1. OBJETIVO

Informar todos os colaboradores do Hospital de Braga no que respeita a aplicação do Regulamento Geral sobre a Proteção de Dados.

2. ÂMBITO

Aplica-se a todos os colaboradores do Hospital de Braga.

3. RESPONSABILIDADES

Compete à Comissão Executiva, ao DPO (*Data Protection Officer*), à Equipa de RGPD, à Direção Clínica, à Direção de Enfermagem, Enfermeiros Chefes, Diretores e Técnicos Coordenadores de Serviços Clínicos e Não Clínicos do Hospital de Braga, bem como a todos os colaboradores que procedam a tratamento de dados a implementação desta política.

4. REFERÊNCIAS E ABREVIATURAS

Critérios do Manual CHKS [2016]: 15.11, 15.14, 15.15, 15.18.

CNPD – Comissão Nacional de Proteção de Dados
DPIA – *Data Protection Impact Assessment* ou Avaliação do Impacto sobre a Proteção de Dados
DPO – *Data Protection Officer* ou Encarregado de Proteção de Dados
RGPD – Regulamento Geral sobre a Proteção de Dados
SNS – Serviço Nacional de Saúde

5. DESCRIÇÃO DO PROCESSO

O Hospital de Braga necessita de recolher e tratar dados pessoais dos seus utentes no âmbito da prestação de serviços de saúde. De facto, no contexto da prestação de cuidados ou tratamentos de saúde, incluindo de medicina preventiva, de diagnóstico médico e de gestão dos serviços de saúde, o tratamento de dados dos utentes é indispensável.

Neste sentido, a presente Política de Privacidade do Hospital de Braga (doravante "Política da Privacidade"), visa ajudar os nossos utentes a compreender que dados pessoais recolhemos, como e por que motivo os usamos, a quem os divulgamos e como protegemos a sua privacidade quando utilizam os nossos serviços.

5.1. Porquê?

O Hospital de Braga está empenhado em proteger a segurança e a privacidade dos seus utentes. Neste contexto, elaborou a presente Política de Privacidade, com a finalidade de afirmar o seu compromisso e respeito para com as regras de privacidade e de proteção de dados pessoais.

Pretendemos que os nossos utentes conheçam as regras gerais de privacidade e os termos de tratamento dos dados que recolhemos, no estreito cumprimento da legislação aplicável neste âmbito, nomeadamente do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 ("Regulamento Geral sobre a Proteção de Dados" ou "RGPD").

O Hospital de Braga procura respeitar as melhores práticas em matéria de segurança e proteção de dados pessoais, de promoção/ sensibilização para as boas práticas neste âmbito, e melhorando sistemas de forma a acautelar a proteção de dados que lhe são disponibilizados pelos seus utentes, no estreito cumprimento das obrigações legais.

O preenchimento dos formulários de recolha de dados e o fornecimento de dados direta ou indiretamente, implicam o conhecimento das condições desta Política, e de quaisquer outros termos, políticas e condições específicas referentes aos serviços prestados.

5.2. O Que São Dados Pessoais?

Entende-se por dados pessoais qualquer informação, de qualquer natureza e independentemente do respetivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável (titular dos dados). É considerada identificável a pessoa que possa ser identificada direta ou indiretamente, designadamente por referência a um número de identificação ou a mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social.

Os dados pessoais poderão ter uma natureza mais sensível em determinadas situações, classificando-os o RGPD como "categorias especiais de dados". Estes podem versar sobre a origem racial ou étnica do seu titular, as suas opiniões políticas, as suas convicções religiosas ou filosóficas, informação genética, identificadores biométricos, vida sexual, orientação sexual ou sobre a sua saúde.

São "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, por exemplo:

i. 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;
ii. 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*.

