

## POLÍTICA DE PRIVACIDADE

Esta Unidade de Saúde pertencente ao Grupo Luz Saúde (doravante “**Luz Saúde**”), no âmbito da sua atividade, procede ao tratamento de Dados Pessoais, relativos quer *a)* aos seus colaboradores (tendo em vista, nomeadamente, a gestão de recursos humanos, medicina do trabalho e o processo de recrutamento), quer *b)* aos seus clientes, na prestação de cuidados de saúde (medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos e gestão de serviços de saúde). Esta Unidade de Saúde atua enquanto Responsável pelo Tratamento dos Dados Pessoais dos referidos titulares, com exceção das situações identificadas na presente Política.

Neste contexto, esta Unidade de Saúde pretende assegurar que o tratamento de tais dados pelos seus colaboradores cumpre a legislação aplicável, nomeadamente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – “**RGPD**”).

Para este efeito, esta Unidade de Saúde aprovou o presente documento, o qual visa consagrar a política de privacidade seguida (doravante “**Política de Privacidade**”), estabelecendo as principais regras que devem ser observadas pelas diversas áreas desta Unidade Luz Saúde no que diz respeito ao tratamento de dados pessoais.

A recolha e tratamento dos dados pessoais fornecidos à Unidade de Saúde, assim como o exercício dos direitos dos seus titulares relativamente a estes dados, regem-se por esta Política de Privacidade, pelos regulamentos internos e pelos restantes instrumentos utilizados por esta Unidade de Saúde.

### I

## INTRODUÇÃO

### 1. Definições-chave <sup>1,2</sup>

- (a) “**Anonimização**”: tratamento de dados que consiste em retirar elementos ou informações relativas a um titular dos dados na medida em que, de forma irreversível, deixe de ser possível identificá-lo.
- (b) “**Autoridade de controlo**”: uma autoridade pública independente criada por um Estado-Membro, com a responsabilidade pela fiscalização da aplicação do RGPD, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação dos dados na União. Em Portugal, a autoridade de controlo será a Comissão Nacional de Proteção de Dados (“**CNPD**”);

<sup>1</sup> No presente documento, sempre que iniciados por letra maiúscula, e salvo quando do contexto claramente decorrer sentido diferente, os termos e expressões indicados terão o significado que a seguir lhes é apontado

<sup>2</sup> Salvo quando do contexto resulte de outro modo, qualquer referência feita na Política de Privacidade a uma disposição legal inclui as alterações a que a mesma tiver sido e/ou vier a ser sujeita

- (c) **“Categorias especiais de dados”**: 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;
- (c) **“Consentimento do titular dos dados”**: qualquer manifestação de vontade, livre, específica, informada e inequívoca, nos termos da qual o titular aceita que os seus Dados Pessoais sejam objeto de tratamento;
- (d) **“Dados Pessoais”**: qualquer informação, de qualquer natureza e independentemente do respetivo suporte, relativa a uma pessoa singular identificada ou identificável; é considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, genética, económica, cultural ou social;
- (e) **“Dados relativos à saúde”**: 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 passado, presente ou futuro. Tal inclui, p.ex., *a)* 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; *b)* 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*;
- (f) **“Definição de perfis”**: qualquer forma de tratamento automatizado de Dados Pessoais que consista na utilização desses Dados Pessoais para, nomeadamente, incluir uma pessoa singular em determinada categoria, respeitante ao seu desempenho profissional, à sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações;
- (g) **“Encarregado da proteção de dados”** (*Data Protection Officer* – **“DPO”**): pessoa nomeada para garantir, numa organização, a conformidade do tratamento de Dados Pessoais com o RGPD, assegurando a comunicação eficiente com os titulares dos dados e a cooperação com as autoridades de controlo em causa, fazendo ainda a ponte com as unidades de negócio dentro da organização;
- (h) **“Legislação relativa à proteção de Dados Pessoais”**: o RGPD, a Lei n.º 67/98, de 26 de outubro (Lei de

