2023

Comissão LGPD

RECOMENDAÇÕES

UNIDAS
AUTOGESTÃO EM SAÚDE

RECOMENDAÇÕES

Comissão Lei Geral de Proteção de Dados - UNIDAS

A Comissão LGPD da União Nacional das Instituições de Autogestão em Saúde, com objetivo de orientar suas filiadas, encaminha as recomendações abaixo referente a Lei Geral de Proteção de Dados (LGPD).

As recomendações são sínteses de posicionamentos dos membros da Comissão, composta por profissionais das mais diversas áreas tais como advogados, profissionais de tecnologia informação, gestores de privacidade, DPOs, gestores, dentre outros. São realizadas após discussões sobre pontos polêmicos escolhidos pela própria Comissão, objeto de dúvidas entre as operadoras de autogestão.

O objetivo de tais recomendações, antes de encerrar o enfrentamento sobre os pontos esclarecidos, é trazer a visão operacional e próxima da realidade da saúde suplementar, principalmente alinhando o conhecimento especializado da saúde suplementar com a nova Lei Geral de Proteção de Dados. Além disso, queremos divulgar a nossa visão sobre as mais diversas problemáticas trazidas pela LGPD na saúde suplementar, apresentando soluções adequadas ao segmento das autogestões.

Esperamos que as recomendações tragam soluções satisfatórias para as filiadas e para toda a comunidade da privacidade e segurança da informação.

Atenciosamente,

Comissão LGPD UNIDAS

RECOMENDAÇÃO Nº 1	As hipóteses previstas no parágrafo 4º do art. 11 da LGPD para tratamento de dados de saúde devem ser obrigatoriamente aplicadas em conjunto com uma das bases legais do art. 7o e 11, sob pena de ilegalidade no tratamento.
RECOMENDAÇÃO Nº 2	O consentimento será uma exceção no âmbito da saúde suplementar, devendo ser utilizado diante da impossibilidade de outras bases da LGPD, em especial, a de procedimentos preliminares e execução do contrato, bem como exercício de direitos previstos em contrato.
RECOMENDAÇÃO Nº 3	Conforme inciso II alínea "d" e parágrafo 4º, II do art. 11 da Lei Geral de Proteção de Dados, o uso de mecanismos de regulação (como a autorização prévia e a auditoria) no âmbito da relação entre prestador e operadora possui como base legal a execução e o exercício de direitos previstos em contrato.
RECOMENDAÇÃO Nº 4	O prazo de 2 (dois) dias uteis para a comunicação à ANPD é contado a partir da ciência do incidente de segurança com dados pessoais. Caso a ciência inicial seja de um operador, é a partir desse termo que o prazo deve ser contado, cabendo ao mesmo avisar ao controlador em tempo menor e razoável. Recomenda-se que esse prazo de comunicação entre operador e controlador seja de 1 (um) dia útil.
RECOMENDAÇÃO Nº 5	Caso a operadora pretenda, com base nos dados pessoais, dados pessoais sensíveis e metadados do BENEFICIÁRIO a que tiver acesso, estes coletados conforme definido no termo de adesão/contrato, definir perfis (perfilamento) e oferecer, de forma ativa, programas de promoção e prevenção à saúde a seus beneficiários, recomenda-se a coleta de consentimento prévio e específico (definido no(s) termo(s) do(s) programa(s), autorizando a abordagem futura por parte de funcionários/colaboradores da operadora
RECOMENDAÇÃO Nº 6	O uso de WhatsApp como ferramenta de comunicação dentro dos processos das autogestões não é recomendado tendo em vista evidentes riscos à privacidade e segurança. Contudo, caso se opte pela utilização dessa ferramenta, recomenda-se a utilização mínima dos seguintes requisitos. Parâmetro de referência: https://ico.org.uk/media/about-the-ico/documents/4020887/dhsc-reprimand.pdf (tradução Anexo I)
RECOMENDAÇÃO Nº 7	Nos programas de prevenção a hipótese de tratamento de dados deverá ser avaliada de acordo com a finalidade do dado, ainda que um mesmo dado coletado tenha diversas finalidades

Atualização 07/2023

ico.
Information Commissioner`s OIffice

Manutenção dos direitos de informação

Wycliffe House, Pista de água, Wilmslow, Cheshire, SK9 5AF
Telefone: 0303 123 1113 F. 01625 524510
www.ico.org.uk

OFICIAL SENSÍVEL

[redacted]
Department of Health and Social Care
[redacted]

Somente por e-mail para:

[redacted] 11 de julho de 2022

Referência: INV /0694/2021

Prezado_

Escrevo ainda para a nossa reunião de 21 de junho de 2022 e correspondência relacionada.

