Universidade Nova de Lisboa
Escola Nacional de Saúde Pública

Protecção de dados de saúde

Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Protecção de Dados da União Europeia

XII Curso de Mestrado em Gestão da Saúde
2016-2018

Ana Rita Ramos Y Rio Tinto

Lisboa, Agosto 2018

Universidade Nova de Lisboa

Escola Nacional de Saúde Pública

Protecção de dados de saúde

Percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Protecção de Dados da União Europeia

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de Mestre em Gestão de Saúde, realizada sob orientação científica de:

Professor Doutor João Miguel Valente Cordeiro

Professora Doutora Paula Lobato Faria

Lisboa, Agosto 2018

Agradecimentos

A elaboração do presente trabalho não teria sido possível sem a colaboração de algumas pessoas especiais às quais agradeço muito.

Aos meus orientadores, o Professor Doutor João Valente Cordeiro e a Professora Doutora Paula Lobato Faria, por toda a sua disponibilidade, compreensão e atenção para comigo ao longo de todos estes meses.

À Paula Cristina Nunes da Silva, secretária do Curso de Administração Hospitalar, o meu agradecimento por toda a disponibilidade demonstrada na fase de aplicação dos questionários.

À minha mãe por me ter sempre apoiado e incentivado a seguir os meus sonhos e por todo o acompanhamento em todas as fases da minha vida.

Ao Miguel Rio Tinto por toda atenção, incentivo, paciência e apoio incondicional demonstrados, não só ao longo de todos estes meses na realização do presente trabalho, como também em muitos outros momentos.

À minha tia e avó o meu agradecimento por todo o esforço depositado ao longo destes anos numa educação de qualidade que me conduziram até aqui.

À Sofia Castanheira pela paciência, amizade e apoio sempre que precisei e à Dora Bonito pela disponibilidade na entrega do trabalho.

Resumo

Palavras chave: privacidade; confidencialidade; dados pessoais; dados de saúde

Remontam a Hipócrates as origens do sigilo profissional, tendo este afirmado que o que quer que visse ou ouvisse da vida dos homens, na sua prática profissional ou fora dela, que não devesse ser falado em público, não o divulgaria e deveria ser mantido em segredo. A confidencialidade no domínio da saúde é assim tão antiga quanto a civilização grega. A partir desses tempos antigos, a privacidade e a confidencialidade para os prestadores de cuidados de saúde tornaram-se uma obrigação legal bem como um dever ético.

A confidencialidade, privacidade e proteção da informação pessoal apresenta-se actualmente como um fenómeno social muito relevante, perante o desenvolvimento tecnológico e dos sistemas de informação e o potencial que estes meios trouxeram para a exploração informática e analítica dos dados, mas também em face das vulnerabilidades criadas pela cada vez mais abrangente e mais sofisticada adoção dos sistemas de informação.

A sociedade debate-se actualmente com múltiplos dilemas associados à devassa dos dados pessoais, agravando-se quando se possa tratar de dados pessoais de saúde. Concomitantemente, nos últimos anos, a questão da privacidade dos dados dos cidadãos em geral, e dos utentes da saúde em particular, tem sido encarada com um maior nível de preocupação.

A protecção de dados surge assim como forma de prevenir este risco de devassa da vida privada das pessoas, tendo sido recentemente elaborado e entrado em vigor o novo Regulamento Geral de Protecção de Dados (doravante RGPD) da União Europeia que estabelece regras relativas à protecção de dados das pessoas singulares, no que concerne aos seus dados pessoais.

Metodologicamente, o presente projecto passou pela realização de uma revisão crítica da literatura científica mais relevante sobre o tema da protecção de dados, pela análise do novo RGPD e pela aferição da percepção e do grau de conhecimento dos Gestores e Administradores Hospitalares da Região de

Lisboa e Vale to Tejo sobre as principais disposições do novo RGPD, mediante a realização de um inquérito.

No que respeita aos resultados apurados verificou-se que a grande maioria dos inquiridos desconhece as disposições do RGPD, não demonstrando assim, um conhecimento adequado acerca da temática da protecção de dados e das novas disposições contidas nesse Regulamento. O conhecimento dos inquiridos relativamente às disposições do RGPD é deficiente em diversas áreas, nomeadamente no que concerne aos principais conceitos constantes no mesmo.

Num primeiro plano, poderá dizer-se que não estarão ainda preparados para responder às exigências da aplicação deste diploma jurídico.

Abstract

Keywords: privacy; confidentiality; personal data; medical and health data

Confidentiality in the physician profession is as old as the Greek civilization, with the Hippocratic Oath, where physicians was required to swear to uphold specific ethical standards, including "…whatsoever I shall see or hear in the course of my profession, as well as outside my profession in my intercourse with men, if it be what should not be published abroad, I will never divulge, holding such things to be holy secrets."

Confidentiality and data privacy of personal information is currently a paramount social phenomenon, given the accelerated technological development that enable us today to use data and explore massive amounts of information analytically to the benefit of society. However, the same technological advances brought new challenges around data privacy, in particular with health and medical data.

The new Regulation [European Union (EU)] 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data [general data protection regulation (GDPR)], 95/46/EC, that just came into force, strengthens and harmonizes the rules for protecting individuals' privacy rights and freedoms within and, under certain conditions, outside the EU territory. This project aims to provide an overview of the new rules enforced by GDPR in the context of previously existing privacy regulation and relevant scientific research. Moreover, its most important objective is to assess the knowledge and preparedness of health managers and administrators about the most relevant GDPR rules that will impact their role, responsibilities and professional activities. To that aim, a questionnaire was answered by a panel of high-level managers and administrators in hospitals in the Lisbon, Portugal region. The analysis of the results of this questionnaire showed that the large majority of hospital managers and administrators do not yet understand that full scope of GDPR in what concerns processing of personal health data, genetic data or biometric data and other kinds of sensitive information whose use is strictly regulated by the GDPR. Moreover, it is the conclusion of this project that the majority of hospital organizations have not

started comprehensive and focused programs to adapt their practices and ensure compliance to the EU law to be enforced in May 2018.

Índice

Siglas e Abreviaturas

CADA – Comissão de Acesso aos Documentos Administrativos (Lei n.º26/2016, de 22 de agosto)

CC – Código Civil

CNECV – Conselho Nacional de Ética para as Ciências da Vida (Parecer 60/CNECV/2011)

CNPD – Comissão Nacional de Protecção de Dados (Lei n.º 67/98 de 26 de outubro)

CRP – Constituição da República Portuguesa

LADA – Lei de Acesso a Documentos Administrativos (Lei n.º 47/2007, de 24 de agosto)

LPD – Lei da Protecção de Dados (Lei n.º 67/98 de 26 de outubro)

RGPD – Regulamento Geral de Protecção de Dados da União Europeia (Regulamento (UE) 2016/679 de 27 de abril de 2016

RSE – Registo de Saúde Electrónico

TFUE – Tratado sobre o Funcionamento da União Europeia

TUE – Tratado da União Europeia

UE – União Europeia

UNESCO – United Nations Educational, Scientific and Cultural Organization

CAPITULO I

1. Introdução

1.1 Pertinência do estudo

O presente trabalho de projecto, intitulado "Protecção de dados de saúde – percepção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Protecção de Dados da União Europeia", insere-se no âmbito do XII Curso de Mestrado em Gestão da Saúde, da Escola Nacional de Saúde Pública da Universidade Nova de Lisboa (ENSP-UNL).

O projecto foca-se na realidade da administração hospitalar portuguesa quanto à temática de privacidade e confidencialidade dos dados, mais concretamente dos dados de saúde, no âmbito do novo Regulamento Geral de Protecção de Dados (RGPD), cuja aplicação se iniciou em Maio de 2018.

A temática da privacidade e protecção de dados de saúde é simultaneamente antiga e inovadora. Por um lado, caracteriza-se como sendo antiga, pois ao longo do tempo tem preocupado filósofos, juristas, profissionais de saúde e pacientes, sendo que é uma área que necessita ainda de alguma atenção (1). Por outro lado, caracteriza-se como sendo inovadora, na medida em que é objecto de desenvolvimentos recentes que prometem ter um impacto significativo na prestação de cuidados de saúde em particular e na área de gestão em saúde em geral. O maior desses desenvolvimentos, no que diz respeito à União Europeia (UE) e a Portugal, corresponde à entrada em vigor do novo Regulamento Geral de Protecção de Dados (RGPD) da UE. O direito à privacidade, à protecção da confidencialidade e dos dados pessoais (incluindo os de saúde) são consignados como direitos fundamentais dos cidadãos, sendo, como adiante se dirá, a informação de saúde merecedora de tutela jurídica especial e reforçada neste Regulamento.

Assegurar e garantir a plena protecção destes dados deve ser uma responsabilidade não apenas dos profissionais de saúde, no decorrer da sua actividade, mas também dos próprios gestores de organizações de saúde. Isto porque a implementação de medidas que assegurem a protecção deste tipo de informação, irá não apenas conferir fiabilidade e segurança à organização e permitir satisfazer os seus compromissos regulamentares e de garantia de

serviço, mas também fortalecer a integridade das próprias organizações, aumentando o grau de confiança dos pacientes. Para garantir a plena protecção dos dados de saúde dos cidadãos, o novo RGPD da UE procura clarificar algumas áreas tradicionalmente indefinidas, que incluem a propriedade da informação, o direito à sua utilização, bem como a extensão dos direitos e deveres do titular dos dados e das entidades que recolhem e processam essa informação. Ao fazê-lo confere aos cidadãos total poder sobre a sua informação pessoal e confere às entidades que recolhem e processam essa informação, tanto privadas quanto públicas, deveres estritos e sanções significativas em caso de violação. É neste contexto que urge aferir o grau de conhecimento dos gestores de saúde, em particular dos Administradores Hospitalares, em Portugal, acerca das principais inovações introduzidas por este documento jurídico essencial.

Considerando a sensibilidade dos dados de saúde e o impacto que pode resultar da sua violação, é crucial que os gestores da área da saúde, em particular os Administradores Hospitalares, estejam sensibilizados para a temática da proteção dos dados pessoais e cientes do contexto regulamentar associado e adoptem as medidas de controlo e mitigação de riscos que se configurem apropriadas.

O meu interesse pessoal na realização deste projeto resulta da confluência de três aspectos. Em primeiro lugar, por ser um tema de extrema actualidade, em grande debate na sociedade e com uma exposição mediática muito importante, em face de casos recentes de violação da privacidade e das consequências advindas (registe-se o caso Facebook - Cambridge Analytica e as suas consequências no resultado da mais recente eleição para Presidente dos Estados Unidos). Em segundo lugar, porque sendo uma ávida utilizadora das novas tecnologias e extremamente crente nos benefícios que as mesmas aportam à sociedade, registo por experiência pessoal que cada vez mais entidades (privadas e públicas) recolhem mais dados sobre mim, sobre a minha vida e sobre as minhas relações sociais. Entendendo o valor aportado pela disponibilização desta informação (por exemplo, a partilha de factos da minha vida e das minhas preferências com a minha família e amigos ou o envio de recomendações mais ajustadas às minhas preferências), interessa-me melhor

compreender as situações em que informação é recolhida, tratada e disponibilizada a terceiros sem o meu consentimento e ao arrepio da lei e do Direito. Finalmente, em terceiro lugar, pelo facto de assuntos relacionados com a área de Direito sempre me terem cativado, durante a minha licenciatura em Gestão, mas também ao ingressar no Mestrado de Gestão da Saúde da ENSP-UNL, onde tive a oportunidade de contactar com Direito da Saúde, em particular quando abordada a temática da Privacidade e Confidencialidade de Dados de Saúde.

Tendo manifestado o meu interesse por esta área, contactei o Professor Doutor João Valente Cordeiro e a Professora Doutora Paula Lobato Faria acerca da realização do projecto nesta área e, aproveitando a entrada em vigor do novo RGPD, decidiu-se então que o projecto incidiria sobre a temática da protecção de dados de saúde e da Administração Hospitalar, no contexto deste inovador Regulamento.

1.2 Objectivos do estudo

Após a escolha do tema do projeto, foi necessária a definição prévia de objectivos concretos e claros para o presente estudo, os quais são:

1. Caracterizar o novo Regulamento Geral de Protecção de Dados da UE, contextualizando o seu conteúdo em relação a outras disposições regulamentares e legais já existentes e analisando o seu potencial impacto particular na área da saúde;
2. Aferir o grau de conhecimento dos gestores de organizações de saúde portuguesas, em particular dos Administradores Hospitalares, acerca das medidas e dos mecanismos necessários à protecção da informação de saúde dos utentes, no âmbito do Regulamento Geral de Protecção de Dados da UE;
3. Avaliar o grau de conhecimento dos referidos Gestores/Administradores acerca das inovações introduzidas pelo novo Regulamento Geral de Protecção de Dados da UE e o seu grau de preparação para responder às exigências da aplicação deste diploma jurídico.

1.4 Sistematização

O presente trabalho encontra-se dividido em 4 partes: Introdução, Metodologia, Enquadramento teórico, Estudo prático e Conclusões.

Na Introdução pretende-se apresentar o projecto de investigação fazendo referência à pertinência do tema do presente trabalho, bem como às motivações que conduziram à realização do mesmo. São aqui também apresentados os objectivos do trabalho, bem como detalhada a metodologia utilizada.

Na secção da metodologia encontra-se descrita de que forma o trabalho de projecto foi realizado, essencialmente focando a revisão crítica da literatura relevante para o tema em causa, as pesquisas efectuadas, bem como a elaboração de um questionário.

No Enquadramento Teórico, são descritas e discutidas as questões mais relevantes para enquadrar o tema em causa. Os tópicos aí abordados são: o direito à vida privada – contextualização e perspectiva histórica, a privacidade e confidencialidade – distinção conceptual, medidas de protecção da confidencialidade (incluindo os tópicos referentes ao segredo profissional e protecção de dados), a confidencialidade e a protecção de dados em saúde, desafios colocados pelo progresso tecnológico e, por fim, o enquadramento normativo visando as principais normas de direito Internacional, da União Europeia e Nacional, em matéria de protecção de dados.

A secção relativa ao Estudo Prático encontra-se, por sua vez, organizada em três partes: apresentação do estudo, apresentação dos resultados e discussão. Nesta secção pretende-se descrever e analisar o grau de percepção dos administradores hospitalares quanto às disposições do RGPD através dos resultados da aplicação do questionário utilizado. São aqui analisados a profundidade de conhecimento dos inquiridos sobre cada tema e o nível de clareza relativo a cada conceito específico presente no RGPD. Na parte relativa ao Estudo prático, são também apresentadas as limitações do estudo em causa.

Na última parte do trabalho de projecto são apresentadas as Conclusões que se extraíram do estudo realizado, bem como sintetizadas algumas recomendações relativas à temática da protecção de dados no que concerne à aplicação do RGPD em meio hospitalar.

CAPITULO II

2. Metodologia

2.1. Tipo de estudo

No decorrer do desenvolvimento do presente projecto, foram consideradas várias abordagens metodológicas, tendo a selecção da metodologia de trabalho recaído sobre aquela que se considerou mais adequada e que assentou na realização e aplicação de um questionário directo a um painel de Administradores Hospitalares, questionário esse que foi informado e enquadrado pela análise exaustiva da literatura sobre o tema em estudo.

Desta forma irá ser apresentada a opção metodológica escolhida, integrando aspectos como a descrição dos instrumentos utilizados para a recolha dos dados, a caracterização da amostra, bem como a análise e tratamento dos resultados obtidos.

O método utilizado para análise consistiu no método quantitativo, sendo que o mesmo é o mais utilizado, dando primazia à frequência com que um determinado grupo/amostra revela certo tipo de atitudes ou comportamentos, bem como opiniões. Neste método, os métodos de recolha dos dados são estruturados, sendo os principais as entrevistas e questionários (2).

A aplicação de questionários por via electrónica corresponde a uma metodologia quantitativa, nomeadamente utilizada quando se pretende medir opiniões, reacções, hábitos, entre outros (3).

Segundo Gil, um questionário é definido como sendo “uma técnica de investigação social composta por um conjunto de questões que são submetidas a pessoas com o propósito de obter informações sobre conhecimentos, crenças, sentimentos, valores, interesses, expectativas, aspirações, temores, comportamento presente ou passado” (4).

A metodologia de recolha de dados utilizada foi o método por questionário estruturado/fechado.

2.2. Revisão da literatura

Numa primeira fase procedeu-se à revisão crítica da literatura científica relevante para o tema. A mesma consistiu na análise de diversos documentos de natureza académica, científica e jurídica relacionados com o tema do estudo, tendo como

objectivo caracterizar, descrever e enquadrar a temática. A revisão da literatura incidiu também sobre a análise de documentos/diplomas legais, a fim de salientar os marcos normativos mais relevantes que mais marcaram a evolução das questões da privacidade e confidencialidade da informação, em particular da informação de saúde, ao longo do tempo.

A pesquisa para o presente estudo científico e consequente revisão da literatura foi realizada tendo por base documentos presentes em diferentes bases de dados, entre as quais:

- B-on – https://www.b-on.pt
- PubMed - https://www.ncbi.nlm.nih.gov/pubmed/
- Mendeley Academic Library - https://www.mendeley.com/
- Scielo - https://www.scielo.org/
- Google Scholar - https://www.scholar.google.pt
- EBSCO - https://www.ebsco.com

Os principais termos utilizados na realização das pesquisas foram: "*privacy", "privacy and data protection", "data protection", "personal data", "health data", "confidentiality/history", "privacy/history", "the right to privacy"*, *"patient privacy AND satisfaction"*, *"privacy in healthcare"*, bem como " protecção de dados pessoais", "dados pessoais", "privacidade e confidencialidade", "sigilo profissional" entre outros. Utilizou-se, para a referida pesquisa, como limite cronológico inferior o ano de 2005 para a maioria das pesquisas, tendo sido pontualmente consideradas matérias legais de anos anteriores, como por exemplo a Lei nº67/98 de 26 de Outubro de 1998, relativa à protecção de dados pessoais e alguns artigos mais antigos considerados relevantes a incluir a fim de contextualizar historicamente o tema. Como limite superior foi considerada data presente (Agosto de 2018).

No que concerne à pesquisa relacionada sobre documentos/diplomas ético-legais, podem ser destacadas as seguintes bases de dados consultadas:

- DIGESTO/Diário da República Electrónico - https://dre.pt/acerca-do-digesto

- Base de dados legislativa - Procuradoria-Geral Distrital de Lisboa http://www.pgdlisboa.pt/leis/lei_main.php
- EUR-Lex - https://eur-lex.europa.eu/homepage.html
- Comissão Nacional de Protecção de Dados (CNPD) - http://www.cnpd.pt/
- Comissão Nacional de Ética para as Ciências da Vida (CNECV) – http://www.cnecv.pt/
- EU General Data Protection – http://www.eugdpr.org
- United Nations Educational, Scientific and Cultural Organization (UNESCO) – http://en.unesco.org/

2.3. Questionário aplicado

Considerando o objectivo central deste trabalho, isto é, a avaliação da percepção e grau de conhecimento dos Administradores Hospitalares acerca das principais disposições do novo Regulamento Geral de Protecção de Dados da União Europeia (doravante RGPD), foi aspecto central deste projecto a realização de um questionário que permitisse avaliar esse mesmo conhecimento diretamente junto de um painel Administradores Hospitalares.

O questionário foi elaborado de forma a incluir os aspetos mais relevantes do RGPD, tendo sido escolhido o formato estruturado/fechado, com opção de escolha múltipla. Este tipo de questionário impõe um limite nas opções de resposta, evitando repetições de respostas e permitido que a análise de dados seja feita de forma mais fácil e objectiva (5).

Para cada questão é apresentado um conjunto fechado de respostas possíveis, em que uma ou mais respostas estão certas e as restantes estão erradas. O conjunto de opções de resposta foi cuidadosamente identificado para permitir aferir, com elevado grau de certeza, duas dimensões relevantes para a análise: a profundidade de conhecimento dos inquiridos sobre cada tema (número e conteúdo das respostas certas seleccionadas) e, simultaneamente, a clareza em relação aos conceitos específicos contidos no RGPD (número e conteúdo das respostas erradas selecionadas)[1].

[1] Tomemos como exemplo a questão sobre o entendimento do inquirido acerca da licitude do tratamento de dados constante no RGPD. O número de respostas certas indicadas (“mediante consentimento do titular” e “defesa de interesses vitais do titular”) permite aferir a completude do conhecimento do inquirido, enquanto que o número de respostas erradas indicadas (“determinado por entidade pública e/ou

O questionário aplicado (Anexo II – Questionário sobre o novo Regulamento Geral de Protecção de Dados da União Europeia) é composto por 27 questões de escolha múltipla que incidem sobre os seguintes temas: informações profissionais do inquirido, definições e questões gerais acerca do Regulamento, direitos dos titulares e procedimentos considerados obrigatórios para protecção da sua informação, forma como o processo de tratamento de dados deve ser executado e potenciais sanções.

O questionário foi disponibilizado de forma electrónica na plataforma online *SurveyMonkey* (https://pt.surveymonkey.com), onde viria a ser directamente preenchido por membros dos conselhos de administração de hospitais públicos de Lisboa e Vale do Tejo (ver *infra* caraterização da Amostra do estudo).

Foi assim enviado um e-mail a cada um dos inquiridos (Anexo II - Questionário sobre o novo Regulamento Geral de Protecção de Dados da União Europeia), o qual continha um link personalizado que remetia diretamente para o questionário na plataforma online *SurveyMonkey*. Com vista a proporcionar uma melhor experiência para o inquirido, o questionário foi desenvolvido colocando uma resposta por página, com botões de navegação que permitiam ao inquirido navegar ao longo das questões, podendo alterar as suas respostas antes da submissão final. O mesmo esteve activo durante 60 dias para resposta pelos inquiridos.

De forma a aumentar a taxa de participação foram enviadas, com a periodicidade de 10 dias, mensagens subsequentes a relembrar o estudo e encorajar a participação.

2.4. Caracterização da amostra

A região selecionada foi Lisboa e Vale do Tejo, tendo os hospitais públicos desta região sido preferidos por uma questão de proximidade geográfica e por em relação a estes existir a possibilidade de um contacto mais próximo e personalizado com a respectiva Administração, o que facilitou o envio dos questionários e o incentivo à sua resposta.

governamental" e "se os dados forem relativos a não residentes da UE") permite aferir o grau de clareza do inquirido sobre o conceito em causa.

Os hospitais seleccionados para os quais se procedeu ao envio de mensagens bem como o envio do próprio questionário foram: Centro Hospitalar Lisboa Norte, Centro Hospitalar Lisboa Central, Centro Hospitalar Lisboa Ocidental, Hospital de Cascais, Hospital Professor Doutor Fernando da Fonseca, Hospital Beatriz Ângelo, Hospital de Vila Franca de Xira, Hospital Garcia de Orta, Centro Hospitalar do Barreiro-Montijo, Centro Hospitalar de Setúbal, Centro Hospitalar do Oeste, Centro Hospitalar do Médio Tejo, Hospital Distrital de Santarém, Centro Hospital Psiquiátrico de Lisboa, Instituto de Oftalmologia Dr. Gama Pinto e Instituto Português de Oncologia de Lisboa.

O racional da escolha da amostra teve como objectivo a obtenção de um número de respostas considerado adequado ao estudo e ao seu enquadramento académico e cronológico (aproximadamente 15 respostas), tendo sido enviados questionários a 20 inquiridos.

Apesar das sucessivas tentativas de contacto, apenas se conseguiram obter 9 respostas, o que corresponde a uma taxa de participação de 45%.

2.5. Análise e tratamento dos dados

Relativamente ao tratamento dos dados, tirou-se partido da facilidade de tratamento automático de resultados disponibilizado pela plataforma SurveyMonkey, o qual se considerou adequado em face do reduzido volume de respostas (https://help.surveymonkey.com/articles/en_US/kb/How-to-analyze-results). [2] Ainda ao nível do tratamento dos resultados, dado que algumas questões permitiam mais do que uma resposta correcta, realizou-se não apenas uma análise certo/errado, mas também a análise do grau de correcção das respostas (número e conteúdo das opções correctas selecionadas em relação ao número total de opções correctas e número e conteúdo de opções erradas selecionadas).

[2] A plataforma SurveyMonkey permite a analise continua de resultados à medida que se efectua a recolha das respostas. Podem ser consultados relatórios sumarizados dos resultados, efectuadas filtragens e cruzamentos sobre os dados (tipo *Pivot Table*), podem ser analisadas respostas individuais ou a categorização de inquiridos para reports personalizados. Em qualquer momento, os dados podem ser exportados para varios formatos e aplicacoes externas. Adicionalmente, podem ser criados graficos de multiplos tipos para facilitar a visualizacao e comparacao dos dados.

CAPITULO III

3. Enquadramento teórico

3.1. O direito à vida privada – contextualização e perspectiva histórica

A privacidade assume uma grande importância na nossa sociedade. Com o crescente desenvolvimento tecnológico e o poder que os *media* assumem actualmente, a formulação de definições relativas à vida privada e à intimidade do indivíduo começou a ter lugar de grande importância e destaque. Contudo, a ideia de vida privada e o respeito pela mesma não existe apenas nos tempos modernos. As mais incipientes noções de privacidade começaram a surgir na Grécia, onde o homem tinha de viver em sociedade num local onde a violência e a força se impunham (6).

A questão da privacidade encontra-se presente em todos os campos da vida pessoa, porém ganha grande destaque na área da saúde, fazendo com que a abordagem a esta temática se torne ainda mais relevante.

Em 400 a.C., Hipócrates, considerado o "pai da medicina", colocou o princípio do segredo médico, como um dos princípios mais importantes a seguir na conduta médica (7) e, através do seu conhecido Juramento, vemos contemplada a questão da privacidade da pessoa como algo importante que deve ser preservado: "Mesmo após a morte do doente respeitarei os segredos que me tiver confiado" (8).

