

AUTORIZAÇÃO N.º 6218/2014

1 – O Pedido

Hospital da Luz, S.A., com sede na Avenida Lusíada, 100, Lisboa, notificou à Comissão Nacional de Protecção de Dados (CNPD) um tratamento de dados pessoais com a finalidade de gestão do processo de adesão e utilização do Portal do Cliente.

O Portal do Cliente é uma área reservada do site do Hospital da Luz através do qual os clientes poderão: (i) agendar consulta e meios complementares de diagnóstico e terapêutica; (ii) consultar resultados de meios complementares de diagnóstico e terapêutica; (iii) consultar parte da sua informação clínica constante da base de dados de gestão de processos clínicos do Hospital da Luz; (iv) disponibilizar informação administrativa e de saúde que entendam ser relevante na relação com o Hospital da Luz; (v) comunicar com os profissionais de saúde do Hospital da Luz; (vi) consultar histórico de visitas e faturação.

Os dados de saúde tratados no Portal do Cliente foram previamente recolhidos diretamente, por forma presencial, por telefone ou por internet, e indiretamente (quando respeitem a resultados de meios complementares de diagnóstico e terapêutica), na base de dados de gestão de processos clínicos do Responsável, objeto de notificação autónoma à CNPD.

São disponibilizados ao utilizador os dados relativos ao seu processo clínico e dados administrativos, incluindo o extrato de faturação.

São ainda tratados os seguintes dados:

Dados relativos a pedidos de marcação de consulta e meios complementares de diagnóstico e terapêutica: seguro/subsistema de saúde, consulta/meio complementar de diagnóstico e terapêutica pretendido, médico, data e hora pretendida, dados de saúde e dados administrativos do utilizador submetidos pelo próprio e outra informação adicional que este pretenda incluir por considerar relevante na relação com o Hospital da Luz.

Acresce o tratamento dos dados de registo e acesso ao Portal do Cliente: email, código de verificação, palavra-passe, logs e IP de acesso.

Relativamente ao prazo máximo de conservação dos dados, é indicado que os dados de acesso ao Portal do Cliente são conservados durante o período em que o utilizador tem a conta de acesso ao Portal ativa, com exceção dos logs de acesso, os quais são conservados por 2 anos, e dos dados de saúde, que são conservados nos termos da Portaria n.º 247/2000, de 8 de maio.

O exercício do direito de acesso é feito de forma presencial ou por escrito junto do responsável.

São indicadas medidas de segurança física e de segurança lógica constantes no campo 10. do formulário.

2 - Apreciação

O presente tratamento visa, entre outros objetivos descritos, possibilitar ao cliente dos serviços de medicina preventiva, de diagnóstico médico, prestação de cuidados ou tratamentos de saúde disponibilizados pelo Responsável o acesso a informação de saúde (*v.g.*, resultados de resultados de exames clínicos), agendar marcação de consultas e de meios complementares de diagnóstico e terapêutica, através da Internet, bem como consultar histórico de visitas e faturação. Esta finalidade do tratamento implica a recolha de dados sensíveis, em especial os relativos à saúde, que se enquadram nos dados elencados no n.º 1 do artigo 7.º da Lei n.º 67/98, de 26 de outubro (LPD).

Quanto a estes, o n.º 2 do mesmo artigo admite excecionalmente o seu tratamento, nas condições aí especificadas, e para o que aqui interessa, mediante autorização da CNPD quando exista do consentimento do titular dos dados, desde que com garantias de não discriminação e com as medidas de segurança do artigo 15.º da LPD. E o n.º 4 do artigo 7.º admite o tratamento de dados de saúde quando for necessário para efeitos de medicina preventiva, diagnóstico médico, prestação de cuidados ou tratamentos médicos ou para gestão dos serviços de saúde, desde que o tratamento

desses dados seja efetuado por profissional de saúde sujeito a sigilo médico ou por outra pessoa obrigada a segredo profissional e desde que estejam garantidas medidas de segurança da informação.

Estando aqui em causa o tratamento de dados pessoais sensíveis realizado no âmbito do portal do cliente, este terá por fundamento o consentimento do titular dos dados, nos termos do n.º 2 do artigo 7.º da LPD.

Simplemente, não obstante a utilização do portal ter como pressuposto um processo de identificação e de autenticação como utilizador, daí não resulta a manifestação do consentimento informado, expresso e específico exigido no n.º 2 do artigo 7.º da LPD, em consonância com o disposto na alínea h) do artigo 3.º da LPD.

Na verdade, não se pode inferir do ato de solicitação de pré-registo – nos termos em que se encontra descrito no formulário e anexo –, nem da introdução diretamente pelo utilizador no portal de alguns dados, o consentimento expresso e específico que a lei exige. Porque não se pode afirmar que tais condutas constituem atos voluntários *diretamente* dirigidos a manifestar a vontade de consentir no tratamento dos dados pessoais. Até porque da introdução da informação no portal dos dados (após a identificação e acreditação) apenas pode resultar uma presunção de que a introdução é feita pelo próprio titular dos dados, o que é claramente insuficiente para o efeito de aí ver um consentimento expresso.

