CÓDIGO DE CONDUTA NO TRATAMENTO DE DADOS PESSOAIS (RGPD – ART.º 40)

«Os seres humanos são em grande parte o centro da proteção dos recursos informacionais numa organização através dos seus comportamentos na interacção com a informação e sistemas de informação». [(1)] Okere, Irene et al.

1. INTRODUÇÃO

O Regulamento Geral de Proteção de Dados (RGPD), relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, entrou em vigor no dia 25 de Maio de 2016, sendo aplicável a partir de 25 de Maio de 2018.

Tendo em vista a implementação das medidas necessárias ao cumprimento das obrigações decorrentes do Regulamento Geral de Proteção de Dados (RGPD), designadamente para o cumprimento dos efeitos previstos nos artigos 37º e seguintes do RGPD, o Conselho de Administração do CHULC, designou o Encarregado da Proteção de Dados (EPD/DPO)[(2)], criou a Comissão de Tratamento de Dados Pessoais (CTDP)[(3)] e aprovou as competências da mesma.

O Encarregado da Proteção de Dados tem como principais funções:

a) Informar e aconselhar o CHULC ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;

b) Controlar a conformidade com o RGPD, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do CHULC ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;

[(1)] Okere, Irene et al. (2012) – "*Assessing Information Security Culture: A critical analysis of Current Approaches*", *IEEE*, 987-1-4673-2159-**4/12**.
[(2)] Circular Informativa n.º 464 de 29 de agosto de 2018 do CHULC.
[(3)] Circular Informativa n.º 594 de 29 de novembro de 2018 do CHULC.

c) Prestar aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35º do RGPD;

d) Cooperar com a autoridade de controlo; É o ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36º do RGPD, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto.

e) No desempenho das suas funções, o EPD tem em devida consideração os riscos associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.

A Comissão de Tratamento de Dados Pessoais depende diretamente do conselho de Administração e tem como principais atribuições as seguintes:

a) Inspecionar as bases de dados pessoais utilizadas no CHULC e operações de tratamento de dados para identificação, classificação e inventariação;

b) Auditar a conformidade das operações de tratamento de dados nos procedimentos internos do CHULC com as obrigações decorrentes do RGPD, nomeadamente no que toca aos registos de atividade, às medidas técnicas e organizativas de segurança implementadas, às avaliações de impacto sobre a proteção de dados e às garantias e direitos dos titulares dos dados, em articulação com o Encarregado de Proteção de Dados (EPD);

c) Identificar as vulnerabilidades e classificar os riscos contra a privacidade e os direitos dos titulares dos dados, em articulação com o EPD, através da elaboração de relatórios periódicos;

d) Apresentar planos de intervenção nos serviços clínicos e administrativos ao CA, tendo em vista o cumprimento do RGPD, com definição de prioridades, após parecer do EPD;

e) Implementar e acompanhar a execução dos planos aprovados pelo CA em matéria de proteção de dados junto dos serviços clínicos e administrativos;

f) Implementar e acompanhar a execução de recomendações do EPD e das Autoridades de Controlo;

g) Fomentar a divulgação de boas práticas e da formação de trabalhadores em matéria de proteção de dados, em articulação com o EPD e com a Área de Formação;

O presente Código de Conduta é elaborado ao abrigo do disposto no art.º 40º do Regulamento Geral de Proteção de Dados (RGPD).

2. DEFINIÇÕES

As definições para os conceitos relacionadas com a temática do tratamento e proteção de dados pessoais contidas no presente Código são as estabelecidas no RGPD (Art.º 4º), nomeadamente:

a) «Dados Pessoais»: Informação relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou por referência a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social da pessoa singular.

b) «Tratamento»: uma operação ou conjunto de operações efetuadas 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.

c) «Definição de perfis», qualquer forma de tratamento automatizado de dados pessoais que consista em utilizar esses dados pessoais para avaliar certos aspetos pessoais de uma pessoa singular, nomeadamente para analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações.

d) «Pseudonimização», o tratamento de dados pessoais de forma que deixem de poder ser atribuídos a um titular de dados específico sem recorrer a informações suplementares, desde que essas informações suplementares sejam mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não possam ser atribuídos a uma pessoa singular identificada ou identificável.