Proteção de Dados Pessoais) em tudo o que não contrarie o RGPD e até à aprovação da Lei de execução do RGPD em Portugal, a Lei n.º 27/2002, de 8 de Novembro (que dá nova redação à Lei n.º 48/90, de 24 de Agosto, a Lei de bases da Saúde), a Lei n.º 12/2005, de 26 de Janeiro, e a Lei n.º 41/2004, de 18 de Agosto (alterada pela Lei nº 46/2012, de 29 de agosto);

- (i) **“Política de Privacidade”**: o presente documento, o qual visa consagrar a política de privacidade desta Unidade Luz Saúde, estabelecendo as principais regras que devem ser observadas pelas diversas áreas no que diz respeito ao tratamento de Dados Pessoais;
- (j) **“Pseudonimização”**: 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;
- (k) **“RGPD”**: Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados;
- (l) **“Responsável”**: o Hospital da Luz Aveiro, a qual determina as finalidades e os meios de tratamento dos Dados Pessoais;
- (m) **“Subcontratante”**: a pessoa singular ou coletiva que trate os Dados Pessoais por conta do Responsável;
- (n) **“Terceiro”**: a pessoa singular ou coletiva, a autoridade pública, o serviço ou qualquer outro organismo que não seja o Titular dos Dados, o Responsável pelo Tratamento ou o Subcontratante e as pessoas que, sob a autoridade direta do responsável pelo tratamento ou do subcontratante, estão autorizadas a tratar os Dados Pessoais;
- (o) **“Titular dos Dados”** ou **“Cliente”**: pessoa singular identificada ou identificável cujos Dados Pessoais são tratados por esta Unidade de Saúde ou por outro Responsável;
- (p) **“Transferências internacionais de dados”**: transferências de Dados Pessoais que sejam ou venham a ser objeto de tratamento após transferência para um país terceiro (não localizado na União Europeia) ou para uma organização internacional, podendo a transferência ocorrer entre dois ou mais responsáveis pelo tratamento ou entre responsáveis pelo tratamento e subcontratantes;
- (q) **“Tratamento de Dados Pessoais”**: qualquer operação ou conjunto de operações sobre Dados Pessoais,

efetuadas 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;

- (r) **“Violação de dados pessoais”**: 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.

## **2. O que é tratado nesta Política de Privacidade?**

A Política de Privacidade define as regras relativas ao tratamento de Dados Pessoais a que a Unidade de Saúde e seus colaboradores deverão obedecer, em cumprimento do disposto na Legislação relativa à proteção de Dados Pessoais.

2.1. Esta Unidade de Saúde poderá aprovar algumas políticas específicas aplicáveis ao tratamento de determinados Dados Pessoais efetuados pelas suas áreas, as quais, depois de divulgadas, farão parte integrante da presente Política de Privacidade.

2.2. O tratamento de dados pessoais recolhidos através do site e app Hospital da Luz será regulado por Política de Privacidade própria disponível na plataforma em questão.

2.3. As regras estabelecidas pela Política de Privacidade serão aplicáveis a todos os trabalhadores da Unidade de Saúde e aos prestadores de serviços desta Unidade Luz Saúde, também designados em conjunto como “colaboradores”.

2.4. Deverá ser assegurado a cada Cliente informação relativa à identidade e contactos do responsável pelo tratamento, contactos do DPO, finalidades do tratamento e fundamentos jurídicos associados, categorias dos dados pessoais tratados, destinatários ou categorias de destinatários dos dados, prazo de conservação dos dados, existência e condições de exercício dos direitos enquanto titular dos dados, entre outros que se apliquem.

## II

### COMO VÃO SER TRATADOS OS SEUS DADOS PESSOAIS?

#### 1. Princípios de Tratamentos de Dados Pessoais

Os Tratamentos de Dados Pessoais levados a cabo por esta Unidade de Saúde deverão processar-se de acordo com os seguintes princípios:

- 1) Licitude, lealdade e transparência;
- 2) Limitação das finalidades;
- 3) Adequação, pertinência e proporcionalidade (minimização dos dados);
- 4) Exatidão;
- 5) Limitação da conservação.

