DOI: 10.32385/rpmgf.v34i5.12466

Proteção de dados e o novo regulamento geral da União Europeia

José Augusto Simões*

A 25 do pretérito mês de maio entrou em vigor na União Europeia o novo Regulamento Geral de Proteção de Dados (RGPD),[1] que substituiu a anterior Diretiva europeia e a legislação nacional de proteção de dados. Os principais princípios deste regulamento são os seguintes:

- Informação aos titulares dos dados. O RGPD obriga a informar os titulares dos dados acerca da base legal para o tratamento dos seus dados, o tempo de conservação e a transferência dos mesmos. É, assim, necessária uma política de privacidade e textos que informem os titulares dos dados.
- Exercício dos direitos dos titulares dos dados. O RGPD obriga a garantir o exercício dos direitos dos titulares dos dados. Desta forma, os pedidos de exercício desses direitos passam a ser monitorizados e documentados com prazos máximos de resposta. Direitos à portabilidade dos dados, à eliminação dos dados e à notificação de terceiros sobre a retificação, o apagamento ou a limitação de tratamento solicitados pelos titulares dos mesmos.
- Consentimento dos titulares dos dados. O RGPD obriga a controlar as circunstâncias em que foi obtido o consentimento dos titulares, como base legal para o tratamento dos seus dados pessoais. Existe um conjunto de exigências para obtenção desse consentimento e o seu não cumprimento obriga à obtenção de um novo consentimento.
- Natureza dos dados. O RGPD define o conceito de dados sensíveis, que estão sujeitos a condições específicas para o seu tratamento, nomeadamente tratamento automatizado. Exemplo de dados sensíveis são os dados biométricos e de saúde. Dependendo da dimensão e contexto desse tratamento de dados específicos, pode ser obrigatória a nomeação de um Encarregado de Proteção de Dados (DPO – *Data Protection Officer*).
- Documentação e registo. O RGPD obriga a manter um registo documentado de todas as atividades de tratamento de dados pessoais. As organizações são obrigadas a demonstrar o cumprimento de todos os requisitos decorrentes da aplicação do regulamento.
- Subcontratação. O regulamento obriga a que o subcontratante garanta que detém todas as autorizações dos responsáveis pelo tratamento de dados. Os contratos de subcontratação têm de incluir um conjunto vasto de informações, com o objetivo de proteger a informação dos titulares de dados, a qual é frequentemente tratada por várias entidades sem que os respetivos titulares tenham conhecimento.
- Encarregado de Proteção de Dados (DPO – *Data Protection Officer*). O RGPD introduz a figura do DPO que tem o papel de controlar os processos de segurança para garantir a proteção de dados no dia-a-dia de uma organização. Embora não seja obrigatório para todas, a existência do mesmo ou de um serviço externo que garanta essa função pode acrescentar muito valor aos processos de cumprimento das obrigações de proteção de dados.
- Processos de segurança e tratamento de dados. O RGPD obriga a um grande controlo do risco associado ao possível roubo de informação. Este controlo de risco deve ser garantido por medidas de segurança efetivas que garantam a confidencialidade, a integridade dos dados e que previnam a destruição, perda e alterações acidentais ou ilícitas ou a divulgação/acesso não autorizado de dados.
- Proteção de dados desde a conceção. O RGPD salienta a necessidade de se avaliar em projetos futuros o tratamento de dados com a devida antecedên-

*Médico de família. UCSP da Mealhada, ACeS Baixo Mondego, ARS Centro. Professor Associado Convidado. Faculdade de Ciências da Saúde, Universidade da Beira Interior.

cia e rigor, de forma a poder avaliar o seu impacto na proteção de dados e adotar as medidas adequadas para mitigar esses riscos.
- Notificação de violações de segurança. O RGPD obriga a que todas as violações de segurança que resultem em risco para os direitos dos titulares sejam comunicadas à autoridade de controlo – Comissão Nacional de Proteção de Dados, em Portugal – assim como aos respetivos titulares dos dados.
- Coimas. O RGPD estabelece um quadro de coimas em função da gravidade da violação da proteção de dados.

Que implicações têm os princípios atrás enumerados para a prática do médico de família?
- Enquanto funcionário do Serviço Nacional de Saúde ou de uma organização de saúde privada, saber que política de privacidade e proteção de dados a sua instituição, pública ou privada, definiu e que normativos estabeleceu para o seu cumprimento.
- Enquanto médico com atividade liberal (consultório particular), estabelecer procedimentos que garantam a proteção e segurança dos dados sensíveis à sua guarda e informar os seus pacientes desses procedimentos, garantindo a confidencialidade dos seus dados.

As Unidades de Saúde Familiares (USF), enquanto unidades funcionais com autonomia funcional, devem igualmente estabelecer procedimentos que garantam a proteção e segurança dos dados sensíveis à sua guarda e informar os seus utentes desses procedimentos, garantindo a confidencialidade dos dados. Todos estes procedimentos devem ser passíveis de auditoria e comprovação, uma vez que perante o estabelecido no novo RGPD são as organizações que têm de provar que atuam de acordo com o estabelecido no regulamento.

Por fim, como proceder perante estudos de ficheiro, avaliação de qualidade e trabalhos de investigação. Aquando da elaboração do protocolo do estudo deve ser ponderado o modo de utilização de dados. Se os dados puderem ser completamente anonimizados deve-se optar por essa solução e garantir que a mesma se cumpre. Na maioria dos estudos observacionais e de qualidade pode-se fazer essa opção. Desde que se garanta a completa anonimização dos dados, ou seja, que não é possível identificar a quem pertencem aqueles dados, o seu tratamento não contraria o estabelecido no RGPD.

Se não for conveniente que os dados sejam anonimizados, por exemplo, estudos de intervenção, então deve-se procurar uma anonimização parcial, ou seja, os dados serem codificados e a chave de leitura desse código, o que permite ligar os dados à pessoa, fique à guarda do seu médico de família ou de quem se responsabilize pela proteção dos dados. Todo esse procedimento tem de estar estabelecido no protocolo do estudo e deve ser passível de auditoria.

Concluindo, deixou de ser necessário pedir autorização à Comissão Nacional de Proteção de Dados (CNPD), mas passou a ser necessário ponderar a segurança dos dados e a garantia da sua confidencialidade. No entanto, perante o tratamento de dados pessoais particularmente sensíveis pode ser realizada uma consulta prévia à CNPD.

Por fim, mantém-se a necessidade de parecer da Comissão de Ética para a Saúde para o protocolo do estudo, particularmente se de investigação clínica e, no mesmo, passam a ter de estar estabelecidos os procedimentos adotados para a garantia de proteção de dados, assim como uma avaliação de impacto sobre a proteção de dados, se particularmente sensíveis.

REFERÊNCIAS BIBLIOGRÁFICAS

1. Parlamento Europeu, Conselho Europeu. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). JOUE. 2016;L(119):1-88.

ENDEREÇO PARA CORRESPONDÊNCIA

jars58@gmail.com