Assim, deve o responsável assegurar que obtém uma declaração autónoma de consentimento expresso e específico, devidamente informado – o que poderá ser feito no momento da realização do pré-registo (presencial) ou no momento do registo como utilizador no portal.

Relativamente aos dados dos menores, o consentimento será declarado pelos seus representantes legais – desde que previamente tenham feito prova da paternidade ou da titularidade do poder paternal –, que assim terão acesso à informação até que os mesmos completem dezasseis anos.

A informação tratada é recolhida de forma lícita (cfr. alínea a) do n.º 1 do artigo 5.º da LPD), para finalidades determinadas, explícitas e legítimas (cfr. alínea b) do mesmo artigo) e não é excessiva.

O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas aptas a proteger os dados, as quais devem assegurar um nível de



proteção adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger (cfr. n.º 1 do artigo 14.º da LPD).

Estando em causa o tratamento de dados pessoais sensíveis, como é o caso, o responsável pelo tratamento de dados deve adotar as medidas de segurança da informação previstas no artigo 15.º da LPD. Tais medidas devem aplicar-se tanto aos dados contidos em ficheiros automatizados, como aos dados manuais. Importa ainda ter em atenção os procedimentos concretos quanto às formas de recolha, processamento e circulação da informação. Devem, pois, ser adotadas medidas de segurança que impeçam o acesso à informação a pessoas não autorizadas.

Entre as medidas de segurança declaradas, afirma-se que o sistema garante uma separação lógica entre os dados referentes à saúde e os restantes dados pessoais, de natureza administrativa, em conformidade com o determinado no n.º 3 do artigo 15.º da LPD. E que a informação é cifrada, sendo acesso ao Portal realizado através de protocolo HTTPS.

Também se declara, como tem sido entendimento da CNPD, que será criado um período de *time out*, sendo bloqueada a sessão para o utilizador, quando ultrapasse um período de inatividade na sessão de cinco minutos. E quanto às tentativas de autenticação, após três tentativas falhadas, deve ser bloqueado o acesso, sendo necessário pedir nova senha de autenticação.

No âmbito das auditorias internas que o responsável declara fazer, com análise periódica dos *logs* de acesso ao Portal do Cliente para deteção de acessos indevidos, devem os correspondentes relatórios ser mantidos à disposição da CNPD pelo período de 3 anos após a eliminação dos *logs*.

Ainda no âmbito das condições de segurança, as cópias de segurança (*backups*) da informação devem ser mantidas em local apenas acessível ao administrador de sistema ou, sob sua direção, a outros técnicos obrigados a segredo profissional. No que diz respeito aos dados contidos em suporte de papel, devem ser adotadas medidas organizacionais, que garantam um nível de segurança idêntico, impedindo acesso e manuseamento indevidos.



Independentemente das medidas de segurança adotadas pelo responsável pelo tratamento, é a este que cabe garantir o resultado da efetiva segurança da informação.

1. Decisão

Assim, tendo em atenção o disposto nas disposições combinadas dos artigos 7.º, n.ºs 2, 28.º, n.º 1, alínea a), e 30.º da LPD, autoriza-se o tratamento de dados pessoais nos seguintes termos:

1. Responsável: Hospital da Luz, S.A.,
2. Finalidade: Gestão do processo de adesão e utilização do Portal do Cliente
3. Categorias dos dados: dados de saúde constantes no processo clínico do titular; dados administrativos do titular, incluindo o extrato de faturação; dados relativos a pedidos de marcação de consulta e meios complementares de diagnóstico e terapêutica: seguro/subsistema de saúde, consulta/meio complementar de diagnóstico e terapêutica pretendido, médico, data e hora pretendida; dados administrativos ou de saúde do utilizador submetidos pelo próprio e outra informação adicional que este pretenda incluir por considerar relevante na relação com o Hospital da Luz; dados de registo e acesso ao Portal do Cliente: email, código de verificação, palavra-passe, *logs* e IP de acesso
4. Comunicação de dados: Não há
5. Formas de exercício do direito de acesso e retificação: Junto da responsável pelo tratamento.
6. Interconexões: Não há
7. Fluxo Transfronteiriços de Dados para Países Terceiros: Não há
8. Prazo de Conservação: os dados de acesso ao Portal do Cliente são conservados durante o período em que o utilizador tem a conta de acesso ao Portal ativa, com exceção dos *logs* de acesso, os quais são conservados por 2 anos, e dos dados de saúde, que são conservados nos termos da Portaria nº 247/2000, de 8 de maio.



COMISSÃO NACIONAL
DE PROTECÇÃO DE DADOS

Da presente Autorização decorrem obrigações que o responsável deve cumprir. Deve, igualmente, dar conhecimento dessas condições a todos os intervenientes no circuito de informação.

Lisboa, 8 de julho de 2014

Filipa Calvão (Presidente)