



AUTORIZAÇÃO N.º 2150/2014

1. O Pedido

Unidade Local de Saúde do Alto Minho, E.P.E., com sede na Estrada de Santa Luzia, 4901-858 Viana do Castelo, notificou um tratamento de dados pessoais com a finalidade de gestão do serviço social.

A aplicação informática utilizada para o tratamento dos dados pessoais é identificada com a denominação *FirstCare*. Esta aplicação informática permite registar e gerir a atividade do Serviço Social na ULSAM, quer na vertente de apoio e acompanhamento ao doente, como também na orientação de ajuda socioeconómica.

Os dados pessoais recolhidos são os seguintes: Dados do processo (n.º de processo, n.º de episódio, módulo, serviço); Dados de identificação (nome, data de nascimento, sexo, nacionalidade estado civil, habilitações literárias, morada, documento de identificação, NIF, NISS); Dados clínicos relevantes para o apoio social; Dados socioeconómicos; Dados profissionais; Dados relativos a cuidadores/família; Procedimentos/Apoio; Alta social (data de alta clínica, data da alta hospitalar, data da alta social, destino após a alta e local de destino após a alta).

Os dados tratados são recolhidos direta e pessoalmente, e indiretamente através da importação de dados demográficos através das aplicações informáticas SONHO (Cuidados Hospitalares) e SINUS (Cuidados Primários).

Declarou não haver comunicação de dados a terceiros, nem interconexões de tratamentos nem fluxos internacionais de dados para países terceiros.

Relativamente ao prazo máximo de conservação dos dados, é indicado que os dados são



conservados nos termos da Portaria nº 247/2000, de 8 de maio.

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

2. Análise

Porque em grande parte referentes à saúde e à vida privada, os dados dos utentes dos serviços prestados pela requerente têm a natureza de sensíveis, razão pela qual o respetivo tratamento, não se verificando os outros fundamentos, só pode basear-se no consentimento expreso, esclarecido e livre dos titulares dos dados ou seus representantes legais, nos termos do disposto no nº 2 do artigo 7º da Lei nº 67/98, de 26 de outubro (LPD).

Por esta razão é necessário o «consentimento expreso do titular», entendendo-se por consentimento qualquer manifestação de vontade, livre, específica e informada, nos termos da qual o titular aceita que os seus dados sejam objeto de tratamento, o qual deve ser obtido através de uma “declaração de consentimento informado” onde seja utilizada uma linguagem clara e acessível.

O consentimento, como se afirmou, tem de ser informado, pelo que, nos termos do artigo 10.º da LPD, deve conter os elementos aí previstos, designadamente, a identificação do responsável pelo tratamento e a finalidade do tratamento, devendo ainda conter informação sobre a existência e as condições do direito de acesso e de retificação por parte do respetivo titular.

A informação tratada é recolhida de forma lícita (artigo 5.º, n.º1 al. a) da LPD), para finalidades determinadas, explícitas e legítimas (cf. alínea b) do mesmo artigo) e não é excessiva.



Aos titulares dos dados ou aos seus representantes deverá ser assegurado o direito de conhecer e corrigir os dados que lhes respeitem.

Quanto à não existência de comunicação de dados, atenta a finalidade, suscitam-se reservas sobre a não impressibilidade de comunicação de informação para a Rede Nacional de Cuidados Continuados Integrados, para o Centro de Conferência de Faturas do ACSS, para subsistemas de saúde e mesmo, nalguns casos, para a Segurança Social, designadamente para o Sistema de Atribuição de Produtos de Apoio (SAPA). Deste modo, por força do princípio da economia procedimental, consignar-se-ão na presente autorização estas comunicações de dados.