##### 1) Licitude, lealdade e transparência

- (i) A Unidade de Saúde deverá dar a conhecer ao Titular dos Dados a realização do tratamento de dados que lhe respeite, indicando, nomeadamente, os seus fundamentos de legitimidade, finalidades, categorias de dados tratados, período de conservação dos dados e outras informações relevantes relativas ao Tratamento de Dados Pessoais.
- (ii) A realização de operações de Tratamento de Dados Pessoais em subcontratação deve ser regida por um contrato ou ato jurídico que vincule o Subcontratante ao Responsável e que estipule, designadamente, obrigações de confidencialidade e de segurança do tratamento, e que o Subcontratante apenas atua mediante instruções do Responsável, incumbindo-lhe igualmente o cumprimento das obrigações referidas no artigo 28.º do RGPD.

##### 2) Limitação das finalidades

- (i) Os Dados Pessoais tratados pela Unidade de Saúde deverão ser recolhidos para finalidades determinadas, explícitas e legítimas, não podendo ser posteriormente tratados de forma incompatível com essas finalidades.
- (ii) A Unidade de Saúde realizará operações de tratamento de Dados Pessoais dos seus Clientes, nomeadamente, para as seguintes finalidades:
  - a) Prestação de cuidados de saúde, incluindo serviços de medicina preventiva, de diagnóstico médico e terapêutica e gestão de serviços de saúde, incluindo as operações e procedimentos de

faturação a terceiros financeiramente responsáveis pelo pagamento dos cuidados;

- b) Auditoria e melhoria contínua dos serviços prestados, acreditação das unidades de saúde ou certificação dos seus serviços, bem como para a avaliação e medição dos níveis de serviço da Unidade de Saúde.
- c) Gestão da relação com os Clientes, incluindo gestão dos canais de contacto com o mesmo, *online*, presenciais e telefónicos (incluindo comunicações por telefone, SMS, e-mail ou correio, nomeadamente sobre agendamento de consultas e meios complementares de diagnóstico ou faturação);
- d) Envio de resposta a reclamações e sugestões;
- e) Envio de comunicações informativas e de marketing, mediante o seu consentimento prévio;
- f) Realização de inquéritos de avaliação da satisfação dos clientes, mediante o seu consentimento prévio;
- g) Emissão e envio de faturas eletrónicas, mediante a sua aceitação;
- h) Realização de estudos e ensaios clínicos;
- i) Segurança e videovigilância.

### **3) Adequação, pertinência e proporcionalidade**

Os Dados Pessoais devem ser adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para os quais foram recolhidos e posteriormente tratados. A Unidade de Saúde só deverá proceder ao tratamento de Dados Pessoais se os mesmos forem necessários para a prossecução da sua atividade, cumprimento de obrigações legais, para a execução de um contrato ou contratos em que o Titular dos Dados seja parte ou de diligências prévias à formação do contrato ou declaração da vontade negocial efetuadas a seu pedido. Para determinadas finalidades, a Unidade de Saúde apenas poderá tratar os Dados Pessoais dos seus Clientes se obtiver o seu consentimento prévio e expresso. Tal será o caso, por exemplo, do tratamento para o envio de comunicações informativas e de marketing que sejam consideradas relevantes para a promoção da sua saúde e para a prestação de um serviço de saúde de excelência, através dos diferentes canais de comunicação, nomeadamente SMS, email ou notificações push<sup>3</sup>.

### **4) Exatidão**

Os Dados Pessoais devem ser exatos e, se necessário, atualizados, tomando esta Unidade de Saúde as medidas adequadas para assegurar que os dados inexatos ou incompletos sejam apagados ou retificados

---

<sup>3</sup> Se tiver ativado esta opção nas definições do seu dispositivo móvel.

sem demora, tendo em conta as finalidades para que foram recolhidos ou para que são tratados posteriormente.

