Doctor System

E-BOOK GRATUITO · SEGURANÇA DE DADOS NA SAÚDE

# Antes do Resgate

## 12 defesas para proteger os dados da sua clínica contra hackers

Casos reais de ataques à saúde no Brasil e no mundo, os riscos de não se prevenir e o passo a passo para proteger o consultório, mesmo sem equipe de TI.

- 13 casos reais com fonte
- 12 defesas práticas
- Plano da primeira hora
- Checklist de 1 página



doctoriasystem.com.br

EDIÇÃO NOVEMBRO DE 2026

SUMÁRIO

# O que você vai encontrar


00 Por que este guia existe

01 O que está acontecendo no mundo: casos reais

02 Os números que todo dono de clínica precisa conhecer

03 Por onde os ataques entram

04 As 12 defesas do consultório

05 O preço de não se prevenir

06 Se o pior acontecer: a primeira hora

07 Como o Doctor System protege os dados da sua clínica

08 Checklist de 1 página

09 Fontes


**Como ler este guia.** Cada caso e cada número traz a fonte logo abaixo dele, com o link completo no capítulo 09. As 12 defesas trazem duas colunas: **o que fazer** e **o risco de não fazer**. Se você tiver só 15 minutos, vá direto ao checklist do capítulo 08.

00 · INTRODUÇÃO

# Ninguém invade um consultório por acaso. Invadem porque dá certo.

Durante anos, ataque hacker parecia problema de banco, governo e multinacional. Os casos dos últimos anos mostram outra coisa: a saúde virou um dos alvos preferidos, e não só os grandes hospitais.

O motivo é simples. Um prontuário reúne, em um só lugar, nome, documento, endereço, telefone, diagnóstico, exames, receitas e, muitas vezes, dados de pagamento. Para um criminoso, isso serve para três coisas: **sequestrar** (travar os arquivos e cobrar resgate), **chantagear** (ameaçar publicar o que o paciente contou ao médico) e **aplicar golpes** (falar com o paciente como se fosse a clínica e pedir um PIX).

E o consultório pequeno costuma ser a porta mais fácil: senha repetida, computador da recepção sem atualização, prontuário em planilha, o mesmo login usado por três pessoas, Wi-Fi do paciente na mesma rede do computador da secretária. Nada disso exige um hacker genial. Exige só alguém tentando.

Este guia foi escrito para médicos, dentistas e donos de clínica que não são de tecnologia e não querem virar. Você vai ver o que aconteceu com quem não se preparou, entender por onde os ataques entram e sair com **12 defesas práticas**, a maioria gratuita e feita em uma tarde.

**Uma verdade que nenhum fornecedor deveria esconder:** não existe sistema 100% invulnerável. Segurança é a soma do que o sistema faz com o que a clínica faz. Por isso, no capítulo 07, mostramos com clareza o que o Doctor System faz por você e o que continua sendo responsabilidade da clínica.

CAPÍTULO 01

# O que está acontecendo no mundo

Casos reais, com data e fonte. Leia pensando em uma pergunta: o que impediria isso de acontecer na minha clínica amanhã?

## Os três casos que todo consultório precisa conhecer

### ⚠ Change Healthcare (UnitedHealth)

EUA · fev/2024

Criminosos entraram com credenciais de um funcionário de suporte e ficaram dias dentro antes de travar os sistemas. Repasses de convênios e farmácias pararam no país inteiro.

**Consequência:** 192,7 milhões de pessoas afetadas e US$ 22 milhões pagos de resgate. Os dados não foram apagados como o grupo prometeu.

**Lição:** Porta de entrada: acesso remoto sem verificação em duas etapas, confirmado pelo próprio CEO ao Congresso americano.

Fonte: AP, 01/05/2024; PYMNTS, 14/08/2025; HIPAA Journal [1] [2] [3]

### ⚠ Vastaamo, clínica de psicoterapia

Finlândia · 2018–2020

Um invasor copiou os registros de cerca de 33 mil pacientes. Sem receber da clínica, passou a cobrar dos próprios pacientes para não publicar o que eles contaram na terapia.

**Consequência:** Pacientes chantageados um a um, cerca de 24 mil queixas à polícia e a clínica faliu em 2021. O invasor foi condenado em 2024.

**Lição:** Não é só hospital grande: uma clínica de porte pequeno foi destruída por um único incidente.

Fonte: SecurityWeek/AP, 30/04/2024 [4]

### ⚠ MedicSolution, software de gestão para clínicas

Brasil · set/2025

O grupo KillSec reivindicou o roubo de mais de 34 GB, quase 95 mil arquivos, com exames, avaliações médicas, radiografias e imagens de pacientes, inclusive de menores, segundo a empresa de segurança Resecurity. A fornecedora não se pronunciou oficialmente.