Tal como explicado, o Information Commissioner's Office (ICO) concluiu a sua investigação sobre a utilização de canais de correspondência privados pelo Departamento de Saúde e Assistência Social (DHSC), e partilhamos, em confiança, o nosso projecto de relatório proposto ao Parlamento sobre esta matéria.

Nesse relatório, é explicado que a ICO emitiu ao DHSC uma reprimenda em relação a questões de conformidade com a proteção de dados sob o Regulamento Geral de Proteção de Dados (GDPR), o Regulamento Geral de Proteção de Dados do Reino Unido (UKGDPR) e a Lei de Proteção de Dados do Reino Unido de 2018 (DPA). Esta carta expõe os detalhes dessa repreensão.

Nossa consideração sobre este caso

Principais problemas de conformidade

É importante ressaltar que a OIC não entende que o DHSC, e os órgãos públicos em geral, *nunca devem* enviar informações contendo dados pessoais para canais de comunicação privados. No entanto, quando esses canais estiverem em uso e o processamento de dados pessoais estiver ocorrendo, eles devem ser operados em conformidade com os requisitos da lei de proteção de dados do Reino Unido.

Tal como estabelecido na nossa proposta de relatório ao Parlamento, a nossa investigação determinou que os canais de comunicação privados eram regularmente utilizados pelo Departamento e que as comunicações trocadas através desses canais não eram em número insignificante.

Dessas comunicações, a maioria, senão a totalidade, das mensagens enviadas e recebidas continham dados pessoais. Tipicamente, esses dados consistiam em nomes, detalhes de contato e informações relacionadas ao trabalho profissional dos indivíduos.

Em um número muito pequeno de exemplos, identificamos dados de categoria especial nessas comunicações. Esses exemplos incluíram: uma referência à situação médica de um membro da família ao enviar um e-mail a um ministro; e uma referência à filiação partidária de um indivíduo (isso foi referenciado em um e-mail relacionado a negócios do governo e foi redirecionado para sistemas oficiais e reflete que os ministros operam em capacidades oficiais e políticas). Um outro exemplo foi identificado de um e-mail que continha dados de categoria especial da identidade da primeira pessoa no Reino Unido a receber uma vacina contra a Covid, no entanto, observamos que a informação já era de domínio público.

Como tal, concluímos que os dados de categoria especial não foram tratados através de canais de comunicação privados em qualquer grau significativo. Embora isso seja tranquilizador, não nega o fato de que os dados pessoais foram regularmente enviados e recebidos por meio desses canais, apesar de contas oficiais sob o controle do DHSC estarem disponíveis.

Verificamos, portanto, que o DHSC não cumpria totalmente os seguintes requisitos do GDPR, GDPR do Reino Unido e DPA18:

- **Artigo 5.o, n.o 1, alínea e)** - Limitação da armazenagem
- **Artigo 5.º, n.º 1, alínea f)** - Segurança
- **Artigo 25.º** - Proteção de Dados desde a conceção e por defeito
- **Artigo 32.º** - Segurança do tratamento

Isso ocorre porque o uso de canais privados de correspondência estava ocorrendo, sem controles adequados para gerenciar suficientemente os riscos que esse processamento apresentava.

Os fatores que contribuem significativamente para as infrações acima mencionadas incluem:

- Embora houvesse políticas locais de DHSC em vigor, que afirmavam que o uso de canais de comunicação privados era proibido (exceto em casos excepcionais

circunstâncias) tais políticas não se aplicavam a Ministros ou Diretores Não-Executivos (NEDs).

