serviços Partilhados do Ministério da Saúde, n.d.).

O RGPD apresenta também a obrigação de se realizarem Avaliações de Impacto na Proteção de Dados, avaliação que permite identificar os riscos associados ao tratamento dos dados pessoais. A realização de Avaliações de Impacto na Proteção de Dados permite que as instituições minimizem ou mitiguem tratamentos passíveis de não estar em conformidade com o RGPD. Apesar do conceito não ser novidade (a realização de Avaliação de

Impacto de Privacidade é uma prática já utilizada nas Avaliações de Risco), o novo regulamento veio formalizar a necessidade de estes serem efetuados. Devem então ser conduzidas Avaliações de Impacto na Proteção de Dados para situações em que sejam implementadas novas tecnologias ou sistemas de informação nas instituições e sempre que o tratamento é provável de representar um risco elevado para os direitos e liberdades dos titulares dos dados (atividades de tratamento sistemáticas e extensivas, incluindo definição de perfis e decisões com impacto legal no individuo, e tratamentos em grande escala de categorias especiais de dados, ou dados relacionados com condenações ou ofensas criminais, onde se inserem os dados de saúde). Os requisitos mínimos para a realização de uma Avaliação de Impacto na Proteção de Dado incluem uma descrição das atividades de tratamento e do seu propósito e uma avaliação da necessidade e da proporcionalidade do tratamento (assim como possíveis riscos e medidas adotadas para mitigar esses riscos, particularmente as salvaguardas e as medidas de segurança para a proteção dos dados pessoais e conformidade com o RGPD).

O RGPD introduz o dever das organizações reportarem violações de dados à autoridade reguladora (em casos particulares pode ser necessário notificar os titulares dos dados). Entende-se por violação de dados pessoais “uma violação de segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento” (Parlamento Europeu, 2016). No entender do regulamento, apesar de existir a obrigação de registar todas as violações de dados pessoais que se verificam na instituição, nem todos os casos são passíveis de serem comunicados à Comissão Nacional da Proteção de Dados e aos respetivos titulares dos dados. Desta forma, apenas devem ser comunicados violações de dados que constituam um risco para aos direitos e liberdades dos indivíduos. As notificações das violações de dados devem ser reportadas à CNPD num prazo de 72 horas.

O RGPD apoia também a utilização de códigos de conduta e mecanismos de certificação para demonstração de conformidade. Apesar de não ser um requisito obrigatório, é recomendável a elaboração de códigos de conduta (até mesmo específicos para os diferentes tipos de indústria) que possam ser utilizados pelas instituições, uma vez que se espera que sejam providenciadas diretrizes que apoiem na demonstração da conformidade com o RGPD, através da melhoria da transparência e responsabilidade da instituição, pro-

videnciando medidas de mitigação contra ações de execução e, essencialmente, estabelecer as melhores práticas na instituição. É importante perceber que a utilização de códigos de conduta e certificações não reduzem as responsabilidades dos responsáveis pelo tratamento no que tange a proteção de dados.

Relativamente à transferência de dados pessoais dos cidadãos da EU para países fora da Área económico Europeia, já bastante reguladas e restritas, o RGPD impõe novas obrigações. A transferência de dados para países terceiros e organizações internacionais está sujeita à garantia das salvaguardas adequadas requeridas para o tratamento de dados segundo o RGPD. Deve também ser garantido que os titulares dos dados pessoais podem usufruir dos direitos oponíveis e de medidas jurídicas corretivas eficazes.

2.6 – OpenEHR

O openEHR é uma norma que apresenta um conjunto de especificações para uma arquitetura de Registos Eletrónicos de Saúde, 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). É composto por uma "comunidade virtual que se centra na interoperabilidade e computabilidade na e-saúde. O seu principal foco está em permitir a construção de sistemas de RES que possam comunicar-se entre si sem que haja perda de significado do conteúdo" (Bacelar e Correia, 2015).

As diretrizes do openEHR foram desenvolvidas e publicadas pela Fundação OpenEHR[4], entidade também responsável pela elaboração e disponibilização de ferramentas que permitem o uso da norma.

Na sua essência, o openEHR permite que continuem a existir inúmeros SIS, mas os dados clínicos do paciente podem ser partilhados para onde quer que ele venha a ser atendido. Esta facilidade na partilha de registos deve-se à interoperabilidade ao nível do conhecimento, sendo também esta característica responsável pela independência tecnológica que o openEHR oferece.

[4] www.openehr.org

Arquitetura openEHR

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 Conteúdo do Modelo de Informação.

O modelo de informação corresponde ao primeiro nível de modelação, sendo constituído por um modelo de referência estável (Beale e Heard 2007). Este modelo contém 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).

Apenas este modelo é implementado no software, o que permite reduzir não só a dependência dos sistemas desenvolvidos, como a variação das definições de conteúdo desses mesmos sistemas. Como consequência, "os sistemas têm a possibilidade de serem muito menores e de mais fácil manutenção que sistemas com um único nível" (Beale e Heard, 2007).

O modelo de conteúdo corresponde ao segundo nível e contém as definições formais de conteúdo clínico na forma de *arquétipos* e *templates*. Os conceitos clínicos são estruturados fora do software, o que permite que os sistemas RES sejam "mais flexíveis, uma vez que as alterações ao nível do conhecimento clínico são suportadas pelas alterações dos arquétipos, sem comprometer a integridade da informação no repositório" (Leslie, 2008).

A modelação a dois níveis do openEHR apresenta assim um novo paradigma de modelação de sistemas, onde "a parte central do sistema é baseada num modelo extremamente estável: o modelo de referência. Por outro lado, o modelo de conteúdo (composto por arquétipos e templates) é flexível, para poder refletir a evolução do conhecimento e as suas restrições de uso" (Bacelar e Correia, 2015).

Arquétipos e Templates

Fundamentalmente, a ideia do openEHR é que todos os sistemas de RES utilizem a mesma estrutura de dados, que como já foi referido, são representados por arquétipos e templates.

Desta forma, para garantir que todos os sistemas são construídos a partir dos mesmos arquétipos, é necessário que todos tenham acesso aos mesmos arquétipos.

O CKM (Clinical Knowledge Manager) – Gestor de Conhecimento Clínico – apresenta-se como um repositório online de conteúdo clínico em forma de arquétipos e templates (Bacelar et al, 2015), onde é possível encontrar o que já existe e extrair para uso em aplicações.

O CKM funciona também como uma plataforma de colaboração onde é possível "traduzir, atualizar, sugerir alterações e interagir com os restantes membros para chegar a consenso sobre a melhor definição de um arquétipo ou template" (Bacelar et al, 2015). A colaboração é aberta a todos os interessados, sendo que os principais participantes incluem clínicos, profissionais de informática, engenheiros de software, entre outros.

O arquétipo openEHR pode ser definido como "um modelo eletrónico computável de um conceito clínico, estruturado e detalhado da forma mais completa possível" (Bacelar e Correia, 2015).

Os arquétipos são peças fundamentais na arquitetura openEHR. É fundamental que estes sejam únicos e que descrevam da forma mais abrangente e completa possível os conceitos clínicos, tais como 'pressão arterial', 'pulsação/batimento cardíaco', 'diagnóstico', entre outros. Apenas descrevendo os arquétipos de forma completa este poderá servir para múltiplas situações de uso. No entanto, é importante salientar que nem toda a informação associada a um arquétipo necessita de ser utilizada, havendo a possibilidade de filtrar os campos de interesse.

A definição do que será utilizado de cada arquétipo ocorre durante a criação do template (Bacelar e Correia, 2015).

Já foi referido anteriormente que o processo de atendimento médico lida resulta em diferentes tipos de informação. Considerando os tipos de informação identificados, torna-se essencial estruturarem-se diferentes tipos de arquétipos, de forma a representarem-se as diferentes necessidades informacionais que ocorrem ao longo do fluxo de atendimento.

As principais classes de arquétipos são (Bacelar e Correia 2015):

Composition

O conteúdo destas classes de arquétipos é composto por mais arquétipos, no momento da modelação específica.

Essencialmente, corresponde a um “documento clínico usado comumente” (Leslie e Heard, 2006), como são exemplos as ‘consultas pré-natal’ e os ‘relatórios de alta’.

Section

Este tipo de arquétipos possuem uma finalidade mais centrada no auxílio na navegação dentro dos RES, uma vez que organizam o seu conteúdo em compartimentos mais específicos (secções ou subsecções).

Correspondem aos cabeçalhos dos documentos, como por exemplo ‘exame pré-natal’ e ‘exame físico’.

Admin Entry

Este tipo de arquétipos não é clinicamente relevante, uma vez que se destina ao armazenamento de informações administrativas sobre o processo clínico, como por exemplo dados administrativos de admissão hospitalar (ex: ‘data de internamento do paciente’).

Clinical Entries

As Clinical Entries constituem as classes de arquétipos que modelam os dados clínicos, sendo compostas por:

Observation

Esta classe de arquétipos representa todo o tipo de informação que pode ser extraída daquilo que é dito pelo paciente no momento do atendimento (sintomas e queixas), os achados de exames e os resultados de testes ou procedimentos clínicos (tais como a medição da pressão arterial ou da pulsação/batimento cardíaco).

Evaluation

Este tipo de arquétipos permite o registo das interpretações das observações.

O ‘diagnóstico’ é um exemplo de um arquétipo Evaluation.

Instruction

Estes arquétipos incorporam as instruções sobre como dar seguimento ao processo de prestação de cuidados, tendo como exemplos as ‘prescrições médicas’ e a ‘solicitação de exames’.

Action

Estas classes de arquétipos são associadas a uma intervenção directa, sendo normalmente precedidas por um Instruction. São exemplos os ‘procedimentos cirúrgicos’ e ‘administração de medicação’.

Cluster

Os arquétipos pertencentes a esta classe funcionam como um fragmento de arquétipo, podendo ser reutilizados dentro dos arquétipos de qualquer um dos outros tipos descritos.

O Archetype Editor é a ferramenta desenvolvida para a edição de arquétipos.

Os templates podem ser definidos como “arquivos que sustentam diversos arquétipos, considerando as respetivas restrições” (Bacelar e Correia 2015), sendo que a criação de um template inicia-se a partir de um arquétipo do tipo Composition.

Desta forma, os templates filtram as partes necessárias de um arquétipo, de forma a constituírem formulários, relatórios e mensagens.

Uma vez elaborados os templates, são desenvolvidas “aplicações com a estrutura de dados necessária para o registo de informação e para a validar a introdução de dados de acordo com as restrições impostas aos arquétipos” (Bacelar e Correia 2015).