e) «Ficheiro», qualquer conjunto estruturado de dados pessoais, acessível segundo critérios específicos, quer seja centralizado, descentralizado ou repartido de modo funcional ou geográfico.

f) «Responsável pelo tratamento», a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro.

g) «Subcontratante», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes.

h) «Destinatário», uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que recebem comunicações de dados pessoais, independentemente de se tratar ou não de um terceiro. Contudo, as autoridades públicas que possam receber dados pessoais no âmbito de inquéritos específicos nos termos do direito da União ou dos Estados-Membros não são consideradas destinatários; o tratamento desses dados por essas autoridades públicas deve cumprir as regras de proteção de dados aplicáveis em função das finalidades do tratamento.

i) «Terceiro», a pessoa singular ou coletiva, a autoridade pública, o serviço ou organismo que não seja o titular dos dados, o responsável pelo tratamento, o subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os dados pessoais.

j) «Consentimento» do titular dos dados, uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento.

k) «Violação de dados pessoais», uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

l) «Dados genéticos»: Dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular, que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

m) «Dados biométricos»: Dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos.

n) «Dados relativos à saúde»: Dados pessoais relacionados com a saúde física ou mental da pessoa, incluindo dados relacionados com a prestação de serviços de saúde, que revelam informações sobre o seu estado de saúde.

o) «Colaborador»: pessoa singular ou colectiva a prestar serviços ou a desenvolver qualquer tipo de actividade no CHULC, EPE, independentemente da natureza do vínculo contratual, quer seja no âmbito da execução de um contrato quer seja ainda que no âmbito de mobilidade, protocolos, estágios ou voluntariado.»

3. OBJETO E ÂMBITO

3.1. O presente código de conduta respeita à disciplina em vigor no Centro Hospitalar Universitário de Lisboa Central, EPE (CHULC) para o tratamento de dados pessoais no âmbito do exercício das suas competências legais.

3.2. O presente documento aplica-se a todos colaboradores do CHULC, independentemente da natureza do seu vínculo, no âmbito da recolha, do tratamento e da utilização de dados pessoais.

3.3. O tratamento por parte dos parceiros, fornecedores ou subcontratantes deverá, ainda, ser regulado por um acordo que estabeleça o objeto, a duração do tratamento, a natureza, as finalidades do tratamento, o tipo de dados pessoais, as categorias dos titulares dos dados e as obrigações e direitos do responsável pelo tratamento. O acordo celebrado deverá estabelecer, nomeadamente, que os subcontratantes:

- obedecem às instruções que lhes são dadas pelo CHULC, EPE;
- assumem um compromisso de confidencialidade, ou que estão sujeitas a adequadas obrigações legais de confidencialidade;
- adotem as medidas técnicas e organizativas de segurança no tratamento;
- apresentem as garantias adequadas, de forma a que o tratamento satisfaça os requisitos legais e,
- assegurem a defesa dos direitos dos titulares dos dados.

4. LICITUDE DO TRATAMENTO E RECOLHA DOS DADOS PESSOAIS

O Centro Hospitalar Universitário de Lisboa Central, EPE (CHULC, EPE) é pessoa coletiva de direito público de natureza empresarial dotada de autonomia administrativa, financeira e patrimonial, nos termos do regime jurídico do setor público empresarial., nos termos do Decreto-Lei n.18/2017, de 10 de fevereiro. Tem por objeto principal a prestação de cuidados de saúde, a todos os cidadãos em geral, e também, desenvolver atividades de investigação, formação e ensino, sendo a sua participação na formação de profissionais de saúde dependente da respetiva capacidade formativa, podendo ser objeto de contratos-programa em que se definam as respetivas formas de financiamento, conforme art.º 2.º dos Estatutos, aprovados pelo Decreto-Lei n.18/2017, de 10 de fevereiro.

No âmbito da sua atividade, o CHULC, EPE procede, de acordo com o princípio da necessidade de conhecer, à recolha e tratamento de dados pessoais para efeitos de cumprimento de contratos ou de obrigações legais a que se encontra vinculado, nomeadamente ao abrigo da alínea h) do art.º 9º do RGPD: “Se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde ou de ação social com base no direito da União ou dos Estados-

Membros ou por força de um contrato com um profissional de saúde, sob reserva das condições e garantias previstas n.º 3".