5.3. Outras Definições Importantes

Tratamento – 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;

Titular dos dados – pessoa singular identificada ou identificável a quem os dados pessoais dizem respeito;

Responsável pelo tratamento – pessoa singular ou coletiva, autoridade pública, 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;

Subcontratante – pessoa singular ou coletiva, autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes;

Terceiro – pessoa singular ou coletiva, autoridade pública, 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;

Encarregado da proteção de dados (*Data Protection Officer* – "DPO") – pessoa ou entidade 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 diferentes áreas de atividade dentro do hospital. O DPO não recebe instruções relativamente ao exercício das suas funções, respondendo diretamente aos órgãos de direção da entidade que o nomeou (responsável pelo tratamento ou do subcontratante);

Consentimento do titular dos dados – 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;

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;

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;

Privacidade desde a conceção (*privacy by design*) – significa levar o risco de privacidade em conta em todo o processo de conceção de um novo produto ou serviço, em vez de considerar as questões de privacidade apenas posteriormente. Tal significa avaliar cuidadosamente e implementar medidas e procedimentos

técnicos e organizacionais adequados desde o início para garantir que o tratamento está em conformidade com o RGPD e protege os direitos dos titulares dos dados em causa;

Privacidade por defeito (*privacy by default*) – significa assegurar que são colocados em prática, dentro de uma organização, mecanismos para garantir que, por defeito, apenas a quantidade necessária de dados pessoais são recolhidos, utilizados e conservados para cada tarefa, tanto em termos da quantidade de dados recolhidos, como do tempo pelo qual eles são mantidos;

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;

Anonimização – técnica que resulta do tratamento de dados pessoais a fim de lhes retirar elementos suficientes para que deixe de ser possível identificar o titular dos dados, de forma irreversível. Mais precisamente, os dados têm de ser tratados de forma a que já não possam ser utilizados para identificar uma pessoa singular utilizando «o conjunto dos meios suscetíveis de serem razoavelmente utilizados», seja pelo responsável pelo tratamento, seja por terceiros. As principais técnicas de anonimização de dados pessoais são a aleatorização e a generalização;

Avaliação de impacto sobre a proteção de dados (*data protection impact assessment* – "DPIA") – processo concebido para avaliar a necessidade e proporcionalidade do tratamento de dados pessoais, permitindo a gestão dos riscos decorrentes desse tratamento para os direitos e liberdades das pessoas singulares. O DPIA é obrigatório em determinados casos (ex.: avaliação sistemática e completa de pessoas singulares, incluindo a definição de perfis, ou tratamento em larga escala de categorias especiais de dados) e deve ser feito antes de se iniciar o tratamento;

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");

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;

Serviços da sociedade da informação – Qualquer serviço prestado normalmente mediante remuneração, à distância, por via eletrónica e mediante pedido individual de um destinatário de serviços. Para efeitos da referida definição, entende-se por:

1. "à distância": um serviço prestado sem que as partes estejam simultaneamente presentes;
2. "por via eletrónica": um serviço enviado desde a origem e recebido no destino através de instrumentos eletrónicos de processamento (incluindo a compressão digital) e de armazenamento de dados, que é

inteiramente transmitido, encaminhado e recebido por cabo, rádio, meios óticos ou outros meios eletromagnéticos; e

3. "mediante pedido individual de um destinatário de serviços": um serviço fornecido por transmissão de dados mediante pedido individual.

Plataforma de Dados da Saúde (PDS) - é uma plataforma *web*, que disponibiliza um sistema central de registo e partilha de informação clínica de acordo com os requisitos da Comissão Nacional de Proteção de Dados. A plataforma permite o acesso a informação dos cidadãos que tenham número de utente do Serviço Nacional de Saúde (doravante **"SNS"**), aos profissionais de saúde em diversos pontos do SNS (hospitais, urgências, cuidados primários, rede nacional de cuidados continuados), sem os deslocar do local seguro onde agora estão guardados. Este acesso pode ser auditado e gerido pelo próprio Utente através do Portal do Utente.

5.4. Quem é o Responsável pelo Tratamento dos Seus Dados Pessoais?

A presente Política de Privacidade visa dar a conhecer aos Utentes os termos de tratamento de dados pessoais levados a cabo pelo Hospital de Braga, determinando as finalidades e meios de tratamento dos seus dados no contexto da prestação de serviços, pelo que este deve ser considerado como a entidade Responsável pelo Tratamento, nos termos do RGPD.