O Template Editor é a ferramenta utilizada para o desenvolvimento de templates.

3. Metodologia de Investigação

O trabalho desenvolvido corresponde a uma investigação suportada por um caso de estudo. Coutinho (2002) define caso de estudo como “plano de investigação que envolve o estudo intensivo e detalhado de uma entidade bem definida: “o caso”.” A mesma autora identifica ainda que pode ser considerado um caso “uma decisão, uma política, um processo“.

Considerando a natureza qualitativa do âmbito de estudo, considera-se o trabalho desenvolvido como uma investigação qualitativa onde propósito é “explorar a questão de pesquisa de uma forma profunda (…). Nestes casos é necessário estabelecer os propósitos da pesquisa e traçar um conjunto de objetivos” (Pickard, 2013). Essencialmente, o objetivo da investigação qualitativa é o de investigar uma intenção ou uma ideia, o que representa o propósito do trabalho desenvolvido.

O trabalho será desenvolvido com recurso a fontes documentais existentes que se relacionam com o objetivo proposto. Na sua essência, pretende-se construir uma “lógica de construção de conhecimento, incorporando a subjetividade do investigador” (Meirinhos and Osório, 2010), traduzindo-se num levantamento de requisitos para um SIS em conformidade com um regulamento europeu e a respetiva correspondência com uma norma de SRES.

O objetivo da investigação proposta é perceber se a arquitetura presente na norma openEHR permite que um sistema de informação de saúde esteja em conformidade com o RGPD, mais concretamente, com os requisitos que possam ser identificados. A partir deste objetivo, definiu-se a questão de pesquisa como sendo: O openEHR permite a construção de um SIS em conformidade com o RGPD?

Para conseguir responder a esta questão principal, foram elaboradas questões secundárias, que compelem os objetivos da pesquisa:

- Quais são os requisitos para um SIS estar em conformidade com o RGPD?
- Quais são os princípios do openEHR face às funcionalidades de um SIS?
- Qual o nível de concordância entre os princípios do openEHR e os requisitos de um SIS em conformidade com o RGPD?

Para responder às questões secundárias, inicialmente definiu-se a necessidade de se proceder a uma análise do regulamento com o objetivo de fazer o levantamento de requisitos para um SIS. Consideraram-se metodologias que suportassem a identificação de requisitos e que oferecessem diretrizes para a elaboração de uma lista.

Definiu-se a seguinte documentação a ser utilizada:

- IEEE Std 1233 Guide for developing system requirementes specifications
- SBIS, Manual para certificação para sistema de registo eletrônico em saúde.

Com base na "IEEE Guide for developing system requirementes specifications", definiu-se a metodologia para a identificação de requisitos. Primeiramente, foi definido que os requisitos de um sistema deveriam identificar "o que o sistema deve fazer" (IEEE, 1998), havendo um foco nas funcionalidades e não nos processos para a construção do mesmo.

Foram consideradas as propriedades que um requisito deveria ter, nomeadamente de ser único, normalizado, completo, consistente, devem ser definidas as suas barreiras, modificável, configurável e granular. Deve também ser considerada a sua ligação a outros requisitos, quando necessário.

Para a organização dos requisitos, houve um foco principal nas capacidades operacionais desejadas, nos parâmetros de performance e nos valores esperados. Alguns requisitos incidem no interface e interações desejadas com o ambiente em que se insere.

Para construir os requisitos para o sistema, segundo a norma mencionada, procurou-se definir a funcionalidade (capacidade do sistema), a condicionantes e as restrições e elaboraram-se requisitos tendo em conta as propriedades apontadas (deve ser abstrato, não ambíguo, permitir a rastreabilidade e ser validável).

Os contornos definidos para a lista de requisitos assentaram na descrição geral do sistema (através da identificação de objetivos gerais identificados) e a listagem das funcionalidades, condicionantes e restrições do sistema. É importante notar que se procurou identificar os requisitos funcionais do sistema.

Com base no "Manual de certificação para sistema de registo eletrônico em saúde da SBIS", foi definida a forma como a lista de requisitos iria ser organizada, definindo-se as informações que iriam constar na tabela que iria suportar a lista de requisitos (com as infor-

mações ID, Título, Requisito e Presença). Contudo, tomou-se a decisão de utilizar as informações “Objetivo” em vez de “Título” e “Prioridade de implementação” em vez de “Presença”). Esta decisão deve-se ao facto de “Objetivo” conseguir expressar diretamente o objetivo que se pretende alcançar com o requisito descrito e “Prioridade de implementação” ser mais adequado ao desenvolvimento de um sistema de informação.

Coluna	Descrição
ID	Identificação do requisito, codificada segundo o padrão
Objetivo	Objetivo do requisito
Requisito	Descrição do requisito (incluindo exemplos e notas explicativas se apropriado para melhor compreensão)
Prioridade de implementação	**M- Mandatório**: deve ser obrigatoriamente cumprido pelo SIS **R- Recomendável**: requisito importante, mas não obrigatório.

Após definir a metodologia para definir os requisitos e a forma como estes iriam ser representados numa tabela, procedeu-se à leitura do RGPD, com o objetivo de identificar os requisitos funcionais necessário a um SIS para estar em conformidade com o regulamento. À tabela resultante chamou-se “Tabela de requisitos para um SIS em conformidade com o RGPD”.

Numa segunda fase, procedeu-se à leitura do “openEHR Architecture overview”, com o objetivo de identificar os seus princípios face às funcionalidades de um sistema. Para a execução desta tarefa não foi necessário o recurso a nenhum tipo de documentação, uma vez que o próprio manual identifica as funcionalidades possíveis de um sistema de informação que utilize o conjunto de especificações openEHR. Desta forma, foram listadas as funcionalidades da norma openEHR, com principal foco nas funcionalidades que permite a um sistema e não na sua arquitetura. Ao resultado obtido chamou-se “Lista de funcionalidades de um sistema openEHR”.

Uma vez cumpridos estes dois objetivos, foi elaborada uma tabela final com os requisitos que se encontram listados na “Tabela de requisitos de um SIS em conformidade com o

RGPD", sendo que, para cada requisito, foi correspondida a especificação da "Lista de funcionalidades de um sistema openEHR" que o permitiria cumprir.

O resultado esperado seria uma tabela de correspondência entre os requisitos de um SIS em conformidade com o RGPD e as especificações openEHR.

4. Resultados

Para o melhor entendimento dos resultados finais, começou-se por analisar os resultados da realização das tarefas iniciais: levantamento de requisitos de um sistema de informação em conformidade com o RGPD e levantamento das especificações do openEHR.

No total, foram identificados 61 requisitos funcionais para um sistema de informação em conformidade com o RGPD. Este conjunto de requisitos divide-se em 4 grupos principais, sendo estes: “Requisitos para cumprimento dos Princípios do tratamento dos dados pessoais”, “Requisitos para cumprimento dos direitos dos titulares”, “Requisito de privacidade e segurança” e “Requisitos para transferência de dados pessoais para países terceiros ou organizações internacionais”. Para cada grupo de requisitos foram identificados os seguintes subgrupos:

1. Requisitos para cumprimento dos Princípios do tratamento dos dados pessoais
    a. Princípio do tratamento dos dados pessoais
        i. Limitação do tratamento dos dados pessoais
        ii. Minimização dos dados pessoais
        iii. Exatidão dos dados pessoais
        iv. Prazo para limitação da conservação dos dados pessoais
        v. Limitação da conservação
        vi. Integridade e confidencialidade
        vii. Responsabilidade
        viii. Demonstração da responsabilidade
    b. Consentimento explícito
        i. Consentimento Explícito
        ii. Consentimento explícito dos titulares dos dados
        iii. Registo do consentimento explícito
        iv. Capacidade do titular dos dados retirar consentimento
        v. Características do consentimento obtido

vi. Licitude do tratamento após retirar consentimento

c. Interesse legítimo

i. Interesse legítimo do tratamento

ii. Informação acerca do interesse legítimo

iii. Objeção dos titulares dos dados ao interesse legítimo

2. Requisitos para cumprimento dos direitos dos titulares

a. Transparência das informações, das comunicações e das regras para exercícios dos direitos dos titulares dos dados

i. Comunicação e informações fornecidas aos titulares dos dados

ii. Meios para a prestação de informações aos titulares dos dados

iii. Verificação da identidade dos titulares

iv. Prazo para resposta ao pedido dos titulares dos dados

v. Formato da resposta ao pedido do titular dos dados

vi. Preservação dos registos de notificações de informação

b. Informações a fornecer aos titulares dos dados pessoais

i. Notificações de informação

ii. Momento da notificação de informação (dados pessoais obtidos diretamente)

iii. Período de notificação de informação ao titular dos dados

iv. Notificação ao titular dos dados de novo tratamentos

c. Acesso dos titulares dos dados, Retificação e Portabilidade

i. Acesso dos titulares dos dados aos dados pessoais

ii. Formulário de resposta ao pedido de acesso dos titulares dos dados

iii. Confirmação do tratamento dos dados pessoais

iv. Informações que titular dos dados tem direito a aceder

v. Resposta ao pedido de acesso do titular dos dados

vi. Acesso direto dos titulares dos dados

vii. Retificação dos dados pessoais por parte titular dos dados

viii. Portabilidade dos dados pessoais dos titulares dos dados

ix. Portabilidade dos dados pessoais entre responsáveis pelo tratamento

x. Interoperabilidade dos formatos e sistemas

d. Direito de objeção

i. Objeção ao tratamento dos dados pessoais por parte do titular dos dados

e. Direito ao apagamento (esquecimento) e direito à limitação do tratamento

i. Apagamento dos dados pessoais a pedido do titular dos dados

ii. Notificação de outras entidades envolvidas no tratamento dos dados pessoais

iii. Limitação do tratamento dos dados pessoais a pedido do titular dos dados

iv. Limitação do tratamento

v. Notificação da anulação da limitação do tratamento dos dados pessoais

3. Requisitos de Privacidade e segurança

a. Proteção de dados pessoais desde a conceção e por defeito

i. Proteção de dados pessoais desde a conceção

ii. Proteção de dados pessoais por defeito

iii. Registo de políticas de proteção de dados pessoais

b. Registo das atividades de tratamento dos dados pessoais

i. Registo de tratamento de dados pessoais

ii. Formato do registo de tratamento de dados pessoais

iii. Disponibilização dos registos de tratamento dos dados pessoais

c. Notificação de violação de dados pessoais

i. Desenvolvimento de procedimento de notificação de violações de dados

ii. Controlo de acesso

iii. Registo de violações de dados pessoais

iv. Descrição da violação de dados pessoais para envio à autoridade reguladora

v. Prazos para notificação de violação de dados pessoais

d. Avaliação de Impacto na Proteção de Dados

i. Preservação de DPIA

ii. Consulta de DPIA

iii. Parecer do DPO

e. Perfil para Encarregado da Proteção de Dados (DPO)

i. Envolvimento do DPO na proteção de dados

f. Códigos de conduta e certificação

i. Conformidade com código de conduta

ii. Conformidade com processos de certificações

4. Requisitos para transferência de dados pessoais para países terceiros ou organizações internacionais

a. Transferência de dados pessoais sujeitos a garantias adequadas

i. Transferências de dados pessoais para países terceiros ou organizações internacionais

ii. Garantias das transferências de dados pessoais

A tabela completa encontra-se no Anexo A, com a descrição dos requisitos indicados e a indicação da prioridade de implementação do requisito face à conformidade com o RGPD.