**Consequência:** Segundo a Resecurity, apareceram arquivos de clínicas e laboratórios clientes. O caso foi comunicado ao CERT.br e à ANPD.

**Lição:** Segundo a Resecurity, não foi uma invasão sofisticada: o armazenamento em nuvem estava aberto. A escolha do fornecedor é decisão de segurança.

Fonte: Convergência Digital, 12/09/2025 [5]

## No Brasil

### Ministério da Saúde / ConecteSUS

Brasil · dez/2021

Um grupo criminoso derrubou o site do ministério e o ConecteSUS e apagou dados de vacinação, depois recuperados por cópias de segurança.

**Consequência:** ConecteSUS ficou 14 dias fora do ar.

**Lição:** O próprio ministério confirmou: a entrada foi uma senha vazada. Não foi preciso nenhuma falha técnica.

Fonte: Canaltech, 13/01/2022 [6]

### ISAC: processo da ANPD

Brasil · 2025 · processo em jul/2026

Organização que administra unidades públicas de saúde em seis estados sofreu ataque de sequestro de dados. Segundo a ANPD e a imprensa, cerca de 500 mil registros ficaram expostos, entre eles de mais de 78 mil crianças e adolescentes.

**Consequência:** A ANPD abriu processo sancionador por segurança inadequada e falha na comunicação aos titulares. O instituto nega vazamento e diz ter restaurado os sistemas afetados pelo backup.

**Lição:** A ANPD já está cobrando, na saúde, a segurança e a comunicação aos pacientes.

Fonte: Canaltech, 08/07/2026; Agência Brasil, jul/2026 [7] [8]

### Hospital Israelita Albert Einstein

Brasil · ago-out/2026

Ataque acessou parte da base de pacientes: nome, CPF, data de nascimento e, possivelmente, receitas e resultados de exames. Sinais detectados em agosto, comunicado em outubro.

**Consequência:** Caso comunicado à ANPD e à Polícia Federal; pacientes avisados por e-mail. O hospital diz não haver evidência de divulgação dos dados.

**Lição:** Nem as instituições com mais estrutura do país estão fora do alvo.

Fonte: DGABC, 08/10/2026 [9]

### Hospital Sírio-Libanês

Brasil · set-out/2026

Ataque a um sistema interno de relatórios ligado a projetos sociais. Segundo o hospital, a base geral de pacientes não foi afetada.

**Consequência:** Possível acesso a nome, documentos, endereço, contatos e dados de saúde. Comunicado à ANPD e à PF; sem evidência de vazamento até a publicação.

**Lição:** Basta um sistema secundário com dados de pacientes para virar incidente.

Fonte: SBT News, 16/10/2026 [10]

### Grupo Fleury

Brasil · jun/2021 e mai/2023

Em 2021, os sistemas do laboratório caíram e as unidades passaram a operar em contingência. Em 2023, um novo ataque cibernético dificultou agendamentos e a consulta a resultados.

**Consequência:** Em 2023, pacientes e hospitais parceiros tiveram dificuldade para marcar exames e ver resultados.

**Lição:** Quem é atacado uma vez pode ser atacado de novo.

Fonte: Baguete, 23/06/2021; ISTOÉ Dinheiro/Estadão, 08/05/2023 [11] [12]

### Golpe do falso funcionário em Santos (SP)

Brasil · jun/2025

Criminosos ligavam para pacientes oncológicos dizendo ser da Santa Casa: "seus exames estão prontos, houve alteração". Ofereciam entrega por motoboy a R$ 9,90 na maquininha.

**Consequência:** Segundo a polícia, o cartão das vítimas teria sido usado depois para saques. Um suspeito foi preso.

**Lição:** Os golpistas sabiam quem era paciente e quando fez exame; a origem dos dados não foi divulgada. Dado de paciente vira arma contra o próprio paciente.

Fonte: VTV News, 11/06/2025 [13]

## No mundo

### Synnovis / NHS (Londres)

Reino Unido · jun/2024

Sequestro de dados atingiu o laboratório que faz exames para hospitais de Londres.

**Consequência:** O King's College Hospital reconheceu que a longa espera por um exame de sangue, causada pelo ataque, foi um dos fatores na morte de um paciente.

**Lição:** Ataque a dado de saúde não é só problema de TI: atrasa atendimento.

Fonte: The Record, 25/06/2025 [14]

### HSE, serviço de saúde da Irlanda

Irlanda · mai/2021

Ataque derrubou todos os sistemas do serviço nacional de saúde. Hospitais voltaram ao papel e consultas e exames foram cancelados em massa.

