MANUAL DE BOAS PRÁTICAS DE TELEMEDICINA E TELESSAÚDE

Saúde Digital Brasil

EXPE
DIENTE

EDITORES

Caio Seixas Soares - Presidente do Conselho de Administração da Saúde Digital Brasil

Carlos Henrique Sartorato Pedrotti - Vice-presidente do Conselho de Administração da Saúde Digital Brasil

CONTEÚDO E REDAÇÃO

Alexandre Domingos de Sousa – DASA
Ana Carolina Lucchese – TUINDA CARE
Carlos Henrique Sartorato Pedrotti – HOSPITAL ISRAELITA ALBERT EINSTEIN
Carolina Gomes Pampolha Pinto Santos Gaudêncio – DOCWAY
Douglas Santos Brancaglion – MEMED
Fábio de Oliveira Tabalipa – MEMED
Fermando Henrique de Paula Uzuelli – SABIN
Fernanda Moura Leite – DASA
Fernanda Thallyta Borba – TUINDA CARE
Filipe Ramalho Molina – SAÚDE ID
Francisco Costa da Silva Junior – SAÚDE ID
Gabriel Rodrigues Couto – MEMED
Humberto Weber Fernandes – CONEXA
Ihvi Maria Aidukaitis – RECEITA DIGITAL
José Benedito Ramos Valladão Junior – TELADOC
Julia Cestari Santos – MEVO
Leonardo Henrique Kappes – TOPMED
Lídia Maria Lourençön Rodrigues – TOPMED
Luana Rizzo Cazzola Rockenbach – CONEXA
Lucas Amâncio Barbosa da Silva – TELADOC
Marcela Mitie Missawa – TELADOC
Marielen Ribeiro Tavares da Silva – TUINDA CARE

Marina Jacob Lopes da Silva Santos – MEMED
Maurício Mathias Cereto – TELADOC
Mayra Motta – PRORADIS
Rayssa Carolina de Araújo Collossal Braga – CONEXA
Renata Albaladejo Morbeck – HOSPITAL ISRAELITA ALBERT EINSTEIN
Renata Zobaran Pereira – TOPMED
Roberta Rubia de Lima – SAÚDE ID
Rodrigo Rubo – TELADOC
Thiago Julio – MEMED
Victor Rafael Andrade Oliveira Prata de Guimarães Souza – CONEXA

REVISÃO

Carolina Machado - Revisão Para quê?

DIREÇÃO DO PROJETO

Juliane Trevisan - MF Marketing & Business Advisor

PROJETO GRÁFICO

Laika Design

FOTOGRAFIA

PEXELS e Unsplash

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Manual de boas práticas de telemedicina e
telessaúde [livro eletrônico] / coordenação Marina Jacob Lopes da Silva Santos...[et al.]. -- 1. ed. -- São Paulo, SP : Saúde Digital Brasil, 2022.
PDF

Outros coordenadores:
Fernanda Moura Leite, Carlos Henrique Sartorato Pedrotti, Victor Rafael Andrade Oliveira Prata de Guimarães Souza.
Vários colaboradores. Bibliografia.
ISBN 978-65-998066-0-5

1. Assistência médica 2. Inovações médicas 3. Saúde digital 4. Tecnologia médica - Metodologia 5. Telemedicina 6. Telemedicina - Brasil I. Santos, Marina Jacob Lopes da Silva. II. Leite, Fernanda Moura. III. Pedrotti, Carlos Henrique Sartorato. IV. Souza, Victor Rafael Andrade Oliveira Prata de Guimarães

22-114272 CDD-610.285

Índices para catálogo sistemático:

1. Telemedicina e telessaúde : Ciências médicas 610.285
Eliete Marques da Silva - Bibliotecária - CRB-8/9380

PRE
FÁCIO

Foi com muita honra que recebi o convite do Dr Caio Soares, atual Presidente da Saúde Digital Brasil (SDB) para prefaciar esta obra, que é o Manual de Boas Práticas de Telemedicina.

Participei pessoalmente de muitas discussões sobre o tema Telemedicina no Brasil, muitas delas com conselho de classe, na maioria das vezes sobre o tema teleconsulta síncrona vídeo assistida, se podia ou não podia, se era legal ou não, mas sempre achei este debate pequeno, pois deveríamos como médicos estar discutindo a melhor forma de usar estas novas ferramentas que estavam sendo apresentadas a nós, para expandir o cuidado aos nossos pacientes, afinal Telemedicina simplesmente é Medicina usando ferramentas de comunicação à distância.

Este Manual reflete o espírito com o qual criamos a SDB, para ser uma associação de empresas que estão comprometidas em primeiro lugar com a segurança do atendimento do paciente usando ferramentas de comunicação à distância, sejam estas ferramentas básicas de videoconferência ou até mesmo avançadas, como a telepropedêutica armada. Sempre o paciente esteve no centro em nossas tomadas de decisão e todo o movimento de construção da associação foi neste sentido, nasceu com a missão de consolidar o Estado da Arte no atendimento à Saúde de forma digital e com isto favorecer todos os brasileiros.

A Telemedicina é apenas uma forma de atendimento ao paciente, sendo parte de algo muito maior que é a Saúde Digital. Foi exatamente por esta razão que ao escolhermos o nome da associação escolhemos Saúde Digital Brasil, para que ela pudesse englobar tudo aquilo que podemos fazer transformando digitalmente o processo assistencial. Estamos na iminência da entrada do 5G no mercado brasileiro, que permitirá não apenas aumentar a velocidade de conexão, mas principalmente liberar todo o potencial da computação em nuvem, assim como permitir um número cada vez maior de dispositivos conectados, gerando dados de saúde de forma passiva e massiva com o paciente chegando cada vez mais rápido e mais fácil até o atendimento do profissional de saúde, e nós profissionais estaremos usando ferramentas de apoio a decisão, com assertividade e produtividade exponencializadas não por inteligência artificial , mas por inteligência aumentada, que é justamente a ampliação da capacidade humana usando estas ferramentas que criamos. Afinal, sempre seremos seres humanos cuidando de outros seres humanos; a tecnologia usada da forma correta não afasta, ela aproxima.

Esta é a primeira obra da Saúde Digital Brasil, tenho certeza que esta nova Era da Saúde está apenas começando. Boa leitura!

EDUARDO CORDIOLI

CONSELHO DE ADMINISTRAÇÃO SDB

PRESIDENTE
CAIO SEIXAS SOARES – TELADOC

VICE-PRESIDENTE
CARLOS PEDROTTI – HOSPITAL ISRAELITA ALBERT EINSTEIN

CONSELHEIRO
FÁBIO CUNHA – DASA

CONSELHEIRO
FÁBIO LUÍS PINTO TIEPOLO – DOCWAY

CONSELHEIRO
GUILHERME DE SOUZA WEIGERT – CONEXA

CONSELHEIRO
DR. WILSON SHCOLNIK – GRUPO FLEURY

CARTA AO LEITOR

CARO LEITOR,

Desde da fundação da Associação Saúde Digital Brasil SDB, em 2020, nosso objetivo sempre foi defender e fortalecer a utilização e disseminação da telessaúde plena no Brasil. Depois desses dois anos de pandemia, é motivo de muito orgulho perceber que a sociedade passou a adotar, acreditar e escolher a telemedicina.

É notável o impacto que ela provocou em toda sociedade, beneficiando, sem exceções, pacientes, médicos, o sistema público e privado, e mostrando-se uma ferramenta de ampliação de acesso e capaz e de autonomia para decidir como cuidar da sua saúde. Profissionais da saúde e pacientes integraram-se de forma inédita, gerando ganhos à saúde pública, ampliando o acesso, diminuindo as distâncias, reduzindo desperdícios e melhorando os desfechos clínicos.

Não há dúvida que avançamos em nossa missão. E como a segurança da prática médica aliada ao desenvolvimento científico-tecnológico da saúde digital fazem parte dos nossos propósitos como entidade, é um privilégio poder lançar esse Manual de Boas Práticas em Telemedicina.

Este documento nasce da nossa preocupação de que cada um dos pacientes e médicos que recorrem à telemedicina tenham uma referência para guiar suas decisões. Somente dessa forma conseguiremos que a tecnologia cumpra, com qualidade e segurança, o seu papel de garantir o acesso da população à assistência médica, onde quer que ela esteja.

O Manual de Boas Práticas em Telemedicina da Saúde Digital Brasil, elaborado pelas principais lideranças e autoridades no tema em nosso país, reúne conhecimento técnico e de excelente qualidade e padroniza as principais práticas para o exercício da telemedicina.

Estamos muito felizes com o resultado e aproveito para agradecer a todos - e foram muitos! - que participaram da construção desse conteúdo. Sem a contribuição e compartilhamento de seus conhecimentos, não conseguiríamos um resultado tão completo e um impacto tão expressivo para a Telemedicina.

Boa leitura!

CAIO SOARES
Presidente da Saúde Digital Brasil

SOBRE A SDB

A Associação Brasileira de Empresas de Temedicina e Saúde Digital – **SAÚDE DIGITAL BRASIL** – é uma entidade representativa dos prestadores de serviço de telessaúde do Brasil.

É focada no avanço pleno da telessaúde de forma ética e responsável, defendendo sua regulamentação e servindo como referência perante o governo e servindo como referência de boas práticas no âmbito de saúde digital. Também busca entender, ampliar e difundir aspectos de inovação tecnológica da saúde virtual e sua integração aos modelos de entrega de Valor em Saúde .

A SDB representa uma rede de prestadores de serviço, desde fornecedores de soluções de telessaúde, assim como provedores de tecnologia para soluções de saúde digital. Nasceu como uma forma de defender os interesses e necessidades do setor, mas também com a missão de consolidar o Estado da Arte no atendimento à Saúde de forma digital e, com isto, favorecer todos os brasileiros.

Missão

Ser uma Instituição facilitadora do relacionamento entre sociedade civil, governo e prestadores privados de telessaúde, defendendo os legítimos interesses de seus membros e ampliar o acesso à saúde digital para a população brasileira.

Visão

Ser a Instituição que representa os prestadores privados de telessaúde e saúde digital do Brasil, liderando o processo de transformação digital do setor.

Valores

- Colaboração
- Ética
- Responsabilidade Social
- Excelência Operacional
- Pioneirismo

sumário

CAPÍTULO**01**

TELEME-DICINA DIRETA AO PA-CIENTE

1. INTRODUÇÃO

O desenvolvimento das tecnologias de comunicação e informação nas últimas décadas tem transformado substancialmente as relações humanas. A crescente disponibilidade de acesso à internet levou à ampliação da oferta de serviços digitais nas mais diversas áreas, como comércio, educação, entretenimento, serviços financeiros e, mais recentemente, serviços de saúde.

A prestação de serviços de saúde possui características únicas, de forma que sua digitalização envolve desafios importantes na evolução das estruturas de relacionamento entre profissionais, pacientes, operadoras e órgãos de regulação, mantendo o elevado nível de qualidade e segurança necessários para os cuidados médicos.

A telemedicina é um dos serviços de saúde digital que mais cresceu nos últimos anos em todo o mundo.

Os serviços digitais em saúde compreendem uma vasta gama de aplicações, o que inclui serviços de telediagnóstico, aplicativos de saúde (e-health), monitoramento de atividades e consultas virtuais com psicólogos, enfermeiros, farmacêuticos, fisioterapeutas, educadores físicos, entre outras numerosas áreas e especialidades.

A telemedicina, definida aqui como a prestação de serviços de assistência médica à distância, é um dos serviços de saúde digital que mais cresceu nos últimos anos em todo o mundo. No Brasil, a assistência diagnóstica e a comunicação digital entre profissionais médicos já é bastante rotineira em grandes serviços. No entanto, o contato direto entre médico e paciente utilizando meios de comunicação digital até o início de 2020 ainda não tinha ganhado tração, especialmente devido à insuficiência de garantias regulatórias e padrões de uso que assegurassem a sustentabilidade dos prestadores.

O advento da pandemia de COVID-19 acelerou sobremaneira a adoção de serviços digitais e, com a segurança jurídica propiciada pela lei 13.989 de 15 de Abril de 2020, a prestação de serviços de telemedicina direta ao paciente se tornaram amplamente disponíveis. Contudo, padrões de boas práticas de telemedicina direta ao paciente ainda não estão bem definidos e, assim, o desenvolvimento sustentável de serviços de excelência pode ser comprometido.

A Saúde Digital Brasil, uma associação que congrega os maiores prestadores de serviços de saúde digital do país, surgiu tendo como um de seus principais objetivos estabelecer critérios bem definidos de qualidade e segurança a serem seguidos por seus associados, que demonstrem a excelência no cuidado ao paciente e na experiência digital em saúde, com garantias à segurança da informação e do respeito às normas regulatórias e devidos processos legais.

As recomendações expostas neste documento fundamentam-se em preceitos éticos essenciais para a prática médica, com a devida reverência ao Código de Ética Médica (CEM) do Conselho Federal de Medicina e à Declaração sobre a Ética da Telemedicina, adotada pela 58ª Assembleia Geral da Associação Médica Mundial.

O alvo de toda a atenção do médico é a saúde do ser humano

O absoluto respeito pela vida humana e consideração pela autonomia do indivíduo, o zelo pelo sigilo e confidencialidade do paciente, a anteposição da não-maleficência e a manutenção de uma boa relação médico-paciente são princípios éticos invioláveis em qualquer cenário de atendimento médico. Portanto, a Saúde Digital Brasil orienta especial atenção aos Capítulos I (Princípios Fundamentais), IX (Sigilo Profissional), X (Documentos Médicos) e XI (Auditoria e Perícia Médica) do CEM no exercício da telemedicina direta ao paciente e enaltece os dizeres do Art. 2º do Capítulo I: “O alvo de toda a atenção do médico é a saúde do ser humano, em benefício da qual deverá agir com o máximo de zelo e o melhor de sua capacidade profissional”.

2. ESCOPO

Este capítulo tem por escopo a atenção médica e de enfermagem prestada diretamente ao paciente, à distância, utilizando-se de meios de comunicação que incluem áudio, vídeo ou texto, seja através da internet ou por sistemas de telefonia.

O presente capítulo visa abordar os cuidados médicos e de enfermagem realizados diretamente entre profissional de saúde e paciente, com o uso de tecnologias de comunicação à distância. Há várias formas de se comunicar com o paciente à distância, como envio de imagens e texto, mensagens de áudio, e comunicação em tempo real por áudio ou videochamada. Em fluxos de atendimento por telemedicina, muitas vezes há superposição entre estes meios e múltiplas abordagens são utilizadas. Com a finalidade de tornar o escopo deste documento mais objetivo, as modalidades de atendimento direto ao paciente por telemedicina foram separadas em três grupos grupos: atendimento assíncrono (chat), atendimento telefônico e atendimento por videochamada. Além disso, são abordados temas como uso de dispositivos de telepropedêutica, além de boas práticas de controle de qualidade e situações especiais.