Em 1890 *Warren* e *Brandeis* publicaram na revista *Harvard Law Review* um artigo jurídico, onde pela primeira vez se faz referência à privacidade como um direito, conhecido desde então como o direito de "ser deixado em paz", sendo este artigo um dos mais importantes no que respeita à história do direito nos Estados Unidos (9).

Após este grande marco histórico como primeiro passo para a consignação da privacidade como um dos direitos fundamentais dos indivíduos, segue-se a Declaração de Genebra em 1948, que constitui maioritariamente uma "revisão" ao Juramento de Hipócrates, tendo como objectivo reforçar o compromisso médico para com o doente, não deixando de lado, mais uma vez, a questão da privacidade (10).

Mais tarde, em 1964, surge a Declaração de Helsínquia, elaborada pela Associação Médica Mundial, a qual determina os princípios éticos para a

investigação médica. Segundo a referida Declaração, é dever do profissional de saúde agir segundo os interesses do doente, em particular em relação aos seus direitos e à privacidade da sua vida, preservando e defendendo os seus interesses em primeiro lugar, mesmo quando a finalidade seja a investigação médica (11).

Em 1973, surge o *AHA Patient's Bill of Rights*, elaborado pelo *American Hospital Association*, que se apresenta como uma carta de direitos dos pacientes e onde se sistematizam doze direitos fundamentais dos pacientes, que deverão imperar para uma melhor satisfação das suas necessidades. Neste documento a questão da privacidade encontra-se contemplada no quinto direito, onde se estabelece que o paciente tem direito a que se respeite a sua privacidade nos mais variados aspectos como sejam a discussão da sua situação médica, a elaboração de exames e a realização de consultas e tratamentos (12).

Em 1995, surge o *Genetic Privacy Act* (13), elaborado com o objectivo de proteger a privacidade genética dos indivíduos, seguindo-se em 1997, a criação da Declaração Universal sobre o Genoma Humano e Direitos Humanos, consagrando igualmente questões sobre a privacidade dos indivíduos, com a ideia central do respeito pela dignidade humana (13).

Mais tarde em 2003, surge a Declaração Internacional da UNESCO sobre os Dados Genéticos Humanos, com o propósito de fazer valer o direito à privacidade dos dados genéticos, essencialmente em matéria de recolha e armazenamento dos mesmos (14), sendo logo após, em 2005, adoptada também a Declaração Universal sobre Bioética e Direitos Humanos, referindo que "a vida privada das pessoas em causa e a confidencialidade das informações que lhe dizem respeito devem ser respeitadas (....) tais informações não devem ser utilizadas para outros fins que não tenham sido aqueles para que foram coligidos ou consentidos (...)" (15).

Embora existam diversas definições de privacidade, este é fundamentalmente um conceito difuso, podendo ter diversas interpretações e aplicações práticas.

O conceito de privacidade pode relacionar-se, por um lado, com aspetos específicos da vida de um indivíduo, cujo acesso pode ser permitido a outros com base em relacionamentos interpessoais e de confiança, e por outro lado pode relacionar-se com a esfera mais íntima da pessoa, ou seja, com aspetos mais restritos e profundos da vida de alguém (16).

Como definição do conceito de privacidade, recorre-se a *Alan Westin*, que define a privacidade como a "reivindicação por parte de indivíduos, grupos ou instituições do direito a determinar, por si mesmos quando, como e em que medida as informações sobre eles são comunicadas a outros" (17).

A privacidade centra-se na proteção das pessoas contra a existência de todo o tipo de interferência alheia na sua vida, permitindo assim que estas possam ser livres de escolher e decidir quem está presente na sua vida. A privacidade é assim considerada um direito fundamental da pessoa, que deve ser salvaguardado, e que reúne em si inúmeros instrumentos que visam a sua protecção (1).

As alterações que se fizeram sentir ao longo do tempo, tanto a nível político, económico, quer mesmo ao nível da sociedade, obrigou de certa forma ao aparecimento e reconhecimento de novos direitos, relacionados com formas de evitar diversos tipos de interferência indesejada na vida de cada um.

Neste contexto, surge o direito a "ser deixado em paz", denominado desta forma segundo o Juiz *Thomas Cooley* (9), sendo este direito equiparado a outros direitos igualmente importantes, como o direito a não ser assaltado ou espancado, o direito a não ser preso sem fundamento, o direito a não ser processado de forma maliciosa e o direito a não ser difamado (9).

O direito a "ser deixado em paz", diz respeito ao facto de existirem pessoas mal intencionadas, que tentam interferir, de forma maliciosa, na vida de alguém, e consigna a proteção da pessoa visada no que respeita à intrusão na sua vida pessoal, tanto nos seus aspetos materiais como imateriais, como por exemplo a sua dignidade (18).

Pode então dizer-se que o direito à privacidade constitui um "direito de personalidade", que visa respeitar a autonomia das pessoas, protegendo-as de eventuais danos decorrentes da devassa da sua vida (1).

3.2. A privacidade e a confidencialidade – distinção conceptual

A privacidade e a confidencialidade são conceitos distintos mas conexos (19), em que as regras que determinam a confidencialidade geralmente limitam a divulgação, enquanto que o conceito de privacidade é mais amplo (20). Por

exemplo, no campo da saúde, ao garantir a confidencialidade das informações que respeitam ao paciente, estamos também a limitar a divulgação das mesmas. Neste âmbito, podemos então começar por analisar estes dois diferentes conceitos num sentido mais lato, passando depois para uma explicação mais restrita no âmbito do campo da saúde.

A privacidade e a confidencialidade embora constituindo dois conceitos diferentes, podem ser facilmente confundíveis, sendo uma das principais distinções entre ambos o facto de a confidencialidade compreender mais do que apenas os direitos de protecção de dados (1).

Ambos os conceitos se referem a informações que, pela sua natureza, se devem encontrar fora do domínio público, existindo, no entanto, algumas diferenças que se fazem notar entre as duas dimensões.

De uma forma geral, quando nos referimos ao direito à privacidade, estamos a referir-nos a informações que apenas o indivíduo possui e que são do seu conhecimento, e ao controlo que o individuo tem sobre as informações que lhe dizem respeito, em particular sobre quem pode aceder e analisar toda essa informação (21). Por outro lado quando nos referimos à confidencialidade estamos perante aspectos que vão para além da esfera mais íntima da pessoa (22).

De facto, uma das principais diferenças entre estes dois conceitos reside no âmbito temporal, uma vez que, o direito à confidencialidade se aplica apenas posteriormente ao direito à privacidade (22), na medida em que para estar em causa a primeira (confidencialidade), ter-se-á obrigatoriamente que comprometer a segunda (privacidade) (23). Consequentemente, segundo *Stanberry*, a confidencialidade consiste num conjunto de "práticas morais, sociais e legais, que trabalham para proteger a privacidade de alguém" (24).

De uma forma mais simples, a privacidade pode ser vista como algo que visa a protecção da esfera íntima da pessoa, enquanto que a confidencialidade se destina a proteger os dados da mesma contra acessos indevidos, por todos aqueles com quem a pessoa não partilhou esses mesmos dados (1,18-20).

Por outro lado, e num plano de análise distinto, o direito à privacidade é por alguns considerado como sendo um direito "negativo", na medida em que este não é violado se não existir alguém que interfira com o mesmo (22). Já o direito à confidencialidade, por sua vez, pode ser visto como um direito "positivo" e

“negativo” simultaneamente, na medida em que, tal como o direito à privacidade, não se viola se não existir interferência alheia mas, uma vez que a informação em causa já não é apenas do conhecimento do próprio, implica a imposição de condutas e deveres que visam assegurar o seu cumprimento. O direito à confidencialidade não pode, assim, ser confundido com o direito à privacidade.

No que respeita à aplicação destes dois conceitos na área da saúde, a questão encontra-se intimamente relacionada com a confiança que deve existir entre o profissional de saúde e o paciente. É importante considerar que a verbalização não é a única forma de transmissão de informação entre paciente e profissional de saúde, pois este último pode aceder a dados pessoais do primeiro sempre que, por exemplo, o paciente realiza algum tipo de exame médico (25), ou o profissional de saúde toma conhecimento da história clínica do paciente, incluindo informação de carácter íntimo e pessoal (por exemplo hábitos de vida, comportamentos de risco, etc.).

Os cuidados de saúde, requerem que o paciente divulgue informações que lhe dizem respeito, para em troca obter o adequado tratamento médico. Esta troca de informação, muitas vezes de cariz sensível, obriga a que exista uma relação de grande confiança entre o paciente e o prestador de cuidados de saúde, pois nesse momento o paciente decide abdicar da sua privacidade. Consideremos a título de exemplo um utente que se encontre numa consulta com o seu médico. Este utente, para efeitos da prestação de cuidados de saúde, terá que fornecer informações pessoais ao médico, estando em causa, após essa transmissão de informação, o direito à confidencialidade relativamente à informação transmitida ao médico (1). O mesmo se poderá dizer da informação constante do processo clínico, e dos diferentes níveis de acesso ao mesmo, estabelecidos como medida de proteção da confidencialidade, para profissionais de saúde, informáticos, administrativos e, claro está, gestores ou administradores.

No campo da saúde, reconhecer esta diferença entre privacidade e confidencialidade pode ajudar a adotar condutas responsáveis (ou mesmo a formular códigos de conduta quando tal se justifique), bem como proteger tanto os utentes quanto os profissionais de saúde e os gestores de falhas, erros e danos que se possam verificar. Por outro lado permitirá distinguir melhor os objetivos do consentimento informado (que enquadram as lícitas incursões na

privacidade) e as medidas de proteção da confidencialidade a adoptar, entre as quais se incluem a proteção de dados, como adiante se dirá (26).

3.3. Medidas de protecção da confidencialidade

A confidencialidade deve ser uma preocupação e a sua proteção uma prática imperativa, sobretudo por ser considerado um direito individual, cabendo a cada um a decisão sobre a informação pessoal que pretende ver resguardada. De uma forma geral, podemos elencar alguns exemplos de medidas que contribuem para a protecção da confidencialidade, entre as quais se salientam a efectiva aplicação do segredo profissional (22) (que será abordado na secção respectiva *infra* Secção do Segredo Profissional); a pseudonimização e cifragem dos dados, como refere o Regulamento Geral de Protecção de Dados da União Europeia (27), a anonimização dos dados [3], que evita que os dados possam ser relacionados com uma pessoa em particular; a limitação da recolha de dados, procedendo à eliminação adequada dos mesmos quando estes já não são necessários; a limitação ao acesso aos dados apenas às pessoas autorizadas para o efeito; ou a aplicação de processos que garantam que informações pessoais são armazenadas de forma "segura", mediante utilização de meios codificados de controlo de acesso (28).

No domínio da saúde, os desafios à confidencialidade são grandes, e por se tratar de um ambiente onde circulam dados considerados "sensíveis" (ver *infra*, secção do enquadramento normativo), as medidas de proteção da confidencialidade devem ser alvo de grande atenção. Tal como *afirma Beltran-Aroca et al*, *"a informação sobre a saúde não é apenas baseada em observações objectivas, diagnósticos e resultados de testes, mas também em impressões subjectivas sobre o paciente, como o seu estilo de vida, hábitos e actividades"* (29)[4].

Vários são os erros que diariamente se cometem em ambiente hospitalar, que fazem com que se verifiquem falhas ao nível da confidencialidade, e

[3] Os conceitos de pseudonimização e anonimização distinguem-se essencialmente através de um ponto fundamental. A anonimização de dados destrói de forma irreversível qualquer forma de identificação dos dados. Por outro lado, a pseudonimização substitui a identidade do titular dos dados de forma a que sejam necessárias informações adicionais para reidentificar o titular dos dados (80).

[4] Tradução livre da autora. No original, *"Health Information is not only based on objective observations, diagnoses, and test results, but also subjective impressions about the patient, their lifestyle, habits, and recreational activities"* (29).

consequentemente, conduzem a que os pacientes envolvidos fiquem, por essa via, expostos à violação dos seus direitos.

Segundo Villas-Bôas, a violação da confidencialidade pode ocorrer por descuido: *"(...) quão comuns são as conversas de corredores e elevadores sobre as enfermidades dos pacientes atendidos, ou ainda a frequência com que se encontram prontuários sobre balcões com os nomes e diagnósticos à mostra (...)"*, mas também de forma maliciosa, por exemplo, através do acesso indevido ao registo de informações do paciente (30).

Um estudo na área da saúde conduzido por *Beltran-Aroca et al* (29), reflecte também outras situações onde se verificou a violação da confidencialidade, sendo elencadas varias tipologias de falhas como o acesso indevido a registos clínicos, entre os quais resultados de exames e testes, fichas de admissão, entre outros; a divulgação dos dados dos pacientes a outras pessoas, nomeadamente a outros profissionais de saúde que não se encontram envolvidos no respectivo processo do paciente; a divulgação pública pela própria estrutura do hospital dos dados clínicos do paciente. Neste estudo, apurou-se que a falha mais frequente a nível da proteção da confidencialidade, é a divulgação dos dados clínicos a pessoas que não se encontram envolvidas no processo médico do paciente. Concomitantemente, as medidas de segurança necessárias à protecção da confidencialidade, devem incidir, sobretudo, na problemática da divulgação de dados clínicos, a qual pode ser melhorada através da mais frequente formação especializada, alertando para uma maior consciencialização de todos os profissionais de saúde acerca da importância e do dever do sigilo profissional (29).

Com a crescente utilização dos meios informáticos, em particular dos dispositivos móveis, torna-se especialmente necessário adoptar medidas de segurança que diminuam o risco do acesso alheio a informação sensível. Alguns exemplos de medidas relevantes de cariz obrigatório são o uso de uma palavra-passe; a utilização da opção de apagar os dados remotamente, nomeadamente quando o dispositivo é perdido ou em situações de roubo; não utilizar aplicações no dispositivo móvel que permitam o acesso remoto ao mesmo; utilizar sistemas de segurança apropriados sempre que se pretenda enviar ou receber informações de saúde, nomeadamente ao usar redes sem fios públicas e apagar toda a informação do dispositivo caso se pretenda substituí-lo (31).

Várias são as falhas que podem ser evitadas com o cumprimento de regras e com a instrução dos profissionais de saúde acerca da adequada discrição e comportamento no decorrer da sua actividade.

3.3.1. O segredo profissional

Um dos aspectos mais importantes a que se deve atender para preservar a confidencialidade do doente e protegê-lo de qualquer ameaça que diga respeito à violação dos seus dados de saúde, é o sigilo profissional, em particular o sigilo médico.

A relação entre médico e paciente deve assentar e desenvolver-se em total contexto de segurança e confiança, confiança essa que o paciente deposita no seu médico e instituição de saúde, esperando que se respeite o sigilo em relação a todas as informações que lhe digam respeito. Não é novidade que os médicos beneficiam de um contacto muito pessoal com os seus pacientes, e estes, perante a figura do profissional de saúde, quase sempre depositam uma total certeza de que das suas conversas e consequente abertura para facultar toda a informação que lhes seja solicitada, não resultarão efeitos indesejáveis nas suas vidas (7). De facto, no decorrer da prestação de cuidados de saúde, o paciente espera que as informações transmitidas ao seu médico sejam salvaguardadas, sendo dever do médico respeitar tal direito (ver *infra* Enquadramento Normativo).

O paciente encontra-se imbuído do direito ao respeito pela sua autonomia no que diz respeito às suas informações pessoais, tal como afirma Villas-Bôas *"(...) o sigilo ou segredo profissional foi contemporaneamente associado ao princípio bioético da autonomia, uma vez que, pertencendo os dados pessoais ao paciente, apenas ele pode decidir, a priori, a quem deseja informá-los"* (30).

Consequentemente, o cumprimento do sigilo médico (e do segredo profissional) é algo fundamental, na medida em que, se o médico não o cumprir, tal pode ter consequências na relação com o doente. Este último pode mesmo chegar a omitir informações relevantes que podem acabar por influenciar os tratamentos necessários e assim prejudicar o seu estado de saúde (32).

A questão do sigilo médico não se impõe apenas diretamente no que respeita à divulgação de informações sobre os pacientes pelo profissional de saúde. É importante que, numa era onde o desenvolvimento tecnológico tem vindo a

aumentar, se aliem as próprias tecnologias à protecção da privacidade e confidencialidade do utente. Por exemplo, o contacto electrónico entre médico e paciente, muito utilizado nos dias de hoje, em que ambos trocam mensagens por via electrónica contendo diversos factos acerca da saúde do paciente, é um canal mais oportuno, eficaz e privado de comunicação entre ambos. No entanto, este canal aumenta o risco de intercepção indevido dessas comunicações por terceiros. Do balanço entre os aspectos positivos e negativos deste meio de comunicação, resultam novas preocupações ao nível da preservação da confidencialidade e privacidade (33).

O facto de não existir uma segurança adequada na troca de mensagens electrónicas entre médico e paciente, pode fazer com que as mesmas sejam lidas por outras pessoas alheias às questões clínicas. Tal pode acontecer simplesmente porque o médico, por descuido ou mero esquecimento, deixa visível no seu computador mensagens trocadas com os seus pacientes (34). Questão semelhante se coloca em termos de acessos indesejados a um processo clínico inadvertidamente deixado aberto num computador numa instituição e saúde (30).

Embora o sigilo profissional não esteja inerente a todas as actividades profissionais (35), é importante referir que o sigilo profissional, não engloba somente os médicos e os profissionais de saúde, mas todos aqueles que, na sua actividade diária, contactam com dados pessoais ou certo tipo de informações (22). Ainda que o sigilo profissional seja predominantemente entendido em relação aos médicos, este aspeto torna-se particularmente importante em relação aos Gestores/Administradores, uma vez que, para todos os efeitos, são estes que coordenam e orientam as actividades dos hospitais e são os responsáveis últimos pelas medidas de controlo de risco relacionadas com confidencialidade e protecção de dados. Mais um aspecto a salientar sobre a importância do presente estudo o qual objectivou focar esta classe profissional.

3.3.2. A Protecção de Dados

Nos dias de hoje, é cada vez mais frequente a disponibilização de dados por via electrónica a terceiros. A tecnologia permeia a nossa vida e, com a proliferação em particular dos dispositivos móveis, a nossa vida encontra-se cada vez mais

integrada com as tecnologias de informação (36). Neste contexto, a necessidade de recorrer a medidas de protecção da confidencialidade tornou-se cada vez mais emergente. Nesse sentido, a protecção de dados por via regulamentar e legal é assim fundamental para garantir o respeito pelos direitos e liberdades fundamentais dos cidadãos.

Ao abordar a temática relativa à protecção de dados, justifica-se distinguir os conceitos de "dados" e de "informação".

Numa era em que cada vez mais os nossos dados se encontram armazenados de forma electrónica, permitindo o acesso mais facilitado a um maior número de pessoas, convém clarificar a diferença entre os dados propiamente ditos e, numa fase posterior, a informação que decorre dos mesmos.

Os primeiros constituem uma forma mais ampla e fragmentada de informação, concentrando-se em elementos na sua forma mais primitiva, antecedida da fase de informação propriamente dita. Por outro lado, a informação consiste na interpretação que surge após a análise realizada aos dados. Nesta fase depreende-se que o nível de incerteza seja menor comparativamente ao que acontece somente na recolha e observação dos dados, sem qualquer tipo de interpretação (37).

Torna-se igualmente pertinente proceder à definição de dados pessoais, sendo que estes são definidos, segundo o RGPD da UE, como sendo "informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados") (27). Note-se desde já que, segundo o RGPD da UE, é em princípio *"proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos, para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"* (27).

Sem prejuízo do que se dirá adiante na secção dedicada ao enquadramento normativo, torna-se relevante indicar, desde já, os principais marcos histórico-normativos em matéria de protecção de dados, tal como consta da tabela seguinte:

Ano	
1948	Declaração Universal dos Direitos do Homem
1950	Convenção Europeia dos Direitos do Homem
1970	Introdução da primeira lei moderna de privacidade pelo estado Alemão (“modern privacy law”)
1973-1974	Criação do *Data Act*, primeira lei nacional de privacidade (Suécia) Resoluções 73/22 e 74/29, contendo princípios para a protecção de dados pessoais nos sectores público e privado respectivamente
1979	Promulgação das leis gerais de protecção de dados (Áustria, Dinamarca, França, Alemanha, Luxemburgo, Noruega e Suécia)
1980	*Guidelines* OCDE sobre a Protecção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais
1981	Convenção do Conselho da Europa para a Protecção das Pessoas relativamente ao Tratamento Automático de Dados Pessoais (Convenção 108)
1995	Directiva 95/46/CE relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.
2000	Directiva 2000/31/CE relativamente a aspectos legais dos serviços da sociedade de informação, em especial do correio electrónico Carta dos Direitos Fundamentais da UE
2001	Protocolo Adicional à Convenção 108 para a protecção dos indivíduos no que respeita ao Processamento Automático dos Dados Pessoais relativo às autoridades de supervisão e fluxos de dados transfronteiriços
2002	Directiva 2002/21/CE, com o objectivo de garantir a coerência entre todos os Estados Membros relativamente a serviços de comunicações electrónicas

	Directiva 2002/58/CE, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas
2006	Directiva 2006/24/CE relativa à conservação de dados gerados ou tratados respeitantes a comunicações electrónicas
2007	Tratado de Lisboa
2009	Directiva 2002/58/CE relativa ao tratamento de dados pessoais e à protecção da privacidade nas comunicações electrónicas

Tabela 1 – Marcos históricos relativos à Protecção de Dados
Adaptado de *Origins and Historical Context of Data Protection Law*, de Sian Rudgard.

Tal como anteriormente referido, cada vez mais é utilizada a tecnologia como forma de armazenar os dados pessoais, nomeadamente o que acontece no campo da saúde. Neste âmbito, recomenda-se a utilização de técnicas de protecção de dados, incluindo dados em movimento ("data at flow") e dados em repouso ("data at rest"), a "autenticação" dos dados, que permite ao usuário confirmar de forma segura a sua identidade, estabelecendo formas de verificar que é o próprio que se encontra a aceder a determinadas informações; a "autorização" ou "controlo de acesso", ou seja o registo de que aquele usuário já autenticado, possui as devidas credenciais para aceder a determinada informação; a "encriptação de dados", que de uma forma geral tem como principal função garantir o impedimento de acesso não autorizado a dados pessoais, devendo este sistema ser o mais eficiente possível e de fácil compreensão tanto para os utentes como para os profissionais de saúde; o "mascaramento" de dados, que visa retirar a identidade dos dados pessoais, nomeadamente o nome e data de nascimento, permitindo assim o tratamento de dados de forma mais facilitada, com um nível mais reduzido de controlo de segurança, e evitando que seja possível a identificação do indivíduo a quem os dados dizem respeito (38).

3.4. A confidencialidade e a protecção de dados em saúde e o impacto nas organizações de saúde

Os dados pessoais médicos ou dados de saúde, são considerados dados "sensíveis" por pertencerem à esfera mais íntima da pessoa, razão pela qual está, em princípio, proibido o seu tratamento e qualquer devassa ou violação deste tipo de dados é considerada mais grave (artigo 7.º da LPD e artigo 9.º do RGPD). Os dados e, concomitantemente, a informação relativa à saúde da pessoa, são desta forma, considerados algo muito íntimo, devendo existir mecanismos mais estritos que assegurem a sua protecção: "os dados médicos e genéticos são considerados dados excepcionalmente sensíveis pelas leis actuais de protecção de dados, contendo um status especial que requer medidas adicionais de protecção, de segurança e confidencialidade" (1).

Antes de nos debruçarmos sobre estes conceitos numa perspetiva jurídica, importa referir que, em Portugal, os dados e informações de saúde, como sejam dados clínicos registados, resultados de análises, exames e demais processos clínicos, pertencem à própria pessoa (artigo 3.º nº1 da Lei nº 12/2005 de 26 de Janeiro relativa à informação genética pessoal e informação de saúde), funcionando as unidades prestadoras de cuidados de saúde como "armazéns" dessa mesma informação (39).

A problemática de violação deste tipo de dados agrava-se quando os próprios hospitais são considerados lugares "devassáveis", nomeadamente por se tratarem de locais partilhados e de fácil acesso a inúmeras pessoas internas e externas às organizações de saúde.

O principio da confiança, no campo da saúde, constitui um dos principais alicerces éticos e jurídicos, pois estão em causa dados sensíveis transmitidos deliberadamente ao profissional de saúde (40). No entanto, considerando a extensão actual da quantidade e tipo de dados e informação que é armazenada ao longo da cadeia de valor da prestação de cuidados de saúde, que envolve não apenas o médico e o paciente, mas também seguradoras, prestadores subcontratados, entidades empregadoras, entre muitos outros, já não se trata apenas de proteger a informação na relação médico-paciente (25).

As organizações de saúde, por lidarem diariamente com grandes quantidades de dados e informação relevante, devem optar por criar e implementar

estratégias que possam fazer face a falhas na segurança desses mesmos dados. Para esse fim, deve recorrer-se a políticas, processos e tecnologias que reduzam significativamente o risco de possíveis violações.

Um estudo conduzido por *Kirimlioglu*, demonstrou a importância da protecção de dados e informação de saúde. O referido estudo, intitulado "*The right to privacy and the patient´s views in the context of the personal data protection in the field of health"*, explora as opiniões de pacientes num Hospital Universitário na Turquia, relativamente a questões de privacidade e confidencialidade, no qual se constatou que quase a totalidade dos utentes concordam que o respeito pela privacidade no que toca às suas informações de saúde constitui um direito seu (41). Posteriormente, constatou-se também que os pacientes se sentem mais confortáveis quando lhes são apresentados os seus direitos relativamente à protecção dos seus dados de saúde e garantias que a organização de saúde lhes proporciona com vista à protecção dos seus dados (28). Adicionalmente, verificou-se ainda que a comunicação de políticas e processos claros e transparentes relativamente ao tratamento e protecção dos dados de saúde contribuem para uma percepção de mais elevado nível de qualidade dos serviços de saúde que são prestados (42).