**Consequência:** Recuperação levou meses; o governo disse que não pagaria o resgate.

**Lição:** A porta de entrada foi um e-mail com planilha infectada, aberto cerca de 8 semanas antes do ataque.

Fonte: Wikipedia (cita RTÉ e TheJournal.ie) [15]

### Ascension

EUA · mai/2024

Sequestro de dados paralisou uma das maiores redes hospitalares dos EUA.

**Consequência:** 5,6 milhões de pessoas afetadas; funcionários relataram atraso em resultados de exames e erros de medicação.

**Lição:** Quando o sistema para, o atendimento inteiro sente.

Fonte: TechCrunch, 20/12/2024 [16]

### Kettering Health

EUA · mai–jun/2025

Queda geral de sistemas em 14 centros médicos e mais de 120 unidades ambulatoriais.

**Consequência:** Cirurgias eletivas canceladas; serviços principais voltaram só 3 semanas depois. Golpistas ligaram para pacientes fingindo ser do hospital e cobrando "despesas médicas".

**Lição:** Depois do ataque vem o golpe em nome da instituição.

Fonte: TechTarget, 12/06/2025 [17]

**O que os casos têm em comum.** Onde a porta de entrada foi divulgada, ela foi simples: senha sem segunda etapa (Change Healthcare), senha vazada (ConecteSUS), e-mail com anexo infectado (HSE) e armazenamento em nuvem aberto (MedicSolution). E, depois do ataque, pode vir o golpe em nome da instituição (Kettering). Em Santos, os golpistas sabiam quem era paciente, e a origem dos dados não foi divulgada. Nos demais casos, a porta de entrada não foi divulgada.

CAPÍTULO 02

# Os números que todo dono de clínica precisa conhecer

Não é para assustar. É para dimensionar o risco com dados de quem mede isso todo ano.

## US$ 6,64 mi

é o custo médio de uma violação de dados na saúde, o setor mais caro pelo 13º ano seguido.

IBM Cost of a Data Breach 2026, via HIPAA Journal (29/07/2026) [18]

## 54%

dos incidentes na saúde tiveram um fator humano envolvido, como clique, erro ou credencial.

Verizon DBIR 2026, via HIPAA Journal (20/05/2026) [19]

## 3.348

tentativas de ataque por semana, por organização, no Brasil. Saúde foi o setor mais atacado.

Check Point Research, nov/2025, via Hardware.com.br (13/12/2025) [20]

## +289 mi

de pessoas tiveram dados de saúde expostos em grandes violações nos EUA só em 2024.

HHS/OCR, via HIPAA Journal (atualizado em 13/11/2026) [21]

## US$ 1,02 mi

é o custo médio de recuperação de um ataque de sequestro de dados na saúde. 36% das vítimas pagaram resgate.

Sophos, State of Ransomware in Healthcare 2025 [22]

## US$ 1,36 mi

é o custo médio de uma violação de dados no Brasil (2024, todos os setores).

Brasscom, Relatório de Cibersegurança 2025, via Movimento Econômico (21/07/2026) [23]

Os números de IBM, Verizon, Check Point e Brasscom foram conferidos em veículos que citam os relatórios originais. Valores em dólar não foram convertidos.

**Traduzindo para o consultório:** em mais da metade dos incidentes há um fator humano envolvido, como um clique, uma senha ou um erro. E, como porta de entrada, lideram a falha não corrigida (20%) e o e-mail falso (14%). As duas coisas estão ao alcance da clínica, e é delas que tratam as 12 defesas do capítulo 04.

CAPÍTULO 03

# Por onde os ataques entram

Quando a porta de entrada é divulgada, ela costuma ser uma destas cinco. Fechá-las reduz muito o risco.

| Porta | Como acontece no consultório | Defesas que fecham |
|---|---|---|
| **1. Senha fraca ou vazada** | A mesma senha do e-mail pessoal é usada no sistema da clínica. Ela vaza em outro site e o criminoso testa em todos os lugares. | 01, 02, 05 |
| **2. E-mail e mensagem falsos (phishing)** | "Boleto em atraso", "resultado de exame", "atualize seu cadastro": um clique instala o programa ou entrega a senha. | 03, 04 |
| **3. Acesso sem segunda etapa** | Login que só pede senha. Quem tem a senha, entra, de qualquer lugar do mundo. | 02, 11 |
| **4. Aparelho desatualizado ou desprotegido** | Computador da recepção sem atualização, celular sem bloqueio, Wi-Fi do paciente na mesma rede. | 06, 08, 09 |
| **5. Dado no lugar errado** | Prontuário em planilha, exames no pendrive, fotos de pacientes na galeria do celular, arquivos no Drive pessoal. | 07, 10, 11 |

**O ponto em comum:** nos casos do capítulo 01 em que a porta de entrada foi divulgada, ela não foi uma falha sofisticada, e sim algo do dia a dia: uma senha, um clique, um acesso remoto sem segunda etapa. É exatamente aí que a clínica pequena tem mais poder de agir.