De seguida, foram identificadas as especificações da arquitetura openEHR, sendo elas:

- Modelação Multinível
- Separação da informação clínica da informação demográfica
- Controlo de Versões
    - Versionamento e Indelebilidade
    - Assinatura Digital
- Controlo de Acesso
    - Lista de controlo de acesso
    - Controlo das configurações de acesso
- Audit trail
- Camada de Serviço

A descrição das especificidades identificadas encontra-se no Anexo B.

Concluído o levantamento dos requisitos do sistema em conformidade com o RGPD e das especificações openEHR, procedeu-se à correspondência entre ambos, de forma a perceber de que forma o openEHR poderia responder à lista de requisitos elaborada.

Dos 61 requisitos identificados, as especificações openEHR corresponderam a 15 requisitos, sendo que 13 dos requisitos respondidos são de prioridade de implementação Mandatória. Os resultados apresentados estão dispostos na Tabela 1.

A especificação **Controlo de acesso – lista de acesso** respondeu a 4 requisitos identificados, sendo eles: **integridade e confidencialidade, acesso dos titulares dos dados aos respetivos dados pessoais, acesso direto dos titulares dos dados** e **proteção dos dados por defeito**.

A especificação **Controlo de acesso – controlo de acesso às configurações de acesso** respondeu a 4 requisitos, sendo eles: **integridade e confidencialidade, acesso dos titulares dos dados aos respetivos dados pessoais, acesso direto dos titulares dos dados** e **proteção dos dados por defeito**.

A especificidade **Controlo de versões – assinatura digital** respondeu a 2 requisitos, sendo eles: **integridade e confidencialidade** e **proteção de dados por defeito.**

A especificidade **Controlo de versões – versionamento e indelebilidade** respondeu a 2 requisitos, sendo eles: **integridade e confidencialidade, confirmação de tratamento de dados pessoais.**

A especificidade **Separação da informação clínica da informação demográfica** respondeu a 5 requisitos, sendo eles: **minimização dos dados, limitação da conservação dos dados pessoais, verificação da identidade dos titulares dos dados, proteção dos dados desde a conceção** e **proteção dos dados por defeito.**

A especificidade **Camada de Serviço** respondeu a 2 requisitos, sendo eles: **acesso direto dos titulares dos dados** e **interoperabilidade dos formatos e sistemas**

A especificidade **Audit Trail** respondeu a 4 requisitos, sendo eles: **integridade e confidencialidade, confirmação do tratamento de dados pessoais, registo das atividades de tratamento dos dados pessoais e disponibilização dos registos de tratamento dos dados pessoais.**

A especificidade **Modelação Multinível** respondeu a 4 requisitos, sendo eles: **acesso dos titulares dos dados aos dados pessoais, portabilidade dos dados pessoais dos titulares dos dados, portabilidade dos dados pessoais entre responsáveis pelo tratamento, interoperabilidade dos formatos e sistemas** e **transferência de dados pessoais para países terceiros ou organizações internacionais**

Tabela 1- correspondência entre openEHR e requisitos de SIS

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento e indelebilidade	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
PRINTRAT1- **Limitação do tratamento de dados**								
PRINTRAT2- **Minimização dos dados pessoais**					✓			
PRINTRAT3- **Exatidão dos dados pessoais**								
PRINTRAT4- **Prazos para limitação da conservação dos dados pessoais**								
PRINTRAT5- **Limitação da conservação dos dados pessoais**					✓			
PRINTRAT6- **Integridade e confidencialidade**	✓	✓	✓	✓			✓	
PRINTRAT7- **Responsabilidade**								
PRINTRAT8- **Demonstração de responsabilidade**								

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
CONSENT1- **Consentimento Explícito**								
CONSENT2- **Consentimento explícito dos titulares dos dados**								
CONSENT3- **Registo do consentimento explícito**								
CONSENT4- **Capacidade do titular dos dados retirar consentimento**								
CONSENT5- **Características do consentimento obtido**								
CONSENT6- **Licitude do tratamento após retirar consentimento**								
INTLEG1- **Interesse legítimo do tratamento**								
INTLEG2- **Informação acerca do interesse legítimo**								
INTLEG3- **Objeção dos titulares dos dados ao Interesse legítimo**								

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
COMINF1- **Comunicação e informações fornecidas aos titulares**								
COMINF2- **Meios para a prestação de informações aos titulares dos dados**								
COMINF3- **Verificação da identidade dos titulares dos dados**					✓			
COMINF4- **Prazo para resposta ao pedido dos titulares dos dados**								
COMINF5- **Formato da resposta ao pedido de informação do titular dos dados**								
COMINF6- **Preservação dos registos de notificações de informação**								

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
INFTIT1- **Notificações de informação**								
INFTIT2- **Momento da notificação de informação (dados pessoais obtidos diretamente)**								
INFTIT3- **Período de notificação de informação ao titular dos dados**								
INFTIT4**- Notificação ao titular dos dados de novo tratamentos**								

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
ACESS1- **Acesso dos titulares dos dados aos dados pessoais**	✓	✓						✓
ACESS2- **Formulário de resposta ao pedido de acesso dos titulares dos dados**								
ACESS3- **Confirmação do tratamento dos dados pessoais**				✓			✓	
ACESS4- **Informações que titular dos dados tem direito a aceder**								
ACESS5-**Resposta ao pedido de acesso do titular dos dados**								
ACESS6- **Acesso direto do titular dos dados**	✓	✓				✓		
RET1- **Retificação dos dados pessoais por parte 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**						✓		✓

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
OBJ1- **Objeção ao tratamento dos dados pessoais por parte do titular dos dados**								
APAG1- **Apagamento dos dados pessoais a pedido do titular dos dados**								
APAG2- **Comunicação com outros responsáveis pelo tratamento dos dados ou subcontratantes**								
LIMIT1- **Limitação do tratamento dos dados pessoais a pedido do titular dos dados**								
LIMIT2- **Limitação do tratamento**								
LIMIT3- **Notificação da anulação da limitação do tratamento dos dados pessoais**								

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento e in-delebilidade	Separação informa-ção clínica e demo-gráfica	Camada de Serviços	Audit Trailing	Modelação Multinível
PROT1- **Proteção de dados pessoais desde a conceção**					✓			
PROT2- **Proteção de dados por defeito**	✓	✓	✓		✓			
PROT3- **Registo de políticas de proteção de dados pessoais**								
REG1- Registo das atividades do tratamento de dados pessoais							✓	
REG2- **Formato dos registos de tratamento de dados pessoais**								
REG3- **Disponibilização dos registos de tratamento dos dados pessoais**							✓	

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso às definições de acesso	controlo versões - assinatura digital	controlo de versões- versionamento	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
DPIA1- **Preservação de registos de DPIA**								
DPIA2- **Consulta de DPIA**								
DPIA3- **Inclusão do parecer do DPO**								
DPO1- **Envolvimento do DPO na proteção de dados**								
CODCON1- **Conformidade com código de conduta**								
CERT1- **Conformidade com processos de certificação**								

openEHR / RGPD	Controlo de Acesso - lista de acesso	controlo de Acesso - controlo de acesso sob a lista acesso	controlo versões - assinatura digital	controlo de versões- versionamento	Separação informação clínica e demográfica	Camada de Serviços	Audit Trailing	Modelação Multinível
TRANSF1- **Transferências de dados para países terceiros ou organizações internacionais**								✓
TRANSF2- **Garantias das transferências de dados pessoais**								
Total de correspondências	4	4	2	2	5	2	4	5

5. Discussão

O objetivo primordial do trabalho desenvolvido passa por perceber se as especificações openEHR permitem o desenvolvimento de um SIS em conformidade com o RGPD.

Os resultados obtidos demonstram que todas as especificações do openEHR reconhecidas correspondem pelo menos a um requisito identificado na lista elaborada.

Como referido na descrição das especificações openEHR, a elaboração de uma **lista de controlo de acesso** permite identificar os utilizadores, e respetivas categorias, cujo acesso ao RES é considerado pertinente e, consequentemente, justificado e legítimo. Esta especificação responde aos seguintes requisitos:

- Integridade e confidencialidade - a lista de controlo de acesso é uma medida que garante a segurança do tratamento de dados, uma vez que limita a possibilidade de ocorrer um tratamento não autorizado ou ilícito (através da definição prévia de quem tem autorização para aceder aos dados). Esta medida garante que os dados mantêm um carácter confidencial e integro.
- Acesso dos titulares dos dados aos dados pessoais – o requisito determina que o sistema deve providenciar uma cópia ao titular dos dados quando requerida. 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 lisa de controlo, não é permitido o acesso e o posterior fornecimento da cópia.
- Acesso direto dos titulares dos dados – este requisito promove a capacidade do sistema fornecer um sistema seguro para o acesso do titular dos dados aos respetivos dados pessoais. Pelo mesmo princípio do requisito anterior, 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 os 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 sobre os mesmos.

O **controlo de acesso às configurações** da lista de controlo acesso permite que um *gate keeper* (por norma o próprio paciente) defina que agentes podem efetuar alterações à lista de controlo de acesso, sendo uma especificação complementar à mesma. O papel do *gate keeper* passa por ser o "dono" do RES. Esta especificação responde aos seguintes requisitos:

- Integridade e confidencialidade - esta especificação constitui uma outra medida de segurança do tratamento de dados, permitindo que seja determinado o indivíduo que pode modificar as configurações do controlo de acesso. Desta forma, acrescenta-se uma camada de segurança à lista de controlo de acesso já existente, contribuindo para que os acessos aos dados sejam legítimos e justificados, garantindo a integridade do tratamento e dos dados pessoais.
- Acesso dos titulares dos dados aos respetivos dados pessoais - esta especificação permite que seja providenciada uma cópia dos dados pessoais ao titular dos dados na medida em que, para o pedido se concretizar, é necessário que seja permitido o acesso aos dados pessoais por parte de quem controla a lista de controlo de acesso (*gate keeper*).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 – o acesso direto dos titulares dos dados pode apenas ser feito em relação a dados pessoais que pertençam ao titular dos dados. 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.