Assim, quando for atendido no Hospital de Braga, a entidade Responsável pelo Tratamento dos dados necessários à prestação dos serviços de saúde (por exemplo, para efeitos de medicina preventiva, diagnóstico médico, gestão administrativa dos processos clínicos, marcações de consultas e exames, admissão e entrega de exames, prescrição eletrónica de medicamentos e de exames complementares de diagnóstico) será o Hospital de Braga.

Contudo, tal não implica que, se for atendido numa unidade de saúde do SNS, os profissionais de saúde dessas unidades acedam aos dados de saúde disponibilizados no Hospital de Braga e disponibilizados na PDS (de acordo com disposições legais do Ministério da Saúde).

Relativamente a esse acesso, a Unidade de Saúde do SNS onde a informação seja acedida será a Responsável pelo Tratamento dos dados dos Utentes, bem como relativamente à informação que seja recolhida diretamente junto dos Utentes nessa Unidade. Todavia, o acesso à sua informação de saúde será de acesso restrito aos profissionais de saúde ou outros sujeitos a equivalentes obrigações de confidencialidade na prestação dos seus cuidados. Para mais informações relativas a quem pode aceder aos seus dados pessoais, consulte a secção "*5.8. Que Profissionais Do Hospital De Braga Têm Acesso Aos Seus Dados?*".

No âmbito de algumas especialidades clínicas, o Hospital de Braga poderá tratar os seus dados conjuntamente com outras entidades, enquanto subcontratadas pelo tratamento, como sucede, por exemplo,

no caso da realização de exames de medicina nuclear, no contexto das quais o Dr. Campos Costa Consultório de Tomografia Computarizada, S.A. atua como corresponsável.

Também existe uma relação de corresponsabilidade pelo tratamento de dados pessoais dos utentes do Hospital de Braga entre o Hospital de Braga e a Entidade Pública Contratante. Tal relação diz respeito ao tratamento de dados dos Utentes do Hospital de Braga para fins de gestão administrativa dos serviços que lhe prestamos e para cumprimento de todas as disposições previstas no Contrato de Parceria Público-Privada de Gestão do Estabelecimento do Hospital de Braga. A Entidade Pública Contratante será corresponsável no que toca ao tratamento de dados necessário para as responsabilidades que lhe estão atribuídas para o acompanhamento do Contrato de Gestão do Hospital de Braga.

Não obstante o referido e relativamente aos tratamentos de dados pessoais acima descritos, os Utentes poderão exercer junto do Hospital de Braga os seus direitos à luz do RGPD (melhor descritos na secção "*5.10. Quais Os Direitos Dos Titulares Dos Dados?*"), através do endereço de correio eletrónico dpo@hospitaldebraga.pt ou de carta endereçada a Encarregado de Proteção de Dados, Hospital de Braga, Sete Fontes – S. Victor, 4710-243 BRAGA.

Quando tenha prestado o consentimento para a participação num estudo ou ensaio clínico, a entidade que atuará como Responsável pelo Tratamento dos seus dados pessoais será a entidade promotora do estudo ou ensaio. Por via de regra, a promotora será uma entidade externa ao Hospital de Braga, pelo que o Hospital de Braga e os seus médicos investigadores, ao abrigo de protocolos celebrados com as promotoras, atuarão meramente como Subcontratantes para efeito do tratamento dos seus dados pessoais nesse contexto.

O Hospital de Braga poderá ser contactado, também relativamente a estes tratamentos de dados, através do e-mail dpo@hospitaldebraga.pt ou de carta endereçada a Encarregado de Proteção de Dados, Hospital de Braga, Sete Fontes – S. Victor, 4710-243 BRAGA.

5.5. Que Dados Pessoais Recolhemos e Através de Que Meios?

O Hospital de Braga recolhe e trata os dados pessoais necessários para a prestação de cuidados de saúde integrados no SNS, incluindo para a gestão dos sistemas e serviços do hospital, auditoria e melhoria contínua dos mesmos. Os seus dados poderão ser recolhidos diretamente, designadamente, quando marca uma consulta/exame, quando vai a uma consulta/fazer um exame, quando utiliza as Plataformas do SNS ou nos contacta. Também podemos receber os seus dados pessoais de forma indireta através dos nossos prestadores de serviços que lhe prestam serviços em nosso nome ou dos nossos parceiros.