CAPÍTULO 04

# As 12 defesas do consultório

Em ordem de impacto. As seis primeiras resolvem a maior parte do risco e custam quase nada.

## 01 Uma senha forte e única para cada sistema

Senha forte não é "Clinica@2025". É uma frase longa que só você conhece e, principalmente, uma senha **diferente** em cada lugar. Um gerenciador de senhas (há opções gratuitas e pagas; o próprio navegador também guarda com proteção da conta) cria e lembra por você.

FAÇA HOJE

- [ ] Troque a senha do sistema da clínica e do e-mail principal.
- [ ] Consulte seu e-mail em haveibeenpwned.com para saber se já apareceu em vazamentos.
- [ ] Proíba senha anotada em post-it no monitor.

RISCO DE NÃO FAZER

Uma senha vazada em qualquer site (loja, rede social, curso) vira a chave do prontuário de todos os seus pacientes.

## 02 Verificação em duas etapas em tudo que importa

Além da senha, um código no celular. É uma das defesas de melhor custo-benefício: mesmo que a senha vaze, o invasor para na segunda porta. Ative no sistema da clínica, no e-mail, no WhatsApp (confirmação em duas etapas), no banco e nas redes sociais.

FAÇA HOJE

- [ ] Ative no e-mail e no sistema da clínica.
- [ ] No WhatsApp: Configurações › Conta › Confirmação em duas etapas.
- [ ] Prefira aplicativo autenticador a SMS quando houver opção.

RISCO DE NÃO FAZER

No maior vazamento de dados de saúde da história dos EUA (capítulo 01), a porta de entrada foi justamente um acesso sem segunda etapa.

## 03 Equipe treinada para reconhecer golpes

A recepção é a linha de frente: abre e-mail, baixa anexo, atende telefone. Dez minutos por mês de conversa evitam a maioria dos cliques errados. Regra de ouro: **urgência + pedido de senha, código ou pagamento = parar e confirmar por outro canal**.

FAÇA HOJE

- [ ] Mostre à equipe 3 exemplos de e-mail falso (boleto, exame, banco).
- [ ] Combine: ninguém passa código recebido por SMS para ninguém.
- [ ] Crie um canal para "achei estranho" sem bronca.

RISCO DE NÃO FAZER

Um clique da recepção basta para instalar programa de sequestro de dados no computador conectado a tudo.

## 04 Proteja seus pacientes do golpe em nome da clínica

Com dados vazados (nome, telefone, data da consulta), golpistas mandam mensagem se passando pela clínica ou pelo médico e pedem PIX para "liberar exame", "confirmar cirurgia" ou "pagar taxa". O paciente perde dinheiro e a clínica perde confiança.

FAÇA HOJE

- [ ] Use um único número oficial de WhatsApp e divulgue isso.
- [ ] Avise na recepção e nas redes: "nunca pedimos PIX por mensagem sem confirmação".
- [ ] Defina quem pode cobrar e por qual canal.

RISCO DE NÃO FAZER

Seu paciente é lesado usando o nome da sua clínica, e a primeira reclamação chega a você.

## 05 Cada pessoa com o próprio acesso, e só o necessário

Login compartilhado ("todo mundo usa o do doutor") apaga o rastro de quem fez o quê e dá a todos acesso a tudo. A secretária precisa da agenda, não do prontuário. O financeiro precisa dos valores, não das evoluções clínicas.

FAÇA HOJE

- [ ] Crie um usuário por pessoa, com o perfil certo.
- [ ] Desligue o acesso de quem saiu no mesmo dia da saída.
- [ ] Revise a lista de usuários uma vez por mês.

RISCO DE NÃO FAZER

Ex-funcionário com acesso ativo, vazamento sem culpado identificável e quebra de sigilo dentro da própria equipe.

## 06 Atualização automática em tudo

Atualização de sistema operacional, navegador e aplicativos fecha brechas que já são conhecidas pelos criminosos. Computador "que funciona bem do jeito que está" e não atualiza há meses é convite aberto. Isso vale também para o roteador da clínica.