Caso a recolha e tratamento dos seus dados pessoais não decorra de uma obrigação legal ou contratual, será pedido o respetivo consentimento para proceder à recolha e tratamento dos dados.

Os dados pessoais serão conservados apenas durante o período de tempo necessário para assegurar a finalidade a que se destinam e que estejam legalmente previstos.

5. OS DIREITOS DOS TITULARES DOS DADOS PESSOAIS

Os titulares dos dados pessoais têm, a qualquer momento, o direito de acesso, retificação, atualização, limitação e apagamento dos seus dados pessoais (sempre que legalmente aplicável), o direito de oposição à utilização dos mesmos fora do âmbito da finalidade do registo, bem como o direito à portabilidade dos seus dados.

6. BOAS PRÁTICAS NA UTILIZAÇÃO DOS RECURSOS INFORMACIONAIS

O Centro Hospitalar Universitário de Lisboa Central, EPE (CHULC, EPE) tem-se pautado pelo desenvolvimento dos sistemas e tecnologias de informação e comunicação, prosseguindo uma política de modernização e otimização dos recursos existentes, no sentido de proporcionar mais e melhores cuidados de saúde à população que serve, assegurando obrigatoriamente o cumprimento dos normativos legais e outras regulamentações ou disposições em vigor.

Neste contexto, as tecnologias de informação servem de suporte à missão e objetivos da organização, na medida em que estão na base da sua atividade, através da existência de infraestrutura físicas (hardware) e aplicações (software), onde é armazenada, transacionada e disponibilizada informação administrativa e clínica, correspondente às atividades diretas de prestação de cuidados de saúde ou às atividades indiretas de suporte a essa prestação.

Assim, o CHULC, EPE compromete-se a realizar o tratamento dos seus dados de forma leal e transparente, garantindo confidencialidade e segurança quanto às informações solicitadas e assegurando que as mesmas serão usadas apenas para os fins expressamente indicados e autorizados.

6.1. 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, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o CHULC e os subcontratantes aplicam as medidas técnicas e organizativas adequadas para promover um nível de segurança adequado ao risco, incluindo, consoante o que for adequado:

- A pseudonimização e a cifragem dos dados pessoais;
- A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.

6.2. No tratamento de dados pessoais, os colaboradores do CHULC analisarão a necessidade de proceder à avaliação de impacto sobre a proteção de dados e consulta prévia, nos termos do indicado no art.º 35º do RGPD.

6.3. Todos os colaboradores do CHULC, independentemente do tipo de vínculo existente, que tratem dados pessoais estão obrigados a cumprir as políticas e os procedimentos sectoriais e multissectoriais definidos no âmbito do Sistema Integrado de Qualidade e Segurança do CHULC, EPE.

6.4. Os colaboradores do CHULC devem ter em conta as seguintes práticas:

6.4.1. Ao nível dos acessos físicos

6.4.1.1. Guardar todos os documentos em papel com dados pessoais em local seguro e de acesso condicionado e controlado e preferencialmente em mobiliário com acesso através de chave cuja utilização deve ser controlada.
6.4.1.2. Não guardar dados pessoais localmente no computador.
6.4.1.3. Não fazer sair documentação do CHULC das suas instalações, sem que tal seja absolutamente necessário para o cumprimento dos respetivos deveres profissionais.
6.4.1.4. Cumprir com a legislação em vigor relativa à conservação e destruição de suportes de dados antigos ou inutilizáveis, nomeadamente daqueles que contenham dados pessoais e/ou sensíveis.

6.4.2. Ao nível dos acessos / autenticação nos sistemas aplicacionais

6.4.2.1. Utilizar passwords seguras e fáceis de memorizar.
6.4.2.2. Manter as passwords confidenciais.
6.4.2.3. Mudar as passwords regularmente, mesmo nos sistemas que não obrigam a fazê-lo.
6.4.2.4. Não gravar as passwords de forma automática nos sistemas, nem em sites na internet.
6.4.2.5. Não utilizar as mesmas passwords para os sistemas do CHULC e para os sistemas pessoais.
6.4.2.6. Bloquear a sessão do computador sempre que ausente do posto de trabalho – os profissionais são responsáveis pela utilização da sua “password” sempre que a mesma resulta de sua culpa ou negligência.