Para mais informações sobre a partilha dos seus dados com outras entidades, consulte a secção "*5.12. Em Que Circunstâncias Existe Comunicação De Dados A Outras Entidades?*".

Neste sentido, os seus dados pessoais podem incluir dados pessoais direta ou indiretamente relacionados com a sua saúde.

CATEGORIA DE DADOS TRABALHADOS	MEIOS E MOMENTOS DE RECOLHA
Nome, data de nascimento, número de telefone/ telemóvel, n.º de Identificação Fiscal. Estes dados pessoais são de fornecimento obrigatório (sendo o Utente devidamente informado da obrigatoriedade da disponibilização destes dados para continuar o processo).	Quando cria uma ficha de Utente, nos secretariados administrativos do Hospital de Braga
Informações sobre as suas marcações, consultas ou exames (incluindo a data e hora da marcação, a especialidade do médico, o exame a realizar/realizado, dados constantes da prescrição médica, entre outros necessários à prestação dos serviços);	Quando efetua uma marcação/quando solicita informações através dos vários canais (e-mail, telefone e contacto direto)
Restantes dados de identificação, tais como: número de processo clínico, nº do cartão de utente, país, distrito e concelho de nascimento, morada (localidade, código postal, país, distrito, concelho, freguesia), profissão, situação profissional, centro de saúde, médico de família, estado civil, nome do cônjuge, nome do pai, nome da mãe (caso Utente seja menor), dados relacionados com o seu seguro ou subsistema de saúde (quando os serviços prestados pelo Hospital de Braga sejam abrangidos pelos mesmos, nomeadamente em caso de acidente).	Quando se dirige, pela primeira vez, ao Hospital de Braga e criamos a seu processo, por exemplo, nos secretariados administrativos.
Informações sobre a sua saúde; incluindo: motivo da consulta/ato, antecedentes pessoais (doenças de infância, imunizações, hábitos, história ginecológica, alergias, medicação, doenças ativas, doenças inativas), antecedentes familiares (situações mais frequentes – diabetes, HTA, TP, cancro, vivo/falecido, causa de morte), exame clínico, diagnósticos, exames complementares, encaminhamento, alertas (diabetes, hipertensão, etc.), grupo sanguíneo; medicamentos prescritos, identificação do prescritor, código do local de prescrição e dados da receita e regime especial de comparticipação; ato e rúbrica do episódio realizado, data de início e fim do episódio, estado do episódio, profissional de saúde que executou o episódio, nº de episódio, tipo de episódio, indicação se existem resultados do episódio e identificador desses resultados. Dados genéticos, origem racial ou étnica e dados relativos à vida sexual e orientação sexual	No decurso da prestação de cuidados de saúde integrados, incluindo para a gestão dos sistemas e serviços do Hospital de Braga, auditoria e melhoria contínua dos mesmos

CATEGORIA DE DADOS TRABALHADOS	MEIOS E MOMENTOS DE RECOLHA
A sua opinião sobre nós	Quando o Utente participa nos nossos inquéritos/ questionários de satisfação
Dados relativos à sua saúde, dados genéticos, origem racial ou étnica e dados relativos à vida sexual e orientação sexual (a especificar pelo monitor ou investigador do estudo/ensaio aquando do pedido de consentimento informado para a participação no estudo/ensaio)	No decurso de estudos/ensaios clínicos, caso o Cliente tenha decidido participar nos mesmos

Categorias Especiais

Ao prestar serviços, o Hospital de Braga terá necessariamente de recolher dados relativos à sua saúde e, em certos casos, dados genéticos, dados relativos à sua origem racial ou étnica e dados relativos à sua vida sexual ou orientação sexual. Tais informações são consideradas "categorias especiais de dados", nos termos do RGPD, pelo que o Hospital de Braga observará os requisitos de proteção mais exigentes dispostos no RGPD relativamente ao tratamento desses dados, quer relativamente aos fundamentos de licitude adequados ao seu tratamento (ver secção "*5.7. Com Que Fundamento Tratamos Os Seus Dados Pessoais?*"), quer relativamente à implementação de medidas técnicas e organizativas adequadas à minimização do seu tratamento, à restrição do acesso a esses dados (ver secção "*5.8. Que Profissionais Do Hospital De Braga Têm Acesso Aos Seus Dados?*") e à garantia da segurança dos mesmos (ver secção "*5.11. Quais As Medidas De Segurança Adotadas Pelo Hospital De Braga?*").