## **5) Limitação da Conservação**

- (i) Os Dados Pessoais recolhidos são tratados no estrito cumprimento da legislação aplicável. Tais dados são conservados num formato que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados.
- (ii) O período de tempo durante o qual os dados são armazenados e conservados varia de acordo com a finalidade para a qual a informação é utilizada. Existem, no entanto, requisitos legais que obrigam a conservar os dados por um determinado período de tempo. Também tomamos por referencial, para determinação do período de conservação adequado, as várias deliberações das autoridades de controlo de proteção de dados, nomeadamente da Comissão Nacional de Proteção de Dados.
- (iii) Nessa medida e em particular:
  - a) os dados relativos à sua saúde são conservados nos termos da legislação aplicável ao arquivo da documentação hospitalar;
  - b) os dados decorrentes dos inquéritos de satisfação serão conservados pelo prazo de 6 meses, após o qual serão anonimizados;
  - c) os dados de faturação (incluindo faturas emitidas e recebidas por via eletrónica) serão conservados pelo prazo de 10 anos para cumprimento de obrigações legais em matéria fiscal;
  - d) os dados utilizados para efeitos de envio de comunicações informativas e de marketing serão conservados enquanto mantiver interesse em receber as referidas comunicações e não retirar o seu consentimento; e
  - e) os demais dados administrativos (incluindo de identificação e contacto) serão conservados apenas durante o período necessário para as finalidades no âmbito das quais são tratados, desde que não seja necessário mantê-los para efeito de cumprimento de obrigações legais do Responsável.

## **2. Com que fundamento poderemos tratar os seus dados pessoais?**

- 2.1. A Unidade de Saúde apenas tratará os Dados Pessoais quando esteja devidamente habilitada para o fazer.

2.2. O tratamento de Dados Pessoais poderá ter por base:

- (i) o consentimento do titular dos dados;
- (ii) a execução de um contrato no qual o titular dos dados seja parte;
- (iii) o cumprimento de obrigações jurídicas a que a Unidade de Saúde esteja sujeita;
- (iv) a defesa de interesses vitais do titular dos dados; ou, ainda,
- (v) a prossecução de interesses legítimos da Unidade de Saúde (exceto se prevalecerem os interesses e liberdades fundamentais do titular).

2.3. Existem, todavia, requisitos acrescidos para o tratamento de categorias especiais de dados pessoais, como os dados relativos à sua saúde. Assim, o tratamento desses dados particularmente sensíveis só poderá ter lugar em determinados casos, nomeadamente quando o titular tenha prestado o seu consentimento explícito, quando o tratamento seja necessário para a defesa de interesses vitais de um titular dos dados incapacitado de dar o seu consentimento, para a declaração, exercício ou defesa de um direito num processo judicial, quando o tratamento for necessário para efeitos de medicina preventiva, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de gestão de sistemas e serviços de saúde, ou ainda, quando o tratamento for necessário por motivos de interesse público no domínio da saúde pública.

2.4. Assim, os tratamentos de dados necessários para a prestação de cuidados de saúde aos Clientes, bem como para comunicar e gerir a relação das Unidades do Grupo Luz Saúde com os mesmos (como, por exemplo, os dados de contacto, como o telefone ou e-mail), terão fundamento na execução do contrato de prestação de serviços de saúde celebrado com os Clientes, ou na execução de diligências pré-contratuais a pedido dos mesmos.

2.5. Quando tais tratamentos implicarem o tratamento de dados relativos à saúde dos Clientes ou de outras categorias especiais de dados (tais como dados genéticos ou dados relativos à vida sexual dos Clientes), aqueles basear-se-ão na necessidade do tratamento para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos de saúde.

2.6. Quanto aos tratamentos de Dados Pessoais realizados pela Unidade de Saúde, nomeadamente, para informar o Cliente sobre novidades na prestação dos serviços, produtos ou serviços do seu interesse, e para personalizar e melhorar a sua experiência enquanto Cliente (através de inquéritos de avaliação da satisfação dos clientes), o fundamento de licitude de tais tratamentos será o consentimento dos titulares



dos dados, ou seja, dos Clientes.