Tal como anteriormente referido, os profissionais de saúde têm acesso às mais variadas informações ao nível da saúde física e mental dos pacientes, pelo que essas mesmas informações devem ser protegidas e não existir qualquer tipo de divulgação das mesmas sem o conhecimento e autorização dos titulares (43).

As barreiras à proteção da confidencialidade, em meio hospitalar, podem ser enfraquecidas em diversas situações, como por exemplo, quando se trata de casos de internamento, onde a posição do paciente é mais vulnerável e onde o aspecto da privacidade pode estar mais em causa tanto para o mesmo como para os profissionais de saúde que se devem esforçar por respeitar o paciente e ter em conta a sua posição mais fragilizada nesse momento (44). Adicionalmente**,** nas situações relativas a internamento hospitalar, as duas dimensões de privacidade que são consideradas como as mais afectadas correspondem à parte física bem como a toda a informação relativa à pessoa que se encontra internada (45).

O desrespeito pela privacidade aquando de um internamento, pode assumir diversos ângulos, como seja a presença de alguém em oposição da vontade do

paciente, o exame do paciente pelo profissional de saúde sem a permissão deste, entre outros aspectos relevantes (42).

Dada a natureza da sua actividade, o sector da saúde recolhe grandes volumes de dados pessoais com vista a prossecução dos serviços que presta aos pacientes (46). Assim sendo, projeta-se que a entrada em vigor do RGPD irá impactar de forma significativa a gestão e tratamento de dados dos pacientes nas organizações em geral, mas em particular nas organizações de saúde e nos hospitais (47).

De acordo com a pesquisa efectuada, decidimos organizar a análise do impacto do RGPD nas organizações de saúde em torno de cinco grandes áreas: (1) Recolha e armazenamento de dados pessoais, (2) Perfis dos pacientes e fragmentação de dados, (3) Implementação dos novos direitos dos pacientes, (4) Utilização de novas fontes de dados e melhoria da prevenção e tratamento através de análise de dados e (5) Sensibilização e formação dos profissionais do sector da saúde.

Recolha e armazenamento de dados pessoais

Segundo o RGPD, "o responsável pelo tratamento ou o subcontratante deverá conservar registos de actividades de tratamento sob a sua responsabilidade. Os responsáveis pelo tratamento e subcontratantes deverão ser obrigados a cooperar com a autoridade de controlo e a facultar-lhe esses registos, a pedido, para fiscalização dessas operações de tratamento (Considerando nº 82 do RGPD). Tal implicará necessariamente que as organizações de saúde deverão inventariar e compreender em detalhe os processos de recolha de informação dos pacientes e onde essa informação é armazenada. Este requisito não afeta apenas os registos digitais, mas qualquer tipo de registo onde constem dados pessoais, por exemplo, os registos em papel.

A maioria das organizações de saúde não possui um catálogo de processos organizado (48), que identifique de forma clara e detalhada, as atividades, intervenientes e plataformas informáticas que suportam os vários processos. No sector financeiro, por exemplo, a existência de catálogos de processos é um requerimento regulamentar, sendo obrigatória a sua existência como matriz onde assentam os processos de controlo interno, auditoria e *compliance* (49).

Concomitantemente, o RGPD obrigará as organizações de saúde a apetrecharem-se com este tipo de técnicas e metodologias, incrementando significativamente a maturidade de gestão dos seus processos. No futuro, qualquer organização de saúde, deverá manter permanentemente actualizado um catálogo de processos, onde serão identificados os pontos de recolha, tratamento e armazenamento de dados, os dados tratados, respectivos intervenientes (pessoal médico e administrativo) e suportes informáticos (aplicações, bases de dados). Essa informação deverá estar disponível para a gestão interna dos processos e sistemas, mas também para auditorias e reporte regulamentar (50).

Perfis dos pacientes e fragmentação de dados

Considerando a cadeia de valor do sector da saúde, que agrega múltiplos intervenientes e entidades independentes que se conjugam para prestar cuidados de saúde aos pacientes, os dados de pacientes que são recolhidos encontram-se significativamente fragmentados (51). Tomemos o exemplo de um paciente que se dirija a um hospital para uma consulta, a quem sejam prescritos vários exames e que posteriormente seja observado por um especialista e encaminhado para uma cirurgia. Ao longo desta cadeia de intervenientes serão recolhidos e armazenados dados, conduzindo à fragmentação dos dados existentes sobre esse paciente.

Um dos elementos chave do novo RGPD, será a necessidade de prestar ao paciente toda a informação sobre o propósito e localização dos dados que serão recolhidos sobre este (Capítulo III do RGPD, artigo12.º). Adicionalmente, o paciente terá o direito de transferir os seus dados para outras entidades ou de redefinir a qualquer momento quem poderá aceder à sua informação (27).

Estes requisitos incentivarão as entidades que prestam serviços ao longo da cadeia de valor a afastarem-se do modelo actual em que cada entidade recolhe e armazena a informação, mas passe a favorecer um modelo mais centralizado de armazenamento do perfil de saúde dos pacientes, onde todas as entidades acedem mediante os direitos de acesso que lhe sejam atribuídos pelos pacientes e contribuem com informação relativa ao serviço que prestam.

A Estónia foi o país pioneiro em 2008 no lançamento do primeiro registo estatal de saúde, desde o nascimento até a morte (52). Neste país, todos os actos

médicos são indexados a este registo centralizado e o seu armazenamento é realizado numa plataforma informática estatal. A implementação das mencionadas disposições do RGPD é muito facilitada neste modelo mais centralizado de armazenamento do perfil dos pacientes. Também em Portugal se dão actualmente os primeiros passos no sentido de um registo centralizado de informação de saúde (RSE – Registo de Saúde Electrónico). Este registo visa a reunir informação essencial de cada cidadão para a melhoria da prestação de cuidados de saúde e é constituído por dados clínicos recolhidos electronicamente para cada cidadão e produzidos por entidades que prestam cuidados de saúde. À semelhança do registo de saúde que encontramos na Estónia, o RSE permite o registo e partilha de informação clínica entre o utente, profissionais de saúde e entidades prestadoras de serviços de Saúde, de acordo com os requisitos da Comissão Nacional de Proteção de Dados (Autorização n.º 940/2013) (53).

Implementação dos novos direitos dos pacientes

Tal como anteriormente referido, a área da saúde é muito sensível e privada. No entanto, presentemente, os resultados de exames médicos são amplamente partilhados com vista a conseguir um diagnóstico adequado, sendo proporcionada aos pacientes muito pouca informação e controlo sobre como esses dados são recolhidos, transmitidos e armazenados, ou sobre quem tem acesso à informação recolhida (54). O novo RGPD coloca os pacientes firmemente no controlo dos seus dados, atribuindo-lhes o direito de saberem a qualquer momento, por exemplo, quem tem acesso aos seus dados, ou a "serem esquecidos" por quem detém os seus dados (27).

Estes requerimentos obrigarão as organizações de saúde a recolherem, não apenas os dados dos pacientes, mas também um conjunto de meta-dados relacionados, como por exemplo, quem tem acesso, onde estão armazenados, qual o fim desses dados. Adicionalmente, esses meta-dados terão que ser geridos através de novos processos de gestão da informação que as organizações de saúde, como outras organizações, terão que implementar (50). Finalmente, no caso das organizações de saúde, será mesmo necessária a criação de novas estruturas orgânicas, como seja o Responsável pelo Dados Pessoais, a quem serão acometidas responsabilidades não apenas jurídicas,

mas também operacionais, que cruzarão toda a organização (27). Responder aos desafios do RGPD requer esforços multidisciplinares nas organizações de saúde, envolvendo desde os especialistas jurídicos, aos especialistas de processos, os sistemas de informação e as unidades operacionais administrativas e clínicas.

Utilização de novas fontes de dados

De acordo com o "Future Health Index" (55), 57% dos pacientes nos Estados Unidos da América já utilizam um dispositivo conectado ("connected care device") para monitorar vários indicadores de saúde e 33% destes já partilham esta informação com os seus médicos. A proliferação destas novas fontes de informação de saúde é uma tendência que tem vindo a acelerar recentemente (56) e que tem proporcionado avanços significativos nas técnicas de prevenção. Adicionalmente, os pacientes e profissionais do sector da saúde utilizam crescentemente as redes sociais para trocar informação entre si (57).

As disposições do RGPD colocam um entrave muito relevante à utilização destes novos meios tecnológicos e fontes de informação, obrigando as organizações de saúde a colaborar com as empresas do sector tecnológico com vista à criação de soluções que, por exemplo, mantenham os dados dos pacientes em território da UE. Adicionalmente, será necessário um esforço de sensibilização e formação relevante dos profissionais do sector da saúde de que falaremos mais adiante (58).

Melhoria da prevenção e tratamento através de análise de dados

No âmbito da UE, foram lançadas as denominadas "European Reference Networks" (ERNs), que visam a promoção de cuidados de saúde multinacionais, especialmente para a pesquisa e tratamento de doenças raras (59). As ERNs assentam no princípio de partilha de conjuntos de dados de vários países europeus, com vista à geração de novas descobertas clínicas, genéricas, comportamentais e ambientais. A maioria da informação e dos dados recolhidos ao longo de décadas pelas organizações de saúde encontra-se ainda desestruturada e inacessível. Através de novas técnicas de "big data", é agora possível gerar novos conhecimentos e descobertas a partir dessa informação (60).

Este é um exemplo concreto sobre o valor da partilha de dados e utilização de novas técnicas de análise de dados que necessitarão de um novo enquadramento ao abrigo do RGPD. Neste novo contexto regulamentar, as organizações de saúde necessitarão de criar novos processos e ferramentas para a utilização de dados para a investigação científica ou a partilha desses dados com outros fins que não seja o tratamento do paciente.

Sensibilização e formação dos profissionais do sector da saúde

Todos os aspetos anteriormente elencados irão exigir um grande esforço de mudança de atitudes e comportamentos dos profissionais da área da saúde. Este esforço deverá incidir sobre a clara definição dos novos comportamentos desejados, comunicação e avaliação frequente e criação de incentivos e consequências (61).

3.5. Desafios colocados pelo progresso tecnológico à protecção de dados de saúde

As tecnologias de informação e comunicação cada vez mais fazem parte da vida das pessoas e estão cada vez mais presentes no decorrer das suas actividades diárias, em particular no campo da saúde (62). Se por um lado, a informatização foi algo que trouxe inúmeras vantagens, como o fácil e mais eficiente acesso à informação, o tratamento massivo de dados e a comunicação em tempo real da informação, permitindo a aceleração do desenvolvimento do conhecimento, da pesquisa e investigação, deixou uma porta aberta a diversos riscos e perigos, que cada vez mais assombram a sociedade.

A par da expansão exponencial da utilização da tecnologia na sociedade em geral e na área da saúde em particular, segundo *Raab e Szekely*, existem também questões relacionadas com o nível cada vez mais avançado da própria tecnologia utilizada (63).

Segundo os mesmos autores, no artigo intitulado "*Data Protection authorities and information technology"*, publicado em *Computer Law and Security Review*, em 2017, constatou-se que o conhecimento ao nível das Tecnologias de Informação e Comunicação (TIC) pelos profissionais de saúde em matéria de protecção de dados não era satisfatório, e que por essa razão seria imprescindível recorrer a profissionais externos especializados nas tecnologias de informação (63). No

mesmo estudo, foram igualmente elencadas as razões consideradas importantes para o aumento de conhecimento nesta área, entre as quais, o facto do conhecimento ao nível das TIC ter de estar constantemente presente no decorrer das suas actividades e não apenas quando é necessário para resolver um determinado caso. Adicionalmente as referidas autoridades devem ter uma preocupação permanente na determinação oportuna do impacto que determinado avanço tecnológico possa ter ao nível da informação e da sua protecção (63).

Se por um lado, os registos electrónicos de saúde trouxeram inúmeras vantagens ao nível da facilidade de partilha de informações e de uma maior facilidade na tomada de decisões clínicas, por outro lado, vieram criar uma ameaça no que respeita à privacidade. A informação passou a ser acessível a diversas pessoas, ao contrário do que acontecia anteriormente com os registos clínicos em papel, que apenas estavam acessíveis a um número restrito de pessoas (64).

Segundo Gonçalves e Raimundo, acerca da actual reforma legal em matéria de protecção de dados pessoais, referem que *"(...) não está claro que essa reforma legal está à altura do desafio dos desenvolvimentos tecnológicos actuais, particularmente à medida que as chamadas tecnologias big data avançam."* (65).

O aumento da informação disponibilizada electronicamente por parte dos profissionais de saúde tem aumentado em larga escala, devido às suas inúmeras vantagens e baixos custos (62), tornando possível que pessoas dentro do hospital, que não sejam directamente responsáveis por um determinado paciente, possam ter acesso facilitado à informação sobre o mesmo, como sejam dados de saúde e outras informações de carácter pessoal (66).

Segundo o Conselho Nacional de Ética para as Ciências da Vida, os principais riscos que podem ocorrer quando a informação acerca de dados de saúde é mantida electronicamente são (67):

i) Fuga de informações, por acessos indevidos e mal-intencionados;
ii) Utilizações para investigação científica sem o conhecimento dos titulares dos dados;
iii) Transferência ilícita de informações respeitantes a dados de saúde;
iv) Perda de confidencialidade dos dados pelo facto de haver uma falha na supervisão do acesso aos mesmos;

A informação mantida electronicamente, apresenta então algumas desvantagens, que podem traduzir-se em sérios riscos para os titulares dos dados, como sejam, por exemplo, o facto de haver uma grande quantidade de informação sensível agregada num mesmo repositório electrónico, ou o perigo de perda de controlo da informação pelos profissionais de saúde, uma vez que, na maioria dos casos, o controlo de acesso existente potencia fugas de informação, quer por parte de profissionais internos ou de pessoas externas (68).
Um estudo conduzido por *Li et al* analisou como as informações de saúde se tornam mais vulneráveis com a utilização das novas tecnologias, como sejam os registos médicos electrónicos e a utilização de aplicações médicas para médicos e pacientes (62). O estudo focou, por um lado, a forma como as informações de uma dada pessoa podem ser usadas comprometendo assim a privacidade da mesma, e por outro lado, a forma como a pessoa pode ser identificada através das informações disponíveis a seu respeito. Este mesmo estudo consistiu na análise de um caso real em que, através do cruzamento de informações sobre a pessoa em causa, em duas redes pessoais médicas, nomeadamente informações sobre a saúde do paciente e outro tipo de informação do foro privado, a pessoa veio a ser identificada. Concluiu-se também que mesmo nos casos em que não se possuam as informações completas de saúde de uma pessoa, foi possível identificar o titular da informação através do cruzamento de outras fontes de informação externas, por exemplo quando certos dados de saúde são publicados (62).
Por outro lado, o autor assinala também as muitas vantagens da adopção destas tecnologias no sector da saúde, como a maior eficácia e rapidez no acesso aos dados e a fácil partilha de informações relacionadas com o cuidado médico, permitido um melhor tratamento (62).
Tal como indicado, existem claras vantagens em armazenar os dados pessoais médicos em suporte electrónico. Contudo, será também necessário tomar as medidas adequadas a redução do risco de ameaça de violações da informação e privacidade dos pacientes, como sejam, incrementar o grau conhecimento dos profissionais de saúde sobre a lei em matéria da preservação de dados, requisitar profissionais de tecnologia que indiquem até que ponto é fiável registar, através de meios electrónicos, certo tipo de informação, envolver especialistas em segurança electrónica para que estes possam avaliar a

ocorrência de possíveis ameaças a segurança dos dados e disponibilizar aos profissionais de saúde os instrumentos e ferramentas necessárias (69).
Neste âmbito, torna-se fulcral que os dados pessoais, nomeadamente os dados de saúde, vejam a sua protecção assegurada sobretudo pelo recurso crescente das tecnologias.

3.6. Protecção de dados: enquadramento normativo

Nesta secção, sintetizam-se as principais normas de direito internacional, direito da União Europeia, bem como do direito nacional, em matéria de protecção de dados.

3.6.1 Direito Internacional

No que diz respeito ao Direito Internacional, a consagração da privacidade como direito fundamental do Homem, que deve ser respeitado em igualdade com os outros direitos, encontra-se consagrado na Declaração Universal dos Direitos do Homem de 1948 (70) contemplando, desta forma, o direito à vida privada, no artigo 12.º, sendo referido que o ser humano tem o direito de não sofrer de intromissões na sua vida privada e familiar, bem como questões relativas a intromissões ao seu domicílio, correspondência, ataques à sua honra e reputação, sendo que contra estes tipos de intromissões, as pessoas possam ver a sua protecção assegurada pela lei.
A Convenção Europeia dos Direitos do Homem, adoptada em 1950, consagra igualmente o direito à privacidade o qual se encontra contemplado no artigo 8º, contendo os mesmos princípios que os descritos na Declaração Universal dos Direitos do Homem, envolvendo o direito pelo respeito relativo à vida privada e familiar, domicílio e correspondência.
Por outro lado, a Convenção de Oviedo, também denominada como a Convenção para a Protecção dos Direitos do Homem e da Dignidade do Ser Humano face às Aplicações da Biologia e da Medicina , é relativa a questões relacionadas com as aplicações da Biologia e da Medicina (71). Este documento, comporta no seu Capítulo III, no artigo 10.º, o direito à vida privada e direito à informação, relativamente a questões relacionadas com a saúde. No presente artigo, é referido que todas as pessoas têm o direito, por um lado, ao respeito

pela sua vida privada, no que respeita a informações acerca da sua saúde, e por outro, o direito que a pessoa tem em conhecer todas as informações que incidam sobre a sua saúde e caso contrário, o direito de não querer ter essa mesma informação deve ser igualmente respeitado.

Com o objectivo de estabelecer normas para a investigação médica nos seres humanos, foi criada a Declaração de Helsínquia de 1964 (11), dando principal destaque ao "material humano" que possa ser identificável. Neste documento é referido que é dever do profissional de saúde agir segundo os interesses do doente, nomeadamente quando se trata de investigação médica, podendo desta forma garantir a segurança do mesmo. A Declaração é primeiramente dirigida aos médicos, sendo que outros participantes em investigações médicas devem igualmente respeitar os princípios presentes na mesma Declaração. A matéria de privacidade encontra-se contemplada no princípio 24.º, o qual refere que devem ser tidas em conta todas as precauções necessárias a fim de proteger a privacidade das pessoas no que respeita à investigação, bem como a confidencialidade dos seus dados pessoais. Também é referido, no princípio 9.º, que é dever do médico, que participe em investigações médicas, respeitar a privacidade e a confidencialidade de informações pessoais acerca do participante, sendo que a responsabilidade da participação deve ser atribuída ao médico ou a outro profissional de saúde envolvido e nunca ao sujeito da participação.

3.6.2 Direito da União Europeia

Relativamente à União Europeia, devemos começar por referir a Carta dos Direitos Fundamentais da UE que, consiste numa Carta onde se encontram contemplados os direitos humanos, sendo formalmente adoptada em 2000. A carta encontra-se dividida em seis partes, as quais, dignidade, liberdades, igualdade, solidariedade, cidadania e justiça. A privacidade encontra-se contemplada no artigo 7.º (Capítulo II), onde é mais uma vez referido o direito à vida privada e familiar e no artigo 8.º (Capítulo II) refere-se a matéria correspondente à protecção dos dados pessoais, no qual se diz que todas as pessoas devem ver os seus dados pessoais protegidos e que estes devem ser tratados licitamente e com o consentimento do titular dos dados.

No que respeita a Directivas, temos em consideração a Directiva 95/46/CE, de 24 de Outubro de 1995, revogada agora pelo novo Regulamento Geral de Protecção de Dados. Esta diz respeito à protecção das pessoas singulares no que respeita ao tratamento de dados pessoais e à livre circulação desses dados. Importa referenciar também o Tratado de Lisboa (composto pelo Tratado sobre o Funcionamento da União Europeia (TFUE) e Tratado da União Europeia (TUE)), que entrou em vigor em dezembro de 2009, e que se deve ter como referência em matéria de protecção de dados o seu artigo 16.º do TFUE, no qual se encontra contemplado que todas as pessoas têm direito à protecção dos dados pessoais que lhe digam respeito. O número 2 do mesmo artigo refere que *"O Parlamento Europeu e o Conselho, deliberando de acordo com o processo legislativo ordinário, estabelecem as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União, bem como pelos Estados-Membros no exercício de actividades relativas à aplicação do direito da União, e à livre circulação desses dados."*.

No TUE, encontra-se contemplado no artigo 39.º que *"(...) o Conselho adopta uma decisão que estabeleça as normas relativas à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelos Estados-Membros no exercício de actividades relativas à aplicação do presente capítulo, e à livre circulação desses dados (...)."*.

Regulamento geral de Protecção de Dados (RGPD)

As leis de protecção de dados da UE desde há muito que são consideradas a referência a nível mundial. No entanto, devido ao constante progresso tecnológico que tem vindo a transformar as nossas vidas de formas que nunca antes tínhamos sequer imaginado, surgiu a necessidade de uma revisão profunda das regras de protecção de dados (72). Tal revisou tomou a forma de um novo diploma jurídico comum, capaz de regulamentar os aspectos respeitantes à protecção de dados em toda a União Europeia: o Regulamento Geral sobre a Protecção de Dados.

Perante um novo quadro normativo relativo à protecção de dados, todo o espaço da União Europeia passa a ter um ordenamento comum ao nível desta matéria. O RGPD estabelece regras relativas à protecção de dados das pessoas

singulares, no que concerne aos seus dados pessoais, defendendo assim os seus direitos e liberdades fundamentais, tratando de aspectos como os direitos dos titulares dos dados acerca do tratamento dos mesmos, os riscos e medidas de segurança do tratamento dos dados, a licitude do tratamento, entre outros aspectos relevantes que aqui serão considerados. O RGPD revoga a Directiva 95/46/CE estabelecida em 1995 e é legalmente aplicável em todos os Estados Membros.

Adoptado a 27 de abril de 2016, o novo RGPD é aplicável a qualquer entidade que reúna em si funções de tratamento ao nível dos dados pessoais, sendo aplicável, como já anteriormente referido, a todo o território da União Europeia. Contudo, é referido no Regulamento que a aplicação do mesmo pode ser extensível a entidades fora da UE que realizem operações de tratamento de dados pessoais. Neste âmbito, torna-se relevante abordar a aplicação material e territorial do novo Regulamento. A aplicação material do RGPD encontra-se contemplada no artigo 2.º, onde é referido no seu nº1 que o Regulamento se aplica "(...) *ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados*".

No artigo 3.º, encontra-se contemplada a aplicação territorial do RGPD, onde é referido, no seu nº1 que "*o presente regulamento aplica-se ao tratamento de dados pessoais efectuado no contexto das actividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União*".

De seguida, irão ser apresentadas as definições mais importantes constantes no RGPD (artigo 4.º), bem como os direitos dos titulares (artigo 12.º, Capítulo III), deveres dos responsáveis pelo tratamento de dados e sanções aplicáveis aquando do não cumprimento das normas constantes no Regulamento.

Definições-Chave do RGPD

Segundo o RGPD da UE, entende-se por dados pessoais toda a "informação relativa a uma pessoa identificada ou identificável ("titular dos dados") (...) sendo que, é também mencionado que uma pessoa considerada identificável corresponde a uma pessoa que "(...) *possa ser identificada, directa ou*

indirectamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização (...)" (artigo 4.º, nº 1))

Consta igualmente no Regulamento a definição de tratamento de dados, o qual é definido como sendo "*uma operação ou um conjunto de operações efectuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o 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 comparação ou interconexão, a limitação, o apagamento ou a destruição*" (artigo 4.º, nº 2).

Segundo o RGPD, o responsável pelo tratamento de dados pessoais corresponde à "*pessoa singular ou colectiva, a autoridade pública, a agencia, ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais* (...)" (artigo 4.º, nº 7).

Uma outra definição-chave no RGPD corresponde aos "dados relativos à saúde", que são definidos como sendo "*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*" (artigo 4.º, nº 15).

Direitos dos Titulares

Um dos pontos-chave do RGPD, assenta nos direitos dos titulares dos dados contemplado no Capítulo III do mesmo. No artigo 13.º, respeitante ao direito à informação são referidas quais as informações que o responsável pelo tratamento de dados deve facultar ao titular dos mesmos, entre elas a identidade e os contactos do responsável pelo tratamento (a)), as finalidades do tratamento a que os dados pessoais se destinam bem como o fundamento jurídico para o tratamento (c)), o prazo de conservação dos dados pessoais (nº2, a)). Um outro direito presente assenta no direito de acesso do titular dos dados, consagrado no artigo 15.º, no qual é referido que o mesmo tem o direito de aceder a informações como as finalidades do tratamento de dados (nº1,a)), as categorias de dados pessoais em causa (nº1,b)), o prazo previsto de conservação dos dados pessoais (nº1,d)), entre outros.

Importa ainda referir o direito de rectificação dos dados, contemplado no artigo 16.º, onde é referido que o titular tem o direito de obter a rectificação dos seus dados pessoais que lhe digam respeito. No artigo 17.º encontra-se contemplado o direito ao apagamento dos dados, onde se encontra mencionado que o titular dos dados tem o direito de obter o apagamento dos mesmos sem demora injustificada, quando nomeadamente, os dados deixaram de ser necessários para a finalidade que justificou a sua recolha ou tratamento (nº1,a)), o titular retira o consentimento relativamente ao tratamento dos seus dados pessoais (nº1,b)), quando os dados foram tratados de forma ilícita (nº1, d)), entre outros motivos. Ainda no âmbito dos direitos dos titulares dos dados, pode ainda ser referido o direito à limitação do tratamento, consagrado no artigo 18.º, o qual refere que o titular dos dados tem o direito de obter a limitação do tratamento dos mesmos nomeadamente quando o tratamento for ilícito (nº1,b)) ou quando o responsável pelo tratamento já não precisar dos dados para fins de tratamento (nº1, c)). Importa ainda referir o direito à portabilidade de dados, contemplado no artigo 20.º, no qual é referido que o titular dos dados tem o direito de receber os dados pessoais que lhe digam respeito e que tenha fornecido, num formato estruturado, de uso corrente e de leitura automática.