5.6. Quais as Finalidades da Recolha dos Seus Dados Pessoais?

Os dados pessoais dos Utentes são tratados para a prestação de cuidados de saúde integrados, incluindo para a gestão dos sistemas e serviços do Hospital de Braga, auditoria e melhoria contínua dos mesmos.

Neste sentido, usamos os seus dados pessoais para os seguintes efeitos:

- **Para a prestação de cuidados de saúde integrados**

  De forma a podermos prestar os nossos serviços, utilizamos as suas informações acima referidas para marcar consultas, marcar exames, diagnóstico médico, para fornecer cuidados de saúde, para a gestão dos sistemas e serviços das várias unidades de saúde do SNS, auditoria e melhoria contínua.

  Os dados relativos à sua saúde apenas serão tratados por ou sob a responsabilidade de profissionais obrigados a sigilo, na estrita medida do necessário à prestação de cuidados de saúde, podendo ser comunicados aos seus familiares, apenas nas circunstâncias expressamente previstas na Lei em vigor.

- **Para comunicar e gerir a nossa relação consigo**

  Podemos contactá-lo por carta, e-mail ou SMS, por motivos administrativos ou operacionais, por exemplo, de modo a enviar-lhe a confirmação das suas marcações e dos seus pagamentos, para o informar sobre quaisquer alterações ou imprevistos acerca das suas marcações.

  Também vamos utilizar os seus dados pessoais para responder aos seus pedidos, sugestões ou contactos, para melhorar os nossos serviços e a sua experiência enquanto Utente do Hospital de Braga.

- **Para a realização de estudos e ensaios clínicos**

  Quando os estudos ou ensaios clínicos realizados no Hospital de Braga, no âmbito dos quais o Hospital de Braga atuará, por regra, como Subcontratante (sendo os Responsáveis pelo Tratamento as promotoras do estudo/ensaio), não puderem ser realizados com recurso a dados anonimizados ou pseudonimizados, o Hospital de Braga recolherá o seu consentimento para o tratamento dos seus dados pessoais nesse contexto.

  Esse consentimento poderá ser pedido de forma mais abrangente, de forma a englobar diversas áreas de investigação, ou ser dado unicamente para determinados domínios ou projetos de investigação específicos. Em todo o caso, o Hospital de Braga respeitará integralmente a decisão dos seus Utentes de se retirarem de um estudo ou ensaio, caso em que deixará de tratar os seus dados para esse efeito.

- **Para melhorar os nossos serviços e cumprir os nossos objetivos administrativos e de nível de serviço**

  Os objetivos de nível de serviço para os quais usamos as suas informações incluem contabilidade, faturação e auditoria, nomeadamente para proteção de interesses vitais dos utentes ou para efeitos de certificação, avaliação e medição dos níveis de serviço do Hospital de Braga, deteção e análise de fraude, segurança, efeitos jurídicos e processuais, estudos estatísticos, bem como para o desenvolvimento e manutenção de sistemas.

- **Para cumprir as nossas obrigações legais**

  Nomeadamente, a obrigação de fornecer os seus dados pessoais à Administração Central do Sistema de Saúde ("ACSS"), à Entidade Pública Contratante e a outras entidades públicas da área da saúde, bem como aos Tribunais, Solicitadores e aos órgãos de polícia criminal, no exercício dos seus poderes e atribuições (para saber mais acerca das categorias de destinatários dos seus dados

pessoais, consulte a secção "*5.13. Em Que Circunstâncias Existe Comunicação De Dados A Outras Entidades?*").