- 2.7. No que concerne aos tratamentos dos dados efetuados pela Unidade de Saúde para melhorar os serviços, auditá-los, e cumprir os objetivos administrativos e comerciais, o fundamento adequado será a prossecução de interesses legítimos da Unidade de Saúde.
- 2.8. Relativamente ao tratamento de dados realizado pela Unidade de Saúde no contexto do cumprimento de obrigações legais, o fundamento de licitude para a realização de tais tratamentos – na sua maioria, comunicações de dados para entidades externas – será a necessidade do tratamento para o efeito do cumprimento de obrigações jurídicas.
- 2.9. O tratamento de dados pessoais no contexto da participação em Ensaios clínicos e estudos não intervencionais terá como fundamento de licitude o consentimento dos titulares dos dados, ou seja, dos Clientes.
- 2.10. Por fim, o tratamento de dados decorrente da videovigilância será efetuado na prossecução de interesses legítimos da Unidade de Saúde para proteção das pessoas e bens nas suas instalações.

### **3. Que informações serão prestadas aos Titulares dos Dados?**

- 3.1. A Unidade de Saúde, através dos seus colaboradores, ou através do e-mail [DPO@luzsaude.pt](mailto:DPO@luzsaude.pt), prestará aos Clientes um conjunto de informações, salvo se já deles forem conhecidas, nomeadamente sobre:
  - (i) Identidade e contactos do Responsável e, se for caso disso, do seu representante;
  - (ii) Contactos do Encarregado de Proteção de Dados (DPO);
  - (iii) Finalidades do tratamento da informação recolhida, bem como o seu fundamento jurídico;
  - (iv) Destinatários ou categorias de destinatários dos dados pessoais, se os houver;
  - (v) A intenção de transferir dados pessoais para um país terceiro e as garantias implementadas para o feito, se for caso;
  - (vi) O prazo de conservação dos dados pessoais ou, se não for possível, os critérios utilizados para definir esse prazo;
  - (vii) A existência e as condições de exercício dos seus direitos enquanto titulares dos dados, tais como o direito de acesso e de retificação, eliminação ou a limitação do seu tratamento, a portabilidade dos seus dados, ou a oposição ao seu tratamento, nos termos da legislação relativa à proteção de Dados Pessoais;

- (viii) O direito de apresentar reclamação a uma autoridade de controlo; e
- (ix) A existência de decisões automatizadas incluindo a definição de perfis.

3.2. Os documentos que sirvam de base à recolha de Dados Pessoais devem conter as informações constantes em 3.1. ou remeter para as mesmas em documento facilmente acessível ou disponibilizado no momento.

3.3. Os Clientes têm o direito de obter do Responsável, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos:

- (i) A confirmação de serem ou não tratados dados que lhe digam respeito, bem como informação sobre as finalidades desse tratamento, as categorias de dados sobre que incide, os destinatários ou categorias de destinatários a quem são comunicados os dados, o prazo previsto de conservação dos dados (ou o critério usado para fixar o prazo), o direito de apresentar uma reclamação a uma autoridade de controlo e de saber a origem dos dados caso os mesmos não sejam recolhidos junto do Titular dos Dados;
- (ii) A comunicação, sob forma inteligível, dos seus dados sujeitos a tratamento e de quaisquer informações disponíveis sobre a origem desses dados;
- (iii) O conhecimento da lógica subjacente ao tratamento automatizado dos dados que lhe digam respeito;
- (iv) A retificação, o apagamento ou a limitação do tratamento dos dados cujo tratamento não cumpra o disposto na Legislação relativa à proteção de Dados Pessoais, nomeadamente devido ao carácter incompleto ou inexato desses dados;
- (v) A notificação aos terceiros a quem os dados tenham sido comunicados de qualquer retificação, apagamento ou limitação do tratamento, salvo se isso for comprovadamente impossível.

3.4. O Cliente tem o direito de, querendo, conhecer todo o seu processo clínico (salvo circunstâncias excecionais devidamente justificadas e em que seja inequivocamente demonstrado que isso lhe possa ser prejudicial).

3.5. O Cliente tem ainda o direito de se opor, a qualquer momento, a seu pedido e gratuitamente, à utilização dos seus Dados Pessoais para efeitos de realização de ações de marketing direto ou qualquer outra

forma de prospeção, incluindo a definição de perfis relacionada com tais ações de marketing direto.

