

## Autorização n.º 7268/2018

### I - Pedido

O Unidade Local de Saúde de Matosinhos, E.P.E., NIPC 506361390, notificou à CNPD um tratamento de dados pessoais com a finalidade de “tratamento estatístico de dados de consumo de medicamentos no âmbito da actividade hospitalar”.

Com o pedido foram entregues elementos descritivos do processo e uma avaliação de impacto na privacidade relativa ao tratamento a desenvolver.

Do pedido de autorização verifica-se que:

- a) Os dados pessoais a tratar são: idade nos intervalos: 0-2, 3-15, 16-40, 41-60, 61-80 e 81; No caso de não existir entropia na sua unicidade a idade pode ser suprimida, conforme consta da dita avaliação de impacto;
- b) A recolha de dados é feita de forma direta, por um agente extrator conforme avaliação de impacto na privacidade submetido;
- a) O exercício do direito de acesso é feito presencialmente e por escrito para a Rua Dr. Eduardo Torres Senhora da Hora, 4464-513 Matosinhos;
- b) São declaradas comunicações de dados a terceiros: à hmR- Health Market Research, Lda.;
- c) Não se verificam interconexões de tratamentos;
- d) Não existem fluxos internacionais de dados para países terceiros;
- e) A requerente pretende conservar os dados pessoais recolhidos pelo prazo máximo de 3 meses para o DataSet de Consumos de Medicamentos e pelo prazo máximo de 6 meses para o DataSet de Diagnósticos.

São indicadas medidas de segurança física e lógica.

### II - Apreciação

A- Deliberação n.º 589/2018, de 22 de maio

Este tratamento foi já analisado na deliberação n.º 589/2018, de 22 de maio, tendo-se aí analisado os aspetos técnicos do mesmo e concluído pela adequação das soluções gizadas para garantir a robustez e segurança do processamento dos dados pessoais

envolvidos. Remete-se, de resto, para a documentação que consta desse processo a configuração do tratamento.

Relembre-se que o que se pretende é utilizar um conjunto de informação, devidamente anonimizada, para tratamento estatístico. Tal deverá permitir orientar a gestão hospitalar de forma mais eficiente, sem com isso colocar em causa a proteção dos dados pessoais dos titulares dos dados cuja informação será utilizada. Nesta senda, os hospitais comprometem-se a implementar um conjunto de medidas técnicas que garantam a pseudonimização dos dados pessoais tratados, remetendo à hmR dados expurgados de identificação e que, para esta, constituem informação anonimizada, uma vez que não logrará de forma direta, indireta ou inferida re-identificar a informação.

#### B- Pedido

1. Como se descreveu na Deliberação da CNPD citada, no âmbito do processo em epígrafe, a hmR (Health Market Research), pretende implementar um projeto “Hospital Intelligence”, que comporta as soluções “Hospital Benchmark”, “Hospital Watch” e “Hospital DiagWatch”. A primeira “compara dados próprios de cada hospital com grupos de referência dinâmicos” e as duas últimas são plataformas eletrónicas de informação estatística sobre o consumo de medicamentos em ambiente hospitalar a nível nacional.

Na submissão do formulário foram entregues diversos documentos com informação adicional ao formulário:

1. Apresentação do projeto Hospital Benchmark;
  2. hmR Hospital Benchmark – Política de Privacidade;
  3. Privacy Impact Assessment – Health Market Research;
  4. Análise de Risco – Protocolo de Anonimização;
  5. Privacy Impact Assessment – Minuta hospitais participantes;
  6. Termos dos Serviços Online, versão 1/08/2016 – Microsoft;
  7. Contrato de fornecimento de dados.
2. Examinando o pedido, nota-se que serão tratados diversos dados, Medicamento (Código do Medicamento, Descrição, Código CHNM, Dose do Medicamento, Unidade