- A orientação do Gabinete do Gabinete sobre o uso de canais de comunicação privados se aplicava, no entanto, a Ministros e Funcionários Públicos. Isso criou uma desconexão entre as políticas do DHSC, aplicadas aos funcionários, e aquelas aplicadas aos ministros e NEDs.

- Dentro da orientação do Gabinete do Gabinete aplicável na época, foi explicado que as próprias políticas de segurança dos Departamentos se aplicariam ao gerar e comunicar informações.

- Como tal, houve uma falta de consistência na aplicação das políticas dos Departamentos, incluindo as Políticas de Gestão da Informação e Uso Aceitável de TIC do DHSC, e a da aplicação das orientações do Gabinete do Gabinete. Consideramos que a obtenção de coerência é essencial para que as expectativas do DHSC em relação aos Ministros e ao pessoal superior em relação à utilização dos canais de comunicação privados sejam claras para todas as partes relevantes.

- O Departamento não dispunha de controlos organizacionais ou técnicos adequados para garantir a segurança eficaz e a gestão dos riscos dos canais de comunicação privados. Isso porque faltavam controles para mitigar os riscos do uso de canais privados de correspondência, onde esse uso não poderia ser evitado.

- Nossa investigação determinou que o material oficial do governo contendo dados pessoais era mantido em plataformas não pertencentes ou gerenciadas pelo Departamento, apesar de os usuários dessas plataformas serem fornecidos com contas oficiais do DHSC. Isso demonstra um acúmulo de informações, incluindo dados pessoais, mantidas fora do patrimônio do DHSC e, portanto, fora do controle direto do Departamento. O uso de canais de correspondência privados criou um nível de risco desnecessário que poderia facilmente ter sido negado se o DHSC tivesse confiado em contas emitidas pelo @dhsc.gov.uk, que de qualquer forma haviam sido fornecidas, para se comunicar com os ministros e NED's. A dependência apenas de contas oficiais teria o efeito de reduzir o risco de acesso inadequado, uma potencial perda de integridade ou confidencialidade ou perda de dados.

- Além disso, a ICO descobriu que volumes menores de informações, marcadas como Sensíveis Oficiais ou contendo material Confidencial Oficial, também foram enviadas para contas fora do patrimônio do DHSC, apesar de esses titulares de contas receberem contas de e-mail oficiais do DHSC. Esses e-mails continham

identificadores pessoais que consistem em nomes e detalhes de contato das pessoas com quem os e-mails foram trocados. Isso levanta preocupações de segurança mais amplas sobre material departamental sensível sendo compartilhado fora do departamento sem controles óbvios em vigor. O Grupo de Segurança do Governo (parte do Gabinete do Gabinete) foi, portanto, informado deste assunto.

- Em síntese, a utilização de tais canais apresentava riscos desnecessários à confidencialidade, integridade e acessibilidade dos dados trocados.

Exceto que o uso de canais de correspondência privados pode ter trazido benefícios operacionais iniciais em um momento em que o Reino Unido estava enfrentando pressões excepcionais no início da pandemia de COVID-19. No entanto, é preocupante que tais práticas tenham sido realizadas, com pouca supervisão ou evidência de consideração dos riscos que isso poderia apresentar e aplicação de medidas de mitigação para minimizar esses riscos.

Resultado da investigação

Após uma análise cuidadosa e com base nas informações fornecidas até à data, o Comissário decidiu emitir uma repreensão ao DHSC, em conformidade com o artigo 58.º do UKGDPR.

A confirmar, esta repreensão foi emitida relativamente às seguintes operações de tratamento:

- **Artigo 5.º, n.º 1, alínea e) Limitação de armazenamento** exige que os dados pessoais sejam *«conservados sob uma forma que permita a identificação dos titulares dos dados durante um período não superior ao necessário para as finalidades para as quais os dados pessoais são tratados; os dados pessoais podem ser conservados por períodos mais longos, na medida em que os dados pessoais sejam tratados exclusivamente para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.º, n.º 1, sob reserva da aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados».*

- **Artigo 5.º, n.º 1, alínea f) Integridade e confidencialidade** requer que dados ser *«tratados de forma a garantir a segurança adequada dos dados pessoais, incluindo a proteção contra o tratamento não autorizado ou ilícito e contra a perda, destruição ou danos acidentais, utilizando medidas técnicas ou organizativas adequadas».*