FAÇA HOJE

- [ ] Ative atualização automática no Windows/macOS e nos celulares.
- [ ] Troque a senha padrão do roteador.
- [ ] Aposente computador sem suporte do fabricante.

RISCO DE NÃO FAZER

Brecha pública vira ataque automático: robôs varrem a internet atrás de quem não atualizou.

## 07 Cópia de segurança que o ataque não alcança

Programas de sequestro de dados procuram e travam também as cópias que estão no mesmo computador ou na mesma rede. A regra prática é **3-2-1**: três cópias, em dois tipos de mídia, uma delas fora do consultório e, de preferência, desconectada. E teste a restauração: cópia que nunca foi testada é esperança, não backup.

FAÇA HOJE

- [ ] Descubra onde estão (e se existem) as cópias dos seus dados.
- [ ] Pergunte ao seu sistema com que frequência copia e por quanto tempo guarda.
- [ ] Faça um teste de restauração por semestre.

RISCO DE NÃO FAZER

Sem cópia íntegra, a clínica fica entre pagar o resgate (sem garantia de receber os dados) e perder anos de prontuário.

## 08 Wi-Fi do paciente separado da rede da clínica

Wi-Fi de cortesia é ótimo para a sala de espera e péssimo quando está na mesma rede do computador da recepção. Peça ao técnico uma rede de convidados isolada, com senha diferente da rede de trabalho.

FAÇA HOJE

- [ ] Ative a "rede de convidados" do roteador.
- [ ] Troque a senha da rede de trabalho e não a divulgue.

RISCO DE NÃO FAZER

Qualquer aparelho na sala de espera, infectado ou mal-intencionado, enxerga os computadores da clínica.

## 09 Aparelhos travados: computador e celular

Notebook roubado e celular perdido são incidentes de dados. Senha ou biometria na tela, bloqueio automático em poucos minutos, criptografia de disco ligada (BitLocker no Windows, FileVault no Mac, padrão nos celulares atuais) e apagamento remoto configurado.

FAÇA HOJE

- [ ] Bloqueio de tela em até 5 minutos em todos os aparelhos.
- [ ] Ative "Encontrar meu dispositivo" (Android e iPhone).
- [ ] Combine com a equipe: saiu da mesa, travou a tela (Windows + L).

RISCO DE NÃO FAZER

Um roubo de celular expõe conversas, fotos clínicas e o WhatsApp com todos os pacientes.

## 10 Prontuário fora de planilha, pendrive e galeria

Dado de saúde é dado pessoal sensível pela LGPD. Ele precisa estar em um lugar com controle de acesso, registro de quem mexeu e cópia de segurança, e não espalhado em planilha, pasta compartilhada, pendrive e galeria do celular.

FAÇA HOJE

- [ ] Liste onde há dado de paciente fora do sistema.
- [ ] Leve tudo para um sistema com acesso por perfil e trilha de auditoria.
- [ ] Tire fotos clínicas da galeria pessoal.

RISCO DE NÃO FAZER

Você não consegue proteger, e nem provar que protegeu, o que nem sabe onde está.

## 11 Escolha fornecedores que respondem perguntas difíceis

Quando o prontuário está em um sistema online, parte da segurança depende do fornecedor. Antes de contratar (ou para avaliar o atual), faça estas perguntas e exija respostas por escrito:

| Pergunta | Resposta que você quer ouvir |
|---|---|
| Onde os dados ficam guardados? | País e região informados, e quais fornecedores tratam dados fora do país. |
| Tem verificação em duas etapas? | Sim, disponível para a equipe toda. |
| Com que frequência faz cópia de segurança? Por quanto tempo guarda? | Frequência e prazo exatos. |
| Uma clínica consegue ver dados de outra? | Não: isolamento por cliente. |
| Fica registrado quem alterou o prontuário? | Sim, e esse registro não pode ser apagado. |
| Consigo exportar todos os meus dados? | Sim, durante o contrato e por um prazo depois dele. |
| Há contrato de tratamento de dados e encarregado (DPO)? | Sim, publicados e com contato. |
| Existe página pública de status? | Sim, aberta a qualquer pessoa. |

FAÇA HOJE

Mande estas 8 perguntas para o seu fornecedor atual.

RISCO DE NÃO FAZER

Você responde perante o paciente e a lei pelo fornecedor que escolheu.

## 12 Tenha um plano para o dia do incidente

No dia do ataque não há tempo para descobrir quem chamar. Um plano de uma página, impresso e guardado fora do computador, faz a diferença entre horas e semanas de clínica parada. O capítulo 06 traz o roteiro da primeira hora.