- 3.6. Nos termos do RGPD, o Cliente tem o direito de retirar o seu consentimento para os tratamentos de dados relativamente aos quais o consentimento constitui o fundamento de legitimidade, o que não invalida, no entanto, o tratamento efetuado até essa data com base no consentimento previamente dado.
- 3.7. O Cliente pode ainda, a qualquer momento, solicitar a eliminação dos seus Dados Pessoais, bem como a portabilidade dos mesmos, nos termos legalmente previstos.
- 3.8. Sem prejuízo de qualquer outra via de recurso administrativo ou judicial, o titular dos dados tem direito a apresentar uma reclamação à CNPD ou a outra autoridade de controlo competente nos termos da lei, caso considere que os seus dados não estão a ser objeto de tratamento legítimo por parte da Unidade de Saúde, nos termos da legislação aplicável e da presente Política.
- 3.9. O Cliente poderá exercer os direitos referidos nos números anteriores através dos contactos identificados no ponto VII **“Como posso obter mais informações e quais os contactos para o efeito?”**.

#### **4. Como é que asseguramos a segurança da Informação em Suporte Papel?**

- 4.1. No que respeita à questão da segurança, o processo clínico em papel é, por natureza, mais vulnerável, devendo ser criados mecanismos eficazes para assegurar a impossibilidade de acesso não autorizado à informação.
- 4.2. A Unidade de Saúde cumprirá, entre outras, as seguintes regras de acesso e consulta dos documentos em suporte de papel:
  - (i) A obrigação de consulta dos processos clínicos para fins diversos da prestação de cuidados médicos (por exemplo, para fins de investigação científica ou outros fins devidamente autorizados) tem de ser feita no próprio arquivo ou em local próprio destinado a esse efeito, não podendo os processos clínicos sair do hospital;
  - (ii) A proibição de levantar qualquer processo clínico por períodos superiores a 10 (dez) dias úteis, salvo autorização especial a conceder caso a caso, em face das razões invocadas;
  - (iii) A proibição dos processos clínicos estarem ao alcance, quer dos próprios doentes a que respeitam,

quer dos respetivos familiares, e/ou dos visitantes;

- (iv) A existência de um controlo permanente do levantamento dos processos clínicos do arquivo;
- (v) O transporte dos processos clínicos para o serviço que o requisitou por colaboradores do serviço requisitante ou responsáveis do arquivo;

4.3. A criação de mecanismos de organização/ordenação que garantam a eficaz localização dos processos clínicos.

## **5. Que medidas tomamos para a segurança da Informação?**

5.1. A Unidade de Saúde implementa medidas de carácter técnico e organizativo necessárias à proteção dos Dados Pessoais contra a respetiva destruição, accidental ou ilícita, a perda accidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, bem como contra qualquer outra forma de tratamento ilícito dos mesmos, devendo tais medidas ser cumpridas pelos seus colaboradores.

5.2. Estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o Tratamento de Dados Pessoais apresenta e à natureza dos Dados Pessoais a proteger. Entre tais medidas salientam-se as seguintes:

- (i) A pseudonimização e a cifragem dos Dados Pessoais;
- (ii) A existência de utilizadores com diferentes níveis de acesso;
- (iii) A atribuição de *passwords* de alteração periódica;
- (iv) A existência de servidores com acesso físico e lógico restrito;
- (v) A existência de *Firewalls*;
- (vi) A realização de cópias de segurança dos dados informatizados;
- (vii) O acesso limitado aos sistemas de informação;

5.3. A Unidade de Saúde adota ainda medidas especiais de segurança aquando do tratamento de Categorias Especiais de Dados.

## **6. Como asseguramos a confidencialidade dos seus Dados Pessoais?**

- 6.1. Os trabalhadores desta Unidade de Saúde e os prestadores de serviços pela mesma contratados comprometem-se a guardar sigilo profissional relativamente a todos os Dados Pessoais a que tenham tido acesso ou que lhe tenham sido transmitidos por esta Unidade Luz Saúde.
- 6.2. Os profissionais de saúde da Unidade de Saúde devem guardar sigilo relativamente a todos os factos que tenham chegado ao seu conhecimento no exercício da sua atividade ou por causa dela, quando revelados pelo cliente ou por terceiro a seu pedido, quando o médico deles se tenha apercebido ou lhe tenham sido comunicados por outro médico, em conformidade com o previsto no artigo 87.º do Código Deontológico da Ordem dos Médicos (CDOM).
- 6.3. Os diretores, chefes de serviço e médicos assistentes dos clientes estão obrigados, singular e coletivamente, a guardar segredo profissional quanto às informações clínicas que, constituindo objeto do segredo profissional, constem do processo individual do cliente (artigo 69.º do CDOM).