3. O ATENDIMENTO POR TELEMEDICINA

O atendimento por telemedicina, ou teleatendimento, compreende o contato entre profissionais de saúde e pacientes, realizado através de tecnologias de telecomunicação, com a finalidade de preservar o bem-estar ou auxiliar no diagnóstico e tratamento de enfermidades de forma preventiva, curativa ou paliativa.

É importante que o profissional de saúde e o paciente estabeleçam uma adequada relação profissional-paciente, pautada na empatia, no acolhimento e no respeito mútuo.

Para que o atendimento transcorra da melhor forma possível priorizando a segurança do paciente, é importante que o profissional de saúde e o paciente estabeleçam uma ***adequada relação profissional-paciente***, pautada na empatia, no acolhimento e no respeito mútuo. Para isso, deve ser dada especial atenção à comunicação verbal e não-verbal, considerando inclusive as particularidades e limitações do canal utilizado para a comunicação.

O termo **teleconsulta** é definido neste Manual de Boas Práticas como o atendimento que ocorre diretamente **entre médico** e paciente, com finalidade de assistência médica visando orientação clínica, diagnóstica e/ou terapêutica. Nesse contexto, a teleconsulta consiste em **ato médico**, trazendo consigo as responsabilidades e obrigações inerentes à relação médico-paciente. Os teleatendimentos das demais categorias profissionais em saúde devem ter suas definições e regulamentações delimitadas e especificadas em outras publicações para esse fim.

São definidas neste documento três modalidades de atendimento por telemedicina:

- **Atendimento assíncrono (troca de mensagens de texto, imagens e áudio de forma assíncrona);**
- **Atendimento telefônico (apenas áudio);**
- **Atendimento por videochamada (áudio e vídeo).**

3.1
O atendimento assíncrono

3.1 O atendimento assíncrono

O atendimento realizado através da troca de mensagens de texto, imagens e trechos de áudio previamente gravados é um meio rápido e eficaz de comunicação entre pacientes e profissionais de saúde. É considerada uma modalidade assíncrona, uma vez que a comunicação pode não ocorrer em tempo real. Comumente é realizada através de SMS (Short Message Service), MMS (Multimedia Message Service), aplicativos de mensagens instantâneas, e-mail, formulários de contato eletrônicos ou serviços de "chat" baseados em web. A **Saúde Digital Brasil (SDB)** recomenda como boas práticas de telemedicina direta ao paciente, por meio de troca de mensagens de texto, imagens e áudio de forma assíncrona, os padrões dispostos nos itens a seguir.

3.1.1 Escopo do atendimento assíncrono

A atenção à saúde através da comunicação assíncrona possui grandes vantagens logísticas, seja pela praticidade, acesso simplificado e ampla disponibilidade, com otimização de recursos humanos e financeiros envolvidos no cuidado. No entanto, possui limitações importantes em relação à segurança clínica, uma vez que não é possível a visualização em tempo real do paciente, com impossibilidade de realização de um exame clínico adequado por telemedicina. Assim, a **Saúde Digital Brasil (SDB)** recomenda que o escopo do atendimento assíncrono seja limitado às seguintes situações:

- Promoção de saúde e orientação em bem-estar e hábitos saudáveis, realizados por profissionais de saúde habilitados.
- Orientações gerais de saúde sobre temas diversos, realizado por profissionais de saúde habilitados, incluindo ações de educação aos pacientes e familiares.
- Orientações por profissionais de enfermagem sobre a realização de procedimentos de enfermagem que incluem curativos, aplicações de injeções subcutâneas, cuidados com feridas e estomas, mobilização, entre outros.
- Monitoramento e orientação, por profissionais de enfermagem, de pacientes com doenças agudas ou crônicas, com diagnóstico e plano terapêutico já previamente estabelecidos por profissional médico, através dos meios adequados.
- Triagem por profissionais de enfermagem para direcionamento do paciente e escolha do serviço mais adequado às necessidades.
- Realização de teleconsultas conforme definido no item a seguir.

3.1.2 - A teleconsulta assíncrona

A **Saúde Digital Brasil** entende que é possível a realização de teleconsulta de forma assíncrona, com o envio prévio de informações textuais, áudio e/ou imagens. No entanto, é imperativo que tanto paciente como médico estejam cientes e concordantes com as relevantes limitações que esta metodologia impõe em alguns cenários.

Dessa forma, a **Saúde Digital Brasil** recomenda as seguintes **boas práticas** em teleconsulta via chat ou assíncrona:

Toda teleconsulta deve ser adequadamente registrada em prontuário

- Toda teleconsulta deve ser adequadamente registrada em prontuário. Isso inclui não só descrição ou transcrição das trocas de texto, imagens e áudios, mas também as impressões clínicas e condutas.
- A ausência do exame clínico audiovisual em tempo real pode ser parcialmente compensada pelo envio de informações, imagens e áudios em forma assíncrona. Cabe ao médico a responsabilidade de, em conjunto com o paciente, decidir sobre tomada de decisões clínicas e condutas médicas baseando-se na suficiência das informações obtidas. Sugere-se que estes termos devam constar na documentação enviada ao paciente.
- A teleconsulta assíncrona pode ser viável para orientação médica geral em situações agudas ou crônicas de pacientes com diagnóstico e plano terapêutico já previamente estabelecidos pela equipe médica responsável.

- A teleconsulta assíncrona pode ser viável para seguimento clínico temporário para solicitação/avaliação de exames complementares ou ajuste terapêutico em pacientes com plano terapêutico já previamente definido por meio adequado, ou conforme protocolo clínico preestabelecido pela equipe médica responsável.
- A teleconsulta assíncrona pode ser viável para pacientes em primeira consulta, em especial para situações em que a análise estática de imagens ou exames complementares, em conjunto com informações clínicas textuais, pode ser suficiente para o diagnóstico, ficando sob responsabilidade do médico assistente a viabilidade de gerar diagnóstico e/ou plano terapêutico através da cuidadosa análise da qualidade e confiabilidade das informações obtidas no atendimento.

Devido às características intrínsecas à transmissão de dados de forma assíncrona, sem interação em tempo real com o paciente, a **Saúde Digital Brasil** entende que, por boa prática, **não se recomenda**:

- A realização de teleconsultas assíncronas apenas por texto, na ausência de complementação com imagens, em pacientes sem acompanhamento prévio no serviço prestador da teleconsulta com diagnóstico e plano terapêutico adequadamente definidos em consulta presencial ou remota via videochamada.
- A realização de teleconsultas assíncronas para avaliações de rotina em pacientes sem acompanhamento prévio no serviço prestador da teleconsulta, com diagnóstico e plano terapêutico adequadamente definidos em consulta presencial ou remota via videochamada, com o objetivo de atestar saúde, atestar incapacidade funcional, emitir receitas de uso contínuo ou de medicação sujeita a controle especial.
- O acompanhamento clínico continuado de doenças crônicas ou recorrentes exclusivamente por chat ou troca de mensagens, imagens e áudios de forma assíncrona para pacientes sem acompanhamento prévio no serviço prestador da teleconsulta, com diagnóstico e plano terapêutico adequadamente definidos em consulta presencial ou remota via videochamada.
- O seguimento clínico contínuo e exclusivo através de chat ou troca de mensagens, imagens e áudios de forma assíncrona, por tempo indefinido.

Não se recomenda o atendimento clínico contínuo e exclusivo de forma assíncrona.

3.1.3 Requisitos de segurança no atendimento assíncrono

A fim de garantir a segurança da informação e adequada identificação dos participantes de um atendimento assíncrono, o meio de comunicação utilizado deve permitir a identificação do paciente com elevado nível de segurança. Recomendam-se como boas práticas de segurança em serviços de atendimento direto ao paciente por troca de mensagens de texto, imagens e áudio de forma assíncrona:

- Em caso de utilização de SMS/MMS ou aplicativos congêneres de mensagens instantâneas, recomenda-se que sejam apenas utilizadas plataformas que utilizam **encriptação de dados ponta-a-ponta** e garantem **identificação do emissor** por e-mail pessoal ou número de telefone celular próprio.
- Em caso de utilização de SMS/MMS ou aplicativos congêneres de mensagens instantâneas, devido às limitações de serviços de mensagens de texto, recomenda-se que o acesso seja verificado através de e-mail ou número de celular **previamente cadastrados e validados**.
- Em caso do uso de aplicações Web ou Mobile proprietárias ou terceirizadas, o acesso do paciente e do profissional de saúde devem ser validados por **login e senha previamente cadastrados e validados ou biometria**, preferencialmente com mais de um fator de autenticação.

3.1.4 Registro e documentação do atendimento assíncrono

O registro adequado é etapa fundamental de qualquer teleatendimento. Dessa forma, todo atendimento assíncrono, considerando o escopo de atenção à saúde, deve ser registrado adequadamente no Prontuário Eletrônico do Paciente (PEP), em uma das seguintes formas:

- Transcrição integral do texto, imagens e anexação das transcrições ou arquivos de áudio (quando aplicável) trocados entre paciente e equipe de saúde, através de integração direta ou indireta entre a plataforma de chat e o PEP.
- Em caso de acompanhamento ou orientação por profissional não médico, o atendimento assíncrono pode ser registrado e seus detalhes inseridos no PEP diretamente pelo profissional de saúde, o que inclui, mas não se limita, à descrição das imagens enviadas, impressões técnicas e sugestões ou orientações fornecidas.
- Em caso de teleconsulta, as informações técnicas do atendimento podem ser incluídas diretamente no PEP. Devem incluir a descrição das imagens enviadas, anamnese, impressões clínicas, orientações fornecidas e, quando pertinente, hipótese diagnóstica e/ou prescrição, além de qualquer outra informação necessária para a documentação adequada do atendimento.

3.2 O atendimento telefônico

3.2 O atendimento telefônico

Define-se como atendimento telefônico quando a comunicação entre paciente e profissional de saúde ocorre em tempo real, com transmissão síncrona de áudio. Pode ocorrer analogicamente através de linhas telefônicas convencionais ou, mais frequentemente, por transmissão de áudio digital através de telefonia fixa, telefonia celular, ou plataformas de comunicação via internet. A **Saúde Digital Brasil** recomenda como boas práticas de telemedicina direta ao paciente, por meio telefônico, os padrões dispostos nos itens a seguir.

3.2.1 Escopo do atendimento telefônico

Se comparada ao atendimento assíncrono, a modalidade telefônica traz maior dinamismo e familiaridade à comunicação entre paciente e profissional de saúde. No entanto, mesmo complementando textos, imagens e áudios previamente enviados, ainda possui limitações relevantes em relação ao exame clínico e capacidade diagnóstica e terapêutica. A **Saúde Digital Brasil** recomenda que o escopo do atendimento telefônico seja limitado às seguintes situações:

- Promoção de saúde e orientação em bem-estar e hábitos saudáveis, realizados por profissionais de saúde habilitados.

  Orientações gerais de saúde sobre temas diversos, realizado por profissionais de saúde habilitados, incluindo ações de educação aos pacientes e familiares.

- Orientações por profissionais de enfermagem sobre a realização de procedimentos de enfermagem que incluem curativos, cuidados com feridas e estomas, mobilização, entre outros.

- Monitoramento e orientação, por profissionais de enfermagem, de pacientes com doenças agudas ou crônicas, com diagnóstico e plano terapêutico já previamente estabelecidos por profissional médico, através dos meios adequados.

- Triagem por profissionais de enfermagem para direcionamento do paciente e escolha do serviço mais adequado às necessidades.

- Realização de teleconsultas conforme definido no item correspondente.

3.2.2 a teleconsulta via telefônica

A **Saúde Digital Brasil** entende que é possível a realização de teleconsulta por telefone, com ou sem o envio prévio de informações textuais, áudio e/ou imagens. A comunicação por áudio em tempo real permite a percepção de diversos elementos subjetivos identificáveis na fala, não disponíveis na comunicação assíncrona. O exame clínico realizado por telefone, embora limitado à análise do áudio, permite a interpretação de parâmetros que podem ter relação com o diagnóstico e nortear condutas de forma mais eficiente, tais como:

- Fluidez do diálogo
- Audição, inteligibilidade e compreensão
- Tonalidade e volume da voz
- Prosódia de fala
- Tiques vocais
- Frequência de interrupções para inspiração
- Elementos patológicos (rouquidão, soluços, verbalizações álgicas, tosse, etc.)
- Outras percepções subjetivas presentes na fala

No entanto, assim como no atendimento assíncrono, é necessário que tanto paciente como profissional estejam cientes e concordantes com as relevantes limitações que a ausência do componente visual na comunicação em tempo real pode impor em alguns cenários.

Dessa forma, a **Saúde Digital Brasil** recomenda as seguintes **boas práticas** em teleconsulta por telefone:

- Toda teleconsulta deve ser adequadamente registrada em prontuário. Isto inclui a descrição da consulta completa, que inclui, mas não se limita, a:
  - queixa e duração;
  - anamnese e exame clínico da fala e linguagem, caso pertinente;
  - descrição e análise de documentos, textos e imagens enviados por outros meios;
  - hipótese diagnóstica (preferencialmente utilizando CID-10 ou equivalente mais apropriado à especialidade ou mais atualizado);
  - impressão clínica e prognóstico;
  - plano terapêutico, orientações e documentos emitidos.
- A ausência do exame clínico visual em tempo real pode comprometer a interpretação de uma série de nuances necessárias a avaliações diagnósticas mais complexas. A **Saúde Digital Brasil** entende que cabe ao médico a responsabilidade de, em conjunto com o paciente, decidir sobre tomada de decisões clínicas e condutas médicas baseando-se na suficiência das informações obtidas. Sugere-se que estes termos devem constar da documentação enviada ao paciente.
- A teleconsulta telefônica é frequentemente suficiente para orientação médica geral em situações agudas ou crônicas de pacientes com diagnóstico e plano terapêutico já previamente estabelecidos pela equipe médica responsável.

A viabilidade da teleconsulta telefônica para tomada de decisão clínica é de responsabilidade do médico assistente

- A teleconsulta telefônica é frequentemente suficiente para solicitação/avaliação de exames complementares e/ou ajuste terapêutico em pacientes com situação clínica já previamente avaliada por meio adequado, durante um intervalo temporal preestabelecido pela equipe médica responsável.
- A teleconsulta telefônica é viável para pacientes em primeira consulta, em especial para situações de baixa complexidade e baixo risco, ficando sob responsabilidade do médico assistente a viabilidade de gerar diagnóstico e/ou plano terapêutico através da cuidadosa análise da qualidade e confiabilidade das informações obtidas no atendimento.

