# PROTOCOLO DE SEGURANÇA DE DADOS v1.3

REDE DE PESQUISA
TDAH
BRASIL

## Resumo Executivo

**Título:** Protocolo de Segurança de Dados – Rede de Pesquisa TDAH Brasil (v1.3 – 2025)

**Objetivo:**
Garantir a confidencialidade, integridade e segurança dos dados pessoais sensíveis e ultrassensíveis coletados nos estudos da Rede de Pesquisa TDAH Brasil, conforme as exigências da LGPD.

**Abrangência:**
Aplica-se a toda a equipe de pesquisa: alunos, técnicos, clínicos, pesquisadores e professores, em todas as etapas de coleta, armazenamento, análise e comunicação de dados.

**Plataformas e canais oficiais:**

- **Otus Solutions** – Coleta e gerenciamento de dados clínicos e laboratoriais.
- **Google Planilhas** – Apoio operacional (com dados pseudonimizados).
- **WhatsApp e e-mails institucionais** – Comunicação exclusivamente por canais autorizados.

**Classificação dos dados:**

- Nível 1 a 5 (do mais sensível ao público).
- Uso de pseudonimização e anonimização progressiva.
- Restrições de acesso conforme a função na equipe.

**Princípios-chave:**

- **Menor privilégio de acesso**
- **Registro de consentimentos e treinamentos**
- **Criptografia e backup automatizado**
- **Revisões periódicas de acessos**
- **Prevenção e resposta a incidentes**

**Incidentes anteriores tratados:**

- Violação de anonimato por bolsista (leve)
- Vazamento percebido em IA (grave, mas originado por familiar do participante)

**Conformidade com a LGPD:**
Avaliação de risco obrigatória antes de novos projetos; mitigação ativa e documentação permanente.

| | | | |
|---|---|---|---|
| **Versão anterior:** | 1.2_2024 | **Data:** | 20/02/2024 |
| **Versão atual:** | 1.3_2025 | **Data:** | 06/05/2025 |
| **Revisado:** | Prof. Dr. Claiton Henrique Dotto Bau | **Data:** | 03/06/2025 |
| **Aprovado:** | Prof. Dr. Eugenio Horacio Grevet | **Data:** | 04/06/2025 |
| **Aprovado:** | Prof. Dr. Diego Luiz Rovaris | **Data:** | 04/06/2025 |

## 1. Objetivo

Estabelecer diretrizes e procedimentos para **garantir a segurança dos dados** coletados e utilizados nos projetos de pesquisa vinculados diretamente à Rede de Pesquisa TDAH Brasil[1]. Considerando a natureza da pesquisa, voltada à saúde mental e psiquiatria, todos os dados coletados devem ser caracterizados como dados pessoais sensíveis ou ultrassensíveis. Isso inclui **qualquer tipo de informação obtida dos participantes da pesquisa**, seja por meio de autorrelato ou a partir de avaliação clínica. Portanto, tais dados exigem níveis elevados de proteção e de respeito à confidencialidade.

## 2. Escopo

Este protocolo **se aplica a todos os membros da equipe de pesquisa (sem exceção)** — incluindo alunos(as) de iniciação científica e de pós-graduação, pós-doutorandos(as), médicos(as), psicólogos(as), professores(as) e demais profissionais técnicos da equipe — e abrange todos os dados manipulados por meio da plataforma digital Otus Solutions®, bem como por outros meios (por exemplo: Google Planilhas, e-mails e dispositivos pessoais, tais como tablets e celulares).