Relativamente aos prazos máximos de conservação de dados, atento o disposto na alínea e) do n.º 1 do artigo 5.º da LPD, devem os dados pessoais ser conservados apenas durante o período necessário para a prossecução das finalidades da recolha e do tratamento posterior. Assim, os mesmos limites que foram estabelecidos na Autorização 6992/2012, para a Rede Nacional de Cuidados Continuados Integrados, são aplicáveis à presente autorização, por argumento de igualdade de razão, fixando-se em seis meses após a morte ou a alta social do titular dos dados, sem prejuízo da sua conservação, não acessível aos utilizadores, para fins de arquivo histórico.

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 (cf. n.º 1 do artigo 14.º 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 contidos em ficheiros manuais. Importa ainda ter em consideração os procedimentos concretos quanto à forma 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 a adotar o sistema deve garantir 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.

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 a 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 acessos e manuseamentos indevidos.

Apenas os profissionais que tenham necessidade de aceder à informação poderão estar credenciados para tal, restringindo-se o seu perfil à informação necessária, adequada e pertinente.

Deste modo, sublinha-se que as palavras-passe não podem ser atribuídas por equipa. Esta opção impossibilitaria a responsabilização individual dos utilizadores. Importa que o responsável pelo tratamento, a ULSAM, saiba, a cada momento, o que foi feito e quem o fez.

Para atingir este objetivo deverá existir uma conta de utilizador individual, com a correspondente palavra-passe, estando as contas agregadas em grupos, em função dos perfis.

Nada é declarado no que respeita aos registos de auditoria do sistema.

Esta é uma questão primordial e essencial para a proteção de dados pessoais, pelo que se entende que um sistema desta natureza tem, necessariamente, que possuir um sistema de auditoria fiável.

Assim, por forma a garantir a rastreabilidade dos acessos impõe-se que se parametrize o



sistema para que os *logs* registem:

- Identificação do utilizador que acedeu;
- Data e hora dos acessos (*timestamp*);
- N.º de utente consultado;
- Operação efetuada.

Os *logs*, para terem validade legal devem estar assinados digitalmente.

O responsável deverá implementar uma política de análise de *logs* e efetuar relatórios periódicos de análise, que devem ser mantidos para efeitos de fiscalização pela CNPD.

No que respeita à conservação dos *logs* estabelece-se o prazo de dois anos.

Atendendo à sensibilidade da informação, circulando a mesma em rede, determina-se que a informação de ser cifrada (n.º 4 do artigo 15º da LPD), com algoritmo seguro, que tenha já sido objeto de verificação de fiabilidade. A chave deve também ser dotada de tamanho que assegure a robustez da encriptação.

Se a opção for a adoção de chaves simétricas, a comunicação das chaves deve ser efetuada por canal seguro de modo a preservar a segurança do sistema. De igual modo devem as chaves ser guardadas de forma protegida.

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

3. Decisão

Assim, tendo em atenção o disposto nas disposições combinadas dos artigos 7.º, n.º 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: Unidade Local de Saúde do Alto Minho, E.P.E.;



2. Finalidade: gestão do serviço social;
3. Categorias dos dados: Dados do processo (n.º de processo, n.º de episódio, módulo, serviço); Dados de identificação (nome, data de nascimento, sexo, nacionalidade estado civil, habilitações literárias, morada, documento de identificação, NIF, NISS); Dados clínicos relevantes para o apoio social; Dados socioeconómicos; Dados profissionais; Dados relativos a cuidadores/família; Procedimentos/Apoio; Alta social (data de alta clínica, data da alta hospitalar, data da alta social, destino após a alta e local de destino após a alta).
4. Comunicação de dados: Rede Nacional de Cuidados Continuados Integrados, Centro de Conferência de Faturas da ACSS, subsistemas de saúde e Segurança Social;
5. Interconexões: Não há
6. Fluxo Transfronteiriços de Dados para Países Terceiros: Não há
7. Exercício do direito de acesso: de forma presencial e por escrito junto do responsável;
8. Prazo de Conservação: seis meses após a morte ou a alta social do titular dos dados, sem prejuízo da sua conservação, não acessível aos utilizadores, para fins de arquivo histórico;

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, 16 de dezembro de 2014

Filipa Calvão (Presidente)