Deveres e procedimentos dos responsáveis pelo tratamento de dados

Uma outra questão importante presente no RGPD diz respeito à licitude do tratamento, que se encontra contemplado no artigo 16.º, onde é referido que o tratamento de dados só é considerado lícito quando se verifique algumas condições, como é o caso do consentimento expresso do titular dos dados (nº1, a)), quando o tratamento for necessário para o cumprimento de uma obrigação jurídica (nº1, c)), quando o tratamento for necessário para a defesa de interesses vitais do titular dos dados (nº1, d)), entre outras.

Torna-se fulcral mencionar a questão do consentimento do titular dos dados, definido no presente Regulamento como sendo *"uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou acto positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objecto de tratamento"* (artigo 4.º, nº11). No âmbito do consentimento, torna-se relevante mencionar o artigo 7.º referente às condições aplicáveis ao consentimento. No referido artigo é mencionado nomeadamente

que, quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos mesmos (nº1, a)), entre outras condições.

No âmbito do tratamento de dados, há dados que não podem ser sujeitos ao tratamento, denominados como *"dados sensíveis"*, o que se encontra contemplado no artigo 9.º, nº1, que refere que é *"proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa"*.

Um dos outros pontos-chave do Regulamento, diz respeito à avaliação de impacto e consulta prévia antes de se proceder ao tratamento dos dados, que se encontra contemplado no artigo 35.º. Este artigo refere que quando um tipo de tratamento utilizar novas tecnologias e for susceptível de implicar um risco elevado para os direitos dos titulares dos dados, torna-se importante realizar uma avalização de impacto antes de se proceder ao tratamento dos mesmos.

Sanções aplicáveis

Outro dos pontos-chave do Regulamento diz respeito às sanções aplicadas aquando do não cumprimento das disposições do mesmo. Estas constam no artigo 58.º nº2, de entre as quais advertências, repreensões, retirada da certificação, bem como uma coima de 20.000.000 de euros ou até 4% do volume de negócios anual a nível mundial, consoante o valor mais elevado. Considerando a gravidade das sanções e coimas contempladas no RGPD, devemos ter então especial atenção ao tratamento dos dados sensíveis relativos a saúde, estando especificamente contemplado no RGPD que *"todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. O que precede inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação, conforme referido na Diretiva 2011/24/UE do Parlamento Europeu e do Conselho (9), a essa pessoa singular; qualquer número, símbolo ou sinal particular*

atribuído a uma pessoa singular para a identificar de forma inequívoca para fins de cuidados de saúde; as informações obtidas a partir de análises ou exames de uma parte do corpo ou de uma substância corporal, incluindo a partir de dados genéticos e amostras biológicas; e quaisquer informações sobre, por exemplo, uma doença, deficiência, um risco de doença, historial clínico, tratamento clínico ou estado fisiológico ou biomédico do titular de dados, independentemente da sua fonte, por exemplo, um médico ou outro profissional de saúde, um hospital, um dispositivo médico ou um teste de diagnóstico in vitro". (Considerando 35)

3.6.3 Direito Nacional

No que respeita ao enquadramento normativo português, deve começar por referir-se que a CRP prevê, no seu artigo 1.º, o direito à dignidade humana e seguidamente o artigo 25.º, correspondente ao direito à integridade pessoal, no qual se encontra referido que a integridade física e moral do indivíduo é inviolável (nº1). A CRP contempla, no seu artigo 26.º nº1, diversos direitos pessoais, nomeadamente o direito à reserva da intimidade da vida privada e protecção legal e no n.º2, a existência de medidas legais contra a obtenção e utilização abusiva de informações de carácter pessoal. Diretamente relacionado com o direito à vida privada, pode referir-se também o artigo 34.º, respeitante à inviolabilidade do domícilio e da correspondência, referindo que tanto o domicílio como o sigilo da correspondência e de outros meios de comunicação são considerados como sendo de carácter inviolável. Ainda no âmbito da CRP, no artigo 35.º, n.º1, é referido que todas as pessoas têm o direito de aceder aos seus dados informatizados que lhe digam respeito, no n.º2, as condições que se aplicam ao tratamento de dados pessoais, no nº3 é referida a proibição da utilização da informática destinada ao tratamento de dados pessoais e, no n.º4, a proibição do acesso a dados pessoais de terceiros, salvo algumas excepções contempladas pela lei. Por fim, a CRP prevê, no seu artigo 64.º o direito à protecção da saúde bem como o dever de a promover e defender (73).

No que concerne à Lei de Bases da Saúde (Lei nº 48/90 de 21 de Agosto) prevê na sua Base XIV, nº1, c), o direito de que os utentes devem ser tratados pelos meios adequados, humanamente e com prontidão, correcção técnica, privacidade e respeito, prezando a privacidade de cada um e também o facto da

confidencialidade sobre os dados pessoais ter de ser rigorosamente respeitada (nº1, d)) (74).

Ainda dentro do âmbito nacional, importa referir a Lei de Protecção de Dados (Lei 67/98 de 26 de Outubro) e o papel da Comissão Nacional de Protecção de Dados (CNPD). Na lei de Protecção de Dados, respeitante à protecção das pessoas singulares relativamente ao tratamento dos dados pessoais e à livre circulação desses dados, pode começar por destacar-se o artigo 2.º, relativo ao tratamento de dados pessoais, no qual se encontra referido que o mesmo deve ser efectuado de forma transparente e no estrito respeito pela reserva da vida privada (Capítulo I). No artigo 3.º da mesma lei, pode destacar-se a definição de dados pessoais e de tratamento de dados pessoais, como sendo, respetivamente, *"qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável"* e *"qualquer operação ou conjunto de operações sobre tratamento de dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição"*. No artigo 7.º, ainda respeitante à referida lei, encontra-se contemplado o princípio da proibição de tratamento dos dados sensíveis, onde é referido no n.º1 a proibição do "*tratamento de dados pessoais referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem racial ou étnica, bem como o tratamento de dados relativos à saúde e à vida sexual, incluindo os dados genéticos"*.

A CNPD, caracteriza-se como sendo uma autoridade administrativa independente, que se aplica a actividades relacionadas com o tratamento de dados (lei nº 67/98 de 26 de Outubro). Tem como atribuição o controlo do cumprimento das disposições legais e regulamentares em matéria de protecção de dados pessoais, sendo que coopera com outras autoridades de controlo com o objectivo de defender os direitos de cidadãos que se encontrem a residir no estrangeiro. Na referida lei, no Capítulo IV, encontram-se contempladas as atribuições da CNPD, das quis se pode destacar o controlo e fiscalização do "*cumprimento das disposições legais e regulamentares, em rigoroso respeito*

pelos direitos do homem e pelas liberdades e garantias consagradas na Constituição e na lei" (artigo 2.º). No artigo 23.º encontram-se contempladas as competências da CNPD, destacando a emissão de "*parecer sobre disposições legais, bem como instrumentos jurídicos em preparação em instituições comunitárias e internacionais, relativos ao tratamento de dados pessoais" (nº1 a)) e "autorizar ou registar, consoante os casos, os tratamentos de dados pessoais*" (nº1, b)) (75).

Por outro lado, podemos ainda referenciar a lei 26/2016 de 22 de Agosto, relativa ao acesso à informação administrativa e ambiental e de reutilização dos documentos administrativos. Esta lei, consagra no seu artigo 1.º nº3, o acesso à informação e a documentos nomeadamente aos que incluem dados de saúde, produzidos ou detidos pelos órgãos ou entidades referidos no artigo 4.º, quando efectuado pelo titular ou por quem tenha um interesse directo, pessoa, legítimo e constitucionalmente protegido na informação.

É importante considerar a LADA – Lei de Acesso aos Documentos Administrativos (Lei n.º 46/2007, de 24 de Agosto), cujo objectivo é regular o acesso a documentos administrativos e a sua reutilização (Capítulo I, artigo 2º). A respeito da mesma lei torna-se pertinente fazer-se referência à definição de "documento administrativo", que se encontra contemplado no artigo 3.º nº1,a), o qual menciona que o mesmo se trata de "*qualquer suporte de informação sob forma escrita, visual, sonora, electrónica ou outra forma material, na posse de órgãos e entidades (...), ou detidos em seu nome*" (76). O artigo 7.º da mesma lei diz respeito à comunicação de dados de saúde, sendo que é referido que a mesma deve ser "*feita por intermédio de médico se o requerente o solicitar*".

Ainda a este respeito, podemos considerar a CADA – Comissão de Acesso aos Documentos Administrativos, constante na lei 26/2016 de 22 de Agosto, que corresponde a uma entidade pública independente que tem como objectivo proteger o acesso a informação administrativa (77). No seu artigo 30.º é possível encontrar as suas competências que incidem essencialmente sobre tópicos como a protecção geral de dados pessoais; protecção de dados pessoais e utilização dos meios informáticos; livre circulação de informação geral; circulação de dados pessoais e seus riscos inerentes e a diversidade de perspectivas sobre a liberdade de circulação e a reserva de dados.

No que respeita especificamente à informação de saúde, a lei 12/2005 de 26 de Janeiro de 2005, trata de informação directa ou indirectamente ligada à saúde, presente ou futura, de uma pessoa, quer se encontre com vida ou tenha falecido, e sua respectiva história clínica e familiar. No artigo 2.º da mesma lei, encontra-se contemplada a definição de informação de saúde sendo esta definida como "*todo o tipo de informação directa ou indirectamente ligada à saúde, presente ou futura de uma pessoa, quer se encontre com vida ou tenha falecido, e sua história clínica e familiar*". Também no artigo 5.º nº1 da presente lei, encontra-se contemplada a definição de "informação médica" e no nº2 do mesmo artigo a definição de "processo clínico", sendo a primeira definida como toda a informação destinada a ser utilizada na prestação de cuidados de saúde e a segunda como correspondendo a qualquer registo, informatizado ou não, que contenha informação de saúde sobre doentes ou seus familiares.

O artigo 3.º da mesma lei, relativo à propriedade da informação de saúde refere, no seu nº1, que a informação de saúde, quer seja os dados clínicos registados resultados de análises e outros exames subsidiários, intervenções e diagnósticos, são propriedade da pessoa, sendo que essa mesma informação não pode ser utilizada para outros fins. No nº2 do mesmo artigo, é referido que o titular da informação de saúde tem o direito de ter conhecimento de todo o processo clínico que lhe diga respeito, e no nº3, o direito de acesso à informação de saúde por parte do titular. No artigo 4.º nº1 da mesma lei, está consagrado que "os responsáveis pelo tratamento da informação de saúde devem tomar as providências adequadas à protecção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais". No nº2 do mesmo artigo, é referido que "*as unidades do sistema de saúde devem impedir o acesso indevido de terceiros aos processos clínicos e aos sistemas informáticos que contenham informação de saúde* (...)" e no nº3, é ainda referido que "*a informação de saúde apenas pode ser utilizada pelo sistema de saúde nas condições expressas em autorização escrita do seu titular ou de quem o represente*".

Neste contexto, relativamente à informação de saúde, é ainda importante mencionar o parecer do Conselho Nacional de Ética para as Ciências da Vida (CNECV) acerca da informação de saúde e registos informáticos de saúde

(60/CNECV/2011), no qual é referido, uma vez mais, que o acesso à informação de saúde deve ser efectuado respeitando sempre a confidencialidade e privacidade do titular. No mesmo parecer, é ainda mencionado que a implantação de registos digitais que implique desmaterialização dos processos clínicos, dada a sua importância e potenciais riscos deve ser ponderada, devido a questões relacionadas com a quebra de confidencialidade e privacidade (67).

O segredo profissional

Uma vez que o segredo profissional em geral, e o sigilo médico em particular, consiste numa das principais formas de protecção da confidencialidade dos pacientes, torna-se adequado proceder a uma abordagem relativa ao enquadramento jurídico mais relevante no que concerne ao sigilo médico, nomeadamente o artigo 18.º da CRP, relativo à força jurídica, com o objectivo de defender os direitos, liberdades e garantias dos indivíduos, em caso de violação do sigilo médico (73).

O Código Penal prevê no seu artigo 195.º disposições relativas à violação de segredo alheio no exercício da actividade profissional e também no seu artigo 192.º, relativo à devassa da vida privada e divulgação sem consentimento de informações privadas da vida de outro, quer seja de carácter da vida familiar ou sexual (78).

No que diz respeito ao segredo profissional médico em particular[5], pode ser considerado o Regulamento de Deontologia Médica (Regulamento n.º 707/2016). No seu Capítulo IV, referente ao segredo médico, encontra-se contemplado no seu artigo 29.º que "*o segredo médico é condição essencial ao relacionamento médico-paciente, assenta no interesse moral, social, profissional e ético, que pressupõe e permite uma base de verdade e de mútua confiança"*.

No mesmo Capítulo, importa destacar o artigo 30.º nº1, no qual se encontra contemplado que "*o segredo médico impõe-se em todas as circunstâncias dado que resulta de um direito inalienável de todos os doentes*" e no seu nº2 ainda é referido que "*o segredo abrange todos os factos que tenham chegado ao conhecimento do médico no exercício da sua profissão ou por causa dela (...)*" sendo elencados alguns exemplos como "*os factos revelados directamente pela*

[5] Outros códigos deontológicos de profissões da área da saúde referem o segredo profissional, como é o caso do Código Deontológico dos Enfermeiros e do Código dos Farmacêuticos.

pessoa, por outrem a seu pedido ou por terceiro com quem tenha contactado durante a prestação de cuidados ou por causa dela" (a)). Ainda no âmbito no mesmo artigo, importa referir o seu n.º 4 no qual é dito que o segredo se mantém mesmo após a morte do doente.

No que concerne à protecção dos dados médicos mantidos electronicamente, importa fazer referência ao artigo 36.º, mais especificamente o seu n.º 1, no qual se encontra contemplado que os ficheiros automatizados, as bases e bancos de dados médicos, contendo informações extraídas de histórias clínicas sujeitas a segredo médico, devem ser equipados com sistemas, e utilizados com procedimentos de segurança que impeçam a consulta, alteração ou destruição de dados por pessoa não autorizada a fazê-lo e que permitam detectar desvios de informação. No artigo 37.º n.º1 encontra-se contemplado de que forma é que os responsáveis pelo tratamento dos dados de saúde devem agir, sendo referido que os mesmos "*devem tomar as providências adequadas à protecção da sua confidencialidade, garantindo a segurança das instalações e equipamentos, o controlo no acesso à informação, bem como o reforço do dever de sigilo e da educação deontológica de todos os profissionais*".

CAPITULO IV

4. Estudo Prático

4.1 Breve Apresentação

Considerando que o objectivo central do presente projecto consiste em aferir o grau de conhecimento dos gestores de organizações de saúde portuguesas acerca das medidas e mecanismos necessários à proteção de informação de saúde dos utentes no contexto do novo regulamento geral de proteção de dados da UE e o seu grau de preparação para responder às exigências da aplicação deste diploma jurídico, e tendo em conta o que se deixou dito no enquadramento teórico, foram identificados os principais temas chave do RGPD na óptica dos gestores de saúde, em particular dos administradores hospitalares.

Estes temas foram selecionados tendo em conta a análise detalhada do documento em si e da revisão bibliográfica realizada focando sobretudo o papel do gestor de saúde e foram organizados conforme o esquema conceptual que se apresenta na Figura 1.

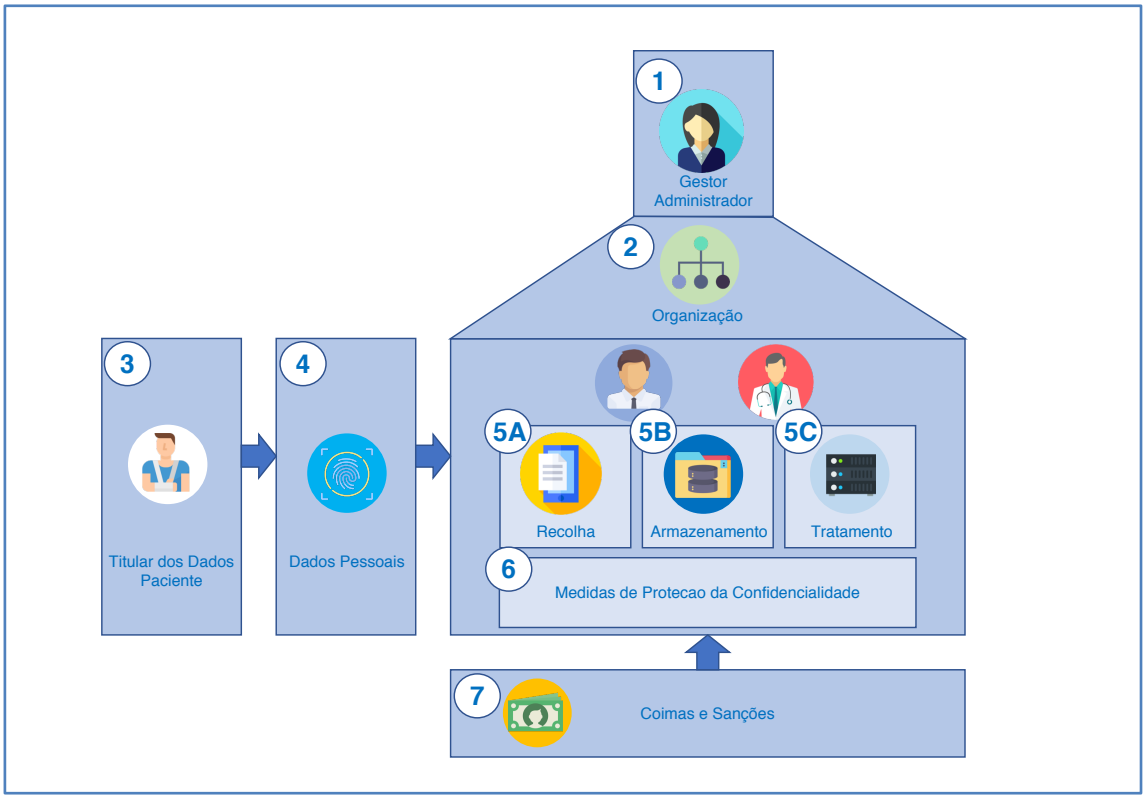


Fig. 1 – Premissa e enquadramento conceptual do presente trabalho

O Administrador Hospitalar tem por principais funções garantir a execução diária das actividades do hospital, coordenando as acções de todos os departamentos do hospital, por forma a garantir que a organização funciona como um todo, executando os serviços que oferece com qualidade e eficiência (1 – Gestor/Administrador Hospitalar) (75).

Como principais actividades com relevância para a temática da proteção de dados, os Administradores Hospitalares coordenam a organização hospitalar, composta por diversas unidades orgânicas (2 - Organização Hospitalar), as quais executam os vários processos do hospital, incluindo a interação com os pacientes (3 – Paciente / Titular dos Dados), que são os titulares dos respectivos dados (4 - Dados), os quais são recolhidos pelos vários profissionais da organização hospitalar (5A – Recolha de Dados), armazenados em suportes electrónicos ou não electrónicos (5B – Armazenamento de Dados) e que são posteriormente tratados com diversos fins, como seja o diagnostico clínico, execução de processos administrativos ou investigação e desenvolvimento (5C – Tratamento de Dados), razão pela qual são relevantes medidas de protecção da confidencialidade entre as quais se incluem o segredo profissional e a protecção de dados (6 – Medidas de Protecção da Confidencialidade), foco principal do presente trabalho.

O RGPD prevê uma série de direitos dos titulares dos dados, deveres dos responsáveis pela recolha armazenamento e tratamento dos mesmos e sanções para possíveis violações (7 – Coimas e Sanções). O conhecimento e respeito por estas disposições é essencial para a boa gestão em saúde, em particular para o bom desempenho da função do administrador hospitalar.

4.2 Apresentação de Resultados

Como referido supra, para aferir o grau de conhecimento dos gestores de organizações de saúde portuguesas acerca das medidas e mecanismos necessários à proteção de informação de saúde dos utentes no contexto do RGPS, elaborou-se um questionário estruturado segundo o esquema conceptual acima descrito, o qual foi respondido por um painel representativo de Gestores/Administradores de hospitais públicos da região da Grande Lisboa e Vale do Tejo (ver *supra*, secção da Metodologia).

O questionário foi elaborado de forma a incluir os aspectos mais relevantes do RGPD na óptica dos Administradores Hospitalares, tendo sido escolhido o formato estruturado/fechado, com opção de escolha múltipla. Para cada questão foi apresentado um conjunto fechado de respostas possíveis, em que uma ou mais respostas estão certas e as restantes estão erradas. O conjunto de opções de resposta foi cuidadosamente identificado para permitir aferir, com elevado grau de certeza, duas dimensões relevantes para a análise: a profundidade de conhecimento dos inquiridos sobre cada tema (número e conteúdo das respostas certas seleccionadas) e, simultaneamente, a clareza em relação aos conceitos específicos contidos no RGPD (número e conteúdo das respostas erradas selecionadas).[6]

Apresentar-se-ão em seguida os principais resultados obtidos a partir da análise das respostas dos inquiridos, incluindo-se os dados detalhados das respostas no Anexo III - Transcrição Integral das Respostas Obtidas.

Gestor / Administrador Hospitalar (1)

As duas primeiras perguntas do questionário procuravam determinar o nível de experiência dos Gestores/Administradores Hospitalares na função (Questão 1) e aferir, segundo a sua própria autoavaliação, qual o nível de conhecimento que pensam deter sobre o RGPD (Questão 2). A analise das respostas obtidas revelou que a maioria dos Gestores/Administradores Hospitalares possui mais de dez anos de experiência na função. Apenas 2 dos 9 inquiridos possuem menos de cinco anos de experiência na função.

Relativamente à sua própria autoavaliação quanto ao nível de conhecimento que nesse momento possuíam sobre o RGPD, a maioria indicou possuir um conhecimento médio (6 respostas) ou baixo (2 respostas). Apenas um dos inquiridos indicou possuir um conhecimento elevado sobre o RGPD.

[6] Tomemos como exemplo a questão sobre o entendimento do inquirido acerca da licitude do tratamento de dados constante no RGPD. O número de respostas certas indicadas (“mediante consentimento do titular” e “defesa de interesses vitais do titular”) permite aferir a completude do conhecimento do inquirido, enquanto que o número de respostas erradas indicadas (“determinado por entidade pública e/ou governamental” e “se os dados forem relativos a não residentes da UE”) permite aferir o grau de clareza do inquirido sobre o conceito em causa.

Organização Hospitalar (2)

Relativamente à organização hospitalar que o Gestor/Administrador coordena, interessava saber se a mesma já teria nomeado responsáveis pela temática do RGPD e iniciado algum programa ou iniciativa de preparação para a entrada em vigor do Regulamento.

Em primeiro lugar, foi perguntado qual o entendimento que o inquirido tinha sobre se o responsável pelo tratamento deveria ser um individuo ou uma estrutura orgânica e questionadas as principais responsabilidades que lhe são acometidas ao abrigo do RGPD (Questão 3), tendo sido elencadas três opções: (i) um profissional que assume a responsabilidade pelos processos de tratamento de dados pessoais e pela manutenção do cadastro dos titulares dos dados, (ii) a pessoa singular ou colectiva, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios de tratamento de dados pessoais, (iii) uma entidade subcontratada pela entidade beneficiaria a quem caberá controlar e auditar os processos, bases de dados e sistemas informáticos utilizados pelos seus colaboradores no tratamento de dados pessoais. Das três opções elencadas, apenas 4 dos 9 inquiridos identificou a definição correcta do RGPD, a opção (ii). Posteriormente, foi perguntado se já existia actualmente no hospital do inquirido um Departamento/Gabinete específico que tenha sido nomeado responsável pelas questões relacionadas com a protecção dos dados de saúde dos utentes (Questão 4). A maioria dos inquiridos (7 em 9) confirmou que as suas respectivas organizações já tinham nomeado um Departamento/Gabinete responsável pela questão do RGPD. Em apenas dois dos Hospitais ainda nenhum responsável tinha sido nomeado. Seguidamente, para os casos em que um responsável tinha sido nomeado, perguntámos em que categorias se enquadrava o Departamento/Gabinete em questão (as categorias elencadas foram: Departamento/Gabinete Jurídico, Departamento/Gabinete de Sistemas de Informação, Departamento/Gabinete de Gestão de Utentes, Departamento/Gabinete Planeamento e Controlo de Gestão, Departamento/Gabinete de Auditoria Departamento/Gabinete de *Compliance*, Comissão de Ética ou Outro, caso o Departamento/Gabinete em causa não se enquadrasse em nenhuma das categorias identificas e em que se pedia que o inquirido o especificasse (Questão 5). Em cinco casos, os inquiridos indicaram

que o Departamento/Gabinete que foi nomeado responsável foi o Departamento/Gabinete Jurídico. Em três destes cinco casos, para além do Departamento/Gabinete Jurídico, os inquiridos indicaram que foram também nomeados todos os restantes Departamentos/Gabinetes dos Hospitais. No que concerne aos restantes inquiridos, num caso, foi indicado que foram nomeados responsáveis o Departamento/Gabinete de Sistemas de Informação, juntamente com o Departamento/Gabinete de Gestão de Utentes.

