



AUTORIZAÇÃO N.º 284 /2014

I. Do Pedido

A CORMEDIS – Centro Diagnóstico Cardiológico, S.A. notificou à Comissão Nacional de Protecção de Dados (CNPD) um tratamento de dados pessoais com a finalidade de gestão administrativa de utentes.

O responsável pelo tratamento de dados presta serviços médicos, designadamente de clínica geral e ambulatório e pertence ao Grupo IMAG.

Os dados pessoais objeto de recolha são os seguintes: nome, data de nascimento, morada, contactos telefónicos, NIF, n.º de beneficiário, sistema de saúde, história clínica, dados de exames realizados no Grupo IMAG e dados de faturação.

Os dados são recolhidos de forma direta e pessoalmente.

Pretende ainda a responsável pelo tratamento que haja uma interconexão de dados entre todas as empresas do grupo, de modo a que possam ser prestados cuidados de saúde integrados em qualquer unidade do Grupo IMAG.

Apenas o médico assistente e o corpo clínico da unidade têm acesso à informação de saúde, mediante protocolo HTTPS com certificado SSL e autenticação direta no Portal através de nome de utilizador e palavra-passe. A ligação das aplicações nas clínicas com os servidores é feita por VPN configurada nas *gateways* de destino e de origem.

Aos titulares dos dados é assegurado o direito de conhecer e corrigir os dados que lhes respeitem.

I. Da Análise

A responsável pelo tratamento solicita a centralização da informação clínica das várias clínicas do grupo, para que sejam prestados cuidados de saúde integrados. Para esse



efeito, será criado um portal que agregará e disponibilizará informação recolhida nas várias clínicas ao profissional de saúde assistente, independentemente da unidade de saúde onde o utente se dirija dentro do Grupo IMAG. Deste modo, os médicos poderão prestar cuidados de saúde de forma continuada e consultar as imagens e elaborar os respetivos relatórios, independentemente do local onde haja sido realizado o exame.

Os resultados dos exames são centralizados em servidor próprio do Grupo IMAG e consultados pelo médico assistente ou pelo corpo clínico da unidade.

Porque referentes à saúde, os dados dos utentes dos serviços prestados pela requerente têm a natureza de sensíveis, nos termos do disposto no n.º 2 do artigo 7.º da Lei n.º 67/98, de 26 de outubro (Lei de Protecção de Dados – LPD).

Em regra, o tratamento de dados sensíveis é proibido, de acordo com o disposto no n.º 1 do artigo 7.º do diploma supra mencionado.

Todavia, o tratamento de dados de saúde é permitido, quando seja necessário para efeitos de medicina preventiva, de diagnóstico médico ou prestação de cuidados de saúde, desde que efetuado por um profissional de saúde obrigado a sigilo e observadas que sejam as medidas adequadas de segurança da informação (cf. n.º 4 do artigo 7.º da LPD).

O tratamento de dados notificado enquadra-se na situação supra.

O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para 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 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.

O sistema deve garantir uma separação lógica entre os dados referentes à saúde e os restantes dados pessoais, de natureza administrativa (cf. n.º 3 do artigo 15.º da LPD).

Devem, pois, ser adotadas medidas de segurança que impeçam o acesso à informação a pessoas não autorizadas.

Ainda no âmbito das condições de segurança, devem ser feitas cópias de segurança (*backups*) da informação, as quais deverão 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.

No que respeita à informação de saúde, deve ser implementado um sistema de filtros de segurança, para que a informação de saúde seja apenas visível pelo seu médico assistente, quando o doente o solicite. Admite-se que outros médicos possam aceder a essa informação em casos excepcionais, ficando registada a identificação do médico que acedeu a essa informação classificada como confidencial e o motivo desse acesso. Essa informação apenas poderá ser consultada por outros médicos em casos excepcionais e justificados, podendo os médicos que acedam injustificadamente a essa informação ser responsabilizados por essa violação do sigilo.

No que respeita à interconexão de dados, os dados serão conservados nos servidores próprios do Grupo IMAG, de modo centralizado.

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



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

II. Da Conclusão

Em face do exposto, a Comissão Nacional de Protecção de Dados (CNPD) autoriza o tratamento de dados pessoais *supra* apreciado, nos termos do n.º 4 do artigo 7.º, alínea a) do n.º 1 do artigo 28.º e n.º 1 do artigo 30.º da LPD, consignando-se o seguinte:

Responsável pelo tratamento: CORMEDIS – Centro Diagnóstico Cardiológico, S.A.

Finalidade: Gestão de processos clínicos.

Categoria de Dados pessoais tratados: nome, data de nascimento, morada, contactos telefónicos, NIF, n.º de beneficiário, sistema de saúde, história clínica, dados de exames realizados no Grupo IMAG e dados de faturação.

Entidades a quem podem ser comunicados: Não há.

Formas de exercício do direito de acesso e retificação: Junto do responsável pelo tratamento.

Interconexões de tratamentos: Os resultados dos exames são centralizados em servidor próprio do Grupo IMAG.

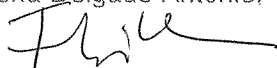
Transferências de dados para países terceiros: Não há.

Prazo de conservação:

- a) **Dados de saúde:** Nos termos do anexo à Portaria n.º 247/2000, de 8 de Maio;
- b) **Dados de faturação:** 10 anos.

Lisboa, 7 de Janeiro de 2014

Luís Paiva de Andrade (Relator), Luís Barroso, Ana Roque, Carlos Campos Lobo, Helena Delgado António, Vasco Almeida


Filipa Calvão (Presidente)