de medida, Via de Administração, Forma de Apresentação, Forma Farmacêutica, Grupo Farmacoterapêutico, Código ATC, Preço Unitário, Código da Família, Descrição da Família, Se está categorizado como Dispositivo Médico, Se está categorizado como Material Consumo Clínico); Caracterização de movimentos (Tipo de movimento - se é um consumo, devolução, compra ou retorno ao fornecedor; Descrição do tipo de movimento, Tipo de movimento - detalhe, Valor de Movimentação, Data do Movimento, Quantidade de Movimentação, Unidade de Movimentação, Lote, Prazo Validade, Marca, Estado, Preço Unitário, Valor); Fornecedores (Código do Fornecedor, Nome do Fornecedor, Número de Contribuinte); Dados de visita (Código do Serviço, Descrição do Serviço, Código da Valência, Descrição da Valência, Código do Centro de Custo, Descrição do Centro de Custo); ID doente e episódio - Consumo e Prescrição (Tipo de Doente, Número Interno do doente - Dado codificado na origem, Tipo de episódio, Número de Episódio - Dado codificado na origem); Informação específica da prescrição (Dosagem, Data, Duração, Frequência); Informação relativa a diagnósticos/GDHs (Ano de nascimento do doente (Intervalo de anos), Diagnósticos (icd9) principal (1) e secundários (2 a 20), Procedimentos cirúrgicos realizados (icd9), Peso à nascença (Kg) (se aplicável), Tipo de admissão, Classificação GDH segundo a classificação All Patients versão 21, Classificação GCD segundo a classificação All Patients versão 21 (GCD são os agrupadores de GDH s), Número de Episódio (Dado codificado na origem), Serviço de alta, Data de alta). Tal é, de resto, explicitado pela própria requerente nos documentos de apoio juntos ao processo.

De todos os elementos carreados ao processo resultou claro que se pretende tratar os dados supradescritos para efeitos de auxílio à gestão hospitalar, apoiando as unidades de saúde com essa informação.

Para efetivar esse tratamento de informação evitando riscos para os dados pessoais e privacidade dos seus titulares, propõe-se um processo de pseudonimização (com base em codificação) da informação pelo qual a identidade ou identificação de qualquer pessoa singular seja inalcançável à empresa hmR. Refira-se que será esta que tratará os dados codificados e, desse tratamento, resultará a informação a disponibilizar aos hospitais e demais intervenientes interessados do setor da saúde (públicos ou privados). Para tanto, serão instados dois servidores adicionais na Unidade Local de Saúde (ULS),

com a função de (num deles) recolher a informação necessária e (no restante) codificá-la para que posteriormente seja remetida à hmR. A esta última caberá apenas tratar a informação que lhe seja remetida pelo segundo servidor.

3. Também da informação remetida junto com o processo, resultou claro que à HMR nunca chegarão dados pessoais, isto é, nos termos do artigo 3.º, al. a), da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015 de 24 de agosto (Lei da Protecção de Dados, doravante LPDP): «qualquer informação, de qualquer natureza e independentemente do respectivo 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 directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social».

Para lá do facto de apenas a ULS ter acesso à informação que contenha dados pessoais, os algoritmos de anonimização indicados (revistos de acordo com as indicações da CNPD), e que são aplicados ao conjunto de elementos transmitidos à hmR para tratamento estatístico, apresentam uma robustez técnica<sup>1</sup> suficientemente sólida para afastarem essa mesma informação do conceito de dados pessoais citado. Isto, claro, apenas em relação a esta empresa, mantendo aqueles dados a qualificação do artigo 3.º, al. a), da LPDP, quanto à ULS que recolhe e conserva os dados pessoais dos seus utentes e profissionais.

Esta avaliação da CNPD encontra suporte na Orientação n.º 4/2007, sobre o conceito de dados pessoais, do Grupo do Artigo 29.<sup>º2</sup>. Nela se refere que «Se, levando em consideração “todos os meios que potencial e razoavelmente serão usados pelo responsável ou qualquer outra pessoa”, essa possibilidade [de identificação do titular dos dados] é inexistente ou negligenciável, a pessoa não deve ser considerada “identificável”, e a informação não deverá ser considerada “dado pessoal”. O critério

---

<sup>1</sup> Atente-se na versão 3.2 do documento onde vem descrito o algoritmo de anonimização, mais especificamente no seu ponto 2.

<sup>2</sup> Grupo consultivo, previsto no artigo 29.º da Diretiva 95/46/CE, de 24 de outubro, onde todas as autoridades de controlo da União Europeia têm assento.



“conjunto dos meios suscetíveis de serem razoavelmente utilizados quer pelo responsável quer por qualquer outra pessoa” deve levar em particular consideração todos os fatores em causa. O custo do processo de identificação é um dos fatores, mas não único. A finalidade pretendida, a forma como o tratamento está estruturado, a vantagem esperada pelo responsável pelo tratamento, os interesses dos titulares dos dados que estejam em causa, bem como o risco de organizações disfuncionais (v.g. quebras de deveres de confidencialidade) e falhas técnicas devem todos ser levados em consideração.<sup>3</sup>».

Com efeito, através das medidas mitigadoras do risco de identificação ou re-identificação aplicadas (desidentificação da informação prévia à transmissão da mesma para a hmR, algoritmos sólidos de anonimização, apagamento de informação sobre pacientes cujas patologias, pelo seu carácter atípico, poderia ser, ainda que sujeita à anonimização prevista, facilitadora da re-identificação dos titulares dos dados), a probabilidade ou, até, a possibilidade técnica de chegar à identidade dos titulares dos dados é praticamente nula.