## 3. Plataformas Utilizadas

A seguir estão descritas as ferramentas utilizadas pela Rede de Pesquisa TDAH Brasil. **A classificação de risco, bem como orientações sobre manejo estão descritas nas seções subsequentes.**

[1] Processos:
CAAE 44505621.3.0000.5467
CAAE 44505621.3.3001.5327
CAAE 44505621.3.3002.0068
CAAE 44505621.3.3005.0076
CAAE 44505621.3.3004.5505

### 3.1. Otus Solutions®: Versão Rede TDAH Brasil (otus-prodah.otus-solutions.com.br)

A plataforma Otus (*Otus Solutions*®) é parte integral do gerenciamento e coleta de dados na Rede TDAH Brasil. O domínio é gerenciado por um Pesquisador Responsável (PR)[2]. O processo de coleta e gestão de dados de forma digital apresenta diversos benefícios em relação ao processo não automatizado, dentre eles estão a padronização dos dados coletados, confiabilidade e redução no custo operacional de estudos que envolvem coletas de muitos indivíduos e/ou que apresentam um protocolo extenso. A automatização é necessária para agilizar tarefas repetitivas e minimizar erros em processos sensíveis. A plataforma Otus, foi a solução selecionada pela Rede de Pesquisa TDAH Brasil para suprir as necessidades dos seus estudos, permitindo realizar a gestão de indicadores coletados e o processo de captação destes dados, integrando atividades como construção e aplicação de questionários, gestão laboratorial, transporte de amostras, acompanhamento de indicadores e demais recursos gerenciais, essenciais para que a equipe de pesquisa possa monitorar adequadamente o andamento do estudo.

Por se tratar de uma ferramenta *open source* a possibilidade de customização a nível de programação é possível e sua compatibilidade com diversos outros meios de coleta torna a integração algo mais simples. Dentre os serviços que são utilizados a partir do contrato vigente:

1. Infraestrutura de servidores: Todos os servidores, DNS (*Domain Name System*) e meios de disponibilização do acesso são construídos e mantidos em território nacional e todos os dados são isolados de qualquer outro acesso. Para análise dos dados coletados, o *download* de arquivos em diferentes formatos (ex.; .csv, .sav, .txt) é efetuado **do servidor da *Otus Solutions*® diretamente para o servidor do laboratório (Tordilho Negro *Server*) ou computador pessoal de trabalho do analista sênior autorizado[3]**.
2. Segurança: Certificados digitais para criptografia são fornecidos para garantir o anonimato das comunicações, impedindo o vazamento de dados ultrassensíveis.
3. *Backup*: O processo de *backup* pela *Otus Solutions*® é realizado de forma automatizada e mantido digitalmente seguro a partir de plataformas específicas para tal finalidade.
4. Treinamento: São realizados treinamentos quando novas funcionalidades são disponibilizadas, o que permite manter a equipe constantemente envolvida e atualizada.

### 3.2. Google Planilhas

[2] Diego Luiz Rovaris.
[3] Eduardo Schneider Vitola.

Usado para controle operacional, listas de participantes, organização de coletas etc. O Google Planilhas (ou ***Google Sheets***, em inglês) é um aplicativo do Google para **criação, edição e compartilhamento de planilhas online**. A ferramenta funciona de forma semelhante ao Microsoft Excel, mas com a vantagem de estar integrado à nuvem (*Google Drive*), o que permite:

- Acesso de qualquer lugar, com salvamentos automáticos, desde que haja conexão de *internet*.
- Edição colaborativa em tempo real, podendo vários membros da equipe de pesquisa trabalhar na mesma planilha ao mesmo tempo, com diferentes níveis de acesso às planilhas.
- Histórico de versões, sendo possível ver e restaurar versões anteriores de cada planilha, além de controlar quem (e quando) fez edições (**ponto positivo em termos de minimização de riscos**).
- Suporta funções matemáticas, lógicas, estatísticas, bem como a criação de gráficos e filtros.
- Integração com outros serviços do Google, como Google Formulários e *Google Docs*.

### 3.3. *WhatsApp*

O *WhatsApp* é uma aplicação de mensagens instantâneas e chamadas de voz e vídeo que oferece uma plataforma para comunicação pessoal e profissional, utilizando a internet para enviar e receber dados. A segurança do *WhatsApp* é um ponto fundamental, sendo **protegida por criptografia de ponta a ponta**, o que significa que as mensagens e chamadas só são decifradas pelos remetentes e destinatários, e não pelo próprio *WhatsApp* ou por terceiros. As comunicações entre participantes de pesquisa e a equipe poderá ser realizada por dois contatos de *WhatsApp*: 1) Rede de Pesquisa TDAH Brasil [redacted]) Agendamentos de avaliações clínicas (Vanice) [redacted]