Finalmente, perguntámos em que medida a unidade de saúde em que o inquirido exerce funções se preparou para a entrada em vigor e respectiva implementação do RGPD (Questão 6). Para esse fim, categorizámos um conjunto abrangente de medidas que o inquirido podia seleccionar: (i) não levou a cabo qualquer acção específica nesse sentido, (ii) realizou acções de formação dirigidas aos colaboradores, (iii) procedeu à revisão de procedimentos que envolvem o tratamento de dados pessoais na sua unidade de saúde, (iv) efectuou o levantamento das bases de dados existentes na unidade de saúde e verificou a sua adequação ao RGPD e, finalmente, uma opção aberta (outras acções) que em se pedia ao inquirido que especificasse.

A análise das respostas obtidas, revelou que a maioria dos Gestores/Administradores (6 inquiridos) indicou já terem sido iniciadas medidas especificas no âmbito da preparação para o RGPD. Apenas 3 inquiridos em 9, indicaram não ter iniciado ainda nenhuma acção específica. Dos 6 inquiridos que indicaram já ter iniciado acções especificas, 4 indicam ter iniciado o levantamento das bases de dados existentes na unidade de saúde e verificado a sua adequação ao RGPD, 4 especificaram realizaram acções de formação dirigidas aos colaboradores e 2 indicaram que procederam à revisão de procedimentos que envolvem o tratamento de dados pessoais na unidade de saúde.

Paciente / Titular dos Dados (3)

Prosseguindo a análise, nesta terceira secção do questionário, procurou-se determinar o grau de conhecimento do Gestor/Administrador Hospitalar sobre os direitos do titular dos dados, nomeadamente, direito de acesso do titular, direito de apagamento dos dados, direito de limitação do tratamento dos dados e direito de portabilidade dos dados.

Relativamente ao direito de acesso (Questão 7), a pergunta contextualizava esse direito, indicando que o mesmo implica que o titular dos dados tem o direito de obter junto do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objecto de tratamento, mas solicitava ao inquirido que especificasse que outras informações que o responsável pelo tratamento também era obrigado a fornecer ao titular, dando como opções de resposta: (i) a localização geográfica do seu armazenamento e tratamento (dentro ou fora da União), (ii) as finalidades do tratamento de dados, (iii) a lista de entidades subcontratadas que procedem ao tratamento dos dados, (iv) o prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para fixar esse prazo, (v) a lista de entidades a quem essa informação irá ser divulgada e (vi) qualquer rectificação aos dados pessoais originalmente fornecidos. Das opções elencadas, apenas as opções (ii) e (iv) são requeridas pelo RGPD. Nenhum dos inquiridos identificou de forma absolutamente correcta os deveres do responsável pelo tratamento no contexto do direito de acesso, falhando a identificação das respostas correctas (1 caso) e/ou indicando obrigações que não estão comtempladas no RGPD (todos os 9 inquiridos).

Relativamente ao direito de apagamento dos dados (Questão 8), a respectiva pergunta começava por contextualizar este direito, indicando que o mesmo implicava que o titular dos dados tem o direito a obter, junto do responsável pelo tratamento, o apagamento dos seus dados pessoais sem demora injustificada, mas solicitava a identificação do conjunto de motivos que podem justificar essa solicitação, à luz do RGPD, indicando as seguintes opções: (i) os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento, (ii) sempre que se registar o falecimento do titular dos dados, bastando o apagamento ser solicitado pelos seus legais representante, (iii) o titular retira o consentimento em que se baseia o tratamento dos dados, se não existir outro fundamento jurídico para o referido tratamento, (iv) será sempre obrigatório o apagamento dos dados mediante declaração expressa nesse sentido do titular dos mesmos, independentemente dos motivos para tal requerimento. Das opções elencadas, apenas as opções (i) e (iii) estão correctas. Neste contexto, apenas 2 inquiridos responderam correctamente. Os

restantes 7, identificaram apenas parcialmente as respostas correctas e/ou indicaram motivos não requeridos pelo RGPD.

No que concerne o direito de limitação do tratamento dos dados (Questão 9), pretendeu-se testar o conhecimento dos Gestores/Administradores Hospitalares sobre o direito que assiste aos titulares dos dados de obter do responsável pelo tratamento a limitação desse tratamento. Para esse fim, perguntou-se em que situações tal pode ser requerido segundo o RGDP, fornecendo-se as seguintes opções de resposta: (i) o titular passou a residir em território fora da União Europeia, (ii) o tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização, (iii) cessação da actividade do estabelecimento, (iv) o responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial, (v) contestar a exatidão dos dados pessoais durante um período que permita ao responsável pelo tratamento verificar a sua exatidão, em que apenas as opções (ii), (iv) e (v) são correctas. Relativamente a esta pergunta, 2 dos inquiridos identificaram completamente as respostas correctas. Todos os restantes 7 inquiridos identificaram parcialmente as respostas correctas e/ou identificaram motivos não contemplados no RGPD.

Finalmente, no que concerne o direito de portabilidade dos dados (Questão 10), a respectiva questão pedia ao inquirido que identificasse, segundo as disposições do RGPD, as implicações para o responsável pelo tratamento de dados decorrentes do dever de assegurar o direito do titular à portabilidade dos mesmos, fornecendo-se as seguintes opções: (i) fornecendo ao titular dos dados os dados pessoais que lhe digam respeito, num formato estruturado de uso corrente e de leitura automática, (ii) transmitindo os dados, num formato estruturado de uso corrente e de leitura automática, a outro responsável pelo tratamento, mediante determinadas condições, (iii) transmitindo os dados à Autoridade Nacional Competente, para que esta decida se os mesmos podem ser disponibilizados a outras entidades, (iv) assegurando o armazenamento dos dados pessoais em formato normalizado, usando tecnologia portável e standards de mercado, (v) transmitindo os dados num formato estruturado de uso corrente e de leitura automática a outro responsável pelo tratamento, mediante determinadas condições. Relativamente às opções elencadas, apenas a opção

(v) é requerida pelo RGPD. Nenhum dos inquiridos respondeu corretamente à questão.

Dados Pessoais (4)

Relativamente à quarta área do esquema conceptual, pretendia-se determinar o grau de entendimento do Gestor/Administrador Hospitalar sobre a delimitação do que se entende por dados pessoais e dados pessoais sensíveis relativos a saúde.

Relativamente à delimitação de dados pessoais (Questão 11), foram apresentadas aos inquiridos as seguintes definições, em que apenas a opção (iv) corresponde à definição do RGPD, devendo o inquirido selecionar uma dessas opções: (i) informação relativa a uma pessoa singular, identificada ou identificável (titular dos dados), directa ou indirectamente, em especial por referência a um identificador como por exemplo um número de identificação, (ii) informação relativa a uma pessoa singular ou colectiva, identificada ou identificável (titular dos dados), diretamente por referência a um identificador como por exemplo um numero de identificação, (iii) dados resultantes de tratamentos técnicos específicos relativos as características físicas, fisiológicas ou comportamentais de uma pessoa, que permitam ou confirmem a identificação dessa pessoa, (iv) qualquer tipo de dados detidos pela entidade relativamente a uma pessoa singular. Apenas 3 dos Gestores/Administradores Hospitalares inquiridos identificaram a definição correcta do RGPD.

A pergunta seguinte focou a definição mais especifica de dados de saúde à luz do RGPD (Questão 12), visando testar o conhecimento dos inquiridos sobre a delimitação deste tipo de dados sensíveis. Foram então elencadas três opções: (i) um subconjunto de dados pessoais, relativos a informação biométrica e biológica, (ii) todos os dados pessoais recolhidos por unidades que prestem serviços de saúde, (iii) 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, em que a opção (iii) corresponde à definição do RGPD. As opções assim formuladas, visavam relacionar caracterizar os dados de saúde segundo três óticas: em que medida os dados caracterizam a saúde o titular, quem os recolhe e, finalmente, em que medida identificam o titular. Cinco dos inquiridos identificaram correctamente a

definição de dados de saúde. No entanto, os restantes 4 definiram erradamente esses dados segundo a entidade que os recolhe e não segundo as características dos próprios dados.

Recolha de Dados (5A)

No que toca à recolha de dados pelas organizações hospitalares, foi incluída uma questão especifica sobre a delimitação do âmbito e objetivos do RGPD (Questão 13), elencando-se duas enunciações deferentes: (i) um novo enquadramento jurídico, mais abrangente, em matéria de proteção de dados, (ii) uma mera atualização, sem grandes inovações, da legislação europeia na área da proteção de dados e ainda a opção (iii) não sabe/não responde. Neste âmbito, todos os Gestores/Administradores Hospitalares (9 inquiridos) respondem com o entendimento correcto de que se trata de um novo enquadramento jurídico na área da proteção de dados a nível da UE.

Armazenamento de Dados (5B)

Ainda no âmbito dos processos e procedimentos, focou-se o armazenamento dos dados, em particular o âmbito de aplicação territorial do RGPD e as respetivas limitações territoriais e os conceitos de violação de dados pessoais armazenados. Para tal perguntou-se em primeiro lugar, em que âmbito territorial de armazenamento e tratamento de dados aplica o RGPD (Questão 14), sendo elencadas varias alternativas de âmbito geográfico (tanto relativas a origem geográfica do responsável do tratamento dos dados, quando a localização do próprio armazenamento e tratamento: (i) no contexto das actividades de um estabelecimento responsável pelo tratamento situado no território da UE, independentemente desse tratamento ocorrer dentro ou fora da UE, (ii) relativo a qualquer cidadão da UE, independentemente do local do tratamento e do local de estabelecimento do responsável pelo tratamento, (iii) realizado apenas dentro da UE, independentemente do local de estabelecimento do responsável pelo tratamento e do local da residência dos titulares dos dados. A maioria dos Gestores/Administradores Hospitalares não tem um percepção correcta do âmbito de aplicação territorial do RGPD (apenas 2 em 7 responderam correctamente).

Ainda relativamente ao armazenamento e tratamento de dados (incluindo a sua transmissão), foi perguntado aos inquiridos o que entendem por violação de dados pessoais (Questão 15) e confrontadas as suas respostas com a definição constante no RGPD, em particular no que concerne três dimensões: a existência, ou não, de dolo, a natureza da violação dos dados (perda, alteração, destruição, acesso) e licitude (autorizado ou não autorizado). A esse fim, enunciaram-se quatro opções (combinações das dimensões anteriormente enunciadas): (i) uma violação da segurança que provoque, de modo acidental ou doloso, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer ouro tipo de tratamento, (ii) uma violação da segurança que provoque, de modo ilícito, o acesso, não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer ouro tipo de tratamento, (iii) uma violação da segurança que provoque, de modo acidental ou lícito, 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, (iv) uma violação da segurança que provoque, de modo ilícito, o acesso e a divulgação, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. Segundo o RGPD, a primeira opção, que é a mais abrangente das quatro opções elencadas, constitui uma violação de dados e 6 em 9 dos inquiridos coincidem na identificação da definição correcta.

Tratamento de Dados (5C)

Finalmente, no que concerne os processos de recolha, armazenamento e tratamento de dados, focamos a área do tratamento de dados e questionamos os inquiridos sobre quatro aspectos fundamentais contemplados no RGPS que são de extrema importância para a actividade das organizações hospitalares: em que condições é lícito tratar os dados, o que constitui o consentimento para o tratamento de dados, quais os requerimentos para o tratamento de categorias especiais de dados e que derrogações são possíveis no tratamento de dados pessoais, nomeadamente para fins de investigação e desenvolvimento.

Relativamente à licitude do tratamento (Questão 16), perguntou-se em que condições o Gestor/Administrador Hospitalar considera o tratamento de dados lícito à luz do RGPD, enunciando-se as seguintes opções: (i) o tratamento dos

dados for determinado por entidade pública ou órgão governamental, (ii) o titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas, (iii) o tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular, (iv) os dados pessoais tratados forem relativos a cidadãos não residentes na UE. Cerca 33% (3 em 9) dos inquiridos identifica correctamente as condições de tratamento lícito, sendo que os restantes apenas reconhecem licitude do tratamento nas situações em que o consentimento é dado pelo titular dos dados (4 respostas) ou em situações que não são contempladas no RGPD (2 respostas).

Seguidamente, perguntou-se quais as condições aplicáveis ao consentimento para o tratamento de dados pessoais (Questão 17): (i) o consentimento dos dados deve ser dado livremente por parte do titular dos dados, (ii) se o consentimento do titular dos dados for dado no contexto de uma declaração escrita, este deve ser apresentado de forma que o distinga claramente de outros assuntos, (iii) o titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. Optou-se nesta questão por incluir três opções correctas a luz do RGPD, tendo 6 dos 9 inquiridos identificado correctamente as três condições, 2 dos inquiridos identificaram correctamente apenas duas das condições e 1 inquirido apenas identificou uma das condições correctas.

Prosseguiu-se com a questão sobre as situações em que é proibido o tratamento de dados, em particular quanto às categorias de dados cujo tratamento não é autorizado (Questão 18). Foram elencadas quatro opções: (i) a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, (ii) dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, (iii) dados relativos à saúde, (iv) todas as opções anteriores. Como sabemos, apenas a opção (i) constitui categorias de dados pessoais cujo tratamento não e autorizado, sendo que 5 dos inquiridos identificam correctamente a resposta. No entanto, é relevante o número de inquiridos (4 em 9) que considera erradamente que os dados de saúde ou os dados genéticos não são passíveis de autorização para tratamento.

Finalmente, no que concerne as derrogações previstas no RGPD (Questão 19) para o tratamento de dados, em particular quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos,

contextualizou-se que, segundo o RGPD, o Direito da União ou dos Estados-Membros pode, sob certas condições, prever derrogações a alguns direitos dos titulares dos dados. Perguntou-se aos inquiridos que identificassem, de entre as seguintes opções, que direitos podem ser derrogados: (i) direito de acesso do titular dos dados, (ii) direito de portabilidade dos dados, (iii) direito de rectificação dos dados, (iv) direito ao apagamento dos dados ("direito a ser esquecido"). Segundo o RGPD, apenas o direito de acesso e o direito ao apagamento dos dados podem ser derrogados. Apenas 2 dos inquiridos identificaram correctamente as derrogações possíveis segundo o RGPD. Os restantes, (7 em 9) não responderam correctamente (5 em 8) ou responderam de forma incompleta (3 em 8).

Medidas de Protecção e Confidencialidade (6)

Relativamente à sexta área do esquema conceptual, pretendia-se determinar o grau de conhecimento do Gestor/Administrador Hospitalar acerca das medidas de protecção e confidencialidade dos dados, abarcando as principais disposições do RGPD neste domínio, nomeadamente a proteção de dados desde a concepção e por defeito, segurança do tratamento dos dados, notificação da violação dos dados, avaliação de impacto, consulta prévia e certificação.

No que concerne ao entendimento do inquirido acerca da protecção de dados desde a concepção e por defeito (Questão 20), fornecendo-se as seguintes opções de resposta: (i) protecção de dados no momento da definição dos meios de tratamento e no momento do próprio tratamento, (ii) restrição do tratamento apenas aos dados pessoais que forem necessários para cada finalidade específicas, (iii) Protecção dos dados apenas no momento do seu armazenamento, (iv) Tratamento de dados generalizado mas armazenamento apenas dos dados necessários para cada finalidade específica. Apenas a opção (i) e (ii) estão correctas.

Relativamente a esta pergunta, apenas 2 dos inquiridos identificaram completamente as respostas correctas e os restantes 7 inquiridos identificaram parcialmente as respostas correctas e/ou identificaram definições não contempladas no RGPD.

No que respeita à pergunta que se destina ao entendimento dos inquiridos acerca da segurança do tratamento dos dados (Questão 21), foram fornecidas as seguintes opções de resposta: (i) o apagamento regular dos dados tidos por confidenciais, (ii) a utilização permanente das técnicas de anonimização de dados mais recentes, (iii) a pseudonimização e a cifragem dos dados pessoais, (iv) um processo para testar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento, (v) assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento, sendo que as respostas correctas correspondem às opções (iii), (iv) e (v). Verificou-se que nesta questão apenas 1 inquirido identificou completamente a resposta certa, sendo que os restantes inquiridos identificaram parcialmente as respostas correctas e/ou identificaram medidas não contempladas no RGPD.

Relativamente à questão que se destina ao entendimento do inquirido relativamente à notificação da violação dos dados (Questão 22), foram elencadas as seguintes opções de resposta: (i) dar imediatamente a conhecer ao titular que ocorreu a violação dos seus dados, independentemente do risco para os direitos, liberdades e garantias das pessoas singulares, (ii) notificar esse facto à autoridade de controlo competente, sem demora injustificada, até 72 horas após ter tido conhecimento da violação de dados pessoais, a menos que a violação não resulte num risco para os direitos, liberdades e garantias das pessoas singulares, (iii) lançar um procedimento interno para fazer face ao problema, a menos que a violação não resulte num risco para os direitos, liberdades e garantias das pessoas singulares, (iv) comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada, em caso de elevado risco para os direitos, liberdades e garantias das pessoas singulares. Para esta questão as opções (ii) e (iv) estão correctas, sendo que 3 dos inquiridos identificaram completamente a resposta certa e os restantes 6 inquiridos identificaram parcialmente a resposta correcta e/ou identificaram procedimentos não contemplados no RGPD.

No que respeita à questão que se destina ao entendimento do inquiridos relativamente à avaliação de impacto das operações de tratamento de dados (Questão 23), foram fornecidas as seguintes opções de resposta: (i) sejam contratados prestadores de serviços externos que realizem operações de

tratamento de dados, (ii) sejam alterados processos internos que impliquem mudanças no tratamento dos dados pessoais, (iii) sempre que o conjunto de dados pessoais recolhidos junto dos titulares seja aumentado, (iv) o tratamento, tendo em conta a sua natureza, âmbito e finalidades, for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares. Relativamente a esta questão apenas a opção (iv) está correcta, sendo que 4 dos 9 inquiridos respondeu correctamente.

No que concerne à questão destinada ao entendimento do inquiridos acerca da consulta prévia relativa ao tratamento de dados (Questão 24), foram elencadas as seguintes opções de resposta: (i) o tratamento dos dados implicar a sua transmissão para território fora da União Europeia, (ii) a avaliação de impacto sobre a protecção de dados indicar que do tratamento resultará num elevado risco para o titular dos dados, (iii) sempre que o tratamento incidir sobre dados pessoais sensíveis, (iv) nunca é necessária a consulta no caso de tratamento de dados pessoais não sensíveis, sendo que a opção correcta é a (ii). Verificou-se que 4 dos 9 inquiridos respondeu correctamente.

Relativamente à questão que pretende avaliar o conhecimento dos inquiridos acerca da existência de certificação em matéria de protecção de dados (Questão 25), foram apenas elencadas as opções (i) sim ou (ii) não, sendo que a primeiro opção é a correcta. Constatou-se que a maioria dos inquiridos (6 em 9) responderam correctamente.

Ainda a respeito da certificação, a questão que pretendia avaliar o entendimento dos inquiridos face à duração da mesma (Questão 26), elencava as seguintes opções de resposta: (i) permanente, (ii) válida por um período de 2 anos, (iii) válida por um período máximo de 3 anos, (iv) ainda não se encontra definido o prazo, sendo que a opção correcta corresponde à opção (iii). Relativamente a está questão verificou-se que apenas 1 dos 9 inquiridos identificou correctamente a resposta, sendo que todos os restantes mencionaram não estar definido qualquer prazo.

Coimas e Sanções (7)

Relativamente à última área do esquema, pretendia-se determinar o grau de conhecimento do Gestor/Administrador Hospitalar acerca das coimas e sanções

previstas no RGPD, aquando incumprimento das normas constantes no mesmo (Questão 27).

Para tal, elencamos na questão seguinte varias alternativas de coimas e sanções, que pretendiam cobrir um intervalo que incluísse sanções simbólicas até sanções e coimas de valor significativo, as quais, de facto, são as que constam do RGPD: (i) coima de 1.000 € dia até correcção das infracções detectadas; (ii) coima de 20.000.000€ ou 4% do volume de negócios anual a nível mundial (consoante o montante que for mais elevado), (iii) ordens para que se cumpram disposições específicas do Regulamento, (iv) advertências, repreensões ou retirada da certificação, sendo que as opções correctas correspondem às opções (ii), (iii) e (iv). Verificou-se que nenhum dos inquiridos identifica completamente as opções correctas, uma vez que todos acertam parcialmente a resposta ou identificam sanções não previstas no RGPD.

4.3 Discussão

Na presente secção, prosseguiremos com a discussão das próprias questões aplicadas e dos respectivos resultados obtidos em cada pergunta, de forma critica, a luz do enquadramento teórico do tema e organizando a análise de resultados de forma alinhada com o esquema conceptual que anteriormente se descreveu.

Gestor/Administrador Hospitalar (1)

Com base no inquérito efectuado, determinou-se que o painel de inquiridos que respondeu corresponde a Gestores/Administradores Hospitalares com experiencia (78% - 7 em 9 - possuem mais de 10 anos e experiencia na função). A maioria (66%) considera possuir um nível conhecimento medio (6 em 9 respostas) ou baixo (2 em 9 respostas) sobre o RGPD. Apenas um inquirido diz ter um conhecimento elevado acerca do RGPD. Considerando que o questionário foi respondido sensivelmente no mês em que o RGPD entrou em vigor na EU, salienta-se que mesmo segundo a própria autoavaliação dos gestores, o seu nível de preparação e conhecimento não será o desejável. Nas secções seguintes, avaliaremos esse nível de conhecimento de forma mais objectiva.

Organização Hospitalar (2)

Relativamente aos aspectos mais relevantes do RGPD para a actividade do Gestor/Administrador Hospitalar que tocam a sua Organização Hospitalar, é de salientar o aspecto muito positivo de que na maioria dos Hospitais (67%) se encontra já designado um departamento dedicado às questões de protecção de dados dos utentes e do RGPD. No entanto, o departamento designado, é quase exclusivamente, o Departamento Jurídico ou Departamento de Sistemas de Informação, podendo afirmar-se que administração hospitalar considera a temática do RGPD como uma questão meramente jurídica ou dizendo respeito aos apenas a área de sistemas de informação. Depreende-se da resposta dos administradores hospitalares que em nenhuma unidade de saúde inquirida se considera a questão do RGPD e da proteção de dados e da confidencialidade como uma questão estratégica ou transversal a toda a organização.

Relativamente ao grau de preparação das organizações de saúde para a entrada em vigor do RGPD, pôde verificar-se que 33% das organizações de saúde não levaram a cabo nenhuma acção de preparação para o RGPD. Quanto às organizações que tomaram iniciativas prévias, constatou-se que a iniciativa mais posta em prática (cerca de 44%) consistiu no levantamento das bases de dados existentes na unidade de saúde, verificando a adequação das mesmas ao RGPD, seguindo-se para as restantes organizações, a realização de acções de formação para os colaboradores da organização (33%).

Quanto à existência de um responsável formalmente designado para fins de tratamento de dados, verificou-se que 44% dos inquiridos identificou a definição correcta. Constata-se que a maioria dos restantes define o responsável pelo tratamento como sendo um profissional que assume a responsabilidade pelos processos de tratamento de dados pessoais e pela manutenção do cadastro dos titulares dos dados, o que mostra uma certa confusão sobre o conceito em causa, que determina que essa responsabilidade seja acometida a uma estrutura orgânica do Hospital.

Paciente/Titular dos Dados (3)

Relativamente aos direitos dos Pacientes/Titulares dos Dados que são consignados no RGPD, as respostas ao questionário demonstram que os inquiridos revelam apenas um entendimento parcial acerca destes conceitos, e

apenas 1 dos 9 inquiridos assinalou as opções correctas segundo o RGPD. Relativamente ao significado do direito de acesso, todos identificam a "finalidade do tratamento" bem como o "prazo de conservação" como elementos constituintes do direito de acesso, mas ao mesmo tempo confundem também este direito com a obrigatoriedade de comunicar ao titular outras informações não consideradas no RGPD (por exemplo, a informação sobre as entidades a quem os dados serão facultados para tratamento, sejam entidades subcontratadas ou outras).

No que concerne o direito de "ser esquecido", verificou-se que apenas 33% (3 em 9) dos inquiridos identificou correctamente este conceito, constatando-se, no entanto, que a maioria acaba por confundi-lo com outras disposições, nomeadamente a percepção de que será sempre obrigatório o apagamento dos dados mediante declaração expressa do seu titular.

No que respeita ao direito do titular à portabilidade dos dados, apenas 22% (2 em 9) dos inquiridos identificou correctamente os parâmetros deste direito. Mais uma vez, os conceitos não estão plenamente compreendidos.

Considerando as respostas dos inquiridos a temática dos direitos do titular dos dados, pode afirmar-se que a maioria não domina os conceitos relevantes, confundindo frequentemente outros aspectos que não são consignados no RGPD (por exemplo, aplicação territorial ou estrutura e conteúdo dos dados em causa).

Dados Pessoais (4)

No que concerne a secção relativa aos Dados Pessoais e ao grau de conhecimento do Gestor/Administrador Hospitalar sobre o elemento fulcral do Regime Geral de Proteção de Dados: a própria definição de dados pessoais, dados sensíveis e dados de saúde, constatou-se que 33% (3 em 9) dos inquiridos identificou a definição correcta de dados pessoais, como sendo a "informação relativa a uma pessoa singular, identificada ou identificável (titular dos dados), directa ou indirectamente, em especial por referência a um identificador como por exemplo um número de identificação". A maioria dos inquiridos considera que qualquer dado detido por uma determinada entidade relativamente a uma pessoa singular devera ser sempre considerado um dado pessoal na áptica do RGPD. Ou seja, verifica-se uma interpretação errada de

que a condição que determina que os dados sejam pessoais é o facto de dizerem respeito a uma pessoa singular, qualquer que seja a sua natureza e sem consideração pelo facto de essa pessoa ser, ou não, identificável a partir desses dados.