O titular dos dados só pode aceder aos dados pessoais caso estes lhe pertençam.

- Proteção de 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, ou seja, o controlo das configurações de acesso permite assegurar, em todos os momentos, a integridade do tratamento dos dados em relação a quem lhes acede.

A possibilidade das versões criadas conterem uma **assinatura digital** aufere uma caraterística importante de integridade e veracidade da informação. A assinatura digital é um método de autenticação da informação que permite o não-repúdio dos dados digitais, neste caso, que assegura a integridade dos RES. A possibilidade da assinatura digital incluir um selo temporal permite registar a data e hora em que foi assinalado um evento num SI. No caso do sistema openEHR, é registada a data e hora em que foi efetuada uma ação num RES. Esta especificação 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 de 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,** nomeadamente o versionamento dos RES, assegura ao SIS uma característica de indelebilidade, garantindo que nenhuma informação no RES é apagada. Quando são realizadas alterações aos RES, essas são materializadas numa nova versão, sendo que nenhuma informação ou dado do registo alterado é verdadeiramente apagado. Esta funcionalidade responde aos seguintes requisitos:

- Integridade e confidencialidade – esta especificação assegura a integridade dos dados e a segurança do tratamento. A indelebilidade dos RES como parte integrante das funcionalidades do SIS, 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 – este requisito impõe que que o sistema tenha a capacidade de confirmar se dados pessoais são ou não objeto de tratamento. Através do versionamento dos registos, é possível perceber que ações foram realizadas ao RES. Uma vez que todas as ações requeridas são implementadas em novas versões, com informações associadas à identificação do utilizador, data e hora e razão do procedimento para a alteração do registo, é possível perceber se foi efetuado algum tipo de tratamento nos dados pessoais, possibilitando a confirmação de tratamento para com os titulares dos dados.

A **separação do RES da informação demográfica** é uma forte garantia de segurança e privacidade dos dados pessoais. Com a separação da informação clínica da informação identificável do indivíduo, e consequente armazenamento em diferentes repositórios, o anonimato do titular dos dados é assegurado. Esta funcionalidade responde aos seguintes requisitos:

- Minimização dos dados - a separação da informação clínica e demográfica 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). Esta especificação garante a pertinência e adequação dos dados pessoais dos titulares dos dados.
- Limitação da conservação dos dados pessoais – este requisito é garantido pela separação da informação clínica e demográfica na medida em que 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, permitindo identificação dos titulares dos dados apenas durante o período necessário para a finalidade do tratamento.

- Verificação da identidade do titular dos dados – o requisito indicado solicita que o SIS tenha a capacidade de comprovar a identidade do titular dos dados. A separação dos dados clínicos dos dados demográficos garante a separação da informação identificável dos dados do RES. No entanto, 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 a identidade do titular dos dados face à informação clínica, ao titular dos dados é associado um identificador que o liga ao RES.
- Proteção dos dados desde a conceção – como resposta à capacidade de pseudonimização e medidas de minimização dos dados pessoais, a separação da informação clínica da informação demográfica 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. No decorrer da prestação de cuidados, apenas os dados do RES são considerados.
- Proteção de dados por defeito, a separação da informação clínica da demográfica garante que, no momento da prestação de cuidados, apenas sejam consideradas os dados pessoais de saúde, salvaguardando a informação demográfica.

A **camada de serviços** permite definir o interface gráfico que possibilita a consulta dos dados do RES. As vistas criadas e respetivas funcionalidades, são definidas por este modelo. Esta especificação responde aos seguintes requisitos:

- Acesso direto do titular dos dados aos dados pessoais – a necessidade de ser providenciado um sistema seguro para que o titular dos dados possa aceder aos seus dados pessoais é solucionada pela possibilidade da camada de serviços, através do Virtual EHR API e do EHR Service, criarem uma vista que permite a consulta dos dados. Desta forma, o titular dos dados pode, com segurança, aceder e consultar ao seu RES.

- Interoperabilidade dos formatos e sistemas - a definição da camada de serviço permite que se criem diferentes interfaces gráficos, 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. Desta forma a interoperabilidade é garantida, pois o interface dos diferentes sistemas suportam a mesma estrutura do RES.

A especificação **Audit Trail** assegura que todas as alterações ou ações realizadas no RES são registadas para auditoria. Responde aos seguintes requisitos:

- Integridade de confidencialidade - o audit trail funciona como medida importante de segurança e proteção dos dados e respetivo tratamento. Garantindo o registo de dados importantes como os logs de acesso, as identidades dos utilizadores e o tempo e duração da ação. Desta forma, garante-se não só a integridade do tratamento, mas também, em caso de violação de dados, a possibilidade de perceber que dados foram danificados, que acesso foram injustificados, que tratamentos não autorizados foram efetuados.
- Confirmação do tratamento de dados pessoais – para ser possível confirmar ao titular dos dados se os seus dados pessoais são ou não alvo de tratamento, é necessário que exista um registo de todas as atividades realizadas em relação aos dados do RES. 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 –a capacidade do SIS manter um registo de todas as atividades de tratamento dos dados pessoais torna-se possível com o audit trail, que regista todas as informações relacionadas com ações executadas no RES.
- Disponibilização dos registos de tratamento dos dados pessoais – o audit trail, ao permitir a rastreabilidade das ações relativas aos RES, permite a criação de um registo relativo ao tratamento dos dados passível de ser disponibilizado à autoridade de controlo, caso seja requerido ou em caso de auditoria.

- Registo das violações de dados pessoais – pelo mesmo princípio, o audit trail 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** constitui uma especificação básica do openEHR, definindo toda a sua arquitetura. Através da separação do modelo de referência do modelo de conteúdo, o openEHR garante a interoperabilidade semântica dos dados, tornando-os independentes da tecnologia e software. Responde aos seguintes requisitos:

- Acesso do titular dos dados aos dados pessoais – este requisito permite que seja providenciado ao titular dos dados uma cópia dos dados pessoais que são alvos de tratamento. A Modelação Multinível, no que tange a modelação de arquétipos, permite que estes, pelas suas características, sejam exportados. Desta forma, esta especificação permite que os dados 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. O facto de os dados serem separados do software desenvolvido aufere-lhes uma plasticidade importante para garantir a sua portabilidade sem que ocorra perda de conteúdo e sem ter haver preocupações relativas ao software de onde foram extraídos. Os mesmos dados são lidos da mesma forma em diferentes sistemas e softwares.
- Portabilidade dos dados pessoais entre responsáveis pelo tratamento - a Modelação Multinível garante a portabilidade dos dados da mesma forma que foi mencionado no requisito anterior. Utilizando a arquitetura openEHR, os dados mantêm o sue conteúdo semântico e o seu significado independentemente do software que os suporta. Desta forma, qualquer sistema desenvolvido utilizando a arquitetura openEHR, mesmo pertencendo a diferentes fornecedores, consegue suportar os mesmos dados (modelados na forma de arquétipos e templates). Dessa forma, a transmissão de dados pessoais para outros responsáveis pelo tratamento fica garantida, assegurando-se a portabilidade e a segurança dos dados.
- Interoperabilidade dos formatos e sistemas - a Modelação Multinível, baseada na modelação do modelo de referência e modelação dos arquétipos e

templates separadamente, garante a interoperabilidade dos 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 através da modelação a dois níveis do modelo de referência e dos arquétipos e templates.

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.

Outros requisitos requeridos para um SIS em conformidade com o RGPD, que envolvem a definição de novos formulários de notificação (para titulares dos dados e autoridades reguladoras), criação de meios de comunicação para registos e preservações de Avaliações de Impacto na Proteção de Dados e registos de conformidade com códigos de conduta e certificações existentes não são respondidos pela implementação da norma openEHR, tratando-se de requisitos que devem ser abordados do ponto de vista organizacional, quer através de reformas dos processos existentes, quer através da definição de novos processos.

Contudo, apesar de não oferecer resposta a certos requisitos de uma forma direta, as especificações openEHR assumem-se como ferramenta importante para o cumprimento desses requisitos. O controlo de versões e o audit trail permitem alimentar o registo de

informações relacionadas com o tratamento dos dados e possíveis violações de dados. Apesar do openEHR não permitir a criação de documentação de registos de tratamento de dados pessoais e registos de violações de dados pessoais, essa documentação é suportada pelas especificações mencionadas que, pelas suas características, permitem a rastreabilidade quer dos dados, quer das ações e agentes a eles associados.

Em relação aos requisitos associados ao consentimento explícito para o tratamento de dados pessoais, as especificações do openEHR, apesar de não possibilitarem uma correspondência direta, facilitam a sua realização. Apesar de ser mandatório que os SIS garantam uma forma de obter, registar e retirar o consentimento explícito dos titulares dos dados, e considerando que as especificações identificadas não garantem estas funcionalidade, o openEHR facilita a realização destas tarefas. O controlo de versões e o audit trail permitem ao SIS registar e verificar qualquer ação e acesso que tenha sido feito aos dados do RES. Sabendo o prazo limite para o tratamento dos dados pessoais, com base no consentimento dos titulares dos dados, é possível a instituição de saúde identificar se estão a ser realizados tratamentos em dados pessoais sem o consentimento dos respetivos titulares.

Desta forma, apesar das funcionalidades openEHR não permitirem que estes requisitos sejam cumpridos diretamente, apresenta-se como apoio importante em relação aos processos que a instituição tem de implementar.

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 que são 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.

6. Conclusão

Considerando a multidisciplinaridade dos sistemas na área da saúde e a necessidade das soluções tecnológicas serem desenvolvidas tendo em conta as implicações do RGPD, o trabalho desenvolvido e os respetivos resultados são de máxima relevância.

No que refere a reforma dos SIS, o openEHR é considerado uma forte solução. Como conjunto de especificações para sistemas de RES, o openEHR permite responder a necessidades funcionais centradas na privacidade e segurança dos dados pessoais de saúde, apresentando-se também como forte solução para a portabilidade dos dados e para a proteção de dados desde a conceção e por defeito, que passam a ser requeridas pelo RGPD.

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.

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.