Devido às características intrínsecas à comunicação exclusiva por áudio, sem interação por vídeo do paciente em tempo real, a **Saúde Digital Brasil** entende que, por boa prática, **não se recomenda**:

- A realização de teleconsultas telefônicas para avaliação de rotina em pacientes *sem acompanhamento prévio* no serviço prestador da teleconsulta, com diagnóstico e plano terapêutico adequadamente definidos em consulta presencial ou remota via videochamada, com a finalidade de atestar saúde, atestar incapacidade funcional, emitir receitas de uso contínuo ou de medicação sujeita a controle especial.
- Seguimento clínico contínuo e exclusivo através de teleconsultas telefônicas por um período maior do que o preconizado para a condição clínica do paciente, assim definido pelo médico assistente.

3.2.3.- Requisitos de segurança no atendimento telefônico

A fim de garantir a segurança da informação e adequada identificação dos participantes de atendimento telefônico, os processos de contato devem permitir a identificação do paciente com elevado nível de segurança. Seguem boas práticas de segurança em serviços de telemedicina direta ao paciente utilizando a modalidade telefônica:

- Em caso de utilização de linhas telefônicas, recomenda-se que seja verificado o número de origem da chamada e conferência de dados pessoais **previamente cadastrados e validados**, preferencialmente com envio eletrônico de documentos que garantam a identificação adequada do paciente.
- Em caso do uso de aplicações Web ou Mobile proprietárias ou terceirizadas, o acesso do paciente e do profissional de saúde devem ser verificados por **login e senha previamente cadastrados e validados ou biometria**, preferencialmente com mais de um fator de autenticação.
- Em caso de gravação do teleatendimento, deve haver consentimento expresso do paciente.

3.2.4.Registro e documentação do atendimento telefônico

A **Saúde Digital Brasil** entende que o registro adequado é etapa fundamental de qualquer atendimento por telemedicina. Assim, considerando o escopo de atenção à saúde, os atendimentos telefônicos devem ser registrados adequadamente no Prontuário Eletrônico do Paciente (PEP), em uma das seguintes formas:

- Transcrição integral dos áudios através da utilização de *software* validado para transcrição automatizada de áudio em português (*speech-to-text*), com anexação ao PEP através de integração automatizada. Recomenda-se que, além da transcrição, seja inserida uma descrição do atendimento, contendo impressões clínicas e sugestões ou orientações fornecidas.

O registro adequado é etapa fundamental de qualquer atendimento por telemedicina

- Não se recomenda de rotina a gravação e anexação dos arquivos dos áudios completos ao PEP. Em caso de opção por essa modalidade, ou de registro de pequenos trechos com finalidade assistencial, é necessário expresso consentimento do paciente e manuseio adequado dos arquivos a fim de proteger a privacidade do paciente e adequação aos princípios da LGPD.
- Nesta modalidade recomenda-se que haja inserção manual no PEP de descrição do atendimento, contendo, mas não se limitando às impressões clínicas e sugestões ou orientações fornecidas.
- Em caso de acompanhamento ou orientação por profissional não médico, o atendimento telefônico pode ser registrado e seus detalhes inseridos no PEP diretamente pelo profissional de saúde, o que inclui, mas não se limita, à descrição da documentação enviada (se aplicável), impressões técnicas e sugestões ou orientações fornecidas.
- Em caso de teleconsulta, as informações técnicas do atendimento podem ser incluídas diretamente no PEP. Recomenda-se incluir a descrição da queixa e duração, anamnese, exame clínico da fala, impressões clínicas, orientações fornecidas e, quando pertinente, hipótese diagnóstica e/ou prescrição.

3.3 O atendimento por videochamada

Define-se por videochamada a comunicação em tempo real através da transmissão de áudio e vídeo. Pode ser realizada utilizando redes privadas ou internet, através de telefonia fixa, celular, fibra óptica, rádio frequência ou via satélite. A **Saúde Digital Brasil** recomenda como boas práticas de telemedicina direta ao paciente, por vídeochamada, os padrões dispostos nos itens a seguir.

3.3.1 Escopo do atendimento por videochamada

A **Saúde Digital Brasil** considera o atendimento por videochamada uma modalidade ***equivalente ao atendimento presencial***, em sentido amplo. Caberá aos profissionais envolvidos no cuidado a responsabilidade sobre a viabilidade da tomada de decisão técnica diante das informações obtidas, sempre com o consentimento amplamente esclarecido do paciente.

Diante do exposto, a **Saúde Digital Brasil** recomenda que o escopo do atendimento por videochamada compreenda as mais variadas ações médicas e de enfermagem, com o objetivo de prestar atenção à saúde, entre as quais destaca-se:

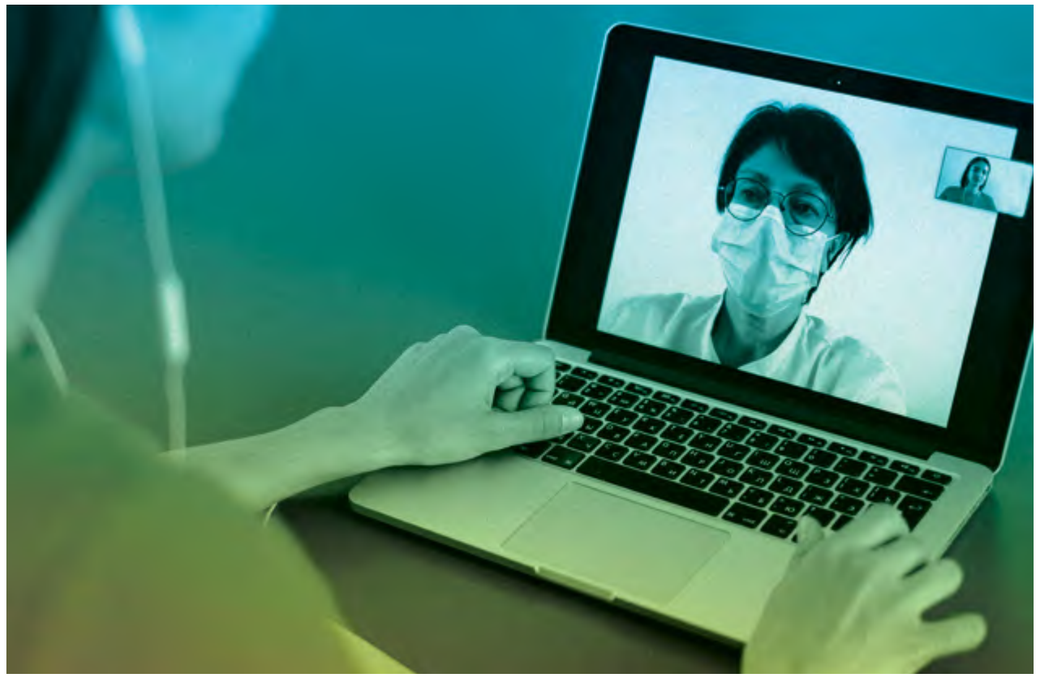
- Promoção de saúde e orientação em bem-estar e hábitos saudáveis, realizados por profissionais de saúde habilitados.
- Orientações gerais de saúde sobre temas diversos, realizado por profissionais de saúde habilitados, incluindo ações de educação aos pacientes e familiares.
- Orientações por profissionais de enfermagem sobre a realização de procedimentos de enfermagem que incluem curativos, aplicações de injeções subcutâneas, cuidados com feridas e estomas, mobilização, entre outros.
- Monitoramento, orientação, triagem, direcionamento e navegação, por profissionais de enfermagem, de pacientes com doenças agudas ou crônicas, dentro do escopo do atendimento presencial de enfermagem.
- Realização de teleconsultas conforme definido no item correspondente.

3.3 O atendimento por videochamada

3.3.2 A teleconsulta por videochamada

A teleconsulta por videochamada é a modalidade mais completa de consulta médica por telemedicina. Permite a realização de amplo exame clínico audiovisual, admitindo raciocínio clínico e diagnóstico considerados equivalentes à consulta presencial, particularmente quando exame clínico realizado no local não trará informações relevantes à análise do caso em questão.

O uso de recursos audiovisuais em tempo real, complementado ou não pelo envio de imagens estáticas ou uso de dispositivos de propedêutica avançada por telemedicina, como câmeras especiais e estetoscópios digitais, possibilita a realização de uma consulta médica completa e resolutiva. A teleconsulta por videochamada pode incluir, mas não se limita, a:



- Anamnese completa;
- Exame clínico:
  - Estado geral do paciente;
  - Análise do comportamento, fala e demais elementos do exame do estado mental;
  - Análise da frequência respiratória;
  - Inspeção geral e específica da pele, mucosas e fâneros (ectoscopia);
  - Autoexame e manobras propedêuticas abdominais;
  - Autoexame e manobras propedêuticas ortopédicas;
  - Manobras propedêuticas neurológicas.
- Impressões clínicas;
- Hipótese diagnóstica;
- Planejamento terapêutico.

É necessário, porém, que tanto paciente como médico estejam cientes e concordantes com as limitações decorrentes da ausência do exame clínico presencial. Tais restrições são particularmente evidentes quando um exame clínico palpatório, auscultatório ou avaliação de cavidades são cruciais para a decisão clínica, e dispositivos de propedêutica avançada por telemedicina que poderiam potencialmente substituí-los não estão disponíveis. Da mesma forma, oscilações na qualidade do áudio e do vídeo podem impor restrições significativas, que, a julgamento do médico teleconsultor, devem ser analisadas de forma crítica na tomada de decisão clínica ou encaminhamento para avaliação presencial.

É necessário que tanto paciente como médico estejam cientes e concordantes com as limitações decorrentes da ausência do exame clínico presencial.

Com o intuito de garantir a segurança e a qualidade dos atendimentos médicos, a Saúde Digital Brasil recomenda as seguintes boas práticas em teleconsultas por videochamada:

- A ausência do exame clínico presencial, particularmente em situações de maior risco imediato e complexidade, pode comprometer a interpretação de uma série de nuances necessárias a avaliações diagnósticas mais complexas. A Saúde Digital Brasil entende que cabe ao médico a responsabilidade de, em conjunto com o paciente, decidir sobre tomada de decisões clínicas e condutas médicas baseando-se na suficiência das informações obtidas. Sugere-se que estes termos devem constar da documentação enviada ao paciente.

- Recomenda-se que a plataforma ou fluxo de atendimento por videochamada permita avaliar potenciais riscos ambientais ou comportamentais que trariam perigo à segurança da informação, privacidade e respeito na relação profissional-paciente, ou prejuízo à viabilidade do teleatendimento, tais como:
  - instabilidade da conexão de internet;
  - baixa qualidade de áudio e imagem;
  - ruído ambiente elevado;
  - iluminação inadequada;
  - ausência de privacidade do paciente;
  - incapacidade de o paciente se comunicar adequadamente no meio utilizado para o teleatendimento;
  - trajes inadequados;
  - situação de risco, como estar na direção de veículo em movimento, caminhando, ou em área exposta a perigos;
  - paciente sob responsabilidade de outro serviço médico (como, por exemplo, paciente admitido em internação hospitalar ou durante atendimento médico presencial).

- Toda teleconsulta deve ser adequadamente registrada em prontuário. Isto inclui a descrição da consulta completa, que inclui, mas não se limita, a:
  - queixa e duração;
  - anamnese e exame clínico;
  - descrição e análise de documentos, textos e imagens enviados;
  - hipótese diagnóstica (preferencialmente utilizando CID-10 ou equivalente mais apropriado à especialidade ou mais atualizado);
  - impressão clínica e prognóstico;
  - plano terapêutico, orientações e documentos emitidos.

- A teleconsulta por videochamada é frequentemente suficiente para orientação médica geral, atendimento médico em primeira consulta, seguimento clínico de doenças agudas ou crônicas, solicitação/avaliação de exames complementares, ajuste terapêutico e definição terapêutica. Caberá ao médico assistente a responsabilidade sobre a viabilidade da tomada de decisão técnica diante das informações obtidas, sempre com o consentimento amplamente esclarecido do paciente.

3.3.3. Requisitos de segurança no atendimento por videochamada

Visando garantir máxima segurança e qualidade à prática da telemedicina por áudio e vídeo em tempo real, a **Saúde Digital Brasil** recomenda as seguintes boas práticas em segurança nos atendimento por vídeochamadas:

- A identificação adequada do paciente é a primeira meta internacional de segurança em serviços de saúde. O acesso do paciente e do profissional de saúde devem ser verificados por **login e senha previamente cadastrados e validados ou biometria**, preferencialmente com mais de um fator de autenticação.
- A estabilidade de conexão e a qualidade de áudio e vídeo devem ser verificadas previamente ao atendimento por sistema automatizado ou por profissional habilitado do serviço provedor de telemedicina.

3.3.4.Registro e documentação do atendimento por videochamada

A prática da telemedicina por áudio e vídeo em tempo real, em sendo equivalente a um atendimento presencial, possui os mesmos requisitos de registro e documentação que o atendimento presencial. No entanto, com a disponibilidade de ferramentas de registro digitais e a necessidade de identificação adequada dos profissionais, a **Saúde Digital Brasil** recomenda as seguintes boas práticas no registro e documentação de atendimentos por vídeochamada:

- Se optado pela transcrição integral dos áudios, recomenda-se a utilização de software validado para transcrição automatizada de áudio em português (speech-to-text), com anexação ao PEP através de integração automatizada.
- **Não se recomenda a gravação e anexação dos arquivos dos vídeos completos**, a fim de proteger a privacidade do paciente e característica personalíssima da relação médico-paciente. Em caso de registro de pequenos trechos com finalidade assistencial, além do expresso consentimento do paciente, recomenda-se que o acesso às gravações seja altamente restrito, com rigoroso controle de acesso. O manejo dos arquivos deve seguir as melhores práticas em segurança da informação relacionada à saúde, incluindo, mas não se limitando, ao tráfego e ao armazenamento criptografados de dados, a fim de preservar a privacidade de profissionais de saúde e pacientes, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD).

Não se recomenda a gravação e anexação dos arquivos dos vídeos completos, a fim de proteger a privacidade do paciente e característica personalíssima da relação médico-paciente

- Em caso de acompanhamento ou orientação por profissional não médico, o atendimento por videochamada pode ser registrado e ter seus detalhes inseridos no PEP diretamente pelo profissional de saúde, o que inclui, mas não se limita, à descrição do caso, impressões técnicas e sugestões ou orientações fornecidas.
- Em caso de teleconsulta, as informações técnicas do atendimento podem ser incluídas diretamente no PEP como em uma consulta presencial. Recomenda-se incluir a descrição da queixa e duração, anamnese, exame clínico, impressões clínicas, orientações fornecidas e, quando pertinente, hipótese diagnóstica e/ou prescrição.