Desta forma, teremos de considerar que a hmR não trata dados pessoais.

#### C- Licidade

O n.º 4 do artigo 7.º da Lei n.º 67/98, de 26 de outubro, alterada pela Lei n.º 103/2015, de 24 de agosto – Lei de Proteção de Dados Pessoais (LPDP), 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 de saúde e desde que estejam garantidas medidas de segurança da informação.

Quando os dados são processados para efeitos de medicina preventiva, de diagnóstico médico, de prestação de cuidados de saúde ou tratamentos médicos ou gestão de serviços de saúde há legitimidade para efetuar o seu tratamento automatizado quando este é feito por pessoas vinculadas a segredo profissional. Nessa medida, deve

---

<sup>3</sup> Tradução livre de excerto da página 15 da dita orientação.

compaginar-se a recolha da informação com *o princípio da confidencialidade*, respeitando-se, assim, o respetivo sigilo ou segredo profissional nos termos dos estatutos a que tais profissionais estão legal e estatutariamente vinculados, como forma de garantia à implementação das medidas adequadas a preservar a segurança da informação.

A informação tratada é recolhida de forma lícita (artigo 5.º n.º 1, alínea a), da LPDP), para finalidades determinadas, explícitas e legítimas (cf. alínea b) do mesmo artigo) e a informação recolhida não é excessiva. A CNPD considera que, no caso, existe legitimidade para o tratamento, por força do artigo 7.º, n.º 4, de LPDP.

Quanto ao direito de acesso, deve o mesmo respeitar o disposto no artigo 3.º, n.º 3<sup>4</sup>, da Lei n.º 12/2005, de 26 de janeiro (Lei da Informação Genética Pessoal e Informação de Saúde), na redação que lhe foi dada pela Lei n.º 26/2016, de 22 de agosto, e que agora apenas obriga à intermediação de médico no acesso aos dados de saúde do titular quando este último o solicite. Tal vem, indiscutivelmente, revogar o n.º 5 do artigo 11.º, da LPDP, que fazia depender da intermediação de médico o *“acesso à informação relativa a dados de saúde, incluindo os dados genéticos”*.

A precisão introduzida pela nova versão da Lei da Informação Genética Pessoal e Informação de Saúde não vem, contudo, afastar, as mais elementares regras de proteção de dados pessoais, nomeadamente no que respeita ao direito de acesso. Desta forma, o artigo 3.º, n.º 3, da Lei n.º 12/2005, de 26 de janeiro, deve ser alvo de leitura conjugada com o disposto no artigo 11.º, n.º 1, da LPDP, mantendo-se o direito, por parte do titular, de aceder aos seus dados pessoais e *“...de obter do responsável pelo tratamento, livremente e sem restrições, com periodicidade razoável e sem demoras ou custos excessivos”* tudo quanto vem disposto nas alíneas do referido preceito da LPDP.

Esta novidade não prejudica, ainda, os casos em que não seja apurável a vontade do titular dos dados, onde se mantém a obrigação de intermediação médica no acesso à

---

<sup>4</sup> Que assim dita: “O acesso à informação de saúde por parte do seu titular, ou de terceiros com o seu consentimento ou nos termos da lei, é exercido por intermédio de médico, com habilitação própria, se o titular da informação o solicitar.”.

informação de saúde, como o prescreve o n.º 4 do artigo 3.º da Lei da Informação Genética Pessoal e Informação de Saúde.

Quanto à conservação dos dados de saúde, vem ela melhor explicada na deliberação n.º 589/2018, de 22 de maio, daí decorrendo que “a grande maioria dos dados recolhidos será retida na base de dados local do hospital (no caso, unidade local de saúde) até a um período máximo de 2 meses, com a exceção de um conjunto específico de dados relativos à informação de diagnósticos e procedimentos que provêm do sistema de codificação em GDH, que necessitará de um período de retenção superior (de até 6 meses). Uma vez que o processo de codificação tem por base a premissa da múltipla cardinalidade dos dados que possam ser considerados conspícuos (visíveis), determinados elementos necessitam de ser retidos até que, perante um conjunto de dados cada vez mais completo, o sistema possa afirmar que já há cardinalidade suficiente (conjunto suficiente de dados) para permitir o envio para a hmR, ou, até que, face um conjunto de dados já completo, o sistema determine a necessidade de codificar os dados que não atinjam a cardinalidade necessária. Ora, considerando este conjunto de regras, para um conjunto de dados de evolução temporal lenta como os dados de codificação, que resultam de um processo com poucos automatismos, podendo verificar-se atrasos de até 4 meses para concluir a codificação de um mês, entende-se necessário reter os dados por um período máximo de 6 meses. Para todos os outros dados que são registados diariamente a retenção de dados será no máximo de dois meses”.