### 3.4. E-mail

Um e-mail institucional (corporativo), é um endereço de e-mail fornecido por uma empresa ou instituição, geralmente com o domínio da organização, como "nome@usp.br". Este e-mail é utilizado para comunicação formal e profissional, diferenciando-se dos e-mails pessoais como Gmail ou Yahoo. A segurança do e-mail institucional é crucial para proteger a reputação da instituição, dados confidenciais e evitar ataques cibernéticos. As comunicações entre participantes de pesquisa e a equipe poderá ser realizada por dois e-mails principais: 1) tdahbrasil@usp.br e 2) tdahbrasil@ufrgs.br.

## 4. Atribuição de Acessos

O PR[4] é o único autorizado a conceder, revisar periodicamente e revogar acessos. Na sua ausência, essa atribuição será exercida por um segundo PR[5]. **A concessão de acessos deve sempre obedecer ao princípio do menor privilégio**. A revisão dos acessos deve ser realizada anualmente ou sempre que houver alterações na composição da equipe de pesquisa (por exemplo, a inclusão ou remoção de pessoas). O **Quadro 1** lista os níveis de acesso para cada conjunto de pesquisadores.

## 5. Controle e Classificação dos Dados

- Dados ultrassensíveis (informações médicas) associados a identificação do participante de pesquisa devem ser armazenados **SOMENTE** na plataforma Otus.
- Dados operacionais devem ser pseudonimizados (ID Otus) se estiverem fora da plataforma (ex.: no Google planilhas).
- Dados em bancos de dados para análise devem ser anonimizados (ID alternativo ao ID Otus e rastreável somente pelo analista sênior[6]).
- Classificação dos dados:
    - Nível 1: Dados ultrassensíveis – Acesso restrito, criptografado (somente na plataforma Otus).
    - Nível 2: Dados operacionais internos (sensíveis) – Acesso limitado à equipe de campo (mantê-los pseudonimizados em planilhas e comunicações via e-mail e *WhatsApp*).
    - Nível 3: Dados pseudonimizados em segundo nível para análise por parte do grupo (bancos de dados em R ou .sav).
    - Nível 4: Dados anonimizados para análise em consórcios de pesquisa[7] (bancos de dados em .csv, .txt ou R).
    - Nível 5: Dados públicos ou administrativos – Acesso geral dentro da equipe.

[4] Diego Luiz Rovaris.
[5] Eugenio Horácio Grevet.
[6] Eduardo Schneider Vitola.
[7] De acordo com a LGPD (Art. 5º, inciso XI), dados anonimizados são aqueles que, após o tratamento, não podem ser relacionados, direta ou indiretamente, a um indivíduo. Ou seja, mesmo que se conheça parte dos dados, não se deve conseguir reidentificar a pessoa. Se os dados permanecerem com algum identificador indireto potencial (por exemplo, ID Otus), então o processo é melhor descrito como pseudonimização, e o protocolo deve refletir isso.

**QUADRO 1 – NÍVEIS DE ACESSO**

**1. Pesquisador Responsável (PR)**

- ✅ Acesso completo a todos os dados (identificados e não identificados).
- ✅ Permissão para conceder e revogar acessos.
- ✅ Supervisão de segurança e conformidade bioética.

⬇️

**2. Investigadores Principais (IP)**

- ✅ Acesso a dados anonimizados e não identificados de seus próprios subprojetos.
- ✅ Solicitação de dados identificados (mediante justificativa e aprovação do PR).
- ✅ Autorização para orientar equipe direta (pós-docs, estudantes).
- ✅ Requerem termo de concordância/confidencialidade.

⬇️

**3. Médicos**

- ✅ Acesso apenas a dados clínicos anonimizados (quando atuam somente como pesquisadores).
- ✅ Acesso a dados clínicos com identificação (quando atuam como clínicos e somente para participantes de pesquisa sob sua responsabilidade de atendimento).
- ✅ Requerem termo de concordância/confidencialidade.

⬇️

**4. Bolsista de treinamento técnico/técnico(as)**

- ✅ Acesso a dados com identificação (quando atuam na gestão do recrutamento e nos agendamentos).
- ✅ Requerem termo de concordância/confidencialidade.

⬇️

**5. Pós-Doutorandos(as)**

- ✅ Acesso a dados anonimizados restritos ao escopo do projeto sob sua responsabilidade.
- ❌ Sem acesso direto a dados identificados (**exceto quando participam do recrutamento**).
- ✅ Necessitam de supervisão do IP para modificações na base.
- ✅ Requerem termo de concordância/confidencialidade.

⬇️

**6. Estudantes de Pós-Graduação (Mestrado/Doutorado)**

- ✅ Acesso a extratos específicos de dados anonimizados definidos pelo IP.
- ❌ Sem acesso a dados identificados (**exceto quando participam do recrutamento***).
- ✅ Requerem termo de concordância/confidencialidade.

⬇️

**7. Iniciação Científica**

- ✅ Acesso apenas a subconjuntos de dados simulados ou anonimizados previamente validados
- ❌ Não têm acesso a dados sensíveis (**exceto quando participam do recrutamento***).
- ✅ Trabalho supervisionado por investigadores principais e/ou pós-docs.
- ✅ Requerem termo de concordância/confidencialidade.

*Nesse caso, há a necessidade de acesso a nomes, telefones e informações necessárias relacionadas a logística de coletas. Fica estabelecido que estas atividades serão sempre supervisionadas por um membro sênior (ex.: pós-doc.).

## 6. Google Planilhas e Dados Fora da Plataforma

- Usar contas institucionais **SEMPRE** (exceções deverão ser autorizadas pelo PR).
- As planilhas devem[8]:
    - Ter controle de acesso restrito (planilhas direcionadas com abas direcionadas).
    - Estar nomeadas de forma padronizada.
    - Ter a edição desativada para quem não precisa alterá-las.
    - Ser auditadas periodicamente.
    - **É expressamente proibido o compartilhamento de planilhas via *link* público**.
- Comunicações via *WhatsApp*:
    - Somente nos canais oficiais listados no item "3.3.". Caso algum participante de pesquisa faça contato a partir de número pessoal, o membro da equipe deverá direcionar para as contas oficiais.

## 7. Segurança Física e de Dispositivos

- Proteger dispositivos com senha (computadores, *tablets* e celular da pesquisa).
- Usar autenticação em duas etapas (2FA) sempre que possível.
- Manter *softwares* atualizados e antivírus.
- **NUNCA** fazer *login* na plataforma Otus ou abrir planilhas online da Rede de Pesquisa TDAH Brasil em computadores públicos. Evitar Wi-Fi abertos (exceto os institucionais, quando necessário).

[8] **Nota do PR:** O uso de planilhas online será eliminado no curto/médio prazo. À medida que recursos financeiros adicionais forem captados, será possível customizar ainda mais a plataforma Otus, de modo que todas as planilhas necessárias à logística de recrutamento, coletas e marcação de avaliações clínicas fiquem integradas à plataforma Otus. Atualmente, o modelo disponibilizado pela Otus não atende completamente às necessidades logísticas do estudo.

## 8. Comunicação Segura

- Não compartilhar dados sensíveis por *WhatsApp* ou e-mail comum[9].
- Sempre que possível, usar termos codificados ou pseudônimos para dados operacionais.

## 9. Treinamento e Responsabilidades

- Todos devem assinar um Termo de Concordância/Confidencialidade (submetido na Plataforma Brasil, como documento obrigatório para a inclusão de membros na equipe de pesquisa).
- Realizar reunião de treinamento periódica (documentar e se possível gravar).
- Manter registro de quem recebeu o treinamento.

## 10. Armazenamento e Distribuição de Dados

### 10.1. Processo de Download e Acesso aos Dados

Os dados coletados serão armazenados em servidores seguros mantidos pela empresa Otus, contratada para prover a infraestrutura computacional do projeto. O acesso ao banco de dados será realizado exclusivamente por usuários previamente autorizados, mediante autenticação individual com credenciais pessoais. O *download* dos arquivos brutos, no formato .csv, ocorre por meio de conexão criptografada, dentro do ambiente restrito da Otus, sendo vedado o armazenamento local em equipamentos pessoais. Todas as ações realizadas sobre os dados são registradas automaticamente para fins de auditoria e rastreabilidade, conforme previsto pela Lei Geral de Proteção de Dados (LGPD).

### 10.2. Manipulação, Integração e Anonimização dos Dados

A manipulação inicial dos dados, incluindo a leitura dos arquivos, integração entre diferentes versões de instrumentos e cruzamento entre questionários, é realizada diretamente nos servidores da Otus por meio de *scripts* desenvolvidos em linguagem R. Antes de qualquer análise estatística ou

[9] **Nota do Coordenador Clínico:** Alguns participantes de pesquisa solicitam o envio do relatório clínico utilizado pelos médicos da equipe (que é gerado a partir da avaliação de autorrelato). Nesses casos, deverá haver uma solicitação formal do participante, enviada por meio dos e-mails oficiais listados no item "3.3". Essa solicitação deve incluir o nome, contato e registro profissional do médico ou psicólogo responsável pelo acompanhamento do participante. O relatório clínico será enviado por e-mail diretamente ao profissional de saúde da rede pública ou privada que estiver acompanhando o voluntário. O participante será incluído em cópia nesse e-mail, que seguirá com orientações sobre como interpretar os dados autorrelatados obtidos a partir do Protocolo da Rede de Pesquisa TDAH Brasil.

geração de relatórios, os dados passam por um processo de pseudonimização de segundo nível[10], também conduzido em R, com a remoção ou substituição de identificadores diretos (ex.: nomes) e indiretos (ex.: ID Otus, garantindo a descaracterização dos titulares. Todo o processamento ocorre em ambiente controlado, protegido por *firewalls*, sem possibilidade de exportação externa de dados sensíveis ou dados ultrassensíveis atrelados a dados sensíveis de identificação individual.

O versionamento dos *scripts* e controles de acesso ao código seguem boas práticas de segurança da informação, em conformidade com os princípios da minimização, necessidade e finalidade estabelecidos pela LGPD. Em resumo, o analista sênior[11] realiza a gestão inicial dos dados e disponibiliza à equipe apenas bancos de dados de trabalho pseudonimizados em segundo nível.

Em um contexto específico, relacionado à preparação de material para o recrutamento e coleta de material biológico, é criado um banco de trabalho ultrarreduzido e pseudoanonimizado, contendo informações sobre *red flags* para comportamentos suicidas. Os gerentes de recrutamento no Rio Grande do Sul[12] e em São Paulo[13] são os responsáveis pelo manejo do *script* e pela preparação desse banco.

### 10.3. Pseudonimização de amostras biológicas.

Os tubos com amostras primárias (ex.: sangue, fezes, saliva) são identificados por códigos de barras gerados na plataforma Otus. As etiquetas primárias contêm o nome do voluntário, pois é solicitado que cada participante confira sua identificação antes de a etiqueta ser colada nos tubos, sempre na presença do voluntário. Já as etiquetas dos tubos secundários (ex.: soro, plasma, sangue total, camada de leucócitos) e terciários (DNA isolado) são pseudonimizadas, pois além de conter um código de barras para rastreamento na plataforma Otus, também contém o ID Otus do participante de pesquisa.

## 11. Atualizações do Protocolo

Revisar anualmente ou quando houver mudanças significativas no protocolo de pesquisa.

[10] A anonimização completa é realizada quando os dados são compartilhados em consórcios de pesquisa.
[11] Eduardo Schneider Vitola.
[12] Maria Eduarda de Araújo Tavares.
[13] Yago Carvalho Lima.

## 12. Avaliação de Riscos e Conformidade com a LGPD

Antes do início de qualquer novo projeto ou subprojeto vinculado à Rede de Pesquisa TDAH Brasil, deve ser realizada uma avaliação formal de riscos relacionados à privacidade e à segurança da informação, com base nos princípios da LGPD (Lei nº 13.709/2018). Essa avaliação deve identificar:

- As categorias de dados pessoais e sensíveis que serão coletados.
- As finalidades específicas de uso dos dados.
- Os riscos potenciais associados à manipulação e ao armazenamento dessas informações.
- As medidas técnicas e administrativas adotadas para mitigar esses riscos.

A documentação dessa avaliação deverá ser armazenada e disponibilizada mediante solicitação dos comitês de ética ou de auditoria. O PR é responsável por garantir que cada novo projeto ou modificação substancial em projetos existentes passe por essa análise antes da coleta de dados.

## 13. Plano de Continuidade e Recuperação de Dados

Em caso de falha sistêmica grave, perda de acesso à plataforma Otus ou outro evento que comprometa a continuidade da coleta e gestão de dados, deverá ser ativado um Plano de Continuidade previamente estabelecido. Este plano contempla o redirecionamento provisório da coleta para planilhas locais protegidas, acessadas exclusivamente por dispositivos autorizados com autenticação em duas etapas. Deve haver comunicação imediata à equipe técnica da Otus Solutions® e ao PR para recuperação dos serviços primários. Finalmente, após a resolução do incidente, a integridade dos dados deverá ser verificada, e (se necessário) um relatório de recuperação deve ser emitido e arquivado.

## 14. Incidentes de Segurança

O Quadro 2 detalha os procedimentos em caso de incidente de segurança de dados. Violações ao protocolo de segurança de dados podem resultar em advertência ou afastamento do projeto.

## QUADRO 2 – REPORTE DE INCIDENTES

### Fluxograma para Reporte de Incidentes de Segurança de Dados

1. **Identificação do Incidente**
   Qualquer membro da equipe (pesquisador, técnico, bolsista etc.) identifica um possível incidente de segurança de dados (vazamento, perda, acesso indevido etc.).
2. **Comunicação Imediata ao Pesquisador Responsável (PR)**
   O incidente deve ser comunicado **imediatamente** ao **PR** do projeto.
3. **Avaliação Inicial pelo PR**
   O PR realiza uma **avaliação preliminar** do incidente, considerando:
   - Tipo de dado afetado
   - Escopo do acesso ou vazamento
   - Possível impacto aos participantes da pesquisa
   - Possível violação de termos éticos ou legais
4. **Notificação aos demais PRs e Investigadores Principais (IPs)**
   O PR informa os demais PRs e IPs do estudo sobre o incidente e os resultados da avaliação preliminar.

### Classificação da Gravidade do Incidente

#### *Caminho 1: Incidente de Baixa Gravidade / Manejável pela Equipe*

- Exemplo: erro de acesso restrito, sem vazamento externo nem danos aos participantes.
- Ações:
  - Documentação interna do incidente e da resposta adotada
  - Adoção de medidas corretivas (ex.: revogação de acessos, mudança de senhas, treinamento adicional)
  - Reforço de boas práticas com a equipe

#### *Caminho 2: Incidente Grave*

- Exemplo: vazamento de dados sensíveis, perda de dados sem backup, acesso externo indevido, risco à integridade dos participantes.
- Ações obrigatórias:
  - **Registro de Boletim de Ocorrência (BO)**
  - **Comunicação formal ao Comitê de Ética em Pesquisa (CEP)**
  - **Comunicação ao Comitê de Boas Práticas em Pesquisa da Instituição**
  - Documentação completa do incidente, das medidas emergenciais e plano de mitigação
  - Comunicação aos participantes da pesquisa (se houver risco direto a eles), conforme orientação do CEP

5. **Monitoramento e Prevenção**

- Após o tratamento do incidente, implementar medidas preventivas e revisar políticas de segurança de dados.
- Caso necessário, revisar o plano de gerenciamento de dados do projeto e as autorizações junto ao CEP.