4. DISPOSITIVOS DE PROPEDÊUTICA AVANÇADA POR TELEMEDICINA

Denomina-se ***propedêutica clínica*** o conjunto de técnicas e procedimentos pelos quais um paciente pode ser examinado, visando a construção de um raciocínio clínico que permita uma boa decisão diagnóstica ou terapêutica. Tradicionalmente aprendida e ensinada à beira-leito, a propedêutica clínica tem sido ressignificada para permitir sua execução à distância, através de tecnologias de comunicação e transmissão remota de sons, imagens e outros dados clínicos mensuráveis. Esta evolução leva o nome de ***telepropedêutica***, termo que abrange as técnicas, manobras e dispositivos que permitem o exame clínico via telemedicina.

Os dispositivos de telepropedêutica já inerentes à própria prática da telemedicina são o ***microfone*** e a ***câmera***, seja para áudio e vídeo em tempo real ou para obtenção de áudios ou imagens enviadas de forma assíncrona. Através destes dispositivos já é possível a realização de grande parte do exame clínico, incluindo o exame do estado mental, através da análise da fala e da inspeção visual do paciente (ectoscopia).

A telepropedêutica abrange as técnicas, manobras e dispositivos que permitem o exame clínico via telemedicina.

No entanto, novos sensores e inovações têm permitido o desenvolvimento de dispositivos que ampliam sobremaneira a capacidade propedêutica do teleatendimento, em especial na modalidade de videochamada, permitindo ampliação progressiva do escopo da telemedicina e melhor acurácia diagnóstica. A utilização destes novos dispositivos e técnicas, com a finalidade de complementar o exame clínico por telemedicina, será aqui denominada ***PAT: Propedêutica Avançada por Telemedicina***. Considera-se propedêutica avançada toda a coleta de informações feita com uso de equipamentos auxiliares que não apenas a câmera e o microfone.

São exemplos de dispositivos de propedêutica avançada por telemedicina:

- Aparelhos domiciliares de obtenção de dados clínicos e sinais vitais, como balanças, termômetros, oxímetros, glicosímetros e medidores automáticos de pressão arterial, cujas aferições podem ser transmitidas diretamente ou verbalmente à equipe assistencial.
- Câmeras de alta definição portáteis, com lentes ou adaptadores que permitem avaliação de oroscopia, rinoscopia, otoscopia, dermatoscopia, fundoscopia, entre outras avaliações visuais especializadas.
- Estetoscópios digitais, que permitem ausculta cardíaca, pulmonar, vascular ou abdominal. Alguns estetoscópios permitem a obtenção de traçados de eletrocardiograma de única derivação.
- Dispositivos vestíveis ("*wearables*"), como pulseiras e *smartwatches* que possuem biossensores e permitem o monitoramento da frequência cardíaca e ritmo do coração, sono, movimento, atividade física, equilíbrio, saturação de oxigênio no sangue, entre outros dados, em crescente evolução e disponibilidade.
- Ultrassom portátil, doppler vascular portátil.
- Uso do acelerômetro e de smartphones ou dispositivos especializados para avaliações neurológicas ou ortopédicas específicas envolvendo movimento e coordenação.

Dispositivos de telepropedêutica avançada ampliam as capacidades do atendimento à distância

Com relação ao uso de dispositivos de propedêutica avançada por telemedicina, a **Saúde Digital Brasil** recomenda as seguintes boas práticas:

- O exame físico realizado através do microfone e câmera já são suficientes para a boa prática da teleconsulta por videochamada. O uso de dispositivos de propedêutica avançada por telemedicina é bem vindo e pode constituir método complementar para ampliar as capacidades diagnósticas da teleconsulta. No entanto, seu uso não deve constituir pré-requisito para o atendimento em geral.
- Sempre que possível e pertinente devem ser obtidos sinais vitais como temperatura, frequência cardíaca, frequência respiratória, pressão arterial, oximetria, glicemia capilar e escala de dor. A interpretação dos dados deve considerar a qualidade do equipamento, da aferição, homologação em órgãos regulatórios e capacidade de informação do paciente.
- Para situações específicas, como avaliação otológica, lesões dermatológicas pigmentadas ou outras situações específicas, a disponibilização dos dados provenientes de dispositivos de propedêutica avançada pode ser necessária para o diagnóstico clínico, mas não impede o direcionamento do paciente ao serviço adequado e a adoção de medidas terapêuticas preliminares.
- Recomenda-se que os dados provenientes de dispositivos de telepropedêutica estejam integrados ao sistema de prontuário eletrônico do paciente, e a transmissão e armazenamento dos dados garantam a segurança da informação conforme a Lei Geral de Proteção de Dados Pessoais (LGPD).

5. PROTOCOLOS CLÍNICOS

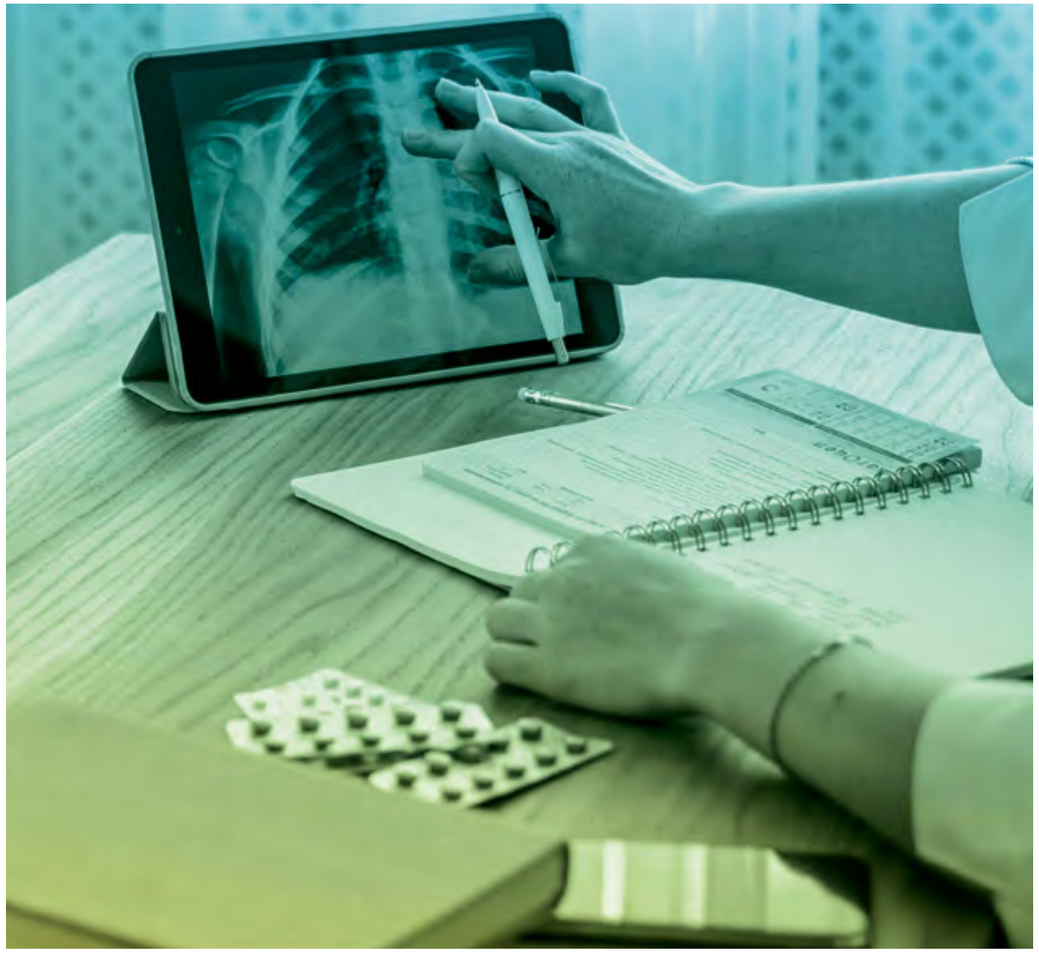
As condutas terapêuticas prescritas nas teleconsultas devem ser pautadas num paradigma de Medicina Baseada em Evidências

A Saúde Digital Brasil entende que as condutas terapêuticas prescritas nas teleconsultas, quando pertinentes, devem ser pautadas num paradigma de Medicina Baseada em Evidências, exatamente como no atendimento presencial. Sempre que possível, ***protocolos clínicos*** devem ser elaborados pelos serviços de telemedicina, seguindo as normas vigentes para a implantação de protocolos e diretrizes assistenciais, de forma a serem facilmente disponibilizados à equipe assistencial.

Com relação aos protocolos clínicos para uso em telemedicina direta ao paciente, a **Saúde Digital Brasil** recomenda as seguintes boas práticas:

- A adoção de protocolos clínicos e a aferição de sua aderência pela equipe e de seus resultados devem ser entendidos num contexto mais amplo de Qualidade e Segurança do Paciente.
- O julgamento clínico individual deve prevalecer sobre os protocolos vigentes, sempre que o profissional assim entender necessário, com base em sua experiência e com base nas particularidades do caso concreto, responsabilizando-se por suas condutas tal qual ocorre no atendimento presencial.
- É imperativo que os serviços de telemedicina preservem a **autonomia total e irrestrita do médico** em optar por encaminhar o paciente para avaliação presencial. Deve-se evitar a presença de incentivos ou penalizações que possam, mesmo de forma subjetiva, desencorajar o médico a encaminhar para avaliação presencial qualquer paciente atendido por telemedicina.

- Recomenda-se que os protocolos clínicos institucionais e/ou de sociedades médicas contenham os seguintes itens:
  - **CONDIÇÃO DE INTERESSE** (CID-10 ou código mais apropriado à especialidade e descrição);
  - **CRITÉRIOS DE TRIAGEM DE SITUAÇÕES DE URGÊNCIA/EMERGÊNCIA**, para encaminhamento breve/imediato ao serviço de pronto atendimento presencial;
  - **CRITÉRIOS DE ELEGIBILIDADE PARA A CONDUÇÃO POR TELEMEDICINA**, em suas várias modalidades (vídeo, telefone, chat, etc.);
  - **INFORMAÇÕES IMPORTANTES** a serem obtidas durante a anamnese;
  - **PARÂMETROS IMPORTANTES** a serem obtidos durante o exame físico por telemedicina, tais como:
    - indicações de manobras propedêuticas que possam ser realizadas pelo paciente sob orientação do profissional de saúde e que sejam relevantes para o referido protocolo;
    - indicações de dispositivos de propedêutica avançada por telemedicina que podem ser utilizados pelos pacientes no contexto do protocolo;
    - registro fotográfico de lesões cutâneas ou similares, os quais possam auxiliar no raciocínio clínico e na documentação das lesões, a serem anexados ao prontuário do paciente;



  - **CRITÉRIOS DE ELEGIBILIDADE PARA A PRESCRIÇÃO E CONTINUIDADE DO TRATAMENTO POR TELEMEDICINA.**
  - **DIAGNÓSTICOS DIFERENCIAIS** a serem considerados;
  - **SUGESTÕES DE CONDUTAS**, incluindo o encaminhamento presencial quando necessário;
  - **SINAIS DE ALERTA**, quando pertinentes, de modo a serem devidamente orientados aos pacientes via teleconsulta, apontando para o atendimento presencial ou o retorno por telemedicina quando indicado.

6. EMISSÃO DE DOCUMENTOS MÉDICOS E PRESCRIÇÃO POR TELEMEDICINA

É parte integrante da teleconsulta a emissão e disponibilização ao paciente de documentos médicos tais como prescrições, pedidos de exames, relatórios, laudos, encaminhamentos, entre outros. Para garantir a máxima qualidade e segurança necessários à prática da telemedicina direta ao paciente, a **Saúde Digital Brasil** recomenda as seguintes boas práticas:

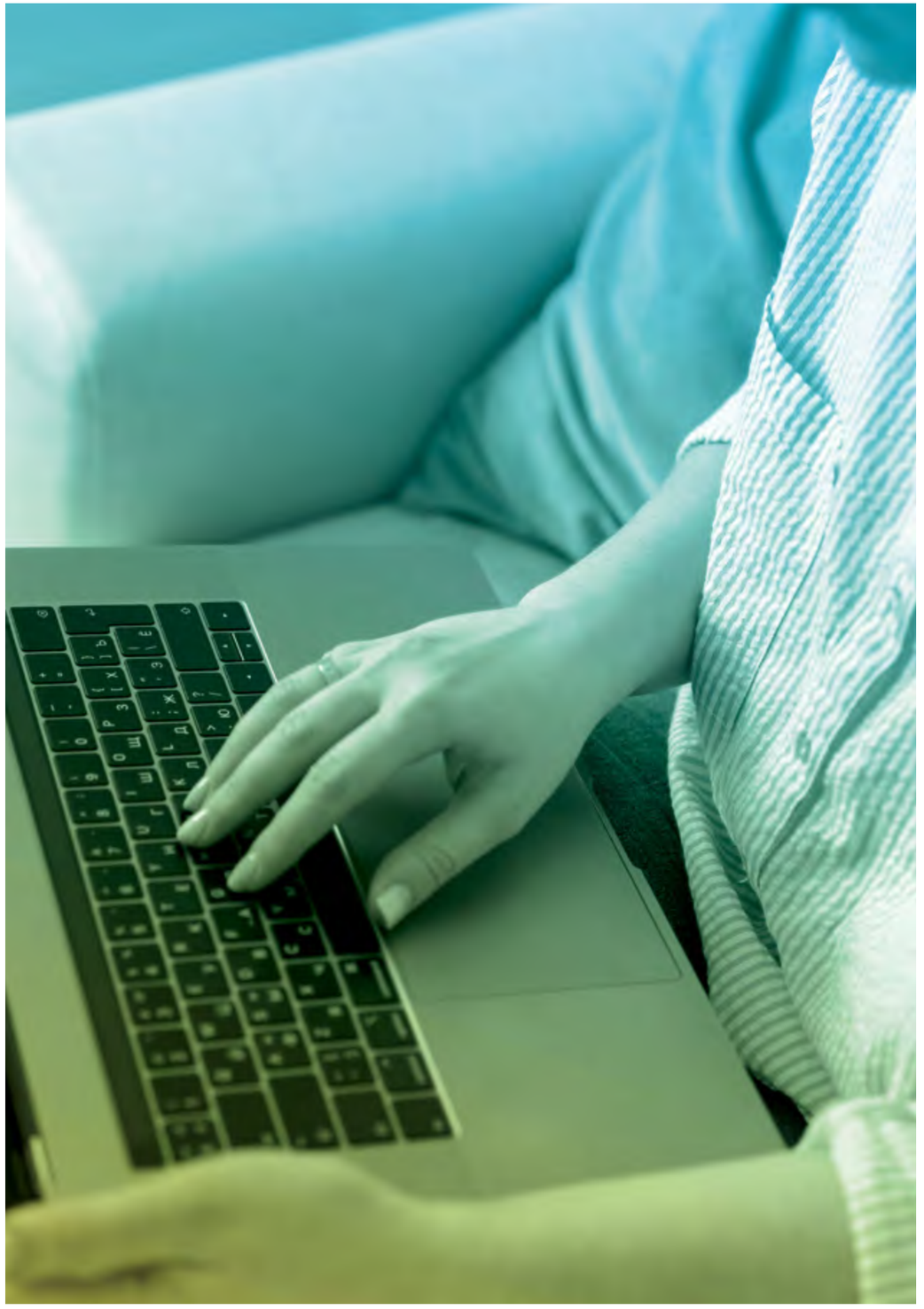
- Quando enviados ou disponibilizados ao paciente relatórios médicos, atestados, prescrições ou outros documentos médicos, estes devem ser assinados digitalmente de forma a garantir a identidade do emissor, autenticidade, veracidade e irrevogabilidade do conteúdo e data/hora de emissão. Os modelos tecnológicos de certificação dos documentos médicos devem seguir as normas e diretrizes dos órgãos e agências regulatórias pertinentes.
- Os documentos médicos resultados de teleconsulta e assinados digitalmente podem ser disponibilizados aos pacientes através de aplicações web. Neste caso, devem ser adequadamente armazenados, criptografados e protegidos por login e senha previamente cadastrados e validados ou biometria, preferencialmente com mais de um fator de autenticação.