No que concerne a definição de dados pessoais relativos a saúde, cerca de metade dos inquiridos (44% - 4 em 9) identificou correctamente que são os "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". Cerca de metade dos inquiridos, mais uma vez, ao invés de considerar as características intrínsecas dos dados para então concluir sobre a sua classificação como dados pessoais saúde, considera erradamente que essa classificação decorre de quem os recolhe ("todos os dados pessoais recolhidos por unidades que prestem serviços de saúde").

Recolha, Armazenamento e Tratamento de Dados (5A, 5B, 5C)

No que respeita ao âmbito de aplicação do RGPD, cerca de 89% dos inquiridos identifica correctamente a definição, sendo que apenas 1 diz não saber responder à mesma.

No que concerne ao âmbito de aplicação territorial do RGPD, verificou-se que apenas 22% (2 em 9) dos inquiridos define correctamente o âmbito de aplicação territorial, sendo que a maioria entende que a aplicação do Regulamento apenas se destina caso o tratamento ocorra dentro da UE, independentemente do local de estabelecimento do responsável pelo tratamento e do local de residência dos titulares dos dados.

Relativamente ao entendimento dos inquiridos acerca do que constitui uma "violação de dados pessoais", constatou-se que mais de metade (6 em 9) identifica correctamente as situações de violação de dados segundo o RGPD. Os restantes inquiridos entendem este conceito de forma mais limitada, como qualquer violação da segurança que provoque, de modo ilícito, o acesso e a divulgação não autorizados a dados pessoais, ao invés da definição mais abrangente considerada no RGPD que considera uma violação da segurança dos dados qualquer tipo de destruição, perda, alteração, divulgação ou o acesso não autorizados a dados pessoais, seja com origem acidental ou dolosa.

No que respeita às condições aplicáveis à licitude do tratamento de dados, verificou-se que apenas um terço dos inquiridos identificou correctamente a resposta na sua totalidade (3 em 9). A maioria dos restantes inquiridos, apenas relaciona a licitude do tratamento segundo uma condição, mais especificamente a que respeita ao consentimento do titular dos dados.

Relativamente às condições aplicáveis ao consentimento para o tratamento de dados pessoais, mais de metade dos inquiridos (5 em 9) identifica correctamente a resposta na sua totalidade, mas quase metade dos inquiridos possui um conhecimento incompleto sobre as condições de consentimento que são a priori necessárias para essa informação poder ser recolhida.

No que concerne à proibição de tratamento a categorias especiais de dados, verificou-se que 44% dos inquiridos respondeu de forma correcta. Os restantes inquiridos afirmam que o tratamento só é proibido se contiver identificação racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, ou seja, aquelas que são as mais óbvias a luz da cultura moderna socialmente aceitável, ao invés de considerarem também, outros conjuntos importantes de dados que o RGPD identifica e cujo tratamento é também.

Relativamente ao entendimento dos inquiridos acerca da "protecção de dados desde a concepção e por defeito", constatou-se que apenas 22% identificou correctamente a resposta na sua totalidade. Na maioria dos casos os inquiridos consegue identificar uma das duas respostas correctas ("protecção de dados no momento da definição dos meios de tratamento e no momento do próprio tratamento" e "restrição do tratamento apenas aos dados pessoais que forem necessários para cada finalidade específica") e apenas 22% (2 em 9) dos inquiridos erra a resposta na sua totalidade. Pode então concluir-se, novamente, que o conceito de dados desde a concepção e por defeito, mais um dos conceitos chave do RGPD, não e ainda totalmente compreendido pelos inquiridos.

No que respeita ao entendimento dos inquiridos acerca da segurança no tratamento de dados, verificou-se que apenas 1 respondeu correctamente à questão na sua totalidade. Cerca de 78% (7 em 9) dos inquiridos identifica de forma errónea a opção relativa à utilização permanente de técnicas de

anonimização de dados mais recentes, o que sugere significativa falta de conhecimento relativamente à matéria de segurança no tratamento de dados.

Quanto ao entendimento dos inquiridos relativamente ao dever de notificação de violação de dados pessoais, constatou-se que 33% dos inquiridos responde correctamente à questão na sua totalidade. Na maioria dos casos as respostas correctas são preferencialmente escolhidas pelos inquiridos, mas por outro lado, cerca de 44% identifica também que não é necessário nenhuma comunicação as autoridades nem lançar nenhum procedimento interno se a avaliação de risco pela organização considere que que da violação dos dados não resulta nenhum risco para os titulares do mesmos, o que é um elemento de desconhecimento muito relevante.

Relativamente à questão das derrogações no tratamento de dados, constatou-se que nenhum inquirido respondeu correctamente à totalidade da pergunta. Cerca de 44% identifica uma resposta correcta e as restantes erradas mostrando um conhecimento parcial, sendo que 88% identifica erradamente como resposta correcta o direito ao apagamento dos dados. Conclui-se que os inquiridos confundem os conceitos em causa.

Medidas de Protecção e Confidencialidade (6)

No que respeita ao entendimento do inquirido acerca da avaliação de impacto relativa ao tratamento dos dados pessoais, verificou-se que 44% identificou a resposta correctamente. Cerca de um terço dos restantes pensa que a avaliação de impacto deve ser realizada quando são contratados prestadores de serviços externos que realizem operações de tratamento de dados.

Relativamente ao conhecimento dos inquiridos em relação à consulta prévia ao tratamento de dados, constatou-se que 44% responde correctamente, sendo que a maioria dos restantes inquiridos considera que a avaliação de impacto deve ser realizada sempre que o tratamento incidir sobre dados sensíveis, ao invés de a mesma ser realizada sempre que se concluir que o tratamento de dados pode resultar num risco elevado para o titular dos mesmos.

No que respeita à percepção dos inquiridos quando confrontados com a existência de certificação em matéria de protecção de dados, mais de metade responde correctamente considerando que, segundo o RGPD a organização de saúde pode obter a certificação. Relativamente à validade da mesma apenas 1

responde correctamente. A maioria dos restantes inquiridos considera que ainda não se encontra definido um prazo para a validade da certificação, ao invés de considerarem um período máximo de 3 anos. Pode então concluir-se que, os inquiridos têm a noção de que existe uma certificação em matéria de protecção de dados mas desconhecem a sua duração.

Coimas e Sanções (7)

No que concerne às coimas e sanções contempladas no RGPD, verificou-se que nenhum dos inquiridos respondeu correctamente à totalidade da questão. Cerca de 78% considera de forma correcta que, em caso de incumprimento das normas constantes no Regulamento, a organização poderá estar sujeita a uma coima de 20.000.000 € ou 4% do volume de negócios anual a nível mundial. É desta forma demonstrado um conhecimento parcial no que respeita à questão de coimas e sanções.

4.3 Limitações do campo de estudo

Podem ser apontadas algumas limitações relativas à realização do presente projecto, as quais são de quatro naturezas distintas.

Em primeiro lugar, a possibilidade de as conclusões deste projecto poderem apresentar um viés de informação no que respeita ao conhecimento real dos administradores hospitalares quanto ao novo RGPD. Como se abordará adiante, a lista perfaz um total de vinte administradores hospitalares, predominantemente do sector público, amostra considerada suficiente e relevante, mas de dimensão reduzida.

Em segundo lugar, a própria novidade do Regulamento Geral de Protecção de Dados em Portugal. Apesar de se tratar de um Regulamento aprovado a nível europeu há mais de dois anos, as acções de sensibilização e preparação para a aplicação deste documento em Portugal foram escassas, em particular no sector da saúde.

Em terceiro lugar, não existe ainda aprovada em Portugal uma nova lei de proteção de dados adaptada a este Regulamento. Tal poderá constituir uma limitação, na medida em que a aplicação deste Regulamento, apesar de não depender da sua transposição para a ordem jurídica interna, traz várias questões

práticas que são de difícil resolução num documento geral único e onde o espaço de soluções é muito abrangente, sendo útil aprovar posterior regulamentação nacional que execute as suas principais disposições.

Por fim, em quarto lugar, a dificuldade na obtenção de respostas por parte dos Administradores Hospitalares a quem se decidiu inquirir. Um dos motivos que contribuiu para tal foi o facto de determinados Administradores considerarem ainda não possuir um conhecimento que seria desejável para poder responder ao questionário, sendo que o objectivo seria que respondessem independentemente do conhecimento que possuíam na altura.

CAPITULO V

5. Conclusão e Recomendações

Em síntese, o presente trabalho de projecto, focou-se na realidade da administração hospitalar portuguesa quanto à temática de privacidade e confidencialidade dos dados, mais concretamente dos dados de saúde, no âmbito do novo Regulamento Geral de Protecção de Dados (RGPD).

A privacidade e protecção de dados de saúde é uma temática muito antiga, mas simultaneamente muito actual e premente na medida em que é objecto de desenvolvimentos recentes que prometem ter um impacto significativo na prestação de cuidados de saúde em particular e na área de gestão em saúde em geral, em virtude da entrada em vigor do novo Regulamento Geral de Protecção de Dados (RGPD) da UE.

Tal como demonstrado ao longo deste trabalho, assegurar e garantir a plena protecção destes dados deve ser uma responsabilidade não apenas dos profissionais de saúde, no decorrer da sua actividade e como agentes principais da prestação de cuidados de saúde, mas principalmente dos gestores de organizações de saúde, na sua capacidade de coordenadores e organizadores dos objectivos e processos das unidades hospitalares, sendo especialmente sobre estes que recaem as responsabilidades decorrentes da implementação e monitorização do RGPD, o qual impõe às entidades que recolhem e processam dados pessoais de saúde, tanto organizações privadas quanto públicas, deveres estritos e sanções significativas em caso de violação. Foi neste contexto que se procurou aferir o grau de conhecimento dos gestores de saúde, em particular dos administradores hospitalares, acerca do RGPD.

Foi muito elevado o meu interesse e motivação pela realização deste trabalho por ser um tema de extrema actualidade, em grande debate na sociedade e com uma exposição mediática muito importante, por ser de extrema relevância pessoal como utilizadora das novas tecnologias e, sendo um tema da área jurídica, apresenta extrema relevância para a área da saúde.

Como a seguir sistematizamos, pensamos ter atingindo os três principais objectivos do projecto: caracterizar o novo Regulamento Geral de Protecção de Dados da UE, contextualizando o seu conteúdo em relação a outras disposições

regulamentares e legais já existentes, aferir o grau de conhecimento dos gestores de organizações de saúde portuguesas, em particular dos Administradores Hospitalares, acerca das medidas e dos mecanismos necessários à protecção da informação de saúde dos utentes, no âmbito do RGPD e avaliar o grau de conhecimento dos referidos gestores acerca das inovações introduzidas pelo novo Regulamento Geral de Protecção de Dados da UE e o seu grau de preparação para responder às exigências da aplicação deste diploma jurídico.

O presente estudo permitiu concluir que o grau de preparação dos administradores hospitalares é, neste momento critico da entrada em vigor do RGPD, manifestamente insuficiente, em particular no que concerne os aspectos relevantes para o desempenho das suas responsabilidades nas organizações que gerem. Aliás, salienta-se que mesmo segundo a própria autoavaliação destes gestores, o seu nível de preparação e conhecimento não é o desejável. Elencam-se seguidamente as conclusões chave que suportam a conclusão enunciada:

1. Os administradores hospitalares consideram a temática do RGPD como uma questão meramente jurídica ou dizendo respeito aos apenas a área de sistemas de informação e em nenhuma unidade de saúde inquirida elevou esta questão ao nível estratégico ou transversal a toda a organização;
2. A maioria das organizações de saúde inquiridas lançaram medidas muito incipientes, consistindo nas acções mais básicas de levantamento das bases de dados existentes na unidade de saúde e a realização de algumas acções de formação para os colaboradores da organização;
3. Existe uma falta de clareza sobre a definição do responsável pelo tratamento de dados e sobre a sua natureza (individuo/estrutura orgânica);
4. Os inquiridos revelam um entendimento muito parcial sobre os direitos dos pacientes a luz do RGPD, em particular sobre novos direitos ai considerados (“direito de portabilidade dos dados” ou “direito ao esquecimento”);

5. Apenas a minoria dos inquiridos entende completamente a definição de dados pessoais e dados pessoais sensíveis, verificando-se interpretações erradas de que a condição que determina que os dados sejam pessoais é o facto de dizerem respeito a uma pessoa singular, qualquer que seja a sua natureza e sem consideração pelo facto de essa pessoa ser, ou não, identificável a partir desses dados.
6. Existe um bom entendimento sobre os objectivos e âmbito de aplicação do RGPD, mas com lacunas importantes no que concerne ao âmbito de aplicação territorial do RGPD;
7. Não existe um adequado domínio sobre as situações que constituem uma violação de dados pessoais, sendo este conceito maioritariamente entendido de forma muito limitada, ao invés da definição mais abrangente considerada no RGPD que passou a incluir a destruição, perda, alteração, divulgação ou o acesso não autorizados a dados pessoais e a desconsiderar se a violação tem origem acidental ou dolosa
8. Os administradores hospitalares não possuem um conhecimento adequado sobre o conceito de "protecção de dados desde a concepção e por defeito", e não dominam totalmente as técnicas de segurança de dados (processuais e tecnológicas)
9. Ainda são largamente desconhecidos os procedimentos e as necessidades de avaliação de impacto de risco no âmbito da segurança dos dados, as condições em que uma violação de dados deve ser comunicada segundo o RGPD, os casos em que derrogações ao tratamento podem ser obtidas
10. Finalmente, não estão ainda interiorizadas nos administradores hospitalares, as sanções e coimas que foram introduzidas com o RGPD.

No contexto das conclusões acima elencadas, deixamos em seguida também recomendações às organizações hospitalares em geral e aos administradores hospitalares em particular:

1. Obtenção de consentimento explicito por parte dos pacientes: o Artigo 9 do RGPD reflecte a base legal para a obtenção de consentimento. Nesta área os administradores hospitalares e os hospitais deverão ir mais além

e garantir que os pacientes entendem e aceitam os termos legais, os quais devem ser urgentemente alterados.

2. Comunicação com os pacientes: segundo o RGPD, o nível de informação que é devido aos pacientes eleva-se a um padrão de exigência nunca antes visto. Como vimos, essa informação devera conter um conjunto mínimo de elementos que devem ser fornecidos aos pacientes de forma imediata. Recomenda-se a inventariação da informação actualmente retida pela organização em relação aos seus pacientes e progressivamente tornar essa informação e o seu acesso completamente compatível com o RGPD.
3. Nomeação de um Responsável pelo Tratamento de Dados: a nomeação deste responsável é obrigatória quando a unidade hospitalar processa um número elevado de informações sensíveis. No entanto, recomenda-se a nomeação deste responsável em todas as organizações hospitalares, com estatura estratégica na organização e com a responsabilidade de liderar o necessário processo de mudança decorrente das disposições do RGPD.
4. Lançamento das avaliações de impacto: uma das responsabilidades dos administradores hospitalares que decorre do RGPD é a necessidade de serem realizados exercícios de avaliação de impacto. Estes exercícios são fundamentais para os administradores hospitalares, pois permitirão, não apenas, identificar os principais riscos e lacunas da organização no âmbito do RGPD, mas também permitirão delinear os necessários programas para a correcção dos riscos relevantes identificados.
5. Registo das actividades de processamento: Também decorre do RGPD que as organizações devem possuir um registo permanente das actividades de processamento que realizam. Como vimos anteriormente, esse registo devera ser estruturado e conter um conjunto mínimo de informação. Neste contexto, o cadastro das actividades de processamento é uma das prioridades das organizações hospitalares
6. Definição e lançamento de um plano de sensibilização e formação: Considerando o globalmente reduzido nível de conhecimento dos administradores hospitalares sobre o RGPD e suas implicações para as organizações hospitalares, recomenda-se o lançamento de programas

estruturados de sensibilização, esclarecimento e formação em torno do conteúdo do RGPD. Tal esforço devera ser seguido da constituição de grupos de trabalho multidisciplinares que possam, em articulação com toda a organização, desenvolver programas coerentes e detalhados de preparação para a conformidade com o RGPD.

Verificou-se que, no domínio da saúde, os desafios da confidencialidade são muito elevados, essencialmente por se tratar de um ambiente onde circulam grandes quantidades de informação e "dados sensíveis", e por isso não só se destaca o reforço das medidas de segurança já existentes como se exige a implementação de novas medidas.

A entrada em vigor do novo Regulamento Geral de Protecção de Dados terá um impacto significativo na gestão e tratamento dos dados pessoais dos pacientes nas organizações hospitalares e a exigência que coloca aos gestores de saúde, considerando o seu actual nível de preparação, será um dos maiores desafios com que se confrontarão nos próximos tempos.

BIBLIOGRAFIA

Bibliografia

1. Faria PL De, Cordeiro JV. Health data privacy and confidentiality rights: Crisis or redemption? Rev Port Saúde Pública [Internet]. 2014 Jul;32(2):123–33. Available from: http://dx.doi.org/10.1016/j.rpsp.2014.10.001
2. Instituto PHG. Pesquisa quantitativa e pesquisa Qualitativa: entenda a diferença [Internet]. [cited 2018 Jul 30]. Available from: https://www.institutophd.com.br/pesquisa-quantitativa-e-pesquisa-qualitativa-entenda-a-diferenca/
3. Manzato AJ, Santos AB. A elaboração de questionários na pesquisa quantitativa. Dep Ciência Comput e Estatística – IBILCE – UNESP [Internet]. 2012;1–17. Available from: http://www.inf.ufsc.br/~vera.carmo/Ensino_2012_1/ELABORACAO_QUESTIONARIOS_PESQUISA_QUANTITATIVA.pdf%0Ahttp://www.inf.ufsc.br/~verav/Ensino_2012_1/ELABORACAO_QUESTIONARIOS_PESQUISA_QUANTITATIVA.pdf
4. Gil AC. Métodos e técnicas de pesquisa social. 6 th. S.Paulo: Editora Atlas; 2008.
5. Carmo V. O uso de questionários em trabalhos científicos. 2013;14. Available from: http://www.inf.ufsc.br/~vera.carmo/Ensino_2013_2/O_uso_de_questionarios_em_trabalhos_cient%EDficos.pdf
6. Norberto Robl Filho I. Direito, intimidade e vida privada: uma perspectiva histórico-política para uma delimitação contemporânea. Rev Electrónica do CEJUR [Internet]. 2006;1:184–205. Available from: https://www.researchgate.net/publication/228639869_Direito_Intimidade_e_Vida_Privada_uma_perspectiva_historico-politica_para_uma_delimitacao_contemporanea
7. Sokalska ME. Medical Confidentiality – Quo vadis? Eur J Health Law. 2004;11:35–43.
8. Ordem dos Médicos. Juramento de Hipócrates: fórmula de Genebra: adoptado pela Associação Médica Mundial em 1983. Lisboa: Ordem dos

Médicos; 2017. [cited. 10.1.2018]. Available from: http://ordemdosmedicos.pt/wp-content/uploads/2017/08/Juramento_de_Hip%C3%B3crates.pdf

9. Warren SD, Brandeis LD. The right to privacy. Harv Law Rev. 1890;4(5):193–220.
10. The World Medical Association. Declaration of Geneva: Adopted by the 2nd General Assemblyof the World Medical Association, Geneva, Switzerland, Semptember 1948. Geneva: The world Medical Association; 2006. [cited. 21.2.2018] Disponível em: https://www.wma.net/policies-post/wma-declaration-of-geneva/wma_declaration-of-geneva_a2_en/
11. Declaração de Helsínquia da Associação Médica Mundial: [versão de outubro de 2013]: Princípios Éticos para a Investigação Médica em Seres Humanos: adoptada pela 18.ª Assembleia Geral da AMM, Helsínquia, Finlândia, junho 1964. Helsínquia: Associação Médica Mundial; 2013. [cited.21.2.2018]. Available from: http://ispup.up.pt/docs/declaracao-de-helsinquia.pdf;
12. American Hospital Association. A Patient's bill of rights. 1992;
13. Annas GJ, Glantz LH, Roche PA. The genetic privacy act and commentary. Boston, MA: Health Law Department. Boston University School of Public Health;. 1995;(617). [cited13.3.2018]. Available from: https://web.ornl.gov/sci/techresources/Human_Genome/resource/privacyact.pdf
14. UNESCO. International Declaration on Human Genetic Data [Internet]. 2003 [cited 2018 Jan 10]. Available from: http://www.unesco.org/new/en/social-and-human-sciences/themes/bioethics/human-genetic-data/
15. UNESCO. Declaração Universal sobre Bioética e Direitos Humanos. 2005;1–12. Available from: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Declara??o+Universal+sobre+Bio?tica+e+Direitos+Humanos#6
16. Braga Paiano D. Direito à intimidade e à vida privada. 2003;19. Available from: https://www.diritto.it/archivio/1/21084.pdf
17. Boguslaw R, Westin AF. Privacy and freedom. Am Sociol Rev [Internet]. 1968;33(1):173. Available from:

http://www.jstor.org/stable/2092293?origin=crossref
18. Wright D, Raab C. Privacy principles, risks and harms. Int Rev Law, Comput Technol [Internet]. 2014 Sep 2;28(3):277–98. Available from: http://www.tandfonline.com/doi/abs/10.1080/13600869.2014.913874
19. Leenen HJJ, Pinet G, Prims AV. Trends in health legislation in Europe. Paris: Masson; 1986.
20. Leenen HJJ. The rights of patients in Europe. Eur J Health Law. 1994;1:5–15.
21. Surbhi S. Difference between privacy and confidentiality [Internet]. 2015 [cited 2017 Dec 10]. Available from: https://keydifferences.com/difference-between-privacy-and-confidentiality.html
22. Cordeiro JV. A quebra do dever de sigilo por imposição do tribunal (art. 135.º do CPP) depois de ouvida a Ordem dos Advogados. Rev Ordem dos Advogados [Internet]. 2016;76:299–338. Available from: http://carlospintodeabreu.com/public/files/sigilo_profissional_jvc.pdf
23. Beauchamp T, Childress J. Principles of biomedical ethics. 6th ed. New York: Oxford University Press; 2009.
24. Stanberry B. Legal and ethical aspects of telemedicine. J Telemed Telecare [Internet]. 2006 Jun 24;12(4):166–75. Available from: http://journals.sagepub.com/doi/10.1258/135763306777488825
25. Comissão Nacional de Protecção de Dados. Fórum de Protecção de Dados [Internet]. 4th ed. Comissão Nacional de Protecção de Dados; 2017. Available from: https://www.cnpd.pt/bin/revistaforum/forum2017_1/files/assets/common/downloads/forum_de_protecao_de_dados_4.pdf
26. Berle I. Privacy and confidentiality: what is the difference? J Vis Commun Med [Internet]. 2011 Mar 7;34(1):43–4. Available from: http://www.tandfonline.com/doi/full/10.3109/17453054.2011.550845
27. União Europeia. Regulamento Geral de Proteção de Dados da União Europeia. Jornal Oficial da União Europeia 2016 p. 156.
28. University VPI and S. Protecting confidentiality & anonymity [Internet]. [cited 2017 Dec 13]. Available from: https://www.irb.vt.edu/pages/confidentiality.htm
29. Beltran-Aroca CM, Girela-Lopez E, Collazo-Chao E, Montero-Pérez-

Barquero M, Muñoz-Villanueva MC. Confidentiality breaches in clinical practice: what happens in hospitals? BMC Med Ethics [Internet]. 2016 Dec 2;17(1):52. Available from: http://www.ncbi.nlm.nih.gov/pubmed/27590300

30. Villas-Bôas ME. O direito-dever de sigilo na proteção ao paciente. Rev Bioética [Internet]. 2015 Dec;23(3):513–23. Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1983-80422015000300513&lng=pt&tlng=pt
31. Salz T. HIPAA: Training critical to protect patients, practice. Med Econ. 2013;43–7.
32. Abbing HR. Medical confidentiality and patient safety: Reporting procedures. Eur J Health Law. 2014;21(3):245–59.
33. Ellis JE, Klock PA, Mingay DJ, Roizen MF. Use of electronic mail for postoperative follow-up after ambulatory surgery. J Clin Anesth [Internet]. 1999 Mar;11(2):136–9. Available from: http://linkinghub.elsevier.com/retrieve/pii/S0952818099000057
34. Freed DH. Patient-physician e-mail: passion or fashion?. Health Care Manag (Frederick) [Internet]. 2003;22(3):265–74. Available from: http://ovidsp.ovid.com/ovidweb.cgi?T=JS&PAGE=reference&D=med4&NEWS=N&AN=12956229
35. Sampaio SS, Rodrigues FW. Ética e sigilo profissional. Serviço Soc Soc [Internet]. 2014 Mar;(117):84–93. Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0101-66282014000100006&lng=pt&nrm=iso&tlng=en
36. Castells M. The impact of the internet on society: a global perspective [Internet]. MIT Technology Review. 2014 [cited 2018 May 12]. Available from: https://www.technologyreview.com/s/530566/the-impact-of-the-internet-on-society-a-global-perspective/
37. Doneda D. A proteção dos dados pessoais como um direito fundamental. Espaço Jurídico [Internet]. 2011;12(2):91–108. Available from: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315
38. Abouelmehdi K, *et al*. Big data security and privacy in healthcare: A Review. Procedia Comput Sci [Internet]. 2017;113:73–80. Available from: https://eds.a.ebscohost.com/eds/detail/detail?vid=2&sid=38a044a7-2f2a-

4db4-b874-
0ed87ca185ea%40sessionmgr4008&bdata=JkF1dGhUeXBlPWlwLGNvb
2tpZSxzaGliLHVpZCZsYW5nPXB0LWJyJnNpdGU9ZWRzLWxpdmUmc2
NvcGU9c2l0ZQ%3D%3D#AN=S1877050917317015&db=edselp