5.7. Com Que Fundamento Tratamos os Seus Dados Pessoais?

O Hospital de Braga apenas tratará os seus dados pessoais quando esteja devidamente habilitado para o fazer. O RGPD exige, para que o tratamento de dados pessoais seja lícito, que exista um fundamento de licitude adequado para cada tratamento específico. Tais fundamentos poderão ser de vária índole.

Assim, e em primeiro lugar, os tratamentos de dados necessários para a prestação de cuidados de saúde integrados aos Utentes, bem como para comunicar e gerir a relação do Hospital de Braga com o mesmo, sempre terão fundamento na execução do contrato de prestação de serviços de saúde celebrado com os Utentes, ou na execução de diligências pré-contratuais a pedido dos Utentes (por exemplo, quando esteja em causa a marcação de uma consulta ou ato clínico).

Adicionalmente, quando tais tratamentos implicarem o tratamento de dados relativos à saúde dos Utentes ou de outras categorias especiais de dados (tais como dados genéticos, dados relativos à vida sexual ou dados relativos á origem étnica dos Utentes), aqueles basear-se-ão na **necessidade do tratamento para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos de saúde** ou, quando o tratamento seja realizado por colaboradores do Hospital de Braga que não sejam profissionais de saúde (ver secção "*5.8. Que Profissionais Do Hospital De Braga Têm Acesso Aos Seus Dados?*"), para efeitos da **gestão dos sistemas e serviços** do Hospital de Braga.

Já quanto aos tratamentos de dados pessoais realizados pelo Hospital de Braga para efeitos da realização de estudos ou ensaios clínicos, sempre que tais estudos ou ensaios não possam ser realizados com recurso a dados anonimizados ou pseudonimizados, o fundamento de licitude no qual o Hospital de Braga funda tais tratamentos será o consentimento dos titulares dos dados, ou seja, dos seus Utentes.

Relativamente aos tratamentos dos seus dados efetuados pelo Hospital de Braga para melhorar os nossos serviços e cumprir os nossos objetivos administrativos e de qualidade, o fundamento de licitude adequado será a prossecução de interesses legítimos da entidade Responsável pelo Tratamento. Tal implica que os titulares dos dados possam opor-se ao tratamento dos seus dados para os efeitos acima referidos, ao abrigo do RGPD, caso apresentem motivos válidos relacionados com a sua situação particular. Em tal eventualidade, o Responsável pelo Tratamento poderá apresentar razões imperiosas e legítimas que justifiquem a continuação desse tratamento, caso em que se reserva o direito de continuar a tratar os seus dados para esses efeitos, tal como nos casos em que tal tratamento seja necessário para efeitos de declaração, exercício ou defesa de um direito num processo judicial.

Embora o tratamento de dados naqueles âmbitos seja feito, tendencialmente, com recurso a informação anonimizada ou pseudonimizada, é possível que, em determinados casos, este envolva, inclusivamente, determinados dados relativos à saúde dos titulares, tais como o seu nº de processo clínico, os identificadores dos atos clínicos por si realizados, entre outros.

Já relativamente ao tratamento de dados realizado pelo Hospital de Braga 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 do Responsável pelo Tratamento. Caso tais tratamentos envolvam categorias especiais de dados pessoais – por exemplo, informação relativa aos medicamentos prescritos a determinado Utente no Hospital de Braga -, os tratamentos fundar-se-ão na gestão de sistemas e serviços do Hospital de Braga.

5.8. Que Profissionais do Hospital de Braga têm Acesso aos Seus Dados?

No âmbito do tratamento dos seus dados pessoais, o Hospital de Braga observa, a todo o tempo, os princípios da proteção de dados desde a conceção (*privacy by design*) e por defeito (*privacy by default*). Tal compromisso implica, entre outros aspetos, que os seus dados pessoais serão de acesso limitado às pessoas que tenham necessidade de os conhecer no exercício das suas funções, no estrita medida do necessário para a prossecução das finalidades de tratamento que já elencámos acima (ver secção "*5.6. Quais As Finalidades Da Recolha Dos Seus Dados Pessoais?*").

Assim, quanto aos dados relativos à sua saúde e outras categorias especiais de dados, estes serão, em observância da lei aplicável, de acesso reservado aos médicos e outros profissionais de saúde adstritos à prestação dos seus cuidados de saúde.