- **Artigo 25.o** Estados *«Tendo em conta o estado da técnica, os custos de execução e a natureza, âmbito, contexto e finalidades do tratamento, bem como os riscos de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares decorrentes do tratamento, o responsável pelo tratamento deve, tanto no momento da determinação dos meios de tratamento como no momento do próprio tratamento, Aplicar medidas técnicas e organizativas adequadas, como a pseudonimização, concebidas para aplicar de forma eficaz os princípios da proteção de dados, como a minimização dos dados, e integrar as salvaguardas necessárias no tratamento, a fim de cumprir os requisitos do presente regulamento e proteger os direitos dos titulares dos dados.*

  O responsável pelo tratamento deve aplicar medidas técnicas e organizativas adequadas para garantir que, por defeito, apenas sejam tratados os dados pessoais necessários para cada finalidade específica do tratamento. Esta obrigação aplica-se à quantidade de dados pessoais recolhidos, à extensão do seu tratamento, ao período do seu armazenamento e à sua acessibilidade. Em especial, essas medidas devem assegurar que, por defeito, os dados pessoais não sejam disponibilizados a um número indefinido de pessoas singulares sem a intervenção do indivíduo.

  Um mecanismo de certificação aprovado nos termos do artigo 42.o pode ser utilizado como elemento para demonstrar o cumprimento dos requisitos estabelecidos nos n.os 1 e 2 do presente artigo».

- **Artigo 32.o** - **Segurança do processamento.** Este estado *«Tendo em conta o estado da técnica, os custos de execução e a natureza, âmbito, contexto e finalidades do tratamento, bem como o risco de probabilidade e gravidade variáveis para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante devem aplicar medidas técnicas e organizativas adequadas para garantir um nível de segurança adequado ao risco, incluindo, nomeadamente, se for caso disso: ... b) A capacidade de assegurar a confidencialidade, a integridade, a disponibilidade e a resiliência contínuas dos sistemas e serviços de tratamento».*

Outras medidas recomendadas

Observamos e saudamos o reconhecimento pelo DHSC dos desafios apresentados pela inconsistência da aplicação em políticas e procedimentos relacionados ao uso de correspondência privada e a necessidade de alinhar as orientações departamentais e intergovernamentais para garantir a consistência.

Juntamente com a decisão da OIC de emitir uma repreensão ao DHSC neste caso, o Comissário também recomenda que o DHSC tome medidas adicionais para melhorar a sua conformidade com o RGPD (Reino Unido) e implementar medidas técnicas e organizacionais suficientes para garantir um nível de segurança adequado ao risco para a segurança, integridade, disponibilidade e resiliência apresentados em relação à sua utilização de canais de correspondência privados. Em particular, recomendamos que o DHSC tome as seguintes medidas:

(1) A fim de melhorar o cumprimento do artigo 5.º, n.º 1, alínea f), e do artigo 32.º do UKGDPR, o DHSC deve proceder a uma revisão para avaliar os controlos de segurança e de acesso em vigor em relação às plataformas em uso regular (Google Mail, Hotmail, Whatsapp) aquando do intercâmbio de comunicações que contenham dados pessoais, e para confirmar a sua adequação e adequação para apoiar a conformidade do DHSC com o UKGDPR e o DPA18.

(2) Como parte desse processo de revisão, avaliar os termos e condições das plataformas acima mencionadas e os avisos de privacidade para entender como as informações seriam processadas, onde seriam armazenadas e considerar quaisquer implicações para (a) a segurança dessas plataformas em relação ao potencial de acesso de terceiros, (b) a extensão em que a limitação de armazenamento é colocada, c) Em que medida os requisitos em matéria de proteção de dados desde a conceção e por defeito podem ser cumpridos se forem utilizados os
É para continuar.