- Os documentos médicos resultados de teleconsulta e assinados digitalmente podem também ser enviados ao paciente por meio eletrônico (e-mail, SMS, MMS, aplicativos de mensagens instantâneas ou similares), seja através de link para aplicações web ou através do envio do documento original. Neste caso, o endereço de e-mail ou número de telefone devem ter sido adequadamente verificados através de cadastramento prévio, e o arquivo ou acesso por link devem preferencialmente estar protegidos por senha ou código pessoal.

- Recomenda-se que os documentos médicos assinados digitalmente, particularmente prescrições, atestados e pedidos de exames, sejam desenhados para transação em formato totalmente digital. Quando forem impressos, é necessário que conste código para possibilitar o download do documento em formato digital original e validação da assinatura digital.

- É recomendado que o acesso pelo paciente à documentação resultante do teleatendimento possa ser monitorado e assegurado. Deve-se dispor de meios de contato ágeis e suporte técnico durante todo o horário de funcionamento do serviço em caso de problemas de acesso à documentação eletrônica.

Recomenda-se que os documentos médicos assinados digitalmente sejam desenhados para transação em formato totalmente digital.



7. CONTROLE DE QUALIDADE DOS PROCESSOS DE TELEATENDIMENTO

A qualidade dos processos de atendimento por telemedicina está intimamente relacionada à entrega de um serviço de saúde com valor agregado tanto para pacientes como para provedores e sistema de saúde. Alguns princípios devem ser norteadores para a prestação de um serviço de telemedicina direta ao paciente de qualidade, tais como:

- eficiência
- eficácia
- equidade
- segurança do paciente
- assistência focada no paciente e em tempo adequado

Todos são aplicáveis na prestação de serviço remoto e devem ser medidos e monitorados através de indicadores com metas bem definidas. As seguintes boas práticas em controle de qualidade de processos assistenciais em telemedicina direta ao paciente são recomendadas pela **Saúde Digital Brasil**:

- Os treinamentos dos profissionais envolvidos no teleatendimento devem ser sistematizados, padronizados e registrados adequadamente em um instrumento de *onboarding*. Há a necessidade de tanto um treinamento técnico como comportamental, focado na conformidade, etiqueta e atitude no uso de ferramentas de comunicação digital.

- Indicadores de eficiência e qualidade devem ser acompanhados, com *feedback* individual inicial e periódico.
- É importante estabelecer quais indicadores medir, estabelecer métricas, se necessário incorporar instrumentos e validar nos sistemas a gênese dos dados a serem considerados. A decisão dos indicadores a serem incorporados nos serviços é de suma importância. Por isso, sugere-se estratificar os indicadores de processo, de estrutura e de resultado.

O Net Promoter Score (NPS) é um dos principais parâmetros objetivos de satisfação do paciente.

- Os resultados devem ser consolidados periodicamente e serem disponibilizados aos envolvidos, gestores, equipe operacional e clientes. Já os resultados individualizados devem ser sigilosos e utilizados com respeito à ética, privacidade e com a finalidade de melhoria da assistência.
- Recomenda-se o acompanhamento da satisfação dos pacientes e profissionais beneficiários dos serviços de telemedicina para garantir a qualidade dos serviços. Parâmetros objetivos de satisfação e lealdade como o *Net Promoter Score* (NPS) são comumente utilizados para monitorar esse indicador.

8. URGÊNCIAS E EMERGÊNCIAS

A caracterização de um caso como URGÊNCIA ou EMERGÊNCIA é atribuição do profissional de saúde responsável pelo atendimento ou triagem e direcionamento.

O Conselho Federal de Medicina, através da Resolução nº 1451/1995, define URGÊNCIA como "a ocorrência imprevista de agravo à saúde com ou sem risco potencial de vida, cujo portador necessita de assistência médica imediata" e EMERGÊNCIA como "constatação médica de condições de agravo à saúde que impliquem em risco iminente de vida ou sofrimento intenso exigindo, portanto, tratamento médico imediato".

No atendimento por telemedicina direta ao paciente, é possível que sejam verificadas condições clínicas definidas como URGÊNCIAS ou EMERGÊNCIAS médicas, situações que por definição necessitam de avaliação médica imediata. A caracterização de um caso como URGÊNCIA ou EMERGÊNCIA é atribuição do profissional de saúde responsável pelo atendimento ou triagem e direcionamento.

Assim, a **Saúde Digital Brasil** recomenda as seguintes boas práticas em situações de urgência e emergência:

- Algoritmos automatizados que utilizam árvores de decisão ou métodos mais avançados de inteligência artificial e comunicação robotizada podem ser úteis como ferramentas de direcionamento primário. Entretanto, não devem constituir obstáculo definitivo ao acesso aos serviços oferecidos ou impedir o contato com um profissional de saúde disponível.
- Os profissionais envolvidos no direcionamento de pacientes devem possuir treinamento específico, e protocolos bem definidos devem ser estabelecidos, preferencialmente desenhados e supervisionados por enfermeiro ou médico.
- Em serviços de telemedicina direta ao paciente que se proponham a atender situações agudas sob demanda espontânea, recomenda-se a disponibilização de meios de direcionamento e encaminhamento de pacientes cuja situação clínica tenha sido caracterizada como URGÊNCIA ou EMERGÊNCIA.
- Caso seja necessário interromper o teleatendimento atual ou encaminhar o paciente a outro serviço (presencial ou remoto), o profissional deve procurar explicar ao paciente as motivações técnicas para tal e orientá-lo a respeito dos procedimentos administrativos necessários para a continuidade do tratamento (ou indicar o canal mais apropriado para obter estas informações).

Protocolos bem definidos devem ser estabelecidos, preferencialmente desenhados e supervisionados por enfermeiro ou médico.

- A constatação de situação clínica como URGÊNCIA ou EMERGÊNCIA deve ser confirmada por médico ou enfermeiro.
- Os pacientes que se enquadrem em situações clínicas definidas como URGÊNCIA ou EMERGÊNCIA médica devem ser encaminhados imediatamente para uma avaliação presencial.
- Os profissionais de saúde envolvidos no atendimento de situações clínicas que foram definidas como URGÊNCIA ou EMERGÊNCIA devem usar de todos os meios necessários para garantir que o paciente tenha compreendido adequadamente a indicação de procurar um atendimento presencial imediato.
- A caracterização do caso como URGÊNCIA ou EMERGÊNCIA deve ser registrada adequadamente em prontuário médico e assinada digitalmente, com nome e número do registro do conselho de classe do profissional responsável.
  - Os dados clínicos relevantes e registro da recomendação e compreensão do encaminhamento para atendimento presencial de urgência devem fazer parte, como rotina, do prontuário, assim como em casos não urgentes.

9. POPULAÇÕES ESPECIAIS

A SDB recomenda a adoção de mecanismos para garantir a inclusão de pacientes pediátricos, idosos e pacientes com necessidades especiais.

O atendimento médico por telemedicina tem como uma das grandes vantagens a ampliação do acesso à saúde, reduzindo a necessidade de deslocamentos e possibilitando maior disponibilidade de contato com profissionais de saúde.

No entanto, grupos etários específicos e pacientes com necessidades especiais podem ter alguma dificuldade de acesso a serviços de telemedicina, seja por dificuldade no manejo da tecnologia, seja por limitações de comunicação.

A **Saúde Digital Brasil** recomenda como boa prática a todos os serviços de telemedicina direta ao paciente a adoção de mecanismos para garantir a inclusão de pacientes pediátricos, idosos e pacientes com necessidades especiais, seguindo as seguintes recomendações:

- **PACIENTES PEDIÁTRICOS** Recomenda-se que todos os pacientes com menos de 16 anos sejam acompanhados durante o atendimento por um responsável maior de idade, cujo nome e parentesco devem ser devidamente registrados no prontuário.
- **PACIENTES IDOSOS** Recomenda-se que haja treinamento da equipe de suporte técnico e o desenvolvimento de protocolos para atendimento de população idosa, em especial para garantir o adequado uso da tecnologia.

  Recomenda-se que idosos com dificuldades cognitivas sejam acompanhados durante o atendimento por um responsável maior de idade, cujo nome e parentesco devem ser devidamente registrados no prontuário.

PACIENTES COM DEFICIÊNCIA AUDITIVA Recomenda-se que haja treinamento da equipe de suporte técnico e o desenvolvimento de protocolos para atendimento de portadores de deficiência auditiva, em especial para garantir o adequado uso da tecnologia, como atendimento utilizando mensagens de texto ou LIBRAS.

Na ausência de mecanismos de atendimento por mensagem de texto ou LIBRAS, recomenda-se que um acompanhante maior de idade seja intermediário das informações prestadas, garantindo comunicação adequada.

A inclusão de pacientes com necessidades especiais é particularmente viável pela telemedicina

PACIENTES COM DEFICIÊNCIA VISUAL Recomenda-se que haja treinamento da equipe de suporte técnico e o desenvolvimento de protocolos para atendimento de portadores de deficiência visual, em especial para garantir o adequado uso da tecnologia.

Na ausência de mecanismos de atendimento a portadores de deficiência visual, recomenda-se que um acompanhante maior de idade seja intermediário das informações prestadas, garantindo comunicação adequada.

PACIENTES COM DEFICIÊNCIA COGNITIVA Recomenda-se que haja treinamento da equipe de suporte técnico e o desenvolvimento de protocolos para atendimento de portadores de deficiência cognitiva, em especial para garantir o adequado uso da tecnologia.

Na ausência de mecanismos de atendimento a portadores de deficiência cognitiva, recomenda-se que um acompanhante maior de idade seja intermediário das informações prestadas, garantindo comunicação adequada.

10. CADASTRAMENTO E ELEGIBILIDADE

A verificação da eligibilidade do paciente aos serviços é aspecto fundamental da jornada pelos serviços de telemedicina

A fim de garantir a sustentabilidade econômico-financeira dos provedores de serviços de telemedicina direta ao paciente, o acesso aos sistemas deve ser restrito a pacientes adequadamente elegíveis. A elegibilidade deve ser previamente determinada em contratos e termos cuja anuência tenha sido garantida pelo paciente ou fonte pagadora do serviço.

A **Saúde Digital Brasil** recomenda as seguintes boas práticas de cadastramento e verificação de elegibilidade para acesso aos serviços da telemedicina.

- O paciente deve realizar um cadastramento para ter sua identidade verificada através da análise de conjuntos de dados pessoais ou conferência de documentos.
- A elegibilidade pode ser aferida em bases de dados do provedor ou por consulta a mecanismos de verificação disponibilizados pelas fontes pagadoras, através de dados cadastrais como CPF, e-mail, número de telefone, número da carteirinha da operadora de saúde ou outro identificador, de forma manual ou automatizada.
- Entre os critérios de elegibilidade podem também constar perfil etário do paciente, presença de responsável durante o atendimento e critérios clínicos ou de urgência/emergência, conforme a característica do serviço disponibilizado. Convém que tais critérios estejam bem definidos no momento da celebração dos contratos de prestação de serviço ou termos de adesão.

11. CONCLUSÕES

A prática da telemedicina diretamente ao paciente é um método de prestação de serviços de saúde que pode prover acesso à saúde com segurança e qualidade, usando tecnologias de comunicação amplamente disponíveis. No Brasil, ganhou adoção maciça após março de 2020 com a pandemia de Covid-19 e regulação através de decreto presidencial.

Este Manual recomenda que os preceitos éticos fundamentais à prática da medicina em sua forma tradicional, presencial, sejam observados plenamente na telemedicina.

O presente Manual de Boas Práticas tem por finalidade disseminar boas práticas em telemedicina direta ao paciente que são seguidas pelos membros associados à Saúde Digital Brasil em avaliações médicas e de enfermagem à distância. Este documento aborda a teleconsulta, definida como o atendimento de pacientes por profissional médico, e também o atendimento de enfermagem na avaliação, orientação e acolhimento dos pacientes atendidos por telemedicina. Optou-se também por separar, a depender do meio de telecomunicação utilizado, os atendimentos por telemedicina em três modalidades: assíncronos (por mensagens de texto, imagens e áudio), telefônicos (por áudio) e por videoconferência.

Este Manual recomenda que os preceitos éticos fundamentais à prática da medicina em sua forma tradicional, presencial, sejam observados plenamente na telemedicina, com ênfase na relação profissional-paciente e atenção à documentação adequada do atendimento. Todos os dados clínicos devem ser cuidadosamente documentados, inclusive os dados do exame clínico realizado por telemedicina, recomendado a todos os atendimentos telefônicos e por videoconferência.

A **Saúde Digital Brasil** se compromete com a qualidade dos prontuários, com mecanismos que permitam sua avaliação constante e recomenda que protocolos clínicos sejam desenvolvidos para garantir a segurança do paciente nos atendimentos, e que sejam disponibilizados facilmente aos profissionais que atuam no serviço.