39. Ferreira da Silva H, Carlos Relvão Caetano J, Curado H. Gestão de informação pessoal em saúde. Rev Adm em Saúde [Internet]. 2011;13(53). Available from: http://recipp.ipp.pt/bitstream/10400.22/3843/1/ART_HumbertaSilva_2011.pdf
40. Sales-Peres A, *et al*. Sigilo profissional e valores éticos. Rev da Fac Odontol [Internet]. 2008;7–13. Available from: http://www.upf.br/seer/index.php/rfo/article/view/583
41. Kirimlioglu N. “The right to privacy” and the patient views in the context of the personal data protection in the field of health. Biomed Res. 2017;28(4):1464–71.
42. Nayeri ND, Aghajani M. Patient’s privacy and satisfaction in the emergency department: a descriptive analytical study. Nursing Ethics. 2010; 17(2):167-177. DOI: 10.1177/0969733009355377
43. Aydin N. Legal dimension of patient rights and their protection. Dumlupinar Univ J Soc Sci. 2008;297–326.
44. Pupulim JSL, Sawada NO. Privacidade física referente à exposição e manipulação corporal: percepção de pacientes hospitalizados. Texto Context - Enferm [Internet]. 2010 Mar;19(1):36–44. Available from: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0104-07072010000100004&lng=pt&tlng=pt
45. Morganheira D, Silva P, Pereira R, Ruivo A. Preservação do direito à privacidade: perceção do doente internado. Revista Ibero-Americana de Saúde e Envelhecimento. 2017 Aug;3:1000–12.
46. Minor D. Harnessing the power of data in health. Stanford Med [Internet]. 2017;(June). Available from: https://med.stanford.edu/content/dam/sm/sm-news/documents/StanfordMedicineHealthTrendsWhitePaper2017.pdf
47. Hordern V. The treatment of health data under the EU data protection regulation – cause for hope? [Internet]. Chronicle of Data Protection -

Privacy & Information Security News & Trends. 2015 [cited 2018 Mar 12]. Available from: https://www.hldataprotection.com/2016/01/articles/health-privacy-hipaa/the-final-gdpr-text-and-what-it-will-mean-for-health-data/

48. López JD, *et al*. Business processes management implementation in health sector. Int J Manag Public Sect Inf Commun Technol [Internet]. 2016;7(4):1–10. Available from: https://pdfs.semanticscholar.org/a927/a640e99d9b6ead29be63fb722201f250db93.pdf
49. Summerfield R. Operational risk management in financial services [Internet]. Financier Worldwide Magazine. 2018 [cited 2018 Jul 20]. Available from: https://www.financierworldwide.com/operational-risk-management-in-financial-services/#.W1ojCIOFM0Q
50. Simoni G De, Edjlali R. Magic quadrant for metadata management solutions. Gart Repr [Internet]. 2017;1–26. Available from: https://www.gartner.com/doc/3778891/magic-quadrant-metadata-management-solutions
51. Ebel T, Larsen E, Shah K. Strengthening health care's supply chain: A five-step plan [Internet]. 2013 [cited 2018 Jul 20]. Available from: https://www.mckinsey.com/industries/healthcare-systems-and-services/our-insights/strengthening-health-cares-supply-chain-a-five-step-plan
52. E-estonia healthcare [Internet]. [cited 2018 Jul 20]. Available from: https://e-estonia.com/solutions/healthcare/e-health-record/
53. SPMS - Serviços Partilhados do Ministério da Saúde. RSE – Registo de Saúde Eletrónico [Internet]. [cited 2018 Jul 29]. Available from: http://spms.min-saude.pt/product/area-cidadao/
54. Me Learning. GDPR and the NHS: Top five GDPR challenges for healthcare [Internet]. 2018 [cited 2018 Jul 22]. Available from: https://www.melearning.co.uk/2018/01/gdpr-nhs-top-five-gdpr-challenges-healthcare/
55. Future Health Index. Building systems for better outcomes [Internet]. [cited 2018 Jul 20]. Available from: https://www.futurehealthindex.com/report/2018/
56. A guide to healthcare IoT possibilities and obstacles [Internet].

TechTarget. [cited 2018 Jul 22]. Available from: https://searchhealthit.techtarget.com/essentialguide/A-guide-to-healthcare-IoT-possibilities-and-obstacles

57. Bar-Yoseph H. Social media use and the doctor-patient relationship - is progression really leading us forward? Harefuah [Internet]. 2017;156(8):527–8. Available from: http://www.ncbi.nlm.nih.gov/pubmed/28853531
58. O'Dowd E. EU Data Privacy Rule GDPR Impacts US Health IT Infrastructure [Internet]. Hit Infrastructure. 2018 [cited 2018 Jul 22]. Available from: https://hitinfrastructure.com/news/eu-data-privacy-rule-gdpr-impacts-us-health-it-infrastructure
59. European Comission [Internet]. [cited 2018 Jul 20]. Available from: https://ec.europa.eu/health/ern_en
60. Hansen MM, Miron-Shatz T, Lau AYS, Paton C. Big Data in Science and Healthcare: A Review of Recent Literature and Perspectives. IMIA Yearb. 2014;9(1):21–6.
61. MetaCompliance. GDPR Best Practices Implementation Guide - Transforming GDPR Requirements into Compliant Operational Behaviours [Internet]. London; Available from: https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000
62. Li F, Zou X, Liu P, Chen JY. New threats to health data privacy. BMC Bioinformatics [Internet]. 2011;12(Suppl 12):S7. Available from: http://bmcbioinformatics.biomedcentral.com/articles/10.1186/1471-2105-12-S12-S7
63. Raab C, Szekely I. Data protection authorities and information technology. Comput Law Secur Rev [Internet]. 2017 Aug;33(4):421–33. Available from: http://dx.doi.org/10.1016/j.clsr.2017.05.002
64. Davies SR. Patient privacy : The evolution of protecting health information historical professional paper. 2016. 2-39 p.
65. Gonçalves ME, Raimundo J. Over troubled water : e-health platforms and the protection of personal data : the case of Portugal. PortJ Public Health 2017;35(1)52–66. doi:10.1159/000477650
66. Griener G. Electronic health records as a threat to privacy. Health Law

Rev [Internet]. 2005;14(1):14–7. Available from: http://www.ncbi.nlm.nih.gov/pubmed/16538771

67. CNECV. Parecer n.º 60 - sobre informação de saúde e registos informáticos de saúde. Cons Nac Ética para as Ciências da Vida. 2011;1–7.
68. CNPD - Comissão Nacional de Protecção de Dados. Comissão Nacional de Protecção de Dados [Internet]. [cited 2018 Nov 10]. Available from: https://www.cnpd.pt/index.asp
69. Myers J, Frieden TR, Bherwani KM, Henning KJ. Privacy and Public Health at Risk: Public Health Confidentiality in the Digital Age [Internet]. Vol. 98, American Journal of Public Health. 2008. p. 793–801. Available from: http://ajph.aphapublications.org/doi/10.2105/AJPH.2006.107706
70. Unidas O-O das N. Declaração Universal dos Direitos do Homem. 1948; Available from: https://www.pcp.pt/actpol/temas/dhumanos/declaracao.html
71. Assembleia da República. Convenção de Oviedo - Convenção sobre os Direitos do Homem e da Biomedicina (Conselho da Europa 1997). Diário da Repub. 2001;1(2):14–36.
72. European Data Protection Supervisor. The history of the general data protection regulation [Internet]. [cited 2018 Jul 10]. Available from: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en
73. Lei Constitucional nº1/2005. D.R. 1ª Série-A.155 (12.08.2005) 4642-4686. Constituiçao da República Portuguesa: sétima revisão constitucional. Artigo 3ª (Soberania e legalidade)
74. Lei n.º 48/90. Diário da República n.º 195/1990, Série I. 1990-08-24 (3452 – 3459). Lei de Bases da Saúde.
75. Lei n.º 67/98. Diário da República n.º 247/1998, Série I-A. 1998-10-26 (5536 – 5546). Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados).
76. Lei n.º 46/2007. Assembleia da República. Lei de Acesso aos

Documentos Administrativos (LADA). 2007;1–9. Available from: http://www.dre.pt/pdf1s/2007/08/16300/0568005687.pdf

77. CADA - Comissão de Acesso aos Documentos Administrativos [Internet]. [cited 2018 Apr 12]. Available from: http://cada.pai.pt/ms/ms/cada-comissao-de-acesso-aos-documentos-administrativos-localizacao-e-contactos-1200-821-lisboa/ms-90047911-p-5/
78. Porto Editora. Código penal. 6ª edição. Porto: Porto Editora; 2017. (Legislação - Edição Académica). ISBN: 978-972-0-00045-3
79. Associação Portuguesa de Administradores Hospitalares. A profissão de Administrador Hospitalar [Internet]. [cited 2018 Aug 15]. Available from: https://apah.pt/administrador-hospitalar/
80. Williamson C. Pseudonymization vs. anonymization and how they help with GDPR [Internet]. Protegrity Blog. 2017 [cited 2018 Jul 20]. Available from: https://www.protegrity.com/pseudonymization-vs-anonymization-help-gdpr/

ANEXOS

Anexo I – Ofício de Solicitação de Colaboração de Aluno do CMGS da ENSP – UNL, para elaboração de Dissertação de Mestrado

Escola Nacional de Saúde Pública
UNIVERSIDADE NOVA DE LISBOA

Exmo(a) Senhor(a)
Presidente do Conselho de Administração

Lisboa, 2018-03-21

Assunto: *Solicitação de colaboração em projeto científico do XII Curso de Mestrado em Gestão da Saúde da Escola Nacional de Saúde Pública da Universidade Nova de Lisboa (ENSP-UNL)*

Venho por este meio solicitar a sua colaboração no projeto científico no âmbito do XII Curso de Mestrado em Gestão da Saúde da ENSP-UNL, intitulado: ***"Proteção de dados de saúde – perceção e conhecimento dos Administradores Hospitalares acerca do novo Regulamento Geral de Proteção de Dados da União Europeia"***. Este projeto é da responsabilidade da discente Ana Rita Ramos Y Rio Tinto, e conta com a orientação do Prof. Doutor João Valente Cordeiro e da Prof.ª Doutora Paula Lobato Faria, ambos Professores da ENSP-UNL. O projeto terá como objetivo principal avaliar a perceção e o grau de conhecimento dos Administradores Hospitalares acerca das principais disposições do novo Regulamento Geral de Proteção de Dados da UE. O projecto tem como metodologia principal a realização de um breve questionário anónimo, que se envia em anexo, a ser preenchido por V. Exa. ou, alternativamente, por outro Administrador Hospitalar, membro do Conselho de Administração. Desta forma, e tendo em vista a melhor realização deste trabalho científico, solicitamos a colaboração na resposta do questionário em anexo.

Os dados resultantes desta investigação são anónimos e confidenciais e serão tratados unicamente pela equipa do projeto acima descrita, no mais absoluto respeito pelos princípios éticos da investigação científica.

Na expectativa do melhor acolhimento deste pedido e agradecendo antecipadamente a sua colaboração, despeço-me com os meus melhores cumprimentos.

João Pereira, *Professor Doutor*
DIRECTOR

Contacto de e-mail da mestranda:
Ana Rita Ramos Y Rio Tinto: a.riotinto@ensp.unl.pt

Anexo II - Questionário sobre o novo Regulamento Geral de Protecção de Dados da União Europeia

Projecto de investigação de Mestrado em Gestão da Saúde, realizado pela aluna Ana Rita Ramos Y Rio-Tinto, da Escola Nacional de Saúde Pública – Universidade Nova de Lisboa, sob a orientação do Prof. Doutor João Valente Cordeiro e da Prof. Doutora Paula Lobato Faria.

Objectivo: O projecto terá como objectivo principal avaliar a percepção e o grau de conhecimento dos Administradores Hospitalares acerca das principais disposições do novo Regulamento Geral de Protecção de Dados da UE.

Tempo de resposta estimado: 15 minutos

Procedimento: O presente questionário é composto por 27 questões de escolha múltipla, compreendendo as diversas áreas do Regulamento, como definições e questões gerais, direitos dos titulares e procedimentos considerados obrigatórios para protecção dos mesmos bem como às formas como o processo de tratamento de dados deve ser executado e potenciais sanções.
Em resposta ao questionário, por favor assinale todas as respostas que entender serem corretas.
A obtenção de uma elevada taxa de resposta a este questionário garantirá uma maior taxa de representatividade das conclusões do presente estudo, pelo que se solicita o maior nível de participação possível.
Muito obrigado pela sua participação.

Rita Rio-Tinto
E-mail: a.riotinto@ensp.unl.pt

***1**: Indique, por favor, o número de anos de experiência que possui em funções de administração hospitalar:*

a) < 5 anos
b) 5 -10 anos
c) > 10 anos

***2**: Entrou em vigor, a 27 de Abril de 2016, do Regulamento da União Europeia relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral de Proteção de Dados (RGPD)), cuja data de aplicação é 25 de Maio de 2018. Como classificaria o seu conhecimento acerca deste diploma?*

a) Elevado (conheço detalhadamente o RGPD e as suas principais disposições)
b) Médio (conheço de forma geral o RGPD e as suas principais disposições)
c) Baixo (apenas tenho conhecimento da existência de um novo Regulamento da UE sobre protecção de dados pessoais)

***3**: De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por "responsável pelo tratamento" de dados pessoais:*

a) Um profissional que assume a responsabilidade pelos processos de tratamento de dados pessoais e pela manutenção do cadastro dos titulares dos dados
b) A pessoa singular ou colectiva, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios de tratamento de dados pessoais
c) Uma entidade subcontratada pela entidade beneficiária, a quem caberá controlar e auditar os processos, bases de dados e

sistemas informáticos utilizados pelos seus colaboradores no tratamento de dados pessoais ☐

***4**: Existe atualmente, no seu hospital, um departamento/gabinete específico que seja responsável pelas questões relacionadas com a proteção dos dados de saúde dos utentes?*

a) Sim ☐
b) Não ☐

***5**: Se a sua resposta à questão anterior foi "Sim", **indique por favor qual, ou quais,** das seguintes categorias melhor enquadrada o departamento/gabinete em questão (escolha todas as opções que considera correctas):*

a) Departamento/Gabinete Jurídico ☐
b) Departamento/Gabinete de Sistemas de Informação ☐
c) Departamento/Gabinete de Gestão de Utentes ☐
d) Departamento/Gabinete Planeamento e Controlo de Gestão ☐
e) Departamento/Gabinete de Auditoria ☐
f) Departamento/Gabinete de Compliance ☐
g) Comissão de Ética ☐
h) Outro (especifique) _____ ☐

***6**. Em que medida a unidade de saúde em que exerce funções se preparou para a entrada em vigor e respetiva implementação do RGPD (escolha todas as opções que considera correctas)?*

a) Não levou a cabo qualquer ação específica nesse sentido ☐
b) Realizou ações de formação dirigidas aos colaboradores ☐
c) Procedeu à revisão de procedimentos que envolvem o tratamento de dados pessoais na unidade de saúde ☐

d) Efetuou o levantamento das bases de dados existentes na unidade de saúde e verificou a sua adequação ao RGPD
e) Outras ações (especifique) _____

***7**: De acordo com a sua percepção e conhecimento do RGPD, o "direito de acesso" do titular dos dados implica que este tem o direito de obter junto do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objecto de tratamento, e se for esse o caso, o direito de aceder às seguintes informações (escolha todas as opções que considera correctas):*

a) A localização geográfica do seu armazenamento e tratamento (dentro ou fora da União)
b) As finalidades do tratamento de dados
c) A lista de entidades subcontratadas que procedem ao tratamento dos dados
d) O prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para fixar esse prazo
e) A lista de entidades a quem essa informação irá ser divulgada
f) Qualquer rectificação aos dados pessoais originalmente fornecidos

***8**: De acordo com a sua percepção e conhecimento do RGPD, o "direito a ser esquecido" do titular dos dados implica que este tem o direito a obter, junto do responsável pelo tratamento, o apagamento dos seus dados pessoais sem demora injustificada, quando se apliquem os seguintes motivos (escolha todas as opções que considera correctas):*

a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento
b) Sempre que se registar o falecimento do titular dos dados, bastando o apagamento ser solicitado pelos seus legais representantes
c) O titular retira o consentimento em que se baseia o tratamento dos dados, se não existir outro fundamento jurídico para o referido tratamento
d) Será sempre obrigatório o apagamento dos dados mediante declaração expressa nesse sentido do titular dos mesmos, independentemente dos motivos para tal requerimento

***9**: De acordo com a sua percepção e conhecimento do RGPD, o titular dos dados tem o direito de obter do responsável pelo tratamento a limitação do tratamento, no caso de se aplicarem as seguintes situações (escolha todas as opções que considera correctas):*

a) O titular passou a residir em território fora da União Europeia
b) O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização
c) Cessação da actividade do estabelecimento
d) O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial

e) Contestar a exatidão dos dados pessoais durante um período que permita ao responsável pelo tratamento verificar a sua exatidão

***10**: De acordo com a sua percepção e conhecimento do RGPD, o responsável pelo tratamento de dados deverá assegurar o direito do titular à portabilidade dos mesmos:*

a) Fornecendo ao titular dos dados os dados pessoais que lhe digam respeito, num formato estruturado de uso corrente e de leitura automática
b) Transmitindo os dados à Autoridade Nacional Competente, para que esta decida se os mesmos podem ser disponibilizados a outras entidades
c) Assegurando o armazenamento dos dados pessoais em formato normalizado, usando tecnologia portável e standards de mercado.
d) Transmitindo os dados, num formato estruturado de uso corrente e de leitura automática, a outro responsável pelo tratamento, mediante determinadas condições

***11**. De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por "dados pessoais":*

a) Informação relativa a uma pessoa singular, identificada ou identificável (titular dos dados), directa ou indirectamente, em especial por referência a um identificador como por exemplo um número de identificação.
b) Informação relativa a uma pessoa singular ou colectiva, identificada ou identificável (titular dos dados), directamente por referência a um identificador como por exemplo um número de identificação.

c) Dados resultantes de tratamentos técnicos específicos relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação dessa pessoa.

d) Qualquer tipo de dados detidos pela entidade relativamente a uma pessoa singular

***12**: De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por "Dados relativos à saúde":*

a) Um subconjunto de dados pessoais, relativos a informação biométrica e biológica

b) Todos os dados pessoais recolhidos por unidades que prestem serviços de saúde.

c) 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.

***13**. De acordo com a sua percepção e conhecimento, o novo Regulamento Geral de Proteção de Dados (RGPD) da UE estabelece:*

a) Um novo enquadramento jurídico, mais abrangente, em matéria de proteção de dados

b) Uma mera atualização, sem grandes inovações, da legislação europeia na área da proteção de dados

c) Não sabe/não responde

***14**. De acordo com a sua percepção e conhecimento, o novo Regulamento Geral de Proteção de Dados (RGPD) da UE aplica-se ao tratamento de dados pessoais:*

a) No contexto das actividades de um estabelecimento responsável pelo tratamento situado no território da UE, independentemente desse tratamento ocorrer dentro ou fora da UE
b) Relativo a qualquer cidadão da UE, independentemente do local do tratamento e do local de estabelecimento do responsável pelo tratamento
c) Realizado apenas dentro da UE, independentemente do local de estabelecimento do responsável pelo tratamento e do local da residência dos titulares dos dados

***15**: De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por "violação de dados pessoais":*

a) Uma violação da segurança que provoque, de modo acidental ou doloso, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer ouro tipo de tratamento.
b) Uma violação da segurança que provoque, de modo ilícito, o acesso, não autorizado, a dados pessoais transmitidos, conservados ou sujeitos a qualquer ouro tipo de tratamento
c) Uma violação da segurança que provoque, de modo acidental ou lícito, 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.
d) Uma violação da segurança que provoque, de modo ilícito, o acesso e a divulgação, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento

***16**: De acordo com a sua percepção e conhecimento, o tratamento dos dados pessoais, segundo o RGPD, só é lícito se e na medida em que se verifique pelo menos uma das seguintes condições (escolha todas as opções que considera correctas):*

a) O tratamento dos dados for determinado por entidade pública ou órgão governamental
b) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas.
c) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular.
d) Os dados pessoais tratados forem relativos a cidadãos não residentes na UE

***17**: De acordo com a sua percepção e conhecimento do RGPD, quais as condições aplicáveis ao consentimento para o tratamento de dados pessoais (escolha todas as opções que considera correctas):*

a) O consentimento dos dados deve ser dado livremente por parte do titular dos dados
b) Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita, este deve ser apresentado de forma que o distinga claramente de outros assuntos
c) O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento.

***18**: De acordo com a sua percepção e conhecimento do RGPD, é, em princípio, proibido o tratamento das seguintes categorias de dados pessoais:*

a) A origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical.
b) Dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca.
c) Dados relativos à saúde.
d) Todas as opções anteriores.

☐

***19**: De acordo com a sua percepção e conhecimento do RGPD, quando os dados pessoais forem tratados para fins de investigação científica ou histórica ou para fins estatísticos, o Direito da União ou dos Estados-Membros pode, sob certas condições, prever derrogações as seguintes direitos (escolha todas as opções que considera correctas):*

a) Direito de acesso do titular dos dados ☐
b) Direito de portabilidade dos dados ☐
c) Direito de rectificação dos dados ☐
d) Direito ao apagamento dos dados ("direito a ser esquecido") ☐

***20**: De acordo com a sua percepção e conhecimento do RGPD, entende-se por "protecção de dados desde a concepção e por defeito", o seguinte (escolha todas as opções que considera correctas):*

a) Proteção de dados no momento da definição dos meios de tratamento e no momento do próprio tratamento ☐
b) Restrição do tratamento apenas aos dados pessoais que forem necessários para cada finalidade específica ☐
c) Protecção dos dados apenas no momento do seu armazenamento ☐
d) Tratamento de dados generalizado mas armazenamento apenas dos dados necessários para cada finalidade específica ☐

***21**: De acordo com a sua percepção e conhecimento do RGPD, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos para os direitos e liberdades das pessoas singulares, o responsável do tratamento deve aplicar medidas técnicas e organizativas, para assegurar um nível de*

segurança adequado ao risco, entre as quais (escolha todas as opções que considera correctas):

a) O apagamento regular dos dados tidos por confidenciais
b) A utilização permanente das técnicas de anonimização de dados mais recentes
c) A pseudonimização e a cifragem dos dados pessoais
d) Um processo para testar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento
e) Assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento

***22**: De acordo com a sua percepção e conhecimento do RGPD, em caso de violação dos dados pessoais, o responsável pelo tratamento deve (escolha todas as opções que considera correctas):*

a) Dar imediatamente a conhecer ao titular que ocorreu a violação dos seus dados, independentemente do risco para os direitos, liberdades e garantias das pessoas singulares.

b) Notificar esse facto à autoridade de controlo competente, sem demora injustificada, até 72 horas após ter tido conhecimento da violação de dados pessoais, a menos que a violação não resulte num risco para os direitos, liberdades e garantias das pessoas singulares

c) Lançar um procedimento interno para fazer face ao problema, a menos que a violação não resulte num risco para os direitos, liberdades e garantias das pessoas singulares

d) Comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada, em caso de elevado risco para os direitos, liberdades e garantias das pessoas singulares.