### **III**

## **COMUNICAÇÃO, TRANSFERÊNCIA E RELACIONAMENTO DE DADOS PESSOAIS**

### **1. A quem serão comunicados os seus Dados Pessoais?**

- 1.1. Esta Unidade de Saúde poderá legitimamente comunicar Dados Pessoais a terceiros quando:
  - (a) o titular dos dados tenha dado de forma inequívoca o seu consentimento;
  - (b) julgue tais comunicações de dados como necessárias ou adequadas *(i)* à luz da lei aplicável, *(ii)* no cumprimento de obrigações jurídicas/ordens judiciais, *(iii)* para responder a solicitações de autoridades públicas ou governamentais ou *(iv)* para efeito acreditação da Unidade de Saúde ou certificação dos seus serviços, bem como para a avaliação e medição dos níveis de serviço da Unidade de Saúde;
  - (c) seja levada a cabo para proteger interesses vitais do titular dos Dados Pessoais.
- 1.2. Neste sentido, a Unidade de Saúde poderá transmitir os Dados Pessoais à Entidade Reguladora da Saúde, à Administração Central do Sistema de Saúde (ACSS), I.P., aos Serviços Partilhados do Ministério da Saúde (SPMS), ao INFARMED, às Administrações Regionais da Saúde, aos Tribunais, Solicitadores, aos órgãos de polícia criminal ou ao Ministério Público quando seja notificado para o efeito ou quando tal seja necessário para o cumprimento de obrigações jurídicas, conforme legalmente previsto.

1.3. Em qualquer das situações acima mencionadas, a Unidade de Saúde compromete-se a tomar todas as medidas razoáveis para garantir a proteção efetiva dos Dados Pessoais que trata.

## **2. E no caso das transferências internacionais de dados?**

Caso ocorram transferências internacionais de Dados Pessoais, a Unidade de Saúde implementará as medidas necessárias e adequadas à luz da lei aplicável para assegurar a proteção dos Dados Pessoais objeto de uma tal transferência, cumprindo rigorosamente as disposições legais relativamente aos requisitos aplicáveis a tais transferências, nomeadamente informando os Clientes neste âmbito.

## **3. Em que condições os seus dados estão disponíveis a outras Unidades de Saúde da Luz Saúde?**

Os seus dados de identificação e contacto, bem como os dados relativos à sua saúde, serão incluídos em bases de dados da Unidade de Saúde que serão relacionadas com as bases de dados das demais unidades de Saúde Luz Saúde, para manutenção de uma ficha de cliente única e prestação de cuidados de saúde integrados em todas as unidades.

## **IV**

### **TRATAMENTO POR SUBCONTRATANTE**

#### **Em que situações os seus dados serão tratados por subcontratados desta Unidade de Saúde?**

A Unidade de Saúde partilha os Dados Pessoais a entidades por ela subcontratadas para efeitos de processamento dos mesmos, por conta e sob as instruções desta Unidade de Saúde, enquanto Entidade Responsável pelo Tratamento.

A realização de operações de Tratamento de Dados Pessoais em subcontratação é regida por um contrato ou ato jurídico que vincula o Subcontratante ao Responsável e que estipula, designadamente, que o Subcontratante apenas atua mediante instruções documentadas do Responsável, entre outros aspetos, incumbindo-lhe igualmente o cumprimento das obrigações referidas no artigo 28.º do RGPD.

Neste sentido, a Unidade de Saúde adotou regras claras de contratualização do tratamento de Dados Pessoais com os seus Subcontratantes, e exige que estes adotem as medidas técnicas e organizacionais apropriadas para proteger os Dados Pessoais.

