

Guião de Apoio no tratamento de dados pessoais no CEREGA

1. Objetivo do Guião

Este documento destina-se a apoiar os investigadores que utilizam o CEREGA no tratamento de dados pessoais para fins de investigação científica, assegurando a conformidade com:

- Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados - RGPD);
- Lei n.º 58/2019;
- Princípios éticos aplicáveis à investigação em saúde;
- Orientações EDPB (*European Data Protection Board*);
- Boas práticas definidas pelos reguladores e autoridades de controlo, europeus;
- Princípios de segurança e governação definidos pela SPG.

2. Quando Deve Ser Utilizado

O presente guião deve ser utilizado sempre que exista:

- recolha de dados pessoais nos projetos de investigação;
- tratamento de dados de saúde – categorias especiais;
- necessidade de utilização de técnicas de gestão do risco e de segurança no tratamento reforçadas, como por ex. a pseudonimização;
- partilha de dados entre centros de investigação;
- utilização de múltiplas bases de dados pessoais;
- exportação e transferência de dados pessoais;
- utilização de soluções de inteligência artificial ou de algoritmos analíticos;
- interoperabilidade entre de bases de dados;
- reutilização de dados clínicos para finalidades de investigação.

3. Papel dos Intervenientes

No âmbito do presente guião de suporte à atividade dos investigadores:

- A Sociedade Portuguesa de Gastroenterologia (SPG) assume o papel de subcontratante, responsável por providenciar o acesso à plataforma CEREGA.

- As estruturas de investigação – ex. Centros de Investigação, assume o papel de responsáveis pelo tratamento dos dados pessoais.

Função	Responsabilidades
Investigador Principal	Garantir licitude e conformidade do tratamento
Centro participante	Garantir base legal e informação aos titulares
Sociedade Portuguesa de Gastroenterologia	Governança da plataforma
DPO	Aconselhamento, supervisão e monitorização
Administrador CEREGA	Gestão de acessos e segurança
Subcontratantes	Cumprimento contratual e medidas técnicas

4. Princípios Fundamentais a Cumprir

4.1 Licitude, lealdade e transparência

Os investigadores devem identificar e documentar claramente:

- finalidade científica;
- fundamento jurídico;
- condições aplicáveis ao tratamento de dados de saúde.

4.2 Limitação das finalidades

Os dados pessoais no âmbito dos projetos de investigação apenas podem ser utilizados:

- para os objetivos científicos definidos;
- de forma compatível com os protocolos e regras aprovadas e em vigor;
- quando estejam devidamente documentados com controlo de registos.

4.3 Minimização dos dados

Em cada projeto de investigação e previamente à utilização da plataforma CEREGA, apenas devem ser recolhidos:

- os dados estritamente necessários;
- os dados que permitam tratar as variáveis clinicamente justificadas;
- os dados e quaisquer informações proporcionais e adequados ao objetivo científico.

4.4 Exatidão

Devem existir mecanismos e instrumentos nos projetos de investigação que possibilitem assegurar:

- a validação dos dados de acordo com critérios e requisitos dos projetos;
- a respetiva atualização, sempre que aplicável, para garantir a exatidão no tratamento dos dados pessoais;
- a correção de registos, de forma controlada e documentada.

4.5 Limitação da conservação

Previamente à utilização da plataforma CEREGA, devem ser definidos:

- os períodos de retenção dos dados pessoais;
- se aplicável, os critérios de anonimização dos dados pessoais;
- os critérios de eliminação dos dados pessoais.

4.6 Integridade e confidencialidade

Para além dos controlos e das medidas e salvaguardas, adequadas e proporcionais que a plataforma CEREGA integra na sua arquitetura, devem ser garantidos pelos investigadores e suportados em procedimentos claros, a validação e a existência de:

- controlo de acessos;
- modelos de autenticação multifator aos vários sistemas de informação;
- registo de logs;
- cifragem dos dados pessoais quando aplicável;
- segregação de perfis de administração e de utilização;
- utilização de técnicas de pseudonimização quando aplicável.

5. Base Jurídica para Investigação Científica

Possíveis fundamentos:

- interesse público na área da saúde pública;
- investigação científica;
- consentimento válido;
- cumprimento de obrigação legal;
- medicina preventiva ou gestão de cuidados de saúde.

6. Categorias de Dados Tratados

Dados potencialmente tratados na plataforma CEREGA:

- dados clínicos e de diagnóstico;
- dados de resultados laboratoriais;
- dados de exames complementares;
- dados de aplicação de terapêuticas;
- dados de resultados clínicos;
- dados demográficos;
- dados e identificação pseudonimizados.

7. Avaliação de Necessidade de AIPD – Avaliação do impacto na proteção de dados

O investigador deve avaliar se o projeto/estudo exige uma AIPD, alinhando-a com as AIPD's produzidas no âmbito da gestão e da utilização da plataforma CEREGA.

Deverá ser consultado o encarregado de proteção de dados da estrutura / Centro de investigação..

Indicadores típicos de obrigatoriedade:

- tratamento de dados de saúde em larga escala;
- cruzamento de dados entre bases de dados;
- utilização de tratamento de dados que produzam profiling ou decisões automatizadas;
- utilização de soluções de IA/algoritmos;
- utilização de dados resultantes de monitorização sistemática;
- tratamento de dados de pessoas especialmente vulneráveis;
- partilha / transferência internacional de dados;

- utilização de processos ou de tecnologia inovadores.