FAÇA HOJE

- [ ] Anote: técnico de confiança, fornecedor do sistema, advogado, contador.
- [ ] Defina quem fala com pacientes e com a imprensa.
- [ ] Saiba onde está a agenda da próxima semana em papel.

RISCO DE NÃO FAZER

Decisões erradas sob pressão: apagar provas, pagar resgate sem orientação, perder o prazo de comunicação à ANPD.

CAPÍTULO 05

# O preço de não se prevenir

O prejuízo de um incidente vai muito além do computador travado.

| Tipo de risco | O que pode acontecer | Base |
|---|---|---|
| **Legal (LGPD)** | Dado de saúde é **dado pessoal sensível**. A ANPD pode aplicar advertência, multa simples de até 2% do faturamento no Brasil, limitada a R$ 50 milhões por infração, publicização da infração e bloqueio ou eliminação dos dados. | Lei 13.709/2018, art. 5º, II e art. 52 [L1] |
| **Dever de comunicar** | Incidente que possa causar risco ou dano relevante precisa ser comunicado à ANPD e aos pacientes. O regulamento da ANPD fixa o prazo de 3 dias úteis a partir do conhecimento do incidente (em dobro para agentes de pequeno porte que se enquadrem na Res. CD/ANPD nº 2/2022). | LGPD art. 48 [L1]; Res. CD/ANPD nº 15/2024 [L2] |
| **Guarda do prontuário** | O prontuário precisa ser guardado por no mínimo 20 anos a partir do último registro. Perder o prontuário é perder um documento que a lei manda preservar. | Lei 13.787/2018, art. 6º [L3] |
| **Ético-profissional** | O sigilo profissional é dever previsto nos códigos de ética dos conselhos de saúde. Vazamento pode virar processo ético, além do cível. | Códigos de ética profissionais (CFM, CFO e demais conselhos) |
| **Operacional** | Agenda parada, consultas canceladas, receita do mês travada, equipe ociosa, horas de técnico. | Casos do capítulo 01 |
| **Reputação** | Pacientes chantageados ou lesados em golpes em nome da clínica. Confiança perdida não volta com um comunicado. | Casos do capítulo 01 |

Este capítulo é informativo e não substitui orientação jurídica. Em caso de incidente real, procure um advogado especializado em proteção de dados.

CAPÍTULO 06

# Se o pior acontecer: a primeira hora

Imprima esta página e guarde longe do computador.

| # | O que fazer | Por quê |
|---|---|---|
| 1 | **Desconecte, não desligue.** Tire o cabo de rede e desligue o Wi-Fi dos aparelhos afetados. | Impede que o ataque se espalhe e preserva provas que somem ao desligar. |
| 2 | **Não apague nada** e não tente "limpar" por conta própria. | Os registros mostram o que foi acessado, e isso define o que comunicar. |
| 3 | **Ligue para o técnico e para o fornecedor do sistema.** | Eles conseguem revogar acessos e verificar a cópia de segurança. |
| 4 | **Troque senhas de um aparelho limpo**, começando pelo e-mail e pelo sistema da clínica, e encerre as sessões abertas. | Corta o acesso do invasor. |
| 5 | **Anote tudo:** horário, o que apareceu na tela, mensagens de resgate (foto). | Base para o boletim de ocorrência e para a comunicação à ANPD. |
| 6 | **Não pague resgate sem orientação.** | Pagar não garante a devolução nem impede a publicação dos dados. |
| 7 | **Fale com o advogado e o encarregado de dados** sobre a comunicação à ANPD e aos pacientes. | O prazo é curto: 3 dias úteis pelo regulamento da ANPD. |
| 8 | **Avise os pacientes pelo canal oficial** para não caírem em golpes usando os dados vazados. | Reduz o dano e preserva a confiança. |
| 9 | **Registre boletim de ocorrência** (há delegacias especializadas em crimes cibernéticos em vários estados). | Documento oficial do crime. |

CAPÍTULO 07

# Como o Doctor System protege os dados da sua clínica

O Doctor System é o sistema de gestão para consultórios e clínicas da área da saúde, com agenda, prontuário, WhatsApp e financeiro no mesmo lugar. Abaixo, só o que é verdade hoje.

**Prontuários e fichas guardados no Brasil**
Ficam em São Paulo. Alguns fornecedores, inclusive os de recursos opcionais que o consultório ativa, podem tratar dados fora do país, como descreve a Política de Privacidade.

**Comunicação criptografada (HTTPS)**
Tudo o que trafega entre o navegador e o sistema vai criptografado.

**Verificação em duas etapas no login**
Além da senha, o consultório pode ativar um código de verificação no celular. É a defesa 02 deste guia, pronta no sistema.

