

# Telemedicina e segurança da informação

A fim de se respeitar as orientações da [Organização Mundial da Saúde \(OMS\)](#) estabelecidas para o enfrentamento à pandemia da [COVID-19](#), tais como a adoção de medidas sanitárias de isolamento social, o Conselho Federal de Medicina reconheceu a possibilidade e eticidade do uso da Telemedicina no país.

Ao longo desse artigo iremos discorrer sobre os principais aspectos a serem levantados para o conhecimento do médico e segurança da informação na Telemedicina. Vamos lá?

## Oportunidade

Dessa forma, a Telemedicina surge como oportunidade de garantir a **continuidade** da realização de atendimentos para muitos consultórios médicos, ao mesmo tempo em que garante a proteção dos profissionais de saúde e seus pacientes do contágio do novo coronavírus.

Entretanto, para que o médico consiga realizar uma jornada de sucesso por essa nova forma de prestação de serviços, é de suma importância que realize a escolha de uma plataforma segura que traga tranquilidade para realização de seus atendimentos. Dessa maneira, o profissional só precisará se preocupar em atender seus pacientes com a mesma qualidade de sempre.

## Legislação

A prática da telemedicina no Brasil é subordinada aos termos da Resolução do Conselho Federal de Medicina (CFM) nº 1.643/2002, atualmente em vigor. Entretanto suas possibilidades foram expandidas, com o ofício (nº 1.756/2020 ( [http://www.portalmedico.org.br/resolucoes/CFM/2002/1643\\_2002.pdf](http://www.portalmedico.org.br/resolucoes/CFM/2002/1643_2002.pdf) ) emitido pelo Conselho Federal de Medicina ao Ministério da Saúde, no dia 19 de março de 2020, em que foi permitida a utilização da telemedicina em caráter excepcional como medida de auxílio para o enfrentamento da COVID-19.

## Teleconsultas em caráter excepcional

Ademais, no dia 25 de março de 2020, foi publicada a Portaria (467/20) ( <http://www.in.gov.br/en/web/dou/-/portaria-n-467-de-20-de-marco-de-2020-249312996> ) pelo Ministério da Saúde, que permitiu também a realização de Teleconsultas em caráter excepcional.

## Possibilidades da modalidade

Com isso, as possibilidades de modalidades abrangidas pela Telemedicina passaram a ser: atendimento pré-clínico, suporte assistencial, consulta, monitoramento e diagnóstico.

Em parágrafo único da portaria 467 ressalta-se a obrigatoriedade do serviço médico ofertado através de meios de tecnologia da informação e comunicação garantirem a integridade, segurança e o sigilo das informações.

## Prévia permissão do paciente

Além disso, de acordo com a Resolução CFM nº 1.643/2002 é determinado que informações sobre o paciente só podem ser transmitidas a outro profissional com prévia permissão do paciente, por meio do seu consentimento livre e esclarecido e sob normas de segurança capazes de garantir a confidencialidade, disponibilidade e integridade das informações.

## Pilares da Segurança da informação

A fim de estabelecer a proteção dos dados do paciente transmitidos e armazenados em atendimentos realizados por Telemedicina, a plataforma escolhida pelo médico deve dispor de ferramentas que atendam os pilares da segurança da informação. Sendo estes:

- **Confidencialidade:** garantia do acesso aos dados exclusivamente por pessoas autorizadas;
- **Integridade:** garantia de que as informações estejam em seu formato verdadeiro e que não possam ser modificadas por pessoas que não possuam autorização, ou seja, é a validação da inviolabilidade informações;
- **Disponibilidade:** os dados devem estar disponíveis para uso de pessoas autorizadas, quando necessário;
- **Conformidade:** garantia de concordância com os protocolos, normas e leis que regem a segurança da informação;
- **Autenticidade:** validação da identidade e da origem da informação.

## Como garantir a segurança da informação em seu consultório?

A **LGPD** determina que qualquer serviço deve possuir privacidade desde a Concepção (Privacy By Design), ou seja, deve garantir privacidade desde as primeiras ações da realização das consultas. Ferramentas como **Google Docs** e **Microsoft Word**, por mais que sejam amplamente utilizadas em muitos consultórios, não possuem uma criptografia que assegura a proteção de suas informações, podendo ser expostos com facilidade. Assim como prontuários físicos, que podem ser acessados por qualquer pessoa.

Portanto, a utilização de plataformas de Telemedicina que integram a funcionalidade de prontuário eletrônico pode ser uma ótima ferramenta para assegurar o cumprimento dos pilares da segurança da informação.

## **Telemedicina e a segurança da informação**

A Lei Geral de Proteção de Dados, responsável pela regulamentação da privacidade dos dados do paciente, atribui tal responsabilidade à toda a cadeia envolvida na estruturação da realização do atendimento por meio da Telemedicina.

Logo, em caso da violação de algum dos pilares da segurança da informação dos dados do paciente, tanto a empresa responsável pela prestação do serviço de tecnologia da informação contratada quanto o contratante devem ser responsabilizados.

Portanto, a escolha de plataformas que respeitem todos esses pilares é fundamental para garantia da segurança dos dados na jornada do médico pela Telemedicina e também sua possibilidade de resguardo perante as leis em vigência.

## **Controle do acesso ao prontuário eletrônico**

Segundo a portaria 467/20 publicada pelo Ministério da Saúde: Art. 4º o atendimento realizado por médico ao paciente por meio de tecnologia da informação deve ser registrado em prontuário clínico, que deve conter os dados clínicos necessários para a boa condução do caso; data, hora, tecnologia da informação e comunicação utilizada para o atendimento e número do Conselho Regional Profissional e sua unidade da federação.

Por meio da utilização de um [prontuário eletrônico](#) integrado à plataforma de Telemedicina, é possível restringir e supervisionar o acesso às informações nele contidas.

## **Diferentes perfis de acesso**

Portanto, a plataforma de Telemedicina contratada deve contar com a possibilidade de criação de diferentes perfis de acesso e níveis de permissão distintos para secretarias, médicos, dono da clínica, entre outros. Nesse sentido, cada usuário deve ter sua senha individual e permissões pré-estabelecidas adequadas de acordo com as necessidades da sua função.

## **Transmissão das informações e criptografia de ponta-a-ponta**

A criptografia de dados é uma ferramenta em que as informações a serem protegidas têm o seu formato alterado de forma a serem convertidas em um código indecifrável e ininteligível em sua origem e posteriormente ser decodificada em seu destino. Sendo assim, apenas alguém autorizado pode conseguir realizar sua decodificação.

Tal funcionalidade é ofertada por plataformas que realizam o seu armazenamento na nuvem, responsável pelo armazenamento digital dos dados em servidores externos administrados por empresas terceirizadas que possuem certificação de segurança.

A fim de se garantir a confidencialidade das informações, a criptografia deve ocorrer em todas as pontas do processo de transmissão.

## **Armazenamento seguro**

A plataforma escolhida para realização de seus atendimentos deve contar com um sistema seguro de armazenamento na nuvem que esteja em conformidade com a HIPAA Compliance (Health Insurance Portability and Accountability Act) e assegure sua disponibilidade quando necessário.

Segundo a resolução 1.821/07 do Conselho Federal de Medicina (CFM), todos exames de imagens, laudos e pareceres médicos são de responsabilidade da instituição de saúde pelo período de 20 anos, portanto o armazenamento dessas informações na nuvem devem ser disponibilizados por, no mínimo, este período de tempo.

## **Certificação Digital**

A fim de se garantir a elegibilidade do médico e validade da emissão de receitas e atestados à distância em meio eletrônico, deve-se utilizar assinatura eletrônica, por meio de certificados e chaves emitidos pela Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil.

Logo, a certificação digital é um recurso que complementa as ferramentas oferecidas pelas plataformas de telemedicina para que sejam cumpridos os pilares de segurança da informação.

## **A Conexa Saúde e as segurança da informação**

A plataforma de Telemedicina [Conexa Saúde](#), por exemplo, oferece o serviço de consultório Virtual em

conformidade com as exigências do CFM, com a LGPD brasileira e também com as leis de segurança de dados internacionais, como a GDPR e HIPAA Compliance. Dessa maneira, o médico só precisa se preocupar em atender seus pacientes com a mesma qualidade de sempre.

[Crie seu CONSULTÓRIO VIRTUAL agora mesmo!](#)

[Confira os 7 passos para começar o seu consultório virtual agora mesmo!](#)

[Atenda a qualquer hora, de qualquer lugar, até mesmo sem sair de casa!](#)