6.4.2.7. Não efetuar nenhuma gravação ou cópia da documentação confidencial a que tiver acesso, fora do contexto profissional.

6.4.3.Ao nível da utilização do correio eletrónico

6.4.3.1. Cumprir as "Regras de Utilização de Correio Eletrónico" do CHULC (SIS112 e CI 222/2016).
6.4.3.2. Verificar sempre os endereços dos destinatários.
6.4.3.3. Não abrir emails e ficheiros de origem desconhecida, eliminá-los imediatamente.
6.4.3.4. Não registar o endereço de e-mail de trabalho em redes sociais.

6.4.4.Ao nível da comunicação

6.4.4.1. Efetuar sempre a comunicação com o utente/doente e/ou parceiros ou fornecedores através dos meios institucionais disponibilizados pelo CHULC.
6.4.4.2. Não divulgar ou aceder a informação confidencial, fora do contexto profissional e em respeito pelo presente código de conduta e a todas normas internas e éticas aplicáveis.
6.4.4.3. Não fornecer qualquer informação com dados pessoais a terceiros, com exceção das situações previstas na legislação em vigor (ex: por consentimento do titular dos dados).

7. DEVER DE SIGILO / SEGREDO PROFISSIONAL

7.1. Todos os colaboradores do CHULC, independentemente do tipo de vínculo existente, que tratem dados pessoais estão obrigados a manter o sigilo sobre os mesmos, nomeadamente não podem revelar ou utilizar, salvo obrigação legal ou decisão judicial.

7.2. A obrigação de confidencialidade indicada no ponto anterior manter-se-á em vigor, mesmo após a cessação das funções ou dos contratos celebrados, seja qual for a causa da cessação dos mesmos, e por todo o tempo que seja necessário ao cumprimento da lei.

8. RESPONSABILIDADES EXISTENTES

8.1. Os colaboradores do CHULC, independentemente do tipo de vínculo existente, que tratem dados pessoais:

8.1.1. Devem ter conhecimento do presente código de conduta, uma vez que ele estabelece a forma de agir do CHULC perante o RGPD e fornece diretivas comportamentais exigidas a todos os agentes, de forma a que o RGPD seja aplicado de forma correta e que defenda a privacidade de todos, conforme o exigido por lei.

8.1.2. São responsáveis civilmente pelos danos e prejuízos que se venham a verificar, quer para o CHULC, quer para o titular dos dados, sem prejuízo da responsabilidade disciplinar, contra-ordenacional e/ou penal, que lhes possa ser imputada, pelo tratamento ilegal dos dados pessoais a que tenham acesso, bem como pela violação do presente Código de Conduta.

9. VIOLAÇÃO DE DADOS PESSOAIS

9.1. Os interessados que pretendam reclamar pela violação dos seus dados, devem-no fazer diretamente ao Encarregado de Proteção de Dados do CHULC, através do endereço eletrónico epd@chlc.min-saude.pt ou qualquer outro meio.

9.2. É dever de todos os trabalhadores que tenham conhecimento de qualquer situação que possa implicar uma violação de dados pessoais comunicá-la, com caráter de urgência, ao Encarregado de Proteção de Dados do CHULC, através do endereço eletrónico epd@chlc.min-saude.pt ou qualquer outro meio.

9.3. Caso o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, suscetível de implicar um risco para os direitos e liberdades das pessoas singulares, deve notificá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após conhecimento do ocorrido.

9.4. Não sendo possível cumprir o prazo referido no número anterior, a notificação deve ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada.

10. LEI APLICÁVEL E FORO

A todas as omissões, ao previsto no presente Código de Conduta, será aplicado o estipulado no RGPD, bem como a legislação nacional em vigor sobre este assunto.

11. ENTRADA EM VIGOR

O presente Código de Conduta entra em vigor, após a sua aprovação pelo Conselho de Administração e, no dia seguinte, à sua publicação na intranet do CHULC.