8. Template Simplificado de AIPD para Investigadores CEREGA

A. Descrição do Projeto

- título do estudo;
- objetivo;
- responsáveis;
- centros participantes;
- categorias de titulares;
- categorias de dados.

B. Fluxo de Dados

- origem dos dados;
- método de recolha;
- armazenamento;
- acessos;
- transferências de dados;
- retenção;
- eliminação.

C. Necessidade e Proporcionalidade

Descrever:

- porque razão os dados são necessários;
- porque razão a finalidade não pode ser concretizada com menos dados;
- que tipo de medidas de minimização serão implementadas.

D. Identificação dos Riscos

Risco	Impacto
Reidentificação	Elevado
Acesso indevido	Elevado
Exportação insegura	Elevado
Uso secundário indevido	Médio/alto
Falha de controlo de acessos	Elevado

E. Medidas de tratamento e de mitigação

Medida	Implementação
Pseudonimização	Obrigatória
MFA – autenticação multifator	Obrigatório
Logs	Obrigatórios
Segregação de acessos	Obrigatória
Revisão periódica	Semestral
Acordos de tratamento de dados	Obrigatórios

Formação em proteção de dados pessoais	Obrigatória
---	--------------------

F. Risco Residual

Avaliar o nível do risco residual:

- baixo;
- médio;
- elevado.

Se o risco residual for elevado:

- consultar o DPO da estrutura/Centro de investigação;
- efetuar uma eventual consulta prévia à Comissão Nacional de Proteção de Dados (CNPD).

9. Regras de Utilização da Plataforma CEREGA

É proibido:

- descarregar conjuntos de dados/datasets identificáveis sem autorização;
- partilhar credenciais;
- utilizar dados para finalidades não aprovadas;
- exportar dados para ferramentas externas sem validação do DPO e dos reponsáveis pelos estudos/projetos;
- utilização de soluções de IA sem avaliação prévia do impacto.

10. Transferências Internacionais

Qualquer transferência para fora do Espaço Económico Europeu exige que a equipa de investigação valide a existência, ou assegure, a utilização de instrumentos como:

- decisões de adequação;
- SCCs – cláusulas contratuais standard;
- Derrogações especiais;
- *Assessment* ao impacto das transferências – *Transfer impact assessment*;
- validação jurídica/DPO.

11. Publicações Científicas

As publicações que resultem dos estudos/projetos de investigação:

- não devem permitir reidentificação;
- devem usar dados agregados;
- devem respeitar a minimização estatística;
- devem possibilitar a avaliação do risco em subgrupos raros.

12. Direitos dos Titulares

Os investigadores são responsáveis e devem estar preparados para responder aos titulares dos dados, ou dar o seu apoio à reposta, no caso do exercício dos direitos de:

- acesso;
- retificação;
- limitação;
- oposição;
- informação;
- portabilidade, quando aplicável;
- gestão do consentimento (quando aplicável).

13. Gestão de Incidentes e de Violações de dados pessoais

Qualquer incidente deve ser comunicado:

- imediatamente;
- ao DPO da estrutura / Centro de investigação e à SPG;
- com descrição factual;
- com as medidas imediatamente adotadas;
- com a avaliação preliminar do impacto.

14. Checklist Operacional Antes do Início do Estudo

Checklist para Investigadores

- Objetivo científico definido
- Base jurídica identificada
- Papéis e responsabilidades no tratamento de dados pessoais, devidamente definido e aprovado
- Informação aos titulares preparada
- Variáveis minimizadas
- Registo de atividades de tratamento para o estudo/projeto de investigação
- AIPD avaliada
- Acessos definidos e perfis de utilização definidos
- Pseudonimização definida e estruturada se aplicável
- Contratos/subcontratantes com acordos de tratamento de dados validados
- Plano de retenção definido
- Aprovação ética obtida
- Aprovação pelo DPO obtida

15. Recomendações Adicionais de Boas Práticas

Governance by Design

Integrar a proteção de dados:

- desde o desenho do estudo;
- durante todo o ciclo de vida do projeto de investigação.

***Least Privilege Access* – Princípio do interesse em conhecer**

A gestão dos acessos deve garantir que os mesmos são:

- limitados;
- auditáveis;
- temporários;
- baseados na função e na necessidade de aceder e de conhecer.

Revisão periódica

Deve ser realizada uma revisão anual ou sempre que existam alterações significativas no estudo/projeto de investigação ao nível de:

- gestão dos acessos;
- necessidade de tratamento e/ou continuidade do tratamento dos dados;
- retenção e conversação;
- medidas de segurança e controlos implementados.

Governança da partilha de dados

Deverão ser formalizados:

- acordos de tratamento de dados entre estruturas de investigação/Centro de investigação;
- definição de papéis e de responsabilidades;
- registo das atividades de tratamento;
- regras de reutilização.

16. Anexos Recomendados – avaliar da necessidade:

Anexo I: Template simplificado AIPD CEREGA

Anexo II: Checklist de minimização de dados – registo de atividades de tratamento

Anexo III: Modelo de registo de acessos

Anexo IV: Modelo de acordo de tratamento de dados

Anexo V: Procedimento de gestão de incidentes e de violação com dados pessoais