## V

### TRATAMENTO DE CATEGORIAS ESPECIAIS DE DADOS

A Unidade de Saúde apenas tratará Dados Pessoais quando exista um fundamento jurídico para o mesmo, nos termos do disposto no artigo 9.º do RGPD.

O tratamento dos Dados Pessoais referidos no número anterior só pode ser efetuado por ou sob a responsabilidade de um profissional sujeito à obrigação de sigilo profissional ou por outra pessoa igualmente sujeita a uma obrigação de confidencialidade, devendo também ser garantidas medidas adequadas de segurança da informação, bem como o direito dos Clientes à informação.

## VI

### TRATAMENTOS ESPECÍFICOS

#### 1. Como é que serão tratados os seus dados no contexto de ensaios clínicos e estudos não intervencionais?

1.1. Quando tenha prestado o consentimento para a participação num estudo ou ensaio clínico, a entidade que atuará como Responsável pelo tratamento dos Dados Pessoais será a entidade promotora do estudo ou ensaio. Na maioria dos casos, a promotora será uma entidade externa ao Grupo Luz Saúde, pelo que esta Unidade de Saúde e os seus médicos investigadores, ao abrigo de protocolos celebrados com as promotoras, atuarão meramente como Subcontratantes para efeito do tratamento dos Dados Pessoais nesse contexto. Existirão outros casos em que unidades do Grupo Luz Saúde poderão atuar como promotoras e, logo, como Responsáveis.

1.2. Sem prejuízo do acima referido, os colaboradores da Unidade de Saúde não devem participar/desempenhar funções em qualquer ensaio clínico ou estudo não intervencional sem verificar se todas as formalidades necessárias já foram realizadas, nomeadamente:

- (i) Emissão de parecer prévio da Comissão de Ética competente;
- (ii) Emissão de autorização prévia do Infarmed, IP;
- (iii) Obtenção de consentimento informado, livre, específico, expresso, escrito, datado e assinado do titular dos dados pessoais (condição de legitimidade do tratamento). Do mesmo documento poderá constar o consentimento para a participação no Ensaio e o consentimento para o tratamento dos Dados Pessoais.

1.3. Caso surja qualquer questão adicional deverá contactar o DPO da Luz Saúde.

## 2. Videovigilância

2.1. A instalação de um sistema de videovigilância implica que seja afixado um aviso informativo sobre a existência dos sistemas de videovigilância, nas instalações, o qual deverá conter o seguinte texto, seguido de símbolo identificativo (uma câmara):

“Para sua proteção este local encontra-se sob vigilância de um circuito fechado de televisão, procedendo-se à gravação de [imagens e de sons]”.

2.2. A gravação de imagens e sons só pode ser conservada pelo prazo de 30 (trinta) dias, período findo o qual terá que ser destruída.

2.3. A visualização e disponibilização das gravações está sujeita a regras específicas, devendo consultar o DPO da Luz Saúde para realizar um pedido de visualização ou de disponibilização de imagens e desde que preenchidos os requisitos legalmente aplicáveis.

## VII

### DISPOSIÇÕES FINAIS

#### 1. Como posso obter mais informações e quais os contactos para o efeito?

Poderá contactar o Encarregado de Proteção de Dados (DPO) do Grupo Luz Saúde para mais informações sobre o tratamento dos seus dados pessoais, bem como quaisquer questões relacionadas com o exercício dos direitos que lhe são atribuídos pela legislação aplicável e, em especial, os referidos na presente Política de Privacidade, através dos seguintes contactos:

- Telefone: +351 217 104 430
- E-mail: [DPO@luzsaude.pt](mailto:DPO@luzsaude.pt)
- Morada: Rua Carlos Alberto da Mota Pinto, 17-9.º, 1070-313 Lisboa.

#### 2. Alterações à Política de Privacidade

A Unidade de Saúde reserva-se o direito de, a qualquer momento, proceder a modificações ou atualizações à presente Política de Privacidade, sendo essas alterações devidamente atualizadas nos nossos canais e plataformas *online* e comunicadas aos Clientes.

Data da última atualização 17/07/2018