***23**: De acordo com a sua percepção e conhecimento do RGPD, a avaliação de impacto das operações de tratamento previstas sobre a protecção de dados deve ser realizada pelo responsável pelo tratamento, antes de iniciar o tratamento, quando:*

a) Sejam contratados prestadores de serviços externos que realizem operações de tratamento de dados

b) Sejam alterados processos internos que impliquem mudanças no tratamento dos dados pessoais

c) Sempre que o conjunto de dados pessoais recolhidos junto dos titulares seja aumentado

d) O tratamento, tendo em conta a sua natureza, âmbito e finalidades, for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares

***24**: De acordo com a sua percepção e conhecimento do RGPD, o responsável pelo tratamento dos dados deve consultar a autoridade de controlo, antes de proceder ao tratamento quando:*

a) O tratamento dos dados implicar a sua transmissão para território fora da União Europeia
b) A avaliação de impacto sobre a protecção de dados indicar que do tratamento resultará num elevado risco para o titular dos dados
c) Sempre que o tratamento incidir sobre dados pessoais sensíveis
d) Nunca é necessária a consulta no caso de tratamento de dados pessoais não sensíveis

***25**: De acordo com a sua percepção e conhecimento do RGPD, encontra-se previsto algum tipo de certificação em matéria de protecção dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente Regulamento.*

a) Sim ☐
b) Não ☐

***26**: No caso de ter respondido "Sim" à questão anterior, manifeste-se quanto à duração máxima da validade da certificação:*

a) permanente ☐
b) válida por um período de 2 anos ☐
c) válida por um período máximo de 3 anos ☐
d) ainda não se encontra definido o prazo ☐

***27**: De acordo com a sua percepção e conhecimento do RGPD a violação das suas disposições pode estar sujeita às seguintes sanções (escolha todas as opções que considera correctas):*

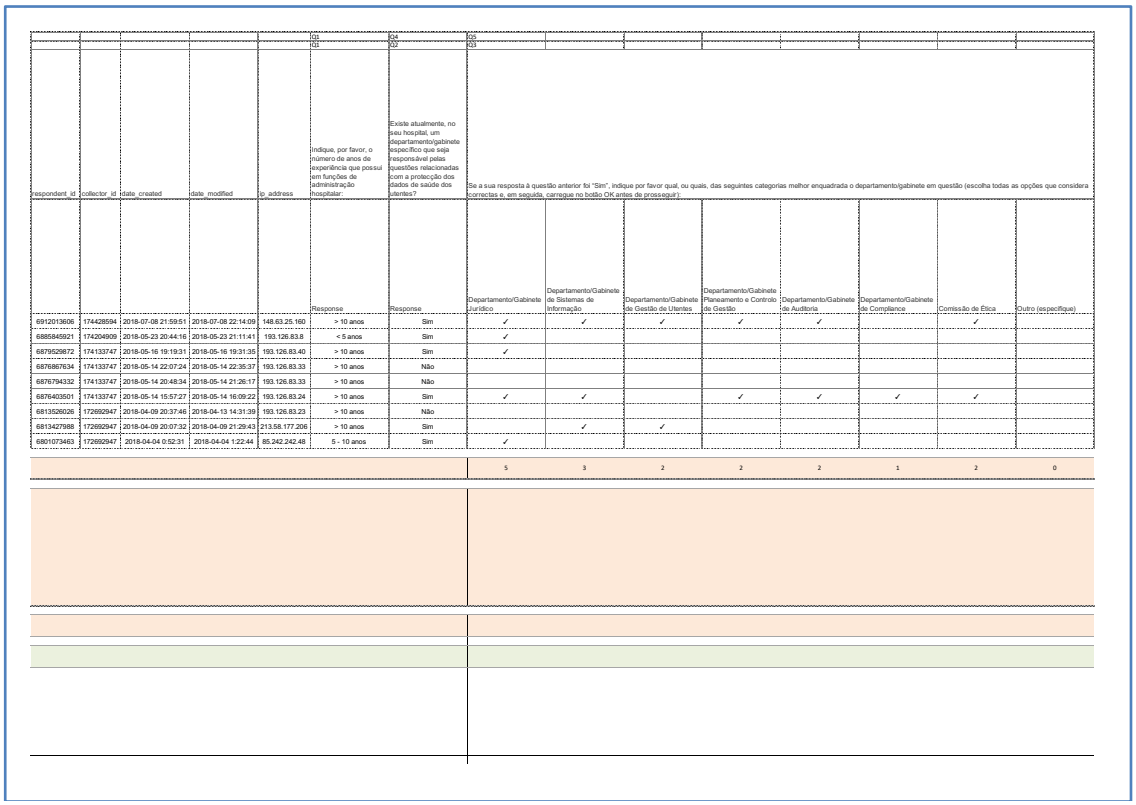
a) Coima de 1.000 € dia até correcção das infracções detectadas ☐

b) Coima de 20.000.000€ ou 4% do volume de negócios anual a nível mundial (consoante o montante que for mais elevado)

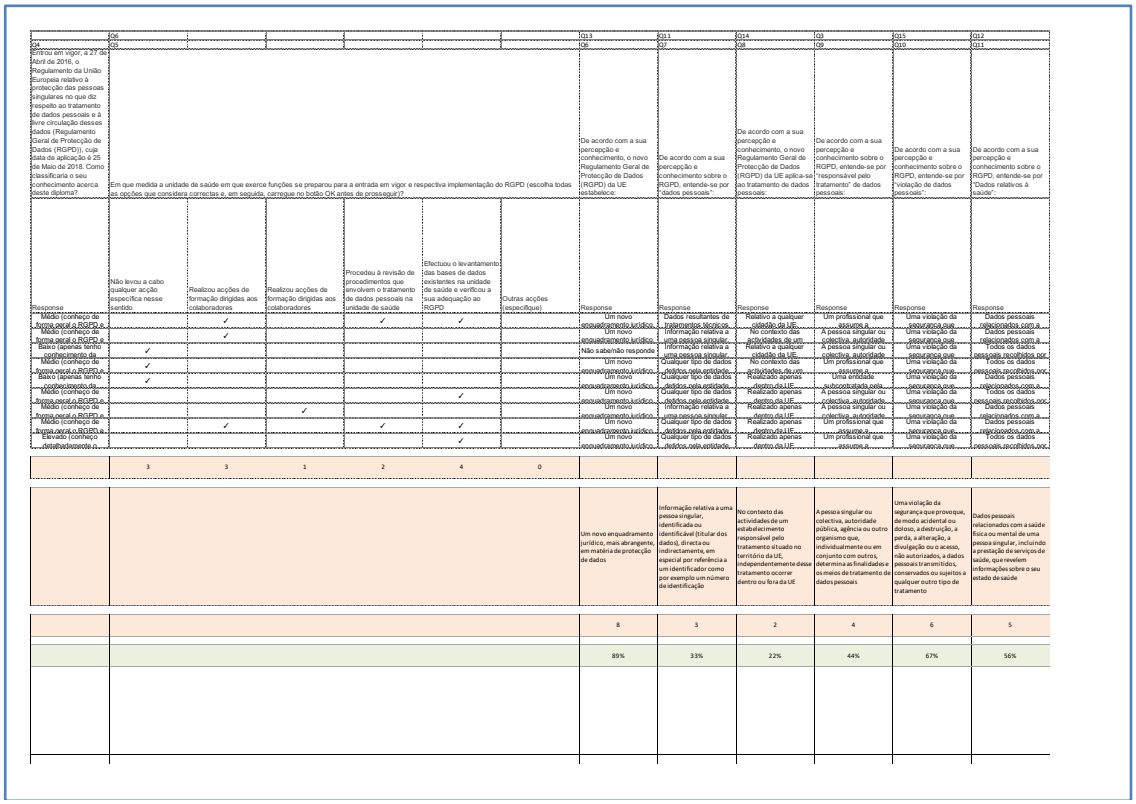
c) Ordens para que se cumpram disposições específicas do Regulamento

d) Advertências, repreensões ou retirada da certificação

Anexo III - Transcrição Integral das Respostas Obtidas



					Q1	Q4	Q3							
					Q1	Q2	Q3							
respondent_id	collector_id	date_created	date_modified	ip_address	Indique, por favor, o número de anos de experiência que possui em funções de administração hospitalar:	Existe atualmente, no seu hospital, um departamento/gabinete específico que seja responsável pelas questões relacionadas com a protecção dos dados de saúde dos utentes?	Se a sua resposta à questão anterior foi "Sim", indique por favor qual, ou quais, das seguintes categorias melhor enquadrada o departamento/gabinete em questão (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):							
					Response	Response	Departamento/Gabinete Jurídico	Departamento/Gabinete de Sistemas de Informação	Departamento/Gabinete de Gestão de Utentes	Departamento/Gabinete Planeamento e Controlo de Gestão	Departamento/Gabinete de Auditoria	Departamento/Gabinete de Compliance	Comissão de Ética	Outro (especifique)
6912013606	174428594	2018-07-08 21:59:51	2018-07-08 22:14:09	148.63.25.160	> 10 anos	Sim	✓		✓	✓	✓		✓	
6885845921	174204909	2018-05-23 20:44:16	2018-05-23 21:11:41	193.126.83.8	< 5 anos	Sim	✓							
6879529872	174133747	2018-05-16 19:19:31	2018-05-16 19:31:35	193.126.83.40	> 10 anos	Sim	✓							
6876867634	174133747	2018-05-14 22:07:24	2018-05-14 22:35:37	193.126.83.33	> 10 anos	Não								
6876794332	174133747	2018-05-14 20:48:34	2018-05-14 21:26:17	193.126.83.33	> 10 anos	Não								
6876403501	174133747	2018-05-14 15:57:27	2018-05-14 16:09:22	193.126.83.24	> 10 anos	Sim	✓	✓		✓	✓	✓	✓	
6813526026	172692947	2018-04-09 20:37:46	2018-04-13 14:31:39	193.126.83.23	> 10 anos	Não								
6813427988	172692947	2018-04-09 20:07:32	2018-04-09 21:29:43	213.58.177.206	> 10 anos	Sim		✓	✓					
6801073463	172692947	2018-04-04 0:52:31	2018-04-04 1:22:44	85.242.242.48	5 - 10 anos	Sim	✓							
							5	3	2	2	2	1	2	0



	Q6						Q13	Q11	Q14	Q8	Q15	Q12
Q4	Q5						Q6	Q7	Q8	Q9	Q10	Q11
Entrou em vigor, a 27 de Abril de 2016, o Regulamento da União Europeia relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral de Protecção de Dados (RGPD)), cuja data de aplicação é 25 de Maio de 2018. Como classificaria o seu conhecimento acerca deste diploma?	Em que medida a unidade de saúde em que exerce funções se preparou para a entrada em vigor e respectiva implementação do RGPD (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir)?						De acordo com a sua percepção e conhecimento, o novo Regulamento Geral de Protecção de Dados (RGPD) da UE estabelece:	De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por dados pessoais":	De acordo com a sua percepção e conhecimento, o novo Regulamento Geral de Protecção de Dados (RGPD) da UE aplica-se ao tratamento de dados pessoais:	De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por "responsável pelo tratamento" de dados pessoais:	De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por "violação de dados pessoais":	De acordo com a sua percepção e conhecimento sobre o RGPD, entende-se por "Dados relativos à saúde":
Response	Não levou a cabo qualquer acção específica nesse sentido	Realizou acções de formação dirigidas aos colaboradores	Realizou acções de formação dirigidas aos colaboradores	Procedeu à revisão de procedimentos que envolvem o tratamento de dados pessoais na unidade de saúde	Efectuou o levantamento das bases de dados existentes na unidade de saúde e verificou a sua adequação ao RGPD	Outras acções (especifique)	Response	Response	Response	Response	Response	Response
Médio (conheço de forma geral o RGPD e princípios base)		✓		✓	✓		Um novo enquadramento jurídico	Dados resultantes de tratamentos técnicos	Relativo a qualquer relação da UE	Um profissional que assegura a	Uma violação da segurança que	Dados pessoais relacionados com a
Médio (conheço de forma geral o RGPD e princípios base)		✓					Um novo enquadramento jurídico	Informação relativa a uma pessoa singular	No contexto das actividades de um	A pessoa singular ou colectiva, autoridade	Uma violação da segurança que	Dados pessoais relacionados com a
Baixo (apenas tenho conhecimento da existência do RGPD)	✓						Não sabe/não responde	Informação relativa a uma pessoa singular	Relativo a qualquer relação da UE	A pessoa singular ou colectiva, autoridade	Uma violação da segurança que	Todos os dados pessoais recolhidos por
Médio (conheço de forma geral o RGPD e princípios base)	✓						Um novo enquadramento jurídico	Qualquer tipo de dados	No contexto das actividades de um	Um profissional que assegura a	Uma violação da segurança que	Todos os dados pessoais recolhidos por
Baixo (apenas tenho conhecimento da existência do RGPD)	✓						Um novo enquadramento jurídico	Qualquer tipo de dados	Realizado apenas dentro da UE	Uma entidade subcontratada pela	Uma violação da segurança que	Dados pessoais relacionados com a
Médio (conheço de forma geral o RGPD e princípios base)					✓		Um novo enquadramento jurídico	Qualquer tipo de dados	Realizado apenas dentro da UE	A pessoa singular ou colectiva, autoridade	Uma violação da segurança que	Todos os dados pessoais recolhidos por
Médio (conheço de forma geral o RGPD e princípios base)			✓				Um novo enquadramento jurídico	Informação relativa a uma pessoa singular	Realizado apenas dentro da UE	A pessoa singular ou colectiva, autoridade	Uma violação da segurança que	Dados pessoais relacionados com a
Médio (conheço de forma geral o RGPD e princípios base)		✓		✓	✓		Um novo enquadramento jurídico	Qualquer tipo de dados	Realizado apenas dentro da UE	Um profissional que assegura a	Uma violação da segurança que	Dados pessoais relacionados com a
Elevado (conheço detalhadamente o					✓		Um novo enquadramento jurídico	Qualquer tipo de dados	Realizado apenas dentro da UE	Um profissional que assegura a	Uma violação da segurança que	Todos os dados pessoais recolhidos por
	3	3	1	2	4	0						

		Um novo enquadramento jurídico, mais abrangente, em matéria de protecção de dados	Informação relativa a uma pessoa singular, identificada ou identificável (titular dos dados), directa ou indirectamente, em especial por referência a um identificador como por exemplo um número de identificação	No contexto das actividades de um estabelecimento responsável pelo tratamento situado no território da UE, independentemente desse tratamento ocorrer dentro ou fora da UE	A pessoa singular ou colectiva, autoridade pública, agência ou outro organismo que, individualmente ou em conjunto com outros, determina as finalidades e os meios de tratamento de dados pessoais	Uma violação da segurança que provoque, de modo acidental ou doloso, 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	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
		8	3	2	4	6	5
		89%	33%	22%	44%	67%	56%

Q12				Q13			Q14	Q15				Q16
De acordo com a sua percepção e conhecimento, o tratamento dos dados pessoais, segundo o RGPD, só é lícito se e na medida em que se verifique pelo menos uma das seguintes condições (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):				De acordo com a sua percepção e conhecimento do RGPD, quais as condições aplicáveis ao consentimento para o tratamento de dados pessoais (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):			De acordo com a sua percepção e conhecimento do RGPD, é, em princípio, proibido o tratamento das seguintes categorias de dados pessoais:	De acordo com a sua percepção e conhecimento do RGPD, entende-se por "protecção de dados desde a concepção e por defeito", o seguinte (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):				De acordo com a sua per responsável pelo tratame direito de aceder às segu (prosseguir):
O tratamento dos dados for determinado por entidade pública ou órgão governamental	O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas	O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular	Os dados pessoais tratados forem relativos a cidadãos não residentes na UE	O consentimento dos dados deve ser dado livremente por parte do titular dos dados	Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita, este deve ser apresentado de forma que o distinga claramente de outros assuntos	O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento	Resposne	Protecção de dados no momento da definição dos meios de tratamento e no momento do próprio tratamento	Restrição do tratamento apenas aos dados pessoais que forem necessários para cada finalidade específica	Protecção dos dados apenas no momento do seu armazenamento	Tratamento de dados generalizado mas armazenamento apenas dos dados necessários para cada finalidade específica	A localização geográfica do seu armazenamento e tratamento (dentro ou fora da União)
	✓			✓	✓	✓	A origem racial ou étnica as opções		✓			✓
	✓	✓		✓	✓	✓	Todas as opções anteriores	✓	✓			✓
	✓				✓	✓	A origem racial ou étnica as opções				✓	
	✓				✓	✓	A origem racial ou étnica as opções	✓	✓			✓
	✓	✓				✓	A origem racial ou étnica as opções				✓	
✓	✓	✓		✓	✓	✓	Todas as opções anteriores	✓	✓		✓	✓
	✓		✓	✓		✓	A origem racial ou étnica as opções	✓				✓
	✓			✓	✓	✓	Todas as opções anteriores	✓				✓
	✓	✓		✓	✓	✓	Todas as opções anteriores	✓				✓

1	9	4	1	7	7	9	6	4	0	3	7

	O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas	O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular	O consentimento dos dados deve ser dado livremente por parte do titular dos dados	Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita, este deve ser apresentado de forma que o distinga claramente de outros assuntos	O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento	Todas as opções anteriores	Protecção de dados no momento da definição dos meios de tratamento e no momento do próprio tratamento	Restrição do tratamento apenas aos dados pessoais que forem necessários para cada finalidade específica	
	0	0	0	0	0	4	0	0	
						44%	0%	0%	
2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	3 33% 1 11% 4 44% 1 11% 0 0% **9**		3 Certas 2 Certas 1 Certa	6 67% 2 22% 1 11% **9**		2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	2 22% 1 11% 4 44% 0 0% 2 22% **9**		2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)

					Q8 Q17			Q9 Q18			
cepção e conhecimento do RGPD, o "direito de acesso" do titular dos dados implica que este tem o direito de obter junto do nto a confirmação de que os dados pessoais que lhe digam respeito são ou não objecto de tratamento, e se for esse o caso, o inles informações (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de					De acordo com a sua percepção e conhecimento do RGPD, o "direito a ser esquecido" do titular dos dados implica que este tem o direito a obter, junto do responsável pelo tratamento, o apagamento dos seus dados pessoais sem demora injustificada, quando se apliquem os seguintes motivos (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):			De acordo com a sua percepção e conhecimento do RGPD, o titular dos dados tem o direito de obter d tratamento a limitação do tratamento, no caso de se aplicarem as seguintes situações(escolha todas a correctas e, em seguida, carregue no botão OK antes de prosseguir):			
As finalidades do tratamento de dados	A lista de entidades subcontratadas que procedem ao tratamento dos dados	O prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para fixar esse prazo	A lista de entidades a quem essa informação irá ser divulgada	Qualquer rectificação aos dados pessoais originalmente fornecidos	Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento	Sempre que se registar o falecimento do titular dos dados, bastando o apagamento ser solicitado pelos seus legais representantes	O titular retira o consentimento em que se baseia o tratamento dos dados, se não existir outro fundamento jurídico para o referido tratamento	Será sempre obrigatório o apagamento dos dados mediante declaração expressa nesse sentido do titular dos mesmos, independentemente dos motivos para tal requerimento	O titular passou a residir em território fora da União Europeia	O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização	Cessação da actividade do estabelecimento	O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial
✓	✓	✓	✓	✓	✓		✓	✓		✓		✓
✓	✓	✓	✓	✓	✓			✓				✓
✓		✓	✓	✓	✓		✓			✓		
✓	✓	✓	✓	✓				✓				✓
✓	✓	✓	✓	✓	✓		✓			✓		✓
✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
✓		✓	✓		✓		✓		✓			✓
✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓
✓		✓					✓	✓		✓		✓

9	6	8	8	7	7	2	7	6	2	6	1	8

As finalidades do tratamento de dados	O prazo de conservação dos dados pessoais ou, se tal não for possível, os critérios usados para fixar esse prazo	Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento	O titular retira o consentimento em que se baseia o tratamento dos dados, se não existir outro fundamento jurídico para o referido tratamento	O tratamento for ilícito e o titular dos dados se opuser ao apagamento dos dados pessoais e solicitar, em contrapartida, a limitação da sua utilização	O responsável pelo tratamento já não precisar dos dados pessoais para fins de tratamento, mas esses dados sejam requeridos pelo titular para efeitos de declaração, exercício ou defesa de um direito num processo judicial
0	0	0	0	0	0
0%	0%	0%	0%	0%	0%
0 0% 8 89% 0 0% 1 11% 0 0% **9**		2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	3 33% 3 33% 0 0% 2 22% 1 11% **9**	3 Certas 3 Certas e Errada(s) 2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	2 22% 1 11% 2 22% 0 0% 2 22% 2 22% 0 0% **9**

	Q10 Q19	Q21 Q20					Q22 Q21				Q23 Q22	
o responsável pelo s opções que considera	De acordo com a sua percepção e conhecimento do RGPD, o responsável pelo tratamento de dados deverá assegurar o direito do titular à portabilidade dos mesmos:	De acordo com a sua percepção e conhecimento do RGPD, tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos para os direitos e liberdades das pessoas singulares, o responsável do tratamento deve aplicar medidas técnicas e organizativas, para assegurar um nível de segurança adequado ao risco, entre as quais (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):					De acordo com a sua percepção e conhecimento do RGPD, em caso de violação dos dados pessoais, o responsável pelo tratamento deve (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):				De acordo com a sua percepção e conhecimento d tratados para fins de investigação científica ou histó dos Estados-Membros pode, sob certas condições (escolha todas as opções que considera correctas prosseguir):	
Contestar a exatidão dos dados pessoais durante um período que permita ao responsável pelo tratamento verificar a sua exatidão	Response	O apagamento regular dos dados tidos por confidenciais	A utilização permanente das técnicas de anonimização de dados mais recentes	A pseudonimização e a cifragem dos dados pessoais	Um processo para testar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento	Assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento	Dar imediatamente a conhecer ao titular que ocorreu a violação dos seus dados, independentemente do risco para os direitos, liberdades e garantias das pessoas singulares	Notificar esse facto a autoridade de controlo competente, sem demora injustificada, até 72 horas após ter tido conhecimento da violacao de dados pessoais, a menos que a violacao nao resulte num risco para os direitos liberdades e garantias da pessoa singular	Lançar um procedimento interno para fazer face ao problema, a menos que a violação não resulte num risco para os direitos, liberdades e garantias das pessoas singulares	Comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada, em caso de elevado risco para os direitos, liberdades e garantias das pessoas singulares	Direito de acesso do titular dos dados	Direito de portabilidade dos dados
✓	Fornecendo ao titular dos dados os dados		✓	✓	✓	✓		✓	✓	✓	✓	✓
✓	Fornecendo ao titular dos dados os dados			✓	✓	✓		✓	✓	✓	✓	✓
	Fornecendo ao titular dos dados os dados	✓	✓			✓		✓		✓		
	Fornecendo ao titular dos dados os dados		✓		✓	✓		✓				
	Fornecendo ao titular dos dados os dados	✓		✓	✓	✓		✓		✓	✓	
✓	Transmitindo os dados, num formato estruturado	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Fornecendo ao titular dos dados os dados		✓	✓		✓		✓		✓		
✓	Fornecendo ao titular dos dados os dados		✓	✓	✓	✓		✓				
	Transmitindo os dados, num formato estruturado		✓		✓			✓	✓		✓	

4	9	3	7	6	7	8	1	9	4	6	4	3

Contestar a exatidão dos dados pessoais durante um período que permita ao responsável pelo tratamento verificar a sua exatidão	Transmitindo os dados, num formato estruturado de uso corrente e de leitura automática, a outro responsável pelo tratamento, mediante determinadas condições			A pseudonimização e a cifragem dos dados pessoais	Um processo para testar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento	Assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento		Notificar esse facto a autoridade de controlo competente, sem demora injustificada, até 72 horas após ter tido conhecimento da violacao de dados pessoais, a menos que a violacao nao resulte num risco para os direitos liberdades e garantias da pessoa singular		Comunicar a violação de dados pessoais ao titular dos dados sem demora injustificada, em caso de elevado risco para os direitos, liberdades e garantias das pessoas singulares	Direito de acesso do titular dos dados	
0	2			0	0	0		8		0	0	
0%	22%			0%	0%	0%		89%		0%	0%	
		3 Certas 3 Certas e Errada(s) 2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	1 11% 4 44% 0 0% 2 22% 0 0% 2 22% 0 0% 9					2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	3 33% 3 33% 2 22% 1 11% 0 0% 9		2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	0 2 1 4 2 9

		Q23 Q23	Q24 Q24	Q25 Q25	Q26 Q26	Q27 Q27			
o RGPD, quando os dados pessoais forem rica ou para fins estatísticos, o Direito da União ou , prever derrogações aos seguintes direitos e, em seguida, carregue no botão OK antes de		De acordo com a sua percepção e conhecimento do RGPD, a avaliação de impacto das operações de tratamento previstas sobre a protecção de dados deve ser realizada pelo responsável pelo tratamento, antes de iniciar o tratamento, quando:	De acordo com a sua percepção e conhecimento do RGPD, o responsável pelo tratamento dos dados deve consultar a autoridade de controlo, antes de proceder ao tratamento quando:	De acordo com a sua percepção e conhecimento do RGPD, encontra-se previsto algum tipo de certificação em matéria de protecção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento.	No caso de ter respondido "Sim" à questão anterior, manifeste-se quanto à duração máxima da validade da certificação	De acordo com a sua percepção e conhecimento do RGPD, a violação das suas disposições pode estar sujeita às seguintes sanções (escolha todas as opções que considera correctas e, em seguida, carregue no botão OK antes de prosseguir):			
Direito de rectificação dos dados	Direito ao apagamento dos dados ("direito a ser esquecido")	Response	Response	Response	Response	Coima de 1.000 € dia até correcção das infracções detectadas	Coima de 20.000.000€ ou 4% do volume de negócios anual a nível mundial (consoante o montante que for mais elevado)	Ordens para que se cumpram disposições específicas do Regulamento	Advertências, repreensões ou retirada da certificação
✓	✓	Sejam alterados processos internos que	Sempre que o tratamento incidir sobre	Sim	Ainda não se encontra definido o prazo	✓	✓	✓	✓
✓	✓	O tratamento, tendo em conta a sua natureza,	A avaliação de impacto sobre a protecção de	Sim	Ainda não se encontra definido o prazo		✓		
	✓	Sejam contratados prestadores de serviços	A avaliação de impacto sobre a protecção de	Não	Ainda não se encontra definido o prazo			✓	✓
	✓	Sejam contratados prestadores de serviços	Sempre que o tratamento incidir sobre	Sim	Válida por um período máximo de 3 anos		✓		
	✓	Sejam alterados processos internos que	Sempre que o tratamento incidir sobre	Sim	Ainda não se encontra definido o prazo	✓			
✓	✓	Sejam contratados prestadores de serviços	Sempre que o tratamento incidir sobre	Sim	Ainda não se encontra definido o prazo		✓		
✓	✓	O tratamento, tendo em conta a sua natureza,	A avaliação de impacto sobre a protecção de	Não	Ainda não se encontra definido o prazo		✓		
✓		O tratamento, tendo em conta a sua natureza,	A avaliação de impacto sobre a protecção de	Sim	Ainda não se encontra definido o prazo		✓		
	✓	O tratamento, tendo em conta a sua natureza,	Nunca é necessária a consulta no caso de	Não	Ainda não se encontra definido o prazo		✓		

5	8					2	7	2	2

Direito de rectificação dos dados		O tratamento, tendo em conta a sua natureza, âmbito e finalidades, for susceptível de implicar um elevado risco para os direitos e liberdades das pessoas singulares	A avaliação de impacto sobre a protecção de dados indicar que do tratamento resultará num elevado risco para o titular dos dados	Sim	Válida por um período máximo de 3 anos		Coima de 20.000.000€ ou 4% do volume de negócios anual a nível mundial (consoante o montante que for mais elevado)	Ordens para que se cumpram disposições específicas do Regulamento	Advertências, repreensões ou retirada da certificação
0		4	4	6	1		0	0	0
0%		44%	44%	67%	11%		0%	0%	0%
0% 22% 11% 44% 22%						3 Certas 3 Certas e Errada(s) 2 Certas 2 Certas e Errada(s) 1 Certa 1 Certa e Errada(s) Errada(s)	0 0% 1 11% 1 11% 0 0% 6 67% 0 0% 1 11% 9		