Entre os casos em que o pessoal administrativo tem acesso aos seus dados de saúde e outras categorias especiais de dados encontram-se o tratamento de dados para efeito de faturação dos serviços de saúde que lhe são prestados, para efeito da marcação de consultas e atos clínicos ou para gestão dos seus pedidos de informação ou reclamações.

5.9. Qual o Período de Conservação dos Seus Dados Pessoais?

Os dados pessoais dos Utentes que o Hospital de Braga recolhe são tratados no estrito cumprimento da legislação aplicável, sendo armazenados em base de dados específicas, criadas para o efeito. 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.

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. Nessa medida, os dados relativos à sua saúde são conservados nos termos da legislação aplicável ao arquivo da documentação hospitalar – REG.024 – *Arquivo Clínico*.

Também tomamos por referencial para determinação do período de conservação adequado as várias deliberações das autoridades de controlo de proteção de dados europeias, nomeadamente da CNPD.

5.10. Quais os Direitos dos Titulares dos Dados?

Nos termos da legislação aplicável, o titular dos dados poderá solicitar, a todo o tempo, o acesso aos dados pessoais que lhe digam respeito, bem como à sua retificação, à portabilidade dos seus dados, ou opor-se ao seu tratamento, diretamente através do e-mail dpo@hospitaldebraga.pt ou de carta endereçada a Encarregado de Proteção de Dados, Hospital de Braga, Sete Fontes – S. Victor, 4710-243 BRAGA, ou mediante contacto presencial com o Hospital de Braga. No caso de dados relativos à informação clínica, o direito de acesso à informação de saúde por parte do titular (ou de terceiros com o seu consentimento ou nos termos da lei) pode ser exercido diretamente, ou por intermédio de um médico se o titular da informação o solicitar, mediante pedido escrito segundo as orientações definidas no site do Hospital de Braga e no PRO.095 – *Regras de Acesso à Informação Contida no Processo Clínico*, dirigido a gaic@hospitaldebraga.pt.

Poderá obter a confirmação dos dados pessoais que lhe dizem respeito que são objeto de tratamento, bem como o acesso aos mesmos, sendo-lhe disponibilizada, caso requeira e não existam restrições legais, uma cópia dos dados objeto de tratamento por parte do Hospital de Braga.

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 do Hospital de Braga, nos termos da legislação aplicável e da presente Política.

5.11. Quais as Medidas de Segurança Adotadas pelo Hospital de Braga?

O Hospital de Braga está empenhado em assegurar a confidencialidade, proteção e segurança dos dados pessoais dos seus Utentes, através da implementação das medidas técnicas e organizativas adequadas para proteger os seus dados contra qualquer forma de tratamento indevido ou ilegítimo e contra qualquer perda acidental ou destruição destes dados. Para o efeito, dispomos de sistemas e equipas destinados a garantir a segurança dos dados pessoais tratados, criando e atualizando procedimentos que previnam acessos não autorizados, perdas acidentais e/ ou destruição dos dados pessoais, comprometendo-se a respeitar a legislação relativa à proteção de dados pessoais dos Utentes e a tratar estes dados apenas para os fins para que foram recolhidos, assim como a garantir que estes dados são tratados com adequados níveis de segurança e confidencialidade.

Porque reconhecemos a sensibilidade desta informação, elaborámos e divulgámos a todos os nossos colaboradores uma política sobre Segurança da Informação (POL.006 – *Segurança da Informação*), que define os procedimentos de proteção de dados pessoais, com vista a assegurar o seu conhecimento acerca das obrigações que lhes são impostas nesta matéria. Para garantir a permanente sensibilização dos nossos colaboradores, desenvolvemos ainda ações de formação junto dos mesmos, os quais assumem o compromisso de não revelar a terceiros ou utilizar para fins contrários à lei, qualquer informação pessoal dos Utentes do Hospital de Braga cujo conhecimento lhes advenha do exercício das suas funções.