Limitações do trabalho desenvolvido

O caso de estudo desenvolvido apresentou algumas limitações:

- Como já referido, 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.
- A ausência de trabalhos realizados no âmbito da implementação do RGPD constitui também uma limitação. Uma vez que as organizações ainda se encontram em processo de reestruturação, face à obrigatoriedade de conformidade com o RGPD a partir de Maio de 2018, pouca literatura se encontra disponível acerca da implementação do RGPD *per si*, existindo um maior foco na sua interpretação, compreensão e visão geral.
- No seguimento desta ausência de literatura face à implementação do RGPD nos processos organizacionais, 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.
- A ausência, em particular, de literatura onde fosse efetuada algum tipo de relação entre o openEHR e o RGPD, o que diminuiu a hipótese de efetuar comparações face a resultados já obtidos ou seguir propostas já feitas. Até à data, na base de dados PUBMED, nenhum resultado é recuperado face à pesquisa “openehr AND general data protection regulation”.

As limitações indicadas apontam essencialmente para a falta de projetos e de estudos de caso com o objetivo de apresentar uma solução para os SIS serem desenvolvidos em conformidade com o RGPD.

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.

7. Referências

Agência dos Direitos Fundamentais da União Europeia, e Conselho da Europa. 2014. *Manual Da Legislação Europeia Sobre Proteção de Dados*. Luxemburgo: Serviço das Publicações da União Europeia. Acedido a 29 de junho de 2017 em http://www.infoeuropa.eurocid.pt/registo/000066668/

Assembleia Geral das Nações Unidas. 1948. "Declaração Universal Dos Direitos Humanos." *Onu*, 1–7. Acedido a 29 de junho de 2017 em http://www.un.org/en/universal-declaration-human-rights/

Assembleia da República. 2005. "Lei Nº 12/2005, de 26 de Janeiro." *Diário Da Republica*, no. 18: 606–611. Acedido a junho de 2017 http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2591&tabela=leis&ficha=1&pagina=1&so_miolo=.

Associação Médica Mundial, 1983 "Juramento de Hipócrates". Acedido a 29 de J junho de 2017 em https://www.ordemdosmedicos.pt/?lop=conteudo&op=217eedd1ba8c592db97d0dbe54c7adfc&id=6b8b8e3bd6ad94b985c1b1f1b7a94cb2

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 29 de junho de 2017 em http://ieeexplore.ieee.org/document/6627881/

Bacelar, Gustavo, e Ricardo Correia. 2015. "As Bases Do openEHR," 1ª ed. Porto: Virtual Care. Acedido a 29 de junho de 2017 em https://www.researchgate.net/publication/282869250_As_Bases_do_openEHR

Beale, Thomas, e Sam Heard. 2007. "openEHR - Architecture Overview." *The OpenEHR Foundation*. Acedido a 29 de junho de 2017 em http://www.openehr.org/releases/1.0.2/architecture/overview.pdf.

Ben-Assuli, Ofir. 2015. "Electronic Health Records, Adoption, Quality of Care, Legal and Privacy Issues and Their Implementation in Emergency Departments." *Health Policy* 119 (3). Elsevier Ireland Ltd: 287–97. Acedido a 29 de junho de 2017 em https://www.ncbi.nlm.nih.gov/pubmed/25483873

Boardman, Ruth, James Mullock, e Ariane Mole. 2017. “Guide to the General Data Protection Regulation,” no. January: 66. Acedido a 29 de junho de 2017 em https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en.

Comissão Europeia. 2000. “The Charter of Fundamental Rights of the European Union.” *Official Journal of the European Communities* C (364): 1–22. Acedido a 29 de junho de 2017 em http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Comissão Europeia. 2010. “Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union.” *COM (2010) 609 Final*, 1–20. Acedido a 29 de junho de 2017 em http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

Comissão Europeia. 2012. “Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century.” *COM (2012) 9 Final*, 1-14. Acedido a 29 de junho de 2017 em http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52012DC0009

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 29 de junho de 2017 em http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52012PC0011

Conselho da Europa. n.d. “Convenção Europeia dos Direitos Do Homem.” Estrasburgo. Acedido a 29 de junho de 2017 em http://www.echr.coe.int/pages/home.aspx?p=basictexts

Conselho da Europa. 1981. “Convention for the Protection of Individuals with regard to automatic processing of personal data" *European Treaty Series*, no. 108: 14. Acedido e 29 de junho de 2017 em http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Correa, Danielle. 2016 “82% of global and IT business pros are concerned about GDPRm compliance”. Acedido a 29 de junho de 2017 em https://www.scmagazineuk.com/82-of-global-and-it-business-pros-are-concerned-about-gdpr-compliance/article/547663/.

Coutinho, Clara. 2002. “O Estudo de Caso Na Investigação Em Tecnologia Educativa Em Portugal.” *Revista Portuguesa de Educação* 15 (1): 221–43. Acedido a 29 de junho de 2017 em http://repositorium.sdum.uminho.pt/handle/1822/492

Donaldson, Molla S e Kathleen N Lohr. 1994. *Health Data in the Information Age*. EUA: National Academy of Science.

Faria, Paula Lobato De, e João Valente Cordeiro. 2014. "Health Data Privacy and Confidentiality Rights: Crisis or Redemption?" *Revista Portuguesa de Saude Publica* 32 (2). Escola Nacional de Saúde Pública: 123–33. Acedido a 29 de junho de 2017 em http://www.sciencedirect.com/science/article/pii/S0870902514000352?via%3Dihub

Gaudino, Francesca Rubina. 2010. "Healthcare ICT and Personal Data Protection : The Applicable Legal Framework.". Apresentada em Applied Sciences in Biomedical and communication Technologies, Roma, Itália, 7 a 10 de novembro de 2010. Acedido a 29 de junho de 2017 em http://ieeexplore.ieee.org/document/5702824/?section=abstract

Goldstein, Melissa M. 2014. "Health Information Privacy and Health Information Technology in the Us Correctional Setting." *American Journal of Public Health* 104 (5): 803–9. Acedido a 29 de junho de 2017 em https://www.ncbi.nlm.nih.gov/pubmed/24625160.

Haux, Reinhold. 2006. "Health Information Systems - Past, Present, Future." *International Journal of Medical Informatics* 75 (3–4): 268–81. Acedido a 29 de junho de 2017 em http://www.sciencedirect.com/science/article/pii/S1386505605001590.

Horvitz, Eric, e Deirdre Mulligan. 2015. "Data, privacy, and the greater good". *Science* 349 (6245): 253–56. Acedido a 29 de junho de 2017 em http://science.sciencemag.org/content/349/6245/253

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

IEEE (The Institute of Electrical and Electronics Engineers). 1998. *IEE Guide for developing System Requirements Specifications*. Acedido a 29 de junho de 2017 em https://sites.google.com/a/mix.wvu.edu/csee480/ieee-std--1233---requirements-specification-1.

Leslie, Heather. 2008. "International Developments in openEHR Archetypes and Templates." *Health Information Management Journal* 37 (1): 38–39. Acedido a 29 de junho de 2017 em https://www.ncbi.nlm.nih.gov/pubmed/18245863.

Leslie, Heather, e Sam Heard. 2006. "Archetypes 101." *HIC 2006 and HINZ 2006 Proceedings*, no. JANUARY 2006: 1–6. Acedido a 29 de junho de 2017 em

https://www.researchgate.net/publication/228702894_Archetypes_101

Meirinhos, Manuel, e António Osório. 2010. “O Estudo de Caso Como Estratégia de Investigação Em Educação.” *EDUSER: Revista de Educação* 2 (2): 49–65. Acedido a 29 de junho de 2017 em https://bibliotecadigital.ipb.pt/bitstream/10198/3961/1/O%20estudo%20de%20caso%20como%20estrat%C3%A9gia%20de%20investiga%C3%A7%C3%A3o%20em%20educa%C3%A7%C3%A3o.pdf

Ministério Público. 1995. DL n.º 48/95, de 15 de Março. *Código Penal*. Lisboa: Procuradoria Geral Distrital de Lisboa. Acedido a 29 de junho de 2017 em http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?ficha=201&artigo_id=&nid=109&pagina=3&tabela=leis&nversao=&so_miolo=

Mountford, N, T Kessie, M Quinlan, R Maher, R Smolders, P Van Royen, I Todorovic, H Belani, H Horak, I Ljubi, J Stage, D Lamas, I Shmorgun, M Perala-Heape, M Isomursu, V Managematin, V Trajkovik, A Madevska-Bogdanova, R Stainov, I Chouvarda, G Dimtrakopoulos, A Stulmanyhaddad, R Alzbutas, N Calleja; M Tilney; A Moen; E. Thygesen; R. Lewandowski; M. Klichowski; P. Oliveira; J. Machado da Silva; T. Loncar Turukalo; B Marovic, K Drusany Staric, B. Cvetkovic, E. Luque, L. Fernandez Luque, S. Burmaoglu, N. Dolu, V Curcin, J. Mclaughlin, B. Caulfield. 2016. *Connected Health in Europe : Where Are We Today ?* Dublin: Univesity College Dublin. Acedido a 29 de junho de 2017 em http://enject.eu/wp-content/uploads/2016/12/Report-Final.pdf

Nass, S. J., e O.Lawrence Levit, L. A. Gostin. 2009. *The Value, Importance, and Oversight of Health Research*. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*. Acedido a 29 de junho de 2017 em http://www.ncbi.nlm.nih.gov/books/NBK9571/ accessed 01/08/2016.

Odoemenam, Joseph Chimezie. 2011. *"Eletronic Health Record"*. Acedido a 29 de junho de 2017 em http://emrguy.com/electronic-health-record/

Parlamento Europeu. 1995. "Diretiva 95/46/CE do Parlamento Europeu e do Conselho de 24 de Outubro de 1995 relativa à proteção das pessoas singulares noque diz respeito ao tratametno de dados pessoais e à livre circulação desses dados". *Jornal Oficial das Comunidades Europeias* 31-50. Luxemburgo Acedido a 29 de junho de 2017 em http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A31995L0046

Parlamento Europeu. 2016. "Regulamento 2016/679 de 27 de Abril de 2016 relativo à proteção 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 29 de junho de 2017 em http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

Patil, Harsh Kupwade, e Ravi Seshadri. 2014. "Big Data Security and Privacy Issues in Healthcare" Apresentada em IEEE International Congress on Big Data, Anchorage, EUA, 27 junho a 2 de julho de 2014. Acedido a 29 de junho de 2017 em http://ieeexplore.ieee.org/document/6906856/

Rindfleisch, Thomas C. 1997. "Privacy, Information Technology, and Health Care". *Communications of the ACM* 40 (8): 93-100. Acedido a 29 de junho de 2017 em http://dl.acm.org/citation.cfm?id=257896

Rudgard, Sian.2012. " Origins and Historical Context of Data Protection Law". em *European Privacy.* 3-17. Portsmouth:International Association of Privacy Professionals

SBIS (Sociedade Brasileira de Informática em Saúde). 2016. *Manual de certificação para sistemas de Registro Eletrônico em Saúde*. Acedido a 29 de junho de 2017 em http://www.sbis.org.br/certificacao/Manual_Certificacao_SBIS-CFM_2016_v4-2.pdf

Serviços Partilhados do Ministério de Saúde. nd. "Privacidade Da Informação No Setor Da Saúde Privacidade Da Informação No Setor Da Saúde."