**Cada consultório vê só os próprios dados**
Isolamento por consultório: as informações de um consultório não aparecem para nenhum outro.

**Acesso por perfil**
Cada pessoa entra com o próprio acesso. A secretária usa agenda, cadastro e atendimento, mas não lê o prontuário e não abre o Financeiro nem os totais do Dashboard. É a defesa 05 deste guia.

**Cópia de segurança todo dia, criptografada**
Os dados são copiados diariamente e cada cópia fica guardada por 35 dias.

**Prontuário que nunca é apagado**
A correção é feita por retificação: o registro anterior é arquivado com o motivo informado, e o histórico continua lá.

**Auditoria travada**
O histórico da ficha e a auditoria da clínica ficam travados no banco de dados: não podem ser alterados nem apagados. O titular vê em Auditoria quem fez o quê e quando.

### Trust Center: recursos ligados com cuidado

Cada recurso novo é ligado aos poucos por uma central de governança, que também pode desligá-lo na hora.

### Seus dados são seus

O titular exporta todos os dados durante o contrato e por 90 dias depois do encerramento.

### Status aberto a todos

Uma página pública mostra, a qualquer hora, se o sistema está funcionando: status.doctoriasystem.com.br.

### LGPD na prática

Política de privacidade, termos de uso, contrato de tratamento de dados e lista de subprocessadores publicados. Encarregado de dados (DPO): dpo@doctoriasystem.com.br.

## Responsabilidade compartilhada: quem cuida de quê

| O Doctor System cuida | A clínica cuida |
|---|---|
| Guarda de prontuários e fichas em São Paulo, criptografia na comunicação, cópia diária, isolamento entre consultórios, trilha de auditoria travada, prontuário sem exclusão. | Senha única e forte para cada pessoa, duas etapas ativadas, usuário por pessoa, desligar quem saiu. |
| Oferecer acesso por perfil e verificação em duas etapas. | Escolher o perfil certo para cada pessoa e ativar a verificação. |
| Manter a página de status pública. | Manter computadores, celulares, navegador e roteador atualizados e travados. |
| Publicar políticas, contrato de tratamento de dados e contato do encarregado. | Treinar a equipe, proteger o WhatsApp e ter o plano da primeira hora. |

PRÓXIMO PASSO

## Veja de perto como o Doctor System protege o prontuário dos seus pacientes

Agenda, prontuário, WhatsApp e financeiro no mesmo sistema, direto no navegador, com as proteções deste capítulo.

Conhecer o Doctor System →

doctoriasystem.com.br

CAPÍTULO 08 · CHECKLIST

# Checklist de 1 página

| Item | Quando | Feito |
|---|---|---|
| Senha única e forte no sistema da clínica e no e-mail | Hoje | ☐ |
| Duas etapas no sistema, e-mail, WhatsApp e banco | Hoje | ☐ |
| Um usuário por pessoa, com o perfil certo | Esta semana | ☐ |
| Acessos de ex-funcionários desligados | Hoje | ☐ |
| Atualização automática ligada em computadores e celulares | Esta semana | ☐ |
| Senha padrão do roteador trocada e Wi-Fi de convidados separado | Esta semana | ☐ |
| Bloqueio de tela e criptografia de disco em todos os aparelhos | Esta semana | ☐ |
| Saber onde estão as cópias de segurança e testar uma restauração | Este mês | ☐ |
| Dados de pacientes fora de planilha, pendrive e galeria | Este mês | ☐ |
| Aviso aos pacientes: canal oficial e "não pedimos PIX por mensagem" | Este mês | ☐ |
| 8 perguntas enviadas ao fornecedor do sistema | Este mês | ☐ |
| Treino de 10 minutos com a equipe sobre golpes | Todo mês | ☐ |
| Plano da primeira hora impresso e guardado | Este mês | ☐ |

CAPÍTULO 09

# Fontes

Links consultados em novembro de 2026.


[1] Change Healthcare (UnitedHealth) — AP, 01/05/2024 — clickondetroit.com/business/2024/05/01/change-healthcare-cyberattack-was-due-to-a-lack-of-multifactor-authentication-unitedhealth-ceo-says/

[2] Change Healthcare (UnitedHealth) — PYMNTS, 14/08/2025 — pymnts.com/cybersecurity/2025/us-health-dept-says-unitedhealth-hack-impacted-192-7-million-consumers-data/

[3] Change Healthcare (UnitedHealth) — HIPAA Journal — hipaajournal.com/change-healthcare-responding-to-cyberattack/