(3) O DHSC também deve exigir que os usuários das plataformas sigam orientações de segurança apropriadas, como as emitidas pelo Centro Nacional de Cibersegurança (NCSC) em relação a:

- Requisitos mínimos de autenticação, por exemplo, controles de autenticação de dois fatores; e
- Controles de acesso remoto (levando em conta a capacidade de acessar a partir de vários dispositivos; e permanecer conectado às contas)

(4) O Departamento também deve revisar as opções seguras de "traga seu próprio dispositivo" para acesso controlado a contas oficiais do DHSC por meio de dispositivos pessoais, de acordo com as Diretrizes do NCSC.

(5) A fim de melhorar o cumprimento do artigo 5.º, n.º 1, alínea e), do UKGDPR, o DHSC deve limitar as situações em que essas contas

(Google Mail, Hotmail, Whatsapp) pode ser usado para impedir o processamento de rotina em tais plataformas.

(6) Além disso, o DHSC deve estabelecer requisitos claros para a exclusão de informações de contas pessoais uma vez adicionadas ao registro oficial.

(7) Além disso, o DHSC deve assegurar que a utilização de dispositivos pessoais aquando do intercâmbio de dados pessoais respeite os princípios de minimização de dados.

(8) A fim de melhorar a conformidade com o Artigo 25 do UKGDPR, o DHSC deve estender a aplicação de políticas e procedimentos específicos do DHSC relacionados ao uso de e-mail a todos os titulares of@dhsc.gov.uk contas como padrão (inclusive para Diretores Não-Executivos e Ministros). Se tal não for possível, devem ser fornecidas informações adaptadas aos titulares de contas oficiais isentos das apólices, como parte dos seus processos de indução.

Para completar, pedimos que o DHSC forneça uma atualização de progresso sobre até que ponto implementou qualquer uma das recomendações acima à OIC até 14 de outubro de 2022. Uma nova atualização sobre o progresso é solicitada até 06 de janeiro de 2023.

Ficaríamos gratos se o DHSC pudesse copiar sua resposta à ICO em relação às recomendações acima ao Comitê Seleto do DHSC. Isto terá o efeito de colocar a resposta no domínio público, o que esperamos que traga uma camada adicional de confiança do público nas medidas tomadas.

A menos que instruído de outra forma, forneça estas atualizações para [redacted]

Deve salientar-se que a decisão da OIC de emitir uma repreensão neste caso não diminui a gravidade deste assunto e foi alcançada no balanço de todas as informações disponíveis para o nosso escritório antes e após as respostas do DHSC e de outras paridades relevantes aos Avisos de Informação, nossa consideração da correspondência que trocamos, e os detalhes discutidos nas reuniões realizadas em apoio a esta investigação.

Portanto, embora as medidas acima sejam nossas recomendações, se mais informações relacionadas às preocupações de conformidade destacadas nesta última vierem à tona, ou se quaisquer outros incidentes ou reclamações de natureza semelhante forem relatados

Para nós, revisitaremos esse assunto e uma ação regulatória formal pode ser considerada como resultado.

Mais informações sobre o cumprimento da legislação de proteção de dados que é relevante para este caso podem ser encontradas no seguinte link: https://ico.org.uk/for organizações/guia para proteção de dados/

Divulgamos ativamente nossa atividade regulatória e nossos resultados, pois isso nos ajuda a alcançar nossos objetivos estratégicos na defesa dos direitos de informação de interesse público. Podemos publicar informações sobre casos que nos são relatados, por exemplo, quando achamos que há uma oportunidade para outras organizações aprenderem ou quando o caso destaca um risco ou um problema novo.

Como sabem, há uma intenção de publicar o resultado desta investigação através de um relatório ao Parlamento. Também podemos tornar públicos detalhes da própria repreensão.

De forma mais geral, publicaremos informações de acordo com nossa Política de Atividade de Regulamentação e Execução de Comunicação, que está disponível on-line no seguinte link:

https://ico.org.uk/media/aboutthe%20ico/policiesandprocedures/1890/ico Enfor comunicações de cimento política.pdf

Por último, em nome da equipa de investigação, gostaria de lhe agradecer a si e aos seus colegas a sua ajuda durante o decurso da nossa investigação. Consideramos agora que o inquérito está encerrado.

Atenciosamente,

Steve Eckersley

Director, Gabinete do Comissário

de Informação sobre

Investigações