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

Sociedade Europeia de Radiologia. 2017. "The New EU General Data Protection Regulation : What the Radiologist Should Know.". *Insights into Imaging* (8): 295-299 Acedido a 29 de junho de 2017 em https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5438318/

Silva, Almerinda Maria Ferreira da. 2007. "O Direito À Privacidade Do Doente No Serviço de Urgência" Tese de Mestrado, Faculdade de Medicina, Universidade do Porto. Acedido a 29 de junho de 2017 em https://repositorio-aberto.up.pt/bitstream/10216/22110/3/tese%202.pdf.

Swire, Peter P e Kenesa Ahmad.2012. *Foundations of Information Privacy and Data Protection.* Portsmouth: International Association of Privacy Professionals

The Breach Level Index. 2016. “Mining for Database Gold.” Acedido a 29 de junho de 2017 em http://www.breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf.

Virone, Maria Gabriella. 2012. “EHR and Data Protection Issues in Italy,” 180: 741–745. Acedido a 29 de junho de 2017 em https://www.ncbi.nlm.nih.gov/pubmed/22874290

Walker, Daniel M., Tyler Johnson, Eric W. Ford, e Timothy R. Huerta. 2017. “Trust Me, I’m a Doctor: Examining Changes in How Privacy Concerns Affect Patient Withholding Behavior.” *Journal of Medical Internet Research* 19 (1).Acedido a 29 de junho de 2017 em https://www.jmir.org/2017/1/e2/.

Wilkowska, W., e M. Ziefle. 2012. “Privacy and Data Security in E-Health: Requirements from the User’s Perspective.” *Health Informatics Journal* 18 (3): 191–201. Acedido a 29 de junho de 2017 em https://www.ncbi.nlm.nih.gov/pubmed/23011814.

Yamamoto, R. 2016. “Large-Scale Health Information Database and Privacy Protection.” *Japan Medical Association Journal* 59 (2–3): 91–109. Acedido a 29 de junho de 201 em https://www.scopus.com/inward/record.uri?eid=2-s2.0-85013421213&partnerID=40&md5=c88c927d6c1951bbf7176acc1a77fb93.

Anexos A – Levantamento de Requisitos de um SIS em conformidade com o RGPD

A seguinte lista descreve os objetivos gerais de um Sistema de Informação de Saúde para que este se encontre em conformidade com o RGPD:

Objetivos do sistema

OSS1 – Deve permitir recolher e registar o consentimento explícito do titular dos dados no momento da recolha de dados pessoais, permitindo demonstrar o consentimento explícito, proveniente de uma manifestação de vontade livre, específica, informada e inequívoca, mediante uma declaração escrita ou oral por parte do titular dos dados.

OSS2 – Deve ajudar a que o tratamento dos dados pessoais respeite os princípios do tratamento dos dados impostos pelo RGPD, permitindo uma recolha, processamento e armazenamento dos dados pessoais transparente, lícita e leal.

OSS3 – Deve garantir a proteção e a privacidade dos dados pessoais, através de medidas técnicas e organizativas a ser aplicadas desde a conceção dos sistemas de informação e por defeito, tais como a minimização do tratamento dos dados e a pseudonimização dos dados.

OSS4 – Deve permitir estabelecer medidas adequadas e específicas que garantam os direitos dos titulares dos dados:

- → medidas para permitir e facilitar procedimentos de solicitação de acesso aos dados pessoais;

→ medidas para conceder acesso aos dados pessoais por parte do titular dos dados;

→ medidas para permitir retificação e/ou apagamento de dados pessoais;

→ informando responsáveis que estejam a tratar os dados pessoais que titulares solicitaram a supressão de quaisquer ligações para esses dados pessoais ou cópias e reprodução das mesmas (informar do pedido dos titulares dos dados).

OSS5 – Deve ser dotado de meios que comprovem a conformidade com o RGPD e respetiva responsabilidade como responsáveis pelo tratamento, através de códigos de conduta e procedimentos de certificação.

OSS6 – Deve permitir limitações de acesso aos dados pessoais, assegurando que estes não são acedidos ou disponibilizados por indivíduos não autorizados.

OSS7 – Deve conservar os registos de todas as categorias de atividades de tratamento de dados realizadas pelos responsáveis pelo tratamento, mantendo o registo das finalidades do tratamento de dados pessoais e todas as informações associadas.

OSS8– Deve assegurar a proteção dos dados pessoais em qualquer tipo de tratamento efetuado aos dados pessoais.

OSS9 – Deve permitir a aplicação de medidas pertinentes que permitam assegurar um nível de segurança adequado ao risco associado ao tratamento de dados, incluindo a capacidade de assegurar confidencialidade, integridade, disponibilidade e resiliência dos sistemas e serviços.

Requisitos para uma arquitetura de um sistema de informação de saúde em conformidade com o Regulamento Geral de Proteção de Dados

1 - Requisitos para cumprimento dos Princípios do tratamento de dados

1.1 - Princípio do tratamento dos dados pessoais (artigo 5º)

A tabela seguinte descreve os requisitos identificados para serem cumpridos os princípios dos dados pessoais:

ID	Objetivo	Requisito	Prioridade de implementação
PRINTRAT1	Limitação do tratamento de dados pessoais	Devem ser definidos os propósitos específicos, explícitos e legítimos para a recolha de dados pessoais, sendo que o tratamento deve limitar-se à finalidade definida.	M
PRINTRAT2	Minimização dos dados pessoais	Dados pessoais devem ser adequados, pertinentes e limitados ao necessário para atingir a finalidade para o qual são tratados	M
PRINTRAT3	Exatidão dos dados pessoais	SI deve permitir atualizar os dados pessoais sempre que necessário e deve permitir que dados inexatos, considerando as finalidades do tratamento, sejam apagados ou retificados.	M
PRINTRAT4	Prazos para limitação da conservação	Devem ser definidos prazos/períodos para tratamento dos dados pessoais, considerando a finalidade do tratamento.	M
PRINTRAT5	Limitação da conservação	Deve ter a capacidade de conservar dados pessoais de forma a que seja permitida a identificação dos titulares dos dados apenas durante o período necessário para a finalidade.	M
PRINTRAT6	Integridade e confidencialidade	SI deve permitir a adoção de medidas técnicas ou organizativas que garantam a segurança do tratamento dos dados pessoais, nomeadamente proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danificação acidental dos dados pessoais.	M
PRINTRAT7	Responsabilidade	SI deve identificar entidade responsável pela recolha/tratamento dos dados pessoais.	M
PRINTRAT8	Demonstração de responsabilidade	SI deve ter a capacidade de demonstrar conformidade com: a. códigos de conduta existentes;	R

		b. procedimentos de certificação aprovados, de maneira a mostrar conformidade com princípios do tratamento de dados.	

1.2 - Consentimento explícito (artigo 7º)

A tabela seguinte descreve os requisitos identificados para a obtenção e validação do consentimento explícito:

ID	Objetivo	Requisito	Prioridade de implementação
CONSENT1	Consentimento Explícito	Deve ter capacidade de representar e demonstrar consentimento explícito do titular dos dados para a recolha dos dados pessoais, bem como para as finalidades de tratamento.	M
CONSENT2	Consentimento explícito do titular dos dados	Consentimento do titular dos dados deve ser obtido através de uma declaração escrita e deve ser: a) Inteligível, informado e inequívoco, redigido numa língua compreensível ao titular dos dados; b) Declaração do consentimento explícito deve especificar natureza da categoria dos dados, detalhes das decisões automatizadas e seus efeitos, ou detalhes dos dados a ser transferidos e riscos de transferência. c) Se dados pessoais forem recolhidos e tratados para diferentes finalidades, SI deve ter a capacidade de obter e registar consentimento explícito relativo às diferentes finalidades do tratamento de dados pessoais.	M
CONSENT3	Registo do consentimento	O pedido de consentimento deve ser apresentado e registado de uma forma que o distinga de outros assuntos e de modo inteligível e de fácil acesso, numa linguagem clara e simples.	M
CONSENT4	Capacidade de titular dos dados retirar consentimento	Deve garantir ao titular dos dados a capacidade de retirar o consentimento (permitir opt –out), de forma fácil e clara, da mesma forma ou formato que consentimento foi obtido. Consentimento deve ser tão fácil de retirar quanto de dar.	M
CONSENT5	Características do consentimento obtido	SI deve garantir que consentimento: a) é ativo, não obtido através de silêncio, inatividade ou caixas pré-marcadas, b) Expressamente e deliberadamente confirmado em palavras.	M
CONSENT6	Licitude do tratamento após retirar consentimento.	SI deve ter a capacidade de garantir que a retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento dado previamente.	R

1.3 - Interesse legítimo (artigo 6º)

A tabela seguinte descreve os requisitos identificados para a garantia do interesse legítimo do tratamento dos dados:

ID	Objetivo	Requisito	Prioridade de implementação
INTLEG1	Interesse legítimo do tratamento	SI deve manter registo da avaliação feita pelos responsáveis pelos dados em relação ao interesse legítimo e fundamentação legal para recolha e tratamento de dados, de forma a poder ser demonstrado que foram considerados os direitos e liberdades dos titulares.	M
INTLEG2	Informação acerca do interesse legítimo	SI deve ter capacidade de fornecer ao titular dos dados informação de onde é apontado o interesse legítimo que permite o tratamento.	M
INTLEG3	Objeção dos titulares dos dados ao interesse legítimo	Deve ter a capacidade de responder ao pedido dos titulares dos dados de objetar ao tratamento dos dados com base no interesse legítimo dos responsáveis pelo tratamento.	M

2 - Requisitos para o cumprimento dos direitos dos titulares

2.1 - Transparência das informações, das comunicações e das regras para exercícios dos direitos dos titulares doa dados (artigo 12º)

A tabela seguinte descreve os requisitos identificados para o cumprimento da transparência das informações e das comunicações a fornecer aos titulares dos dados e das regras para exercícios dos direitos dos titulares dos dados:

ID	Objetivo	Requisito	Prioridade de implementação
COMINF1	Comunicação e informação fornecida aos titulares dos dados	Deve ter a capacidade de fornecer ao titular dos dados qualquer informação específica relativa ao tratamento dos dados pessoais, de forma: a. concisa; b. transparente; c. de fácil acesso; d. escrita em linguagem simples e clara;	M
COMINF2	Meios para a prestação de informações aos titulares dos dados	Deve ter a capacidade de prestar informações por escrito ou por outros meios, incluindo meios eletrónicos.	M

COMINF3	Verificação da identidade dos titulares dos dados.	Deve ter a capacidade de comprovar a identidade do titular dos dados.	M
COMINF4	Prazo para resposta ao pedido do titular dos dados	Após receção do pedido do titular dos dados, deve ter a capacidade de fornecer ao titular dos dados informações sobre medidas tomadas no prazo de um mês.	M
COMINF5	Formato da resposta ao pedido de informação do titular dos dados	Deve ter a capacidade de fornecer a informação pelo mesmo meio que o titular dos dados fez o pedido.	M
COMINF6	Preservação dos registos de notificação de informação	Deve ter capacidade de guardar registos de notificações de informação dadas aos titulares dos dados, de forma a demonstrar conformidade.	M

2.2 - Informações a facultar aos titulares dos dados pessoais (artigo 13º)

A tabela seguinte descreve os requisitos identificados para o cumprimento das informações a facultar aos titulares dos dados pessoais:

ID	Objetivo	Requisito	Prioridade de implementação
INFTIT1	Notificações de informação	a) Deve ter capacidade de fornecer aos titulares dos dados informações como: i. identidade e contacto do responsável pelos dados e DPO; ii. finalidade e base legal para tratamento de dados pessoais; iii. destinatários ou categorias de destinatários dos dados pessoais; iv. prazo de conservação dos dados pessoais. No caso de não ser possível, critérios usados para definir prazos; v. existência de direitos reservados aos titulares dos dados; b) Deve ter capacidade de informar titulares dos dados das categorias dos dados pessoais, assim como da fonte dos dados (incluindo se foram recolhidos em fontes acessíveis publicamente).	M
INFTIT2	Momento da notificação de informação (dados pessoais obtidos diretamente)	Deve ter a capacidade de fornecer as notificações de informação no momento da recolha de dados junto do titular dos dados.	M
INFTIT3	Período de notificação da informação ao titular dos dados	Deve ter a capacidade de fornecer informações no período máximo de um mês após a recolha dos dados pessoais. Se dados pessoais forem usados para comunicar com titular dos dados, notificação das informações deve ocorrer no momento da primeira comunicação. Se dados pessoais forem divulgados a outro destinatário, titulares devem ser informados antes dos dados serem divulgados.	M

INFTIT4	Notificação ao titular dos dados de novos tratamentos	Se dados pessoais forem processados para uma finalidade diferente daquela que os titulares dos dados foram informados, deve ser providenciada uma nova notificação da informação que informe acerca do novo tratamento.	M

2.3 - Acesso do titular dos dados, Retificação e portabilidade (artigo 15º, artigo 16º e artigo 20º)

A tabela seguinte descreve os requisitos identificados para o cumprimento do acesso, retificação e portabilidade dos dados pessoais por pate do titular dos dados:

ID	Objetivo	Requisito	Prioridade de implementação
ACESS1	Acesso dos titulares dos dados aos dados pessoais	Deve permitir que seja providenciada uma cópia dos dados pessoais em fase de tratamento, a pedido dos titulares dos dados.	M
ACESS2	Formulário de resposta para pedidos do titular dos dados	Deve ter a capacidade de desenvolver um formulário de resposta ao pedido de acesso dos titulares dos dados, como forma de garantir que toda a informação requerida é providenciada.	R
ACESS3	Confirmação de tratamento de dados pessoais	Deve ter a capacidade de confirmar ao titular dos dados se dados pessoais que lhe dizem respeito são ou não objeto de tratamento.	M
ACESS4	Informações que titular dos dados tem direito a aceder	Deve ter a capacidade de fornecer informações como: a) finalidade do tratamento dos dados pessoais; b) categorias dos dados pessoais; c) destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados; d) prazo previsto para a conservação dos dados pessoais. Caso não seja possível, critérios usados para fixar prazo de conservação; e) existência de direito do titular dos dados solicitar retificação, apagamento ou limitação do tratamento dos dados pessoais, ou do direito desse opor ao tratamento; f) direito de apresentar reclamação a uma autoridade de controlo; g) informações disponíveis sobre origem dos dados, caso estes não tenham sido recolhidos juntos dos titulares; h) existência de decisões automatizadas, incluindo definição de perfis.	M
ACESS5	Resposta ao pedido de acesso do titular dos dados	Caso o pedido do titular dos dados seja feito por meios eletrónicos, a informação deve ser fornecida num formato eletrónico de uso corrente.	M
ACESS6	Acesso direto do titular aos dados pessoais	Deve ter a capacidade de providenciar um sistema seguro que garanta o acesso direto do titular dos dados aos seus dados pessoais.	R

RET1	Retificação dos dados pessoais, por parte do titular dos dados	Deve ter a capacidade de retificar e/ou completar dado pessoais inexatos.	M
POR-TAB1	Portabilidade dos dados pessoais dos titulares dos dados	Deve ter a capacidade de fornecer os dados pessoais do titular dos dados num formato a) estruturado; b) de uso corrente; c) de leitura automática.	M
POR-TAB2	Portabilidade dos dados pessoais entre responsáveis pelo tratamento	Deve ter a capacidade de transmitir dados pessoais para um SI de outro responsável pelo tratamento, designado pelo titular dos dados.	M
POR-TAB3	Interoperabilidade dos formatos e sistemas	Deve permitir a existência de um sistema interoperável que permita ou facilite a transmissão/portabilidade dos dados pessoais.	R

2.4 - Direito de objeção (artigo 21º)

A tabela seguinte descreve os requisitos identificados para o cumprimento do direito de objeção por parte do titular dos dados pessoais ao tratamento dos dados:

ID	Objetivo	Requisito	Prioridade de implementação
OBJ1	Objeção ao tratamento dos dados pessoais por parte do titular dos dados	Deve ter capacidade de cessar tratamento dos dados pessoais, para fins de investigação científica, face à oposição por parte do titular dos dados.	M

2.5 - Direito ao apagamento (esquecimento) e direito à limitação do tratamento (artigo 17º, artigo 18º e artigo 19º)

A tabela seguinte descreve os requisitos identificados para o cumprimento do direito de apagamento dos dados e limitação do tratamento dos dados pessoais por parte do titular dos dados:

ID	Objetivo	Requisito	Prioridade de implementação
APAG1	Apagamento dos dados pessoais a pedido do titular dos dados	Deve possibilitar apagamento dos dados pessoais de determinado titular dos dados na condição de: a. dados pessoais deixarem de ser necessários para a finalidade que motivou a sua recolha ou tratamento; b. não existir interesse legítimo que justifiquem o tratamento; c. consentimento para o tratamento dos dados pessoais for retirado; d. dados pessoais forem tratados ilicitamente.	M
APAG2	Comunicação com outras entidades responsáveis pelo tratamento de dados ou subcontratantes.	Deve ter capacidade de contactar/notificar outras entidades envolvidas no tratamento dos dados pessoais com detalhes do pedido feito pelo titular dos dados.	M
LIMIT1	Limitação do tratamento dos dados pessoais a pedido do titular dos dados	Deve permitir responder ao pedido dos titulares de limitar o tratamento dos dados enquanto outras queixas (precisão dos dados) são resolvidas.	M
LIMIT2	Limitação do tratamento	Deve ter a capacidade de identificar dados cujo tratamento deve ser limitado enquanto queixas são resolvidas.	R
LIMIT3	Notificação da anulação da limitação do tratamento dos dados pessoais.	Deve ter a capacidade de notificar titular dos dados acerca da anulação da limitação do referido tratamento.	M

3 - Requisitos de privacidade e segurança

3.1 – Proteção de dados pessoais desde a conceção e por defeito (artigo 25º)

A tabela seguinte descreve os requisitos identificados para o cumprimento da proteção dos dados pessoais desde a conceção e por defeito:

ID	Objetivo	Requisito	Prioridade de implementação
PROT1	Proteção de dados desde conceção	a) Deve garantir a capacidade de pseudonimização e encriptação dos dados,	M

		b) Deve ter a capacidade de proceder a medidas de minimização dos dados.	
PROT2	Proteção de dados por defeito	a) Deve assegurar que só são tratados dados pessoais necessários para cada finalidade específica do tratamento, aplicando-se a: i. quantidade de dados pessoais recolhidos; ii. extensão do seu tratamento; iii. prazo de conservação; iv. acessibilidade. b) Deve garantir que, por defeito, os dados pessoais não sejam disponibilizados sem intervenção humana a um número indeterminado de pessoas singulares.	M
PROT3	Registo de políticas de proteção de dados pessoais	Deve permitir o registo de políticas utilizadas para a adoção de medidas técnicas e organizativas de proteção de dados por conceção e por defeito, como forma de demonstrar conformidade.	R

3.2 – Registo das atividades de tratamento dos dados pessoais (artigo 30º)

A tabela seguinte descreve os requisitos identificados para o registo das atividades de tratamento dos dados pessoais nos SIS:

ID	Objetivo	Requisito	Prioridade de implementação
REG1	Registo das atividades do tratamento de dados pessoais	Deve ter a capacidade de manter um registo atualizado e preciso de todas as atividades de tratamento de dados pessoais, com as informações: a) finalidades do tratamento; b) descrição das categorias de titulares de dados e das categorias de dados pessoais; c) categorias dos destinatários a quem dados foram ou serão divulgados; d) prazos previstos para o apagamento das diferentes categorias de dados, se possível; e) descrição geral das medidas técnicas e organizativas no domínio da segurança, se possível.	M
REG2	Formato dos registos do tratamento dos dados pessoais	Registos devem ser efetuados por escrito, incluindo em formato eletrónico.	M
REG3	Disponibilização dos registos de tratamento dos dados pessoais	Deve ter a capacidade de disponibilizar registos do tratamento de dados à autoridade de controlo.	M

3.3 – Notificação de violação de dados pessoais (artigos 33º e 34º)

A tabela seguinte descreve os requisitos identificados para a notificação de violação de dados pessoais por parte dos responsáveis pelo tratamento dos dados pessoais:

ID	Objetivo	Requisito	Prioridade de implementação
NOT1	Desenvolvimento de procedimentos de notificação de violações de dados	Deve apoiar o desenvolvimento de procedimentos de notificação de violações internos.	R
NOT2	Controlo de acesso	Devem ser implementadas medidas técnicas e organizativas que tornem os dados pessoais inteligíveis no caso de acesso não autorizado.	R
NOT3	Registo de violações de dados pessoais	a) Deve ter a capacidade de manter um registo de todas as violações de dados que se verificaram, contendo: i. factos relacionados com a violação de dados pessoais; ii. efeitos que se verificaram; iii. ações tomadas. b) Deve ter a capacidade de registar informações que descrevam, em linguagem simples e clara, a natureza da violação de dados pessoais e providenciar informações como: i. nome e contacto do DPO; ii. as consequências prováveis da violação de dados pessoais; iii. as medidas tomadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive medidas para mitigar possíveis efeitos adversos da violação de dados pessoais.	M
NOT4	Descrição da violação de dados pessoais para envio à autoridade reguladora	Deve ter a capacidade de registar informações relacionadas com a natureza da violação de dados pessoais, incluindo categorias dos dados e número de registos afetados, num formato passível de ser enviado à autoridade reguladora.	M
NOT5	Prazo para notificação de violação de dados pessoais	Deve ter a capacidade de notificar a autoridade de controlo, no prazo de 72h, quando ocorre uma violação de dados pessoais.	M

3.4 – Avaliação de impacto da proteção de dados (artigo 35º)

A tabela seguinte descreve os requisitos identificados para a Avaliação de Impacto da Proteção de Dados:

ID	Objetivo	Requisito	Prioridade de implementação
DPIA1	Preservação de registos de DPIA	Deve possibilitar a preservação de um registo da Avaliação do impacto sobre a proteção de dados (Data Protection Impact Assessment) eu contenha: a. descrição das atividades de tratamento e o seu propósito, b. avaliação da necessidade e proporcionalidade do tratamento de dados pessoais, os riscos que podem surgir e medidas adotadas para mitigar esses riscos, em particular salvaguardas e medidas de segurança para proteger dados pessoais e cumprir o regulamento.	M
DPIA2	Consulta de DPIA	Deve permitir a consulta do PIA sempre que o responsável pelo tratamento dos dados pretender avaliar se tratamento é realizado em conformidade com a avaliação de impacto sobre a proteção de dados.	R
DPIA3	Inclusão do parecer do DPO	Deve incluir o parecer do DPO, encarregue pela realização do DPIA.	M

3.5 – Encarregado da Proteção de Dados (DPO) (artigo 37º - 39º)

A tabela seguinte descreve os requisitos identificados para o envolvimento do Encarregado da Proteção de Dados:

ID	Objetivo	Requisito	Prioridade de implementação
DPO1	Envolvimento do Encarregado de Proteção de Dados	Deve garantir o envolvimento do Encarregado de Proteção de Dados (Data Protection Officer) a todas as matérias e materiais relacionados com a proteção de dados pessoais (acesso aos dados pessoais e às operações de tratamento)	M

3.6 – Códigos de conduta e certificação (artigo 40º - 42º)

A tabela seguinte descreve os requisitos identificados para a conformidade com códigos de conduta e processos de certificação por parte dos responsáveis pelo tratamento:

ID	Objetivo	Requisito	Prioridade de implementação
CODCON1	Conformidade com códigos de conduta	Deve conter o registo de conformidade com procedimentos previstos num código de conduta desenvolvido.	R
CERT1	Conformidade com processos de certificação	Deve ter a capacidade de manter registos de certificações em matéria de proteção de dados, bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento.	R

4 - Requisitos para transferência de dados pessoais para países terceiros ou organizações internacionais

4.1 - Transferências de dados pessoais sujeitas a garantias adequadas (artigo 45º - 46º)

A tabela seguinte descreve os requisitos identificados para a transferência de dados pessoais sujeitas para países terceiros e organizações internacionais:

ID	Objetivo	Requisito	Prioridade de implementação
TRANSF1	Transferência de dados para países terceiros ou organizações internacionais	Deve permitir a transferência de dados para países terceiros ou organizações internacionais	M
TRANSF2	Garantias das transferências de dados pessoais	Deve registar as garantias adequadas apresentadas pelo país terceiro ou organização internacional que permitam a transferência de dados pessoais: a) instrumento vinculativo e com força executiva entre autoridades ou organismos públicos; b) regras vinculativas aplicáveis às empresas; c) cláusulas-tipo de proteção de dados adotadas pela Comissão; d) cláusulas-tipo de proteção de dados adotadas pela autoridade de controlo e aprovadas pela Comissão; e) um código de conduta aprovado; f) um procedimento de certificação.	M

Anexo B - Especificações openEHR

A tabela seguinte apresenta as especificações openEHR e as respetivas explicações.

Especificação openEHR	Explicação
Modelação Multinível	A Modelação Multinível promove a separação do modelo de referência (modelo de informação estável que define as estruturas lógicas dos RES e dos dados demográficos) do modelo de conteúdo (definições do conteúdo semântico clínico na forma de arquétipos e templates. Estes são pontos ou grupos de dados modelados extensivamente por profissionais clínicos, sendo independentes de utilização particular. Por outras palavras, são pontos/grupos de dados externos a um sistema de software específico). O modelo de referência é implementado no software, enquanto o conteúdo clínico é definido através da modelação 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. Fundamentalmente, todos os SIS suportam a mesma estrutura de dados
Separação da informação clínica e informação demográfica	Um dos princípios do openEHR é a completa separação do conteúdo do registo clínico da informação identificável demográfica. A existência de um repositório para os RES e um repositório para a informação Demográfica permite que a informação clínica e demográfica seja separada. Um RES contém referências para as entidades do repositório de informação demográfica. A separação da informação clínica e demográfica permite que, em caso de violação de dados de um RES, a identidade do titular dos dados seja preservada (indícios diretos acerca dos titulares dos dados são mais difíceis de controlar). Com a separação do RES e da informação demográfica em diferentes repositórios obriga a que, no caso de violação de dados, sejam comprometidos dois servidores, ou mesmo até dois computadores físicos. Esta especificidade garante assim o anonimato do titular dos dados face à informação contida no seu RES, uma vez que apenas é utilizada uma instância no RES, denominada de “PARTY_SELF”, para referenciar o sujeito. Essa informação funciona como uma referência externa opcional, sendo que o RES pode ser configurado para providenciar 3 níveis de separação. O identificador externo é assim determinado na instância “PARTY_SELF” da seguinte forma: a) Em lugar algum do RES (cada instancia “Party_self” é deixada em branco). Esta é a forma mais segura e significa que a ligação entre o RES e o paciente tem de ser feita fora do RES, associando identificador do RES (EHR.ehr_id) e o identificador do sujeito; b) Apenas uma vez no objeto “EHR_STATUS” (atributo do sujeito), e em mais lugar nenhum. Medida também muito segura, se o objeto EHR_STATUS estiver protegido de alguma forma; c) Em cada instância do “Party_self”. Esta solução é razoável num ambiente seguro, e conveniente para copiar partes do registo no local.
Camada de Serviços	O modelo de serviços do openEHR permite definir o interface gráfico que o utilizador irá utilizar no sistema, criando as vistas que irão possibilitar a consulta dos dados.

	A camada de serviços atua sobre o modelo de referência e sobre o modelo de arquétipos, permitindo modelar que informação do RES irá ser mostrada nos SIS. A camada de serviços é composta pelo Virtual EHR API, o EHR Service Model, o Archetype Service Model e o Terminology Interface Model. O Virtual EHR API permite definir o interface dos dados do RES, possibilitando a disponibilização dos dados de todo um Compostition ou simplesmente de partes do registo. O EHR Service Model permite que seja feita a consulta dos dados disponibilizados pelo Virtual EHR API. O nível de detalhe dos dados consultados pode variar, podendo permitir o acesso a registos mais complexos, como conjunto de alterações a versões, como pode permitir pesquisa de elemnetaos, `partida, mais simples, como peuqnas respostas, médias, iIDS de pacientes, etc. O Archetype Service Model permite definir o interface para repositório de arquétipos online, funcionando como ferramenta importante para o acesso a informação importante por parte dos profissionais de saúde (ex. precisarem de um arquétipo que não se encontra no seu repositório local para determinado tipo de tratamento de saúde). Por sua vez, o Terminology Interface Model possibilita que todos os serviços mencionados possam aceder a qualquer terminologia disponível no ambiente de informação de saúde. 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 i. Versionamento e Indelebilidade ii. Assinatura digital	A funcionalidade mais básica do openEHR assenta no seu suporte à integridade dos dados. O controlo de versões assume assim um papel preponderante. O repositório RES ou de informação demográfica é gerido como um recipiente de versões controlado (modelado através de uma classe denominada “VERSIONED_OBJECT”). Cada recipiente de versões contém as versões de uma estrutura “Composition” ou Party”, à medida que estes são alterados. O conjunto de alterações denomina-se “Contributions”, que consistem em novas ou alteradas versões dos registos controlados no repositório. Essencialmente, o conjunto de alterações funciona como uma transação, garantindo a consistência e integridade do repositório de dados. As alterações feitas pelos utilizadores (criação de novos registos, apagamento de registos, modificação de registos, 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. Esta especificidade garante aos sistemas uma característica de **indelebilidade** (nenhuma informação pode ser apagada). O controlo de versões engloba ainda a possibilidade de cada versão criada conter uma **assinatura digital**, criada com uma chave-primária encriptada de um *hash* de uma representação aprovada da Versão comprometida. Num sistema de versionamento, a assinatura dos dados atua como uma verificação de integridade, uma medida de autenticação e também uma medida de não-repúdio.
Controlo de Acesso i. Lista de controlo de acesso ii. Controlo de acesso às definições de acesso	O controlo de acesso dos RES openEHR é definido através do objeto denominado “EHR_ACCESS”. Este objeto funciona como porta de entrada para

	toda a informação de aceso, sendo que qualquer decisão no âmbito do acesso à informação deve ser baseada nas políticas e regras nele contidas. O RES do openEHR permite a definição de uma lista de **controlo de acesso**, onde são indicados indivíduos identificados e respetivas categorias. O princípio da definição da lista de controlo de acesso deve passar por considerar a pertinência do acesso ao nível da identidade do utilizador (quem está a prestar cuidados ao paciente) quer em termos de tempo e duração do acesso aos registos. No momento da criação do RES, o openEHR permite também que seja definido um *gate-keeper* responsável pelo **controlo das configurações de acesso** do registo. O *gate-keeper* passa a ser uma das identidades conhecidas no RES, sendo normalmente o próprio paciente (caso seja um adulto mentalmente competente) ou um parente ou tutor legal (caso o registo pertença a uma criança menor ou a um paciente incapaz). O *gate-keeper* determina quem pode fazer alterações à lista de controlo de acesso, sendo que 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.