Entendemos, por isso, que os prazos propostos são justificados e proporcionados à finalidade descrita, devendo a generalidade da informação ser eliminada após 2 meses, com a exceção dos dados relativos à informação de diagnósticos e procedimentos que provêm do sistema de codificação em GDH, que se admite seja eliminada apenas após 6 meses.

Quanto à informação anonimizada em posse da hmR, não se aplica a LPDP, pelo que nenhum prazo se fixa para sua conservação.

A requerente declara existir comunicação de dados para a hmR. Contudo, e porque apenas lhe são transmitidos dados previamente sujeitos a processos de pseudonimização, sendo certa a impossibilidade de a hmR reverter esse processo e

identificar os titulares dos dados, não se aplica a LPDP, inexistindo, para os efeitos da lei, qualquer comunicação.

Deve ser dada especial atenção à necessidade de assegurar:

- a) O direito de informação aos titulares dos dados, nos termos dos artigos 10.º da LPDP;
- b) A separação lógica entre dados administrativos e dados de saúde (cf. artigo 15.º n.º 3 da LPDP);
- c) Devem ser adotadas medidas de segurança que impeçam o acesso à informação a pessoas não autorizadas. A informação de saúde que identifique os titulares dos dados deverá ser de acesso restrito aos médicos ou, sob a sua direção e controlo, a outros profissionais de saúde obrigados a segredo profissional (cf. artigo 7.º n.º 4 da LPDP).

### III – Decisão

Nestes termos e ao abrigo do disposto no n.º 4 do artigo 7.º, artigo 28.º e do artigo 30.º da LPDP, a CNPD autoriza o tratamento notificado, consignando o seguinte:

**Responsável:** Unidade Local de Saúde de Matosinhos, E.P.E.;

**Finalidade:** tratamento estatístico de dados de consumo de medicamentos no âmbito da atividade hospitalar da ULS;

**Categorias de dados pessoais tratados:** Medicamento (Código do Medicamento, Descrição, Código CHNM, Dose do Medicamento, Unidade de medida, Via de Administração, Forma de Apresentação, Forma Farmacêutica, Grupo Farmacoterapêutico, Código ATC, Preço Unitário, Código da Família, Descrição da Família, Se está categorizado como Dispositivo Médico, Se está categorizado como Material Consumo Clínico); Caracterização de movimentos (Tipo de movimento - se é um consumo, devolução, compra ou retorno ao fornecedor; Descrição do tipo de movimento, Tipo de movimento - detalhe, Valor de Movimentação, Data do Movimento, Quantidade de Movimentação, Unidade de Movimentação, Lote, Prazo Validade, Marca, Estado, Preço Unitário, Valor); Fornecedores (Código do Fornecedor, Nome do Fornecedor, Número de Contribuinte); Dados de visita (Código do Serviço, Descrição do Serviço, Código da Valência, Descrição da Valência, Código do Centro de Custo,



Descrição do Centro de Custo); ID doente e episódio - Consumo e Prescrição (Tipo de Doente, Número Interno do doente - Dado codificado na origem, Tipo de episódio, Número de Episódio - Dado codificado na origem); Informação específica da prescrição (Dosagem, Data, Duração, Frequência); Informação relativa a diagnósticos/GDHs (Ano de nascimento do doente (Intervalo de anos), Diagnósticos (icd9) principal (1) e secundários (2 a 20), Procedimentos cirúrgicos realizados (icd9), Peso à nascença (Kg) (se aplicável), Tipo de admissão, Classificação GDH segundo a classificação All Patients versão 21, Classificação GCD segundo a classificação All Patients versão 21 (GCD são os agrupadores de GDH s), Número de Episódio (Dado codificado na origem), Serviço de alta, Data de alta). Os dados são sujeitos a um processo de pseudonimização prévio ao tratamento estatístico;

**Comunicação de dados:** Não há;

**Forma de exercício do direito de acesso e retificação:** presencialmente e por escrito para a morada da responsável;

**Interconexão de dados:** Não há;

**Transferência de dados para países terceiros:** Não há;

**Conservação dos dados:** a generalidade da informação deve ser eliminada após 2 meses, com a exceção dos dados relativos à informação de diagnósticos e procedimentos que provêm do sistema de codificação em GDH, que se admite seja eliminada apenas após 6 meses.

Lisboa, 22 de maio de 2018



Filipa Calvão (Presidente)