Neste âmbito, o Hospital de Braga designou também um Encarregado de Proteção de Dados (*Data Protection Officer* ou "DPO") [e-mail dpo@hospitaldebraga.pt ou de carta endereçada a Encarregado de

Proteção de Dados, Hospital de Braga, Sete Fontes – S. Victor, 4710-243 BRAGA, para acompanhar o cumprimento das políticas e normas aplicáveis em matéria de proteção de dados pessoais.

Conforme descrito na presente Política de Privacidade (ver secção "*5.13. Em Que Circunstâncias Existe Comunicação De Dados A Outras Entidades?*"), podemos nalguns casos transmitir os seus dados pessoais a terceiros. O Hospital de Braga definiu 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 seus dados pessoais. Contudo, nalguns casos, podemos ser obrigados por lei a divulgar os seus dados pessoais a terceiros (tais como autoridades de controlo) relativamente aos quais temos um controlo limitado relativamente à proteção dos dados pessoais.

5.12. Em Que Circunstâncias Existe Comunicação de Dados a Outras Entidades?

O Hospital de Braga recorre a outras entidades para a prestação de determinados serviços. Eventualmente essa prestação de serviços poderá implicar o acesso, por estas entidades, a dados pessoais dos seus Utentes. Tal será o caso das entidades que prestem serviços de suporte dos sistemas informáticos do Hospital de Braga, de certos fornecedores de equipamentos médicos, de prestadores de serviços clínicos em determinados Serviços, de empresas de consultoria e sociedades de advogados, e das entidades terceiras que façam a gestão do arquivo físico do Hospital de Braga.

Assim, qualquer entidade subcontratante do Hospital de Braga tratará os dados pessoais dos nossos Utentes, em nosso nome e por nossa conta, na estrita obrigação de seguir as nossas instruções. O Hospital de Braga assegura que tais entidades subcontratantes oferecem garantias suficientes de execução de medidas técnicas e organizativas adequadas de forma que o tratamento satisfaça os requisitos da lei aplicável e assegure a segurança e proteção dos direitos dos titulares dos dados, nos termos do acordo de subcontratação celebrado com as referidas entidades subcontratantes.

O Hospital de Braga poderá, ainda, transmitir, dados pessoais dos seus Utentes a entidades terceiras, quando julgue tais comunicações de dados como necessárias ou adequadas

i. à luz da lei aplicável,
ii. no cumprimento de obrigações jurídicas/ ordens judiciais;
iii. nas transferências inter-hospitalares;
iv. para responder a solicitações de autoridades públicas ou governamentais, ou;
v. para efeito de certificação, avaliação e medição dos níveis de serviço do Hospital de Braga.

Neste sentido, o Hospital de Braga poderá transmitir os seus dados pessoais à Entidade Reguladora da Saúde, à ACSS, aos Serviços Partilhados do Ministério da Saúde (SPMS), ao INFARMED, à Entidade Pública Contratante ou às Administrações Regionais de 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.

Em qualquer das situações acima mencionadas, o Hospital de Braga compromete-se a tomar todas as medidas razoáveis para garantir a proteção efetiva dos dados pessoais que trata.

5.13. Em Que Circunstâncias Poderão os Seus Dados Ser Objeto de Transferências Internacionais?

O Hospital de Braga 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 Utentes neste âmbito.

5.14. Contacte-nos

Poderá contactar o Encarregado de Proteção de Dados ("DPO") do Hospital de Braga 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:

e-mail: dpo@hospitaldebraga.pt

Morada: Hospital de Braga, Sete Fontes – S. Victor, 4710-243 BRAGA

5.15. Como Pode Ficar a Conhecer Quaisquer Alterações à Nossa Política de Privacidade?

O Hospital de Braga reserva-se o direito de, a qualquer momento, proceder a modificações ou atualizações à presente Política de Privacidade, sendo essas alterações devidamente atualizadas nas nossas Plataformas. Sugerimos que as consulte regularmente para estar a par de eventuais alterações.

6. DOCUMENTOS RELACIONADOS

- POL.006 - Segurança da Informação;
- REG.024 – Arquivo Clínico;
- PRO.095 – Regras de Acesso à Informação Contida no Processo Clínico.

Referências Bibliográficas:

- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 – Regulamento Geral de Proteção de Dados.