[4] Vastaamo, clínica de psicoterapia — SecurityWeek/AP, 30/04/2024 — securityweek.com/finnish-hacker-gets-prison-for-accessing-thousands-of-psychotherapy-records-and-demanding-ransoms/

[5] MedicSolution, software de gestão para clínicas — Convergência Digital, 12/09/2025 — convergenciadigital.com.br/seguranca/ransomware-killsec-ataca-saude-no-brasil-e-captura-34-gb-de-exames-prontuarios-e-imagens/

[6] Ministério da Saúde / ConecteSUS — Canaltech, 13/01/2022 — canaltech.com.br/seguranca/ministerio-da-saude-confirma-que-senha-vazada-permitiu-ataques-ciberneticos-206582/

[7] ISAC: processo da ANPD — Canaltech, 08/07/2026 — canaltech.com.br/seguranca/ataque-que-sequestrou-dados-de-500-mil-pacientes-no-brasil-entra-na-mira-da-anpd/

[8] ISAC: processo da ANPD — Agência Brasil, jul/2026 — agenciabrasil.ebc.com.br/radioagencia-nacional/geral/audio/2026-07/organizacao-social-e-investigada-por-vazamento-de-dados-de-pacientes

[9] Hospital Israelita Albert Einstein — DGABC, 08/10/2026 — dgabc.com.br/Noticia/4351704/einstein-e-alvo-de-ataque-hacker-pf-investiga

[10] Hospital Sírio-Libanês — SBT News, 16/10/2026 — sbtnews.sbt.com.br/noticia/brasil/sirio-libanes-sofre-ataque-hacker-e-apura-acesso-a-dados

[11] Grupo Fleury — Baguete, 23/06/2021 — baguete.com.br/noticias/ataque-no-grupo-fleury-foi-de-ransomware

[12] Grupo Fleury — ISTOÉ Dinheiro/Estadão, 08/05/2023 — istoedinheiro.com.br/fleury-diz-que-ataque-hacker-causou-falha-em-sistema-de-exames

[13] Golpe do falso funcionário em Santos (SP) — VTV News, 11/06/2025 — vtvnews.com.br/baixada-santista/suspeito-de-aplicar-golpes-de-exames-em-pacientes-oncologicos-em-santos-e-preso

[14] Synnovis / NHS (Londres) — The Record, 25/06/2025 — therecord.media/ransomware-attack-contributed-patient-death-uk-nhs

[15] HSE, serviço de saúde da Irlanda — Wikipedia (cita RTÉ e TheJournal.ie) — en.wikipedia.org/wiki/Health_Service_Executive_cyberattack

[16] Ascension — TechCrunch, 20/12/2024 — techcrunch.com/2024/12/20/ransomware-attack-on-health-giant-ascension-hits-5-6-million-patients

[17] Kettering Health — TechTarget, 12/06/2025 — techtarget.com/healthtechsecurity/news/366624205/Cyberattack-causes-system-wide-outage-at-Kettering-Health

[18] IBM Cost of a Data Breach 2026, via HIPAA Journal (29/07/2026) — hipaajournal.com/2026-cost-data-breach-study-ibm/

[19] Verizon DBIR 2026, via HIPAA Journal (20/05/2026) — hipaajournal.com/verizon-dbir-2026-healthcare/

[20] Check Point Research, nov/2025, via Hardware.com.br (13/12/2025) — hardware.com.br/?p=343814

[21] HHS/OCR, via HIPAA Journal (atualizado em 13/11/2026) — hipaajournal.com/healthcare-data-breach-statistics/

[22] Sophos, State of Ransomware in Healthcare 2025 — sophos.com/en-us/blog/the-state-of-ransomware-in-healthcare-2025

[23] Brasscom, Relatório de Cibersegurança 2025, via Movimento Econômico (21/07/2026) — movimentoeconomico.com.br/geral/redacao/2026/07/21/hospitais-e-operadoras-viram-alvos-de-ataques-hacker-com-avanco-da-saude-digital/

[L1] Lei nº 13.709/2018 (LGPD), arts. 5º, 48 e 52 — planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[L2] Resolução CD/ANPD nº 15, de 24/04/2024 (Regulamento de Comunicação de Incidente de Segurança) — in.gov.br; resumo: mattosfilho.com.br/unico/regulamento-incidente-seguranca

[L3] Lei nº 13.787/2018 (digitalização e guarda do prontuário), art. 6º — planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13787.htm

[DS] Recursos de segurança do Doctor System — doctoriasystem.com.br/sobre, /privacidade, status.doctoriasystem.com.br

© 2026 Doctor System, um produto ON DIGITAL. Material educativo, de distribuição gratuita. Não substitui orientação jurídica ou técnica individual.