## 13. Incidentes nas Versões Anteriores

| Incidente 1 | |
|---|---|
| **Descrição** | Incidente de violação de anonimato: Um(a) bolsista de Iniciação Científica convidou para a coleta de material biológico um conhecido que participava do estudo. A conversa configurou uma violação do anonimato. |
| **Classificação** | Incidente de Baixa Gravidade / Manejável pela Equipe. |
| **Medidas corretivas** | O PR conversou com o participante envolvido e esclareceu que o bolsista não tinha acesso a dados ultrassensíveis. Ainda assim, o participante optou por interromper sua participação no estudo. |
| **Desfecho** | Problema manejado pelo PR. |
| **Lições e implementações** | Foi dada orientação expressa à equipe para que, em situações em que conhecidos sejam identificados e não tenham sido convidados diretamente, o membro da equipe em questão se abstenha de participar do processo de recrutamento. |
| **Incidente 2** | |
| **Descrição** | Participante de pesquisa questionou se a equipe divulgou dados sigilosos em plataforma pública de inteligência artificial. |
| **Classificação** | Incidente Grave. |
| **Medidas corretivas** | Revisão interna dos processos; comunicação ao CEPSH do ICB-USP, registro de boletim de ocorrência online (conforme orientação do CEPSH), solicitação formal para que a plataforma de inteligência artificial removesse o conteúdo. |
| **Desfecho** | Após revisão dos processos e interação com (o)a participante e o(a) médico(a) responsável, concluiu-se que (o)a próprio(a) participante de pesquisa compartilhou o atestado médico — enviado diretamente para seu e-mail por meio da plataforma do Conselho Federal de Medicina — com um familiar. Esse familiar realizou o *upload* do documento em uma plataforma de inteligência artificial. |
| **Lições e implementações** | Todos os documentos que configuram devolutiva ao participante (como atestados médicos e relatórios de respostas de autorrelato) passaram a incluir um aviso com o seguinte conteúdo: *'Nossa equipe não fornecerá informações a terceiros sem sua autorização por escrito, conforme especificado no Termo de Consentimento Livre e Esclarecido (TCLE) que você assinou. Portanto, é importante garantir que as plataformas digitais, empresas de armazenamento em nuvem, redes sociais, chats de inteligência artificial e outros sistemas eletrônicos que você utilizar sejam seguros e adequados para armazenar suas informações médicas.'* |

## Anexo 1 - Checklist para Implementação

| Checklist para Implementação | ✅ |
|---|---|
| Acesso e Contas | |
| • PR designado e ciente de suas responsabilidades | |
| • Todos os acessos concedidos com base no menor privilégio | |
| • Contas Google e Otus protegidas por autenticação 2FA | |
| Coleta e Armazenamento | |
| • Dados clínicos apenas na Otus | |
| • Dados operacionais pseudonimizados fora da Otus | |
| • Amostras biológicas etiquetadas com ID Otus + códigos de barras | |
| Planilhas e Comunicação | |
| • Planilhas nomeadas e com abas restritas | |
| • Compartilhamento NUNCA via link público | |
| • Comunicação com participantes somente pelos canais oficiais | |
| Dispositivos e Ambiente | |
| • Dispositivos com senha e antivírus atualizados | |
| • Nunca acessar Otus ou planilhas em computadores públicos | |
| • Evitar Wi-Fi público sempre que possível | |
| Equipe | |
| • Todos assinaram o Termo de Confidencialidade | |
| • Participaram de reunião de treinamento documentada | |
| • Estão cientes das condutas em caso de incidentes | |
| Revisão e Continuidade | |
| • Protocolo revisado anualmente | |
| • Plano de continuidade definido em caso de falhas | |

*Encaminha-se à equipe da Rede de Pesquisa TDAH Brasil para ciência e cumprimento integral.*

*São Paulo, 5 de junho de 2025.*

gov.br Documento assinado digitalmente
DIEGO LUIZ ROVARIS
Data: 05/06/2025 10:35:16-0300
Verifique em https://validar.iti.gov.br

gov.br Documento assinado digitalmente
EUGENIO HORACIO GREVET
Data: 05/06/2025 10:29:53-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Diego Luiz Rovaris
Coordenador Científico da Rede TDAH Brasil
Instituto de Ciências Biomédicas
Universidade de São Paulo

Prof. Dr. Eugenio Horácio Grevet
Coordenador Clínico da Rede TDAH Brasil
Faculdade de Medicina
Universidade Federal do Rio Grande do Sul