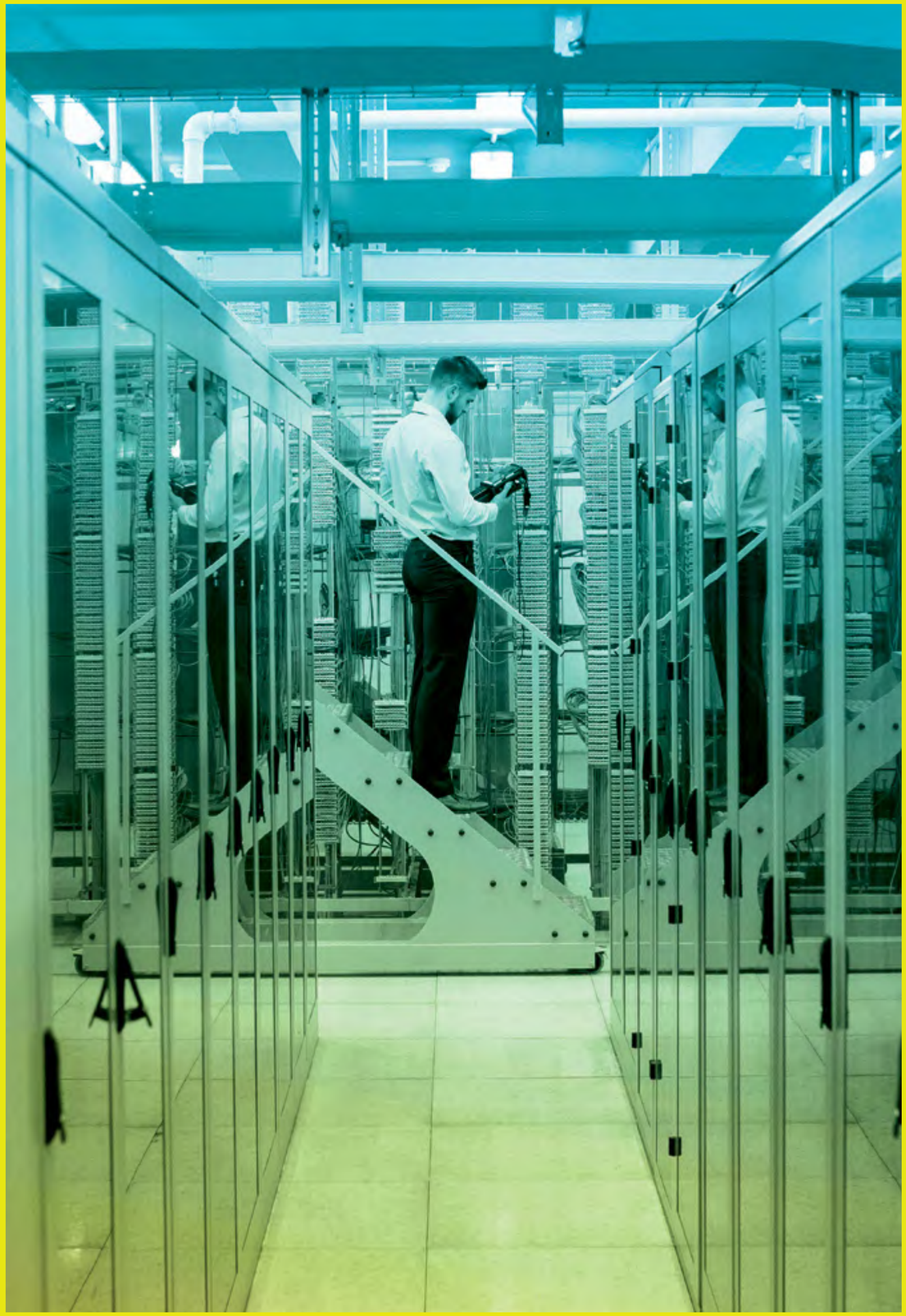
Com relação às modalidades de telemedicina, há recomendações distintas para o escopo do atendimento. Para o atendimento por mensagens assíncronas de áudio, texto e imagens recomenda-se preferência para seguimento de casos já atendidos por outras modalidades, assim como orientações gerais e acolhimento. Da mesma forma, o atendimento telefônico também é preferido para seguimento de pacientes já acompanhados, com maior flexibilidade de tomada de decisão, permitindo primeiras consultas para casos simples, conforme indicação médica. Nos dois casos acima não se recomenda um seguimento de longo prazo, acompanhamento de doenças complexas, tampouco emissão de laudos trabalhistas ou receitas de uso contínuo.

A videoconferência é considerada uma ferramenta que permite uma teleconsulta completa, com exame físico detalhado e possibilidade de criação de vínculo adequado com o paciente.

A videoconferência por sua vez, é considerada uma ferramenta que permite uma teleconsulta completa, com exame físico detalhado e possibilidade de criação de vínculo adequado com o paciente. Cabe ao médico decidir se a ausência física do paciente é impeditiva para sua tomada de decisão e é imperativo que tenha total autonomia para encaminhar o paciente a uma consulta presencial caso assim se faça necessário. Ademais, a incorporação constante de novas tecnologias de propedêutica avançada possibilitará ainda maior resolutividade da telemedicina, com o aprimoramento da avaliação clínica à distância.

Com relação às plataformas tecnológicas utilizadas, este Manual também recomenda a todos os prestadores de telemedicina uma atenção especial à segurança da informação, atendendo à LGPD, além de recomendar um compromisso com o desenvolvimento de mecanismos de interoperabilidade das informações, vital para a sustentabilidade dos sistemas de saúde. Recomenda-se também que as plataformas cumpram todos os requisitos estabelecidos pelas autoridades competentes para emissão de atestados, receitas e outros documentos.

Em suma, este documento demonstra o compromisso dos membros da Saúde Digital Brasil com a qualidade do cuidado, a segurança do paciente e de suas informações, e com a prática ética e responsável da medicina. O intuito é disseminar este compromisso entre todos os prestadores do país, de forma a garantir a melhor experiência possível aos pacientes.



CAPÍTULO**02**

SEGU-RANÇA DA INFOR-MAÇÃO

1. ESCOPO

A segurança da informação, a proteção dos dados pessoais e a privacidade são indissociáveis e de extrema relevância para todo o ecossistema de saúde.

Este Manual de Boas Práticas de Segurança da Informação foi criado com o intuito de contribuir para o ecossistema de saúde digital brasileiro, de modo a abranger todos os associados da Saúde Digital Brasil (SDB) e, além disso, transcender os limites de atuação da SDB para guiar o horizonte regulatório sobre o tema no país.

Por meio deste manual, objetiva-se que os players dos setores público e privado possam construir suas atividades de saúde digital alicerçados pelas melhores práticas de segurança da informação vigentes no mercado, em linha com o entendimento expressamente previsto no artigo 50, caput, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), que autoriza aos entes privados a formulação de regras de boas práticas e de governança sobre as condições de organização e gestão da segurança da informação e da proteção dos dados pessoais.

Entendemos que a segurança da informação, a proteção dos dados pessoais e a privacidade são indissociáveis e de extrema relevância para todo o ecossistema de saúde, sobretudo no âmbito da saúde digital, devendo ser entendidas como padrões a serem seguidos por todas as organizações do setor, ainda que de formas diversas e adaptadas ao porte de cada organização.

2. BOAS PRÁTICAS INTERNAS DE SEGURANÇA DA INFORMAÇÃO

As boas práticas internas de segurança da informação na organização começam pelo comprometimento dos colaboradores e pelo apoio da alta gestão.

O comprometimento e entendimento dos colaboradores, no que diz respeito à segurança da informação, têm que transcender a vida profissional e expandirem-se para a vida pessoal, pois só assim o colaborador irá compreender a importância do assunto nesta era digital.

Todo tipo de política, treinamento e procedimento precisa ser aprovado e compartilhado pela alta gestão.

Todo tipo de política, treinamento e procedimento precisa ser aprovado e compartilhado pela alta gestão, para ser validada a devida importância.

Em relação a políticas, procedimentos, auditorias e tudo o que precisa ser revisado, atualizado ou medido periodicamente, precisa ser levada em conta a melhoria contínua como fator primordial.

3. CULTURA DE PRIVACIDADE E CONSCIENTIZAÇÃO

A disponibilização de treinamento acerca das boas práticas de segurança da informação é essencial para mitigação de riscos e redução da exposição.

A criação de uma cultura de privacidade e segurança da informação nas organizações é um dos pilares mais importantes para o desenvolvimento de uma segurança da informação pujante, tendo em vista que a capacitação de pessoal pode repercutir na disseminação de boas práticas entre as diversas áreas da organização.

Além disso, a disponibilização de treinamentos acerca das boas práticas de segurança da informação é essencial para mitigação de riscos e redução da exposição, sobretudo em relação a ameaças cibernéticas, compartilhamentos de dados não autorizados e manejo das ferramentas disponibilizadas pela organização aos seus colaboradores.

No entanto, a segurança da informação não se limita a resguardar a organização de ameaças cibernéticas. A criação de uma cultura de proteção da informação está ligada, sobretudo, ao bom e adequado funcionamento da organização como um todo, de forma a garantir o seu desenvolvimento positivo.

Para que isso ocorra, a gestão da organização deve absorver como política interna os pilares da segurança da informação, traduzidos na *disponibilidade, integridade, confidencialidade, legalidade, auditabilidade e não repúdio da autoria*.

Isso significa dizer que, para a implementação de uma cultura eficaz de segurança da informação, a organização deve manter suas informações acessíveis aos colaboradores, conforme a necessidade de acesso, com alto nível de confiabilidade, de acordo com as normas legais internas e externas, registradas e rastreáveis segundo a autoria.

Deste modo, é fundamental restringir o acesso às informações conforme a necessidade da própria organização. Em conjunto com a conscientização de todos os colaboradores sobre os deveres éticos e legais no manuseio de dados e informações, a concessão de permissões por usuário auxilia na manutenção do controle e da confiabilidade das informações produzidas e importadas.

A conscientização dos usuários se inicia, antes mesmo dos treinamentos individuais, na percepção do colaborador sobre a própria cultura organizacional. A elaboração e disseminação de manuais de boas práticas, política interna de segurança da informação, código de ética, regimentos internos, servem para, além de instruir o usuário, demonstrar a seriedade e preocupação da alta gestão com o desenvolvimento saudável da organização. Provocar o sentimento de responsabilidade nos colaboradores também faz parte da conscientização e do treinamento institucional.

Provocar o sentimento de responsabilidade nos colaboradores também faz parte da conscientização e do treinamento institucional.

Isso reflete tanto internamente, quanto externamente. A criação de uma cultura de privacidade e segurança da informação, além de trazer estabilidade na gestão operacional, auxilia na gestão de riscos, no tratamento de não conformidades, no mapeamento estratégico, na elaboração de indicadores de desempenho, além de credibilizar a organização frente ao mercado.

4. QUAIS SÃO OS PASSOS INICIAIS?

Um dos principais erros na estratégia de segurança da informação é querer tratar todos os riscos

Identificar os principais riscos para o negócio relacionados à segurança da informação é o primeiro passo. O escopo inicial nesse processo de mapeamento dos riscos deve focar os ativos mais críticos da empresa, ou seja, as tecnologias, os processos e as pessoas que de alguma forma tratam os dados críticos da empresa. Exemplos de ativos críticos são servidores que custodiam dados pessoais, sensíveis, confidenciais, qualquer dado que exposto ou acessado arbitrariamente pode gerar impactos significativos para o negócio: perda financeira, reputação, descumprimento regulatório.

Segurança 100% é o ideal, porém, mesmo com sistemas ultra sofisticados, muito difícil de ser atingida. É por esse motivo que devemos priorizar o tratamento dos riscos mais críticos, aqueles que, se materializados, causarão algum dano ao negócio, além de manter um sistema de vigilância constante.

5. O QUE PRECISO PARA ESTRUTURAR A SEGURANÇA DA INFORMAÇÃO?

Para tratar os riscos inerentes aos negócios de uma empresa, é fundamental que uma área seja devidamente estruturada com suporte de tecnologias, processos e pessoas capacitadas para garantir a confidencialidade, integridade e disponibilidade das informações.

Utilizando guias de referência de mercado, como a ISO 27001 e o Cybersecurity Framework NIST, o responsável por essa área vai estruturá-la levando em consideração o tamanho e o tipo do negócio. Para que essa iniciativa tenha sucesso, é fundamental o patrocínio correto, ou seja, o apoio da alta direção para que as diretrizes e os investimentos necessários sejam atendidos.

É fundamental o apoio da Alta Direção para que as diretrizes e os investimentos necessários sejam atendidos.

6. QUAIS VANTAGENS A EMPRESA TÊM EM UTILIZAR AS FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO?

Sem processos e treinamento das pessoas, as tecnologias de segurança não serão efetivas em seu propósito.

Não é possível proteger as informações das empresas sem a implantação de tecnologias para esse propósito. Para cada cenário de riscos e ameaças que foram mapeadas, há diversas tecnologias disponíveis que objetivam proteger a empresa bloqueando e/ou contendo as ameaças que buscam acesso não autorizado a esses ativos de valor para a empresa.

Para proteger as informações, para detectar tentativas de acessos não autorizados aos ativos de valor e ser capaz de conter os ataques cibernéticos, não é possível tratar esses diferentes cenários sem o uso da tecnologia de segurança adequada. Proteger os ativos de valor significa implantar diferentes tecnologias que, de forma integrada, amenizarão o risco de vazamento e/ou a indisponibilidade de acesso a informações, por exemplo. A adoção de tecnologias é fundamental em uma estratégia de segurança, mas, sem processos e treinamento das pessoas, essas tecnologias não serão efetivas em seu propósito.

7. *STARTUP* – QUE TIPO DE FERRAMENTAS INICIAIS SÃO NECESSÁRIAS?

Ao começarmos uma empresa, geralmente não temos muitas regras e processos, com isso o ambiente pode se tornar desorganizado e desafiador para um futuro próximo. Tendo essa premissa, seguem algumas ferramentas e processos que gerarão maturidade no ambiente desde o início de sua operação:

1.ANÁLISE DE VULNERABILIDADE EM CÓDIGO USANDO FERRAMENTAS SAST (STATIC APPLICATION SECURITY TESTING), EXEMPLOS DE FERRAMENTAS SAST:

- Sonar Qube
- Veracode
- Safety

A vantagem de se usar o SAST em seus projetos é que ele é altamente eficiente em achar vulnerabilidades antes de suas aplicações serem publicadas, é escalável em sua pipeline de desenvolvimento e tem um custo baixo de manutenção por existirem excelentes ferramentas open source.

O SAST tem um bom desempenho quando se trata de encontrar um erro em uma linha de código, mas geralmente não identifica questões relacionadas ao ambiente de execução das aplicações; para cobrir esse gap, usamos o DAST, conforme explicado a seguir.

2. ANÁLISE DE VULNERABILIDADE DAST (DYNAMIC APPLICATION SECURITY TESTING), EXEMPLOS DE FERRAMENTAS DAST

- Acunetix by Invicti
- Appknox
- StackHawk
- Crashtest Security Suite

Diferentemente do SAST, o DAST tenta encontrar erros que não são possíveis encontrar em linha de código, somente ao se executar a aplicação. Entre as principais vantagens do DAST, podemos enumerar:

- Encontra problemas de tempo de execução que não podem ser identificados pela análise estática;
- Identifica mais rapidamente problemas de autenticação e configuração de servidores;
- Lista as falhas que ficam visíveis apenas quando um usuário de fato efetua login.

3. ANÁLISE ATIVA DO AMBIENTE COM FERRAMENTAS DE CORRELAÇÃO DE LOGS (SIEM). EXEMPLOS DE SIEM

- Splunk (free para até 500MB por dia)
- ELK (Elastik Search + Kibana)
- Logz.io
- IBM QRadar

Com um SIEM configurado no ambiente você terá uma visão viva de seu ambiente com alarmes programáveis que são disparados em tempo real. Alguns dos controles que o SIEM pode proporcionar são:

- Alarmes de criação, deleção, alteração de usuários em sua rede ou plataforma na nuvem;
- Não uso de dispositivos de dupla autenticação nas ferramentas programadas para isso;
- Uso em tempo real do banco de dados, para avaliar o que e quando estão usando o banco de dados;
- Gráfico de uso de seus endpoints para que possa enumerar qual cliente mais usa sua ferramenta e se está sofrendo algum tipo de ataque;
- Monitoração de servidores e outros dispositivos em sua rede para prevenir quedas e indisponibilidade.

4. DATA LOSS PREVENTION (DLP)

Essa ferramenta é essencial para prevenção de vazamentos de dados entre as ferramentas de comunicação, e-mail e repositório de código. Com ela, você pode criar exemplos de captura de dados como CPF, endereço, chaves criptográficas, tokens, entre outros, e o DLP bloqueará a saída desses dados para fora da sua corporação.

5. PENTESTS RECORRENTES

Pentest não é somente rodar um escâner de vulnerabilidades nos seus endpoints, mas procurar em toda a internet vestígios ou traços de códigos que possam dar alguma dica ou pista do que se pode e onde se pode ter algum acesso ou obter mais dados que ajudem em uma invasão. Para isso, é imprescindível que haja um profissional de segurança na empresa ou que se contrate uma consultoria terceirizada para que façam o pentest de maneira mais profissional.

Entretanto, como o tópico é de ferramentas, seguem alguns exemplos escâneres de vulnerabilidades:

- Tenable.io
- OpenVas
- Acunetix
- Qualys
- Rapid7 Nexpose
- Burp Suite

6. AUTENTICAÇÃO CENTRALIZADA

Esse método de controle de usuários é muito importante para que não se perca a gerência dos usuários, o que pode causar uma brecha de segurança muito alta: os logins esquecidos.

Sempre devemos utilizar um centralizador de usuários, de preferência, plugado ao SIEM, para que nenhum movimento seja despercebido. Cada infraestrutura pode usar um centralizador, conforme sua infra disponibilize, seja Active Directory, seja Amazon IAM, Jumpcloud etc.

7. COFRE DE SENHAS

O uso de um cofre de senha digital torna a gerência de senhas de aplicações ou ferramentas bastante eficaz e segura, pois você pode compartilhar somente as senhas que aquele perfil ou pessoa necessita ou pode ter acesso. Abaixo estão alguns exemplos de software de gestão de senhas:

- 1Passwd
- Lastpass
- Keeper

Lembre-se de que todas essas ferramentas precisam de configuração e, principalmente, gerência sobre elas, pois a segurança da informação tem que ser viva no ambiente e não somente ferramentas espalhadas pelo ambiente.

8. COMUNICAÇÃO ENTRE AS EMPRESAS/ *STAKEHOLDERS*, MANTER AS BOAS PRÁTICAS

A troca de informações entre empresas deverá ocorrer de forma segura e confiável, por intermédio de plataformas homologadas entre ambas as partes – sempre que possível –, avaliando meios que habilitem chaves criptografadas entre as partes.

No que se refere a procedimentos de acesso e proteção de informações pessoais, a Lei de Acesso à Informação dispõe que o tratamento das informações pessoais deve ser feito de forma transparente e respeitando a intimidade, vida privada, honra e imagem das pessoas. Neste aspecto, é extremamente relevante assegurar a liberdade e as garantias individuais de acesso.

A plataforma de comunicação estabelecida entre as partes deve restringir acessos quando necessário, considerando informações originadas do aspecto de saúde, e dar permissão apenas a pessoas autorizadas, garantindo a acessibilidade a dados sensíveis considerando aspectos de disponibilidade, integridade e confidencialidade.

É extremamente relevante assegurar a liberdade e as garantias individuais de acesso.

Nos casos em que a informação trocada não seja relacionada a nenhum tipo de dado pessoal ou sensível perante a Lei Geral de Proteção de Dados Pessoais (LGPD), a troca poderá ocorrer por e-mail ou qualquer outro tipo de comunicação.

9. POLÍTICAS INTERNAS DE SEGURANÇA DA INFORMAÇÃO

É de extrema importância a definição de políticas internas de segurança da informação.

É de extrema importância a definição de políticas internas de segurança da informação estabelecidas a partir do planejamento estratégico da organização. A alta gestão da organização deve definir os objetivos estratégicos, os alicerces da governança corporativa e o apetite de risco que guiarão a criação das políticas internas.

As boas práticas de segurança da informação mais conceituadas no mercado consagraram algumas políticas importantes, tais como a Política de Segurança da Informação, o Plano de Resposta a Incidente de Segurança da Informação, a Política de Privacidade e o Plano de Continuidade de Negócios.

10. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

(LGPD, GOVERNANÇA, REGULAÇÃO ANPD, CFM, ANS)

As normas sobre privacidade e proteção de dados preceituam a obrigatoriedade do cumprimento das boas práticas de segurança da informação, as quais devem ser desenvolvidas de forma concomitante e inter-relacionada.

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) prevê expressamente em seu artigo 46 que as organizações devem adotar medidas de segurança (da informação) técnicas e administrativas aptas a proteger os dados pessoais, ou seja, há uma nítida intenção do legislador em privilegiar a aderência das organizações às boas práticas de segurança da informação.

As organizações devem adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais.

A Lei do Prontuário do Paciente (Lei nº 13787/2018) no artigo 1º, a Resolução CFM nº 2.299/2021, no artigo 3º, §2º e a Resolução CFM nº 2.314/2022, artigo 3º, igualmente indicam a necessidade de conformidade com a Lei Geral de Proteção de Dados Pessoais, portanto, indiretamente, impõem a necessidade de conformidade com as práticas de segurança da informação.

11. *FRAMEWORKS* DE SEGURANÇA DA INFORMAÇÃO

Existem alguns *frameworks* de segurança da informação utilizados mundialmente para nos ajudar na implantação de políticas e procedimentos relacionados à implementação e ao gerenciamento contínuo de controles de segurança da informação em um ambiente corporativo.

Dois dos mais utilizados são os frameworks do **CIS Controls** e o da norma **ISO/IEC 27001.**

1. CIS CONTROLS

O CIS Controls, Center for Internet Security Controls é um conjunto proprietário de diretrizes utilizado para as organizações melhorarem as suas defesas cibernéticas. Pode ser implementado em vários setores, pois tem o objetivo de ser universalmente aplicável. Foi elaborado por especialistas de agências governamentais e líderes da indústria.

Ele separa os controles em três categorias, com base nas prioridades e nos recursos das empresas: básico, fundamental e organizacional.

As estruturas de segurança mais utilizadas são o framework CIS Controls e a norma ISO/IEC 27001

BÁSICOS são os controles de segurança de finalidade geral que devem ser implementados por todas as organizações para garantir a prontidão essencial da defesa virtual. Aqui estão incluídos: controles de ativos de hardware e software; gerenciamento contínuo de vulnerabilidades; controle sobre o uso de privilégios administrativos; configuração segura de hardware e software em *endpoints* e servidores; e monitoramento e análise de *logs*.

ESSENCIAIS são os controles de segurança críticos que as empresas devem implementar para combater ameaças técnicas mais específicas. Incluem-se aqui: controles de proteção de e-mail e navegador *web*; defesas contra *malware* (ex.: antivírus); controle de portas, protocolos e serviços de rede; recuperação de dados; configuração segura para dispositivos de rede e segurança; defesa de limite; proteção de dados; controle de acesso com base na necessidade de conhecimento; controle de acesso sem fio; e monitoramento e controle de contas.

ORGANIZACIONAIS são os controles mais focados em pessoas e processos envolvidos na segurança cibernética que devem ser implementados para garantir a maturidade da segurança a longo prazo. Incluem: programa de conscientização e treinamento de segurança; segurança do software da aplicação; resposta e gerenciamento de incidentes; e testes de penetração.

CIS CONTROLS V7.1

BÁSICOS

1 INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS

2 INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

3 GESTÃO CONTÍNUA DE VULNERABILIDADES

4 USO CONTROLADO DE PRIVILÉGIOS ADMINISTRATIVOS

5 CONFIGURAÇÃO SEGURA DE HARDWARE E SOFTWARE EM LAPTOPS, DISPOSITIVOS MÓVEIS, ESTAÇÕES DE TRABALHO E SERVIDORES

6 GESTÃO DE REGISTROS DE AUDITORIA

ESSENCIAIS

7 PROTEÇÕES DE E-MAIL E NAVEGADOR WEB

8 DEFESAS CONTRA MALWARE

9 LIMITAÇÃO E CONTROLE DE PORTAS DE REDE, PROTOCOLOS E SERVIÇOS

10 CAPACIDADES DE RECUPERAÇÃO DE DADOS

11 CONFIGURAÇÃO SEGURA DE DISPOSITIVOS DE REDE, COMO FIREWALLS, ROTEADORES E SWITCHES

12 DEFESA PRIMÁRIA DA REDE

13 PROTEÇÃO DE DADOS

14 CONTROLE DE ACESSO BASEADO EM FUNÇÕES

15 CONTROLE DE ACESSO SEM FIO

16 MONITORAMENTO E CONTROLE DE CONTAS

ORGANIZACIONAIS

17 CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA

18 SEGURANÇA DE APLICAÇÕES

19 GESTÃO DE RESPOSTA A INCIDENTES

20 TESTES DE INVASÃO E SIMULAÇÕES

Figura 1 – https://www.cisecurity.org/

Além dos controles básicos, essenciais e organizacionais, na versão mais recente dos Controles CIS, os controles são priorizados nos grupos de implementação (IG). Cada IG identifica quais subcontroles são razoáveis para que uma organização os implemente com base em seu perfil de risco e em seus recursos disponíveis.

As organizações são incentivadas a se autoavaliarem e se classificarem como pertencentes a um dos três IGs para priorizar os Controles CIS para uma melhor postura de segurança cibernética. As organizações devem começar implementando os subcontroles no IG1, seguido pelo IG2 e, em seguida, pelo IG3. A implementação do IG1 deve ser considerada entre as primeiras coisas a serem feitas como parte de um programa de segurança cibernética. O CIS refere-se ao IG1 como "higiene cibernética" – as proteções essenciais que devem ser colocadas em prática para defesa contra ataques comuns.

A implementação do IG1 deve ser considerada entre as primeiras coisas a serem feitas como parte de um programa de segurança cibernética.

GRUPO DE IMPLEMENTAÇÃO 1 (IG1)

As organizações de pequeno a médio porte, com recursos e experiência limitados em TI e segurança cibernética, onde a sensibilidade dos dados é baixa, precisarão implementar os subcontroles que normalmente se enquadram na categoria IG1 e são destinados a impedir ataques gerais não direcionados.

GRUPO DE IMPLEMENTAÇÃO 2 (IG2)

Organizações com recursos moderados, que empregam indivíduos responsáveis por gerenciar e proteger a infraestrutura de TI, com maior exposição a riscos para lidar com ativos e dados mais confidenciais, precisarão implementar os controles IG2 junto ao IG1. Esses subcontroles se concentram em ajudar as equipes de segurança a gerenciar informações confidenciais de clientes ou da empresa.

GRUPO DE IMPLEMENTAÇÃO 3 (IG3)

Organizações maduras com recursos significativos, que empregam especialistas em segurança cibernética, têm alto risco de exposição para lidar com ativos críticos e dados e estão sujeitas à supervisão regulatória e de conformidade. Elas precisam implementar os subcontroles na categoria IG3 junto ao IG1 e ao IG2. Os subcontroles que ajudam a reduzir o impacto de ataques direcionados de adversários sofisticados e reduzir o impacto dos ataques zero-day geralmente se enquadram no IG3.

No momento, o CIS Controls se encontra na versão 8. Segue um comparativo com a versão anterior que pode ser encontrado no site oficial:

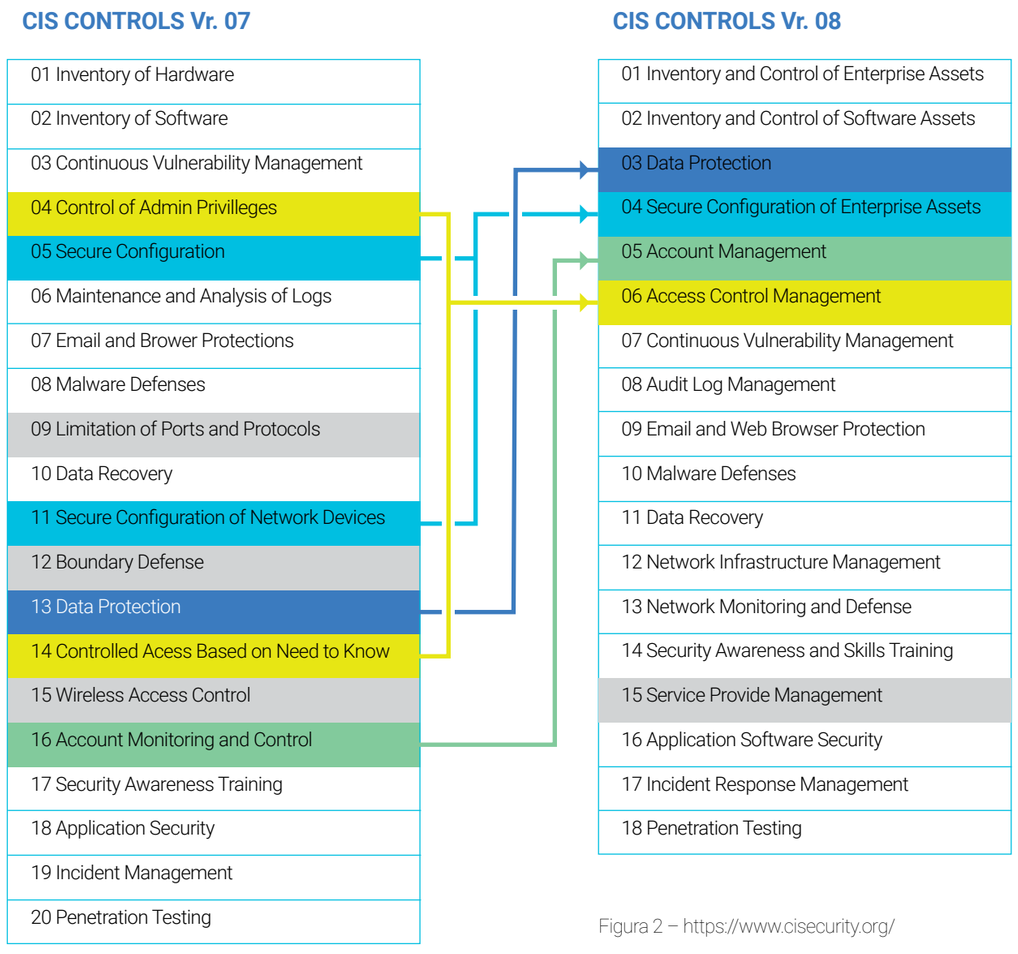
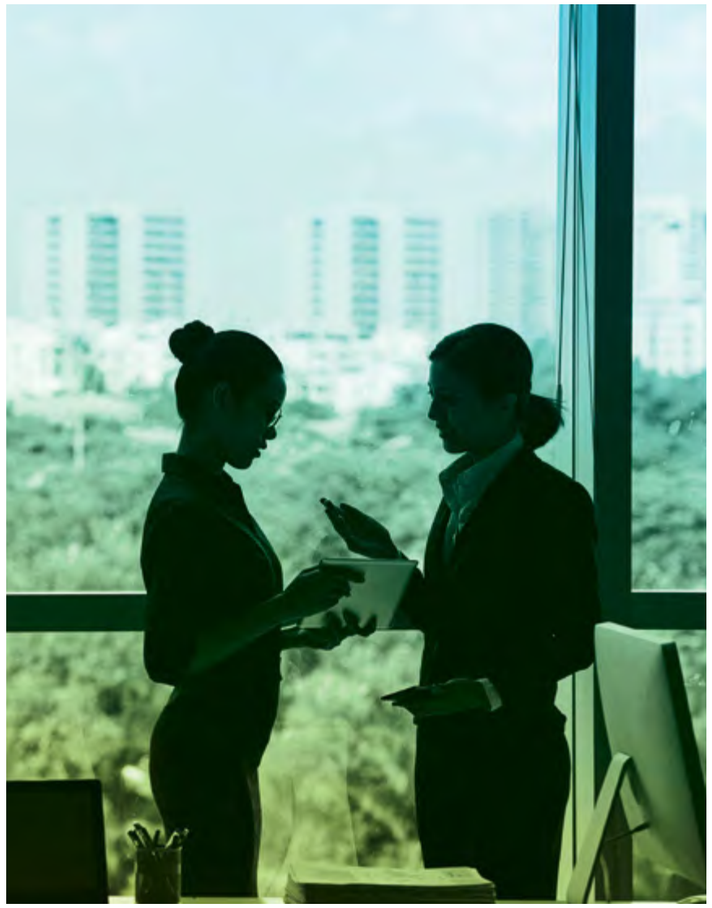


Figura 2 – https://www.cisecurity.org/

2. ISO/IEC 27001

A norma ISO/IEC 27001 é o padrão e a referência internacional para a gestão da segurança da informação pulicada pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission (IEC).

Essa norma descreve a visão geral e o vocabulário do Sistema de Gestão da Segurança da Informação (SGSI) – tradução de Information Security Management System (ISMS) – e referência as normas da família do sistema de gestão da segurança da informação (incluindo a ISO/IEC 27003, ISO/IEC 27004 e ISO/IEC 27005), com termos e definições relacionados.



O objetivo da norma é prover requisitos para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar continuamente os sistemas e processos de gestão de segurança da informação (SGSI) de uma empresa. Esta norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização.

A ISO/IEC 27001 é adequada para organizações de todos os tamanhos, em todos os setores, sendo particularmente útil em setores altamente regulamentados, como bancos, serviços financeiros, saúde, setores públicos e de TI. Também é altamente eficaz para organizações que gerenciam informações em nome de terceiros como forma de demonstrar que os controles de segurança apropriados estão em vigor e em conformidade com os requisitos de proteção de dados e outra legislação aplicável. Ela está para segurança da informação assim como a ISO 9001 está para a gestão em qualidade.

Diferente dos CIS Controls, a empresa precisa receber um certificado para se adequar à norma ISO/IEC 27001, com metas a serem atingidas, que devem ser validadas por auditorias internas e externas.

Os principais benefícios em implementar a norma ISO/IEC 27001 e obter a certificação são:

- Evidenciar a existência, eficiência e eficácia do ISMS e controles de segurança, atendendo aos requisitos de governança corporativa e continuidade de negócios.
- Demonstrar que as leis e os regulamentos aplicáveis são identificados e que existem processos em vigor para garantir a conformidade.
- Conseguir uma vantagem competitiva atendendo aos requisitos contratuais e demonstrando aos clientes que a segurança de suas informações é primordial.
- Comprovar, com uma revisão independente, que os riscos organizacionais são devidamente identificados, avaliados e gerenciados, enquanto formaliza processos, procedimentos e documentação de segurança da informação.
- Confirmar o compromisso da alta administração com a segurança das informações.
- Monitorar e melhorar continuamente o desempenho através de um processo de avaliação regular.

A norma ISO/IEC 27001 tem uma versão brasileira, a NBR ISO/IEC 27001:2013, publicada pela Associação Brasileira de Normas Técnicas (ABNT), que é dividida em duas partes. A primeira trata da implementação do SGSI, composta por cinco seções de requisitos principais, cada um com objetivos e focos específicos. A segunda é um apêndice que contém controles de segurança.

Sistema de Gestão da Segurança da Informação (SGSI).

O SGSI preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de risco e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

A ISO/IEC 27001 adota uma abordagem baseada em risco para planejamento e implementação de seu SGSI, resultando em um nível adequado e acessível de segurança organizacional. Dessa forma, garante que pessoas, processos, procedimentos e tecnologias certos estejam disponíveis para proteger os ativos de informações da organização.

O estabelecimento e a implementação do SGSI de uma organização são influenciados por necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização, sendo esperado que todos esses fatores mudem ao longo do tempo.

A norma especifica os requisitos necessários para a implementação de um Sistema de Gestão da Segurança da Informação, de uma forma genérica, para serem aplicados a todas as organizações. Sua implementação está baseada na metodologia PDCA (plan, do, check e act), conforme exemplificado na imagem a seguir.

A normal ISO/IEC 27001 garante que pessoas, processos,procedimentos e tecnologias estejam disponíveis para proteger os ativos de informações da organização.

ANEXO A OBJETIVOS DE CONTROLE

O Anexo A é um famoso anexo da norma ISO/IEC 27001 (padrão para sistema de gestão da segurança da informação). Apresenta uma uma lista de controles (requisitos técnicos e operacionais) e objetivos de controle, organizados e alinhados com os tópicos da norma, que devem ser implementados para a manutenção da segurança da informação.

No total, são 114 itens de controle que devem ser atendidos e evidenciados para que se obtenha a certificação (salvo exceções justificadas), organizados em 14 seções:

- **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** prover orientação da direção e apoio para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações relevantes.
- **ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO** estabelecer uma estrutura de gerenciamento para iniciar e controlar a implementação e operação de segurança da informação dentro da organização.
- **SEGURANÇA EM RECURSOS HUMANOS** assegurar que os funcionários e as partes externas entendam suas responsabilidades e estejam em conformidade com os papéis para os quais foram selecionados, cientes das ameaças de segurança, e que deixem a companhia ou mudem de função de modo ordenado.
- **GESTÃO DE ATIVOS** identificar os ativos da organização e definir as devidas responsabilidades pela sua proteção.
- **CONTROLE DE ACESSO** limitar o acesso à informação e aos recursos de processamento da informação, prevenindo acesso e uso não autorizado, danos, furto ou roubo.

- **CRIPTOGRAFIA** assegurar o uso efetivo e adequado da criptografia para proteger a confidencialidade, autenticidade e/ou integridade da informação.
- **SEGURANÇA FÍSICA E DO AMBIENTE** prevenir acesso físico não autorizado, danos e interferências nos recursos de processamento das informações e nas informações da organização, a fim de evitar perdas, danos, roubo ou comprometimento dos ativos e interrupção das atividades de negócio.
- **SEGURANÇA NAS OPERAÇÕES** garantir a operação segura e correta dos recursos de processamento da informação, a fim de certificar que as informações são processadas, manuseadas e armazenadas corretamente, incluindo as cópias de segurança.
- **SEGURANÇA NAS COMUNICAÇÕES** assegurar a proteção das informações em redes e dos recursos de processamento que as apoiam, mantendo a segurança na transferência das informações tanto dentro da organização, quanto com entidades externas.
- **AQUISIÇÃO, DESENVOLVIMENTO E MAN UTENÇÃO DE SISTEMAS** garantir que a segurança da informação é parte integrante de todo o ciclo de vida dos sistemas de informação, a fim de tornar as aplicações e os arquivos mais seguros bem como reduzir as vulnerabilidades.
- **RELACIONAMENTO NA CADEIA DE SUPRIMENTO** garantir a proteção dos ativos da organização que são acessados por fornecedores.
- **GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO** assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação efetiva sobre fragilidades e eventos de segurança da informação, possibilitando a implementação de ações corretivas em tempo oportuno.

- **GESTÃO DE CONTINUIDADE DE NEGÓCIOS** evitar a interrupção das atividades de negócio, assegurando a disponibilidade dos recursos de processamento da informação, e proteger os processos críticos dos efeitos de desastres e falhas graves de sistemas.
- **CONFORMIDADE** evitar violação de quaisquer obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e quaisquer requisitos de segurança, bem como assegurar a conformidade de sistemas com as políticas e os padrões de segurança corporativos.

12. *PRIVACY BY DESIGN E SECURITY BY DESIGN*

No Privacy by Design, a privacidade e proteção de dados são incorporados nos projetos desde a concepção.

Privacy by design está relacionado a conceitos e pode ser implementado em forma de framework. Tem como proposta central incorporar a privacidade e a proteção de dados pessoais em todos os projetos desenvolvidos desde a concepção, seja produtos, seja serviços, práticas, tecnologias ou infraestruturas.

O principal objetivo é garantir a privacidade e permitir que os indivíduos (titulares) tenham controle sobre seus dados pessoais. Outras características incluem:

Ser proativo e não reativo

Antecipar e prevenir eventos que possam comprometer a privacidade antes que eles ocorram. Por meio desse princípio, os eventos que possam comprometer o direito fundamental à privacidade devem ser identificados, e as estratégias de tratamento, definidas. Métodos para identificar pontos fracos e prever práticas, riscos e resultados que possam afetar a privacidade de dados podem ser desenvolvidos tendo como objetivo corrigi-los antecipadamente.

Privacidade como configuração padrão

Garantir que os dados pessoais sejam automaticamente protegidos, ou seja, sem que o titular dos dados tenha de fazer configurações adicionais. As configurações referentes à privacidade devem estar definidas de maneira que o máximo de proteção seja refletido na configuração padrão.

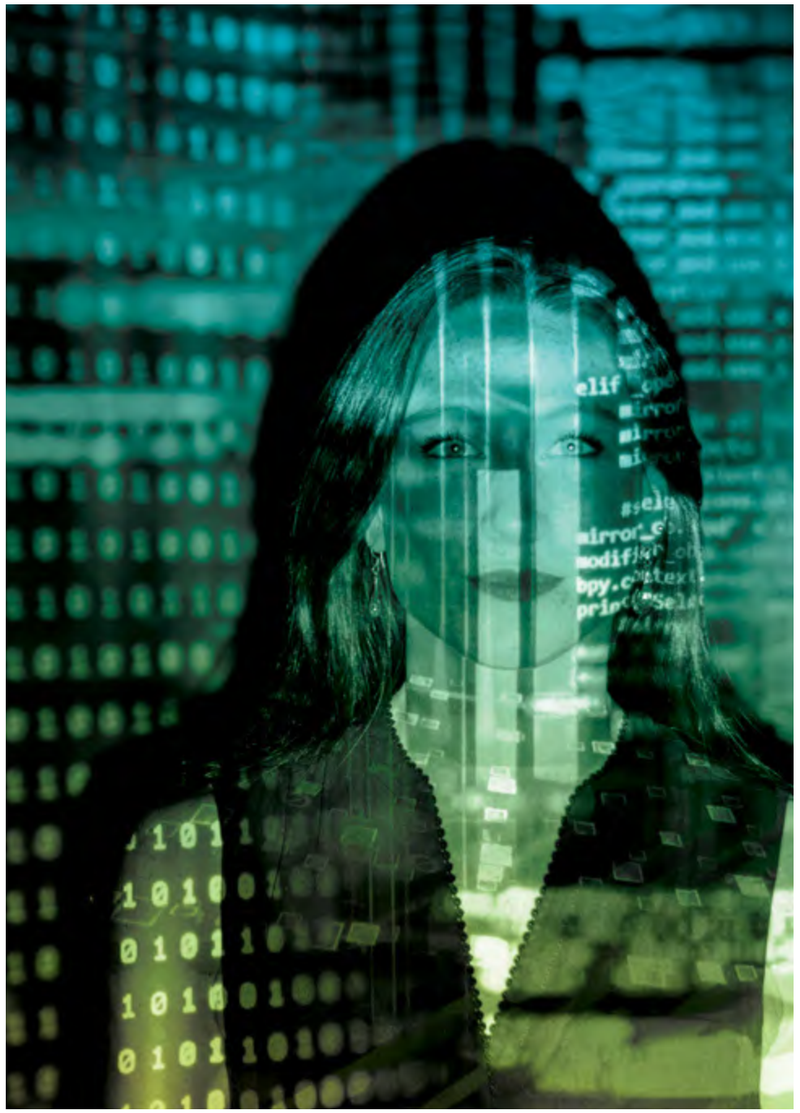
Privacidade incorporada ao design

A proteção dos dados pessoais deve ser parte do projeto de arquitetura da aplicação, do serviço, da infraestrutura, da prática de negócio, e não um componente opcional do tipo suplemento. Esse princípio reduz o esforço do usuário a fim de garantir a privacidade de seus dados.

A proteção dos dados pessoais deve ser parte do projeto de arquitetura da aplicação, do serviço, da infraestrutura, da prática de negócio.

Funcionalidade completa

Assegurar que a proteção de dados pessoais esteja alinhada com os interesses e objetivos legítimos de quem é responsável pelo tratamento dessas informações, sem abrir mão da segurança para obter mais dados. O princípio em questão estabelece uma relação de ganha-ganha entre o titular e os agentes de tratamento de dados.



Segurança de ponta a ponta

A proteção dos dados pessoais deve ser contemplada ao longo de todo o ciclo de vida, ou seja, da coleta até o descarte das informações, passando pelo transporte, processamento e armazenamento.

Visibilidade e transparência

Conceder visibilidade ao titular do dado quanto à finalidade da coleta e com quem estão sendo compartilhados esses dados e o porquê, bem como abertura para realização de auditorias para assegurar que as informações pessoais estejam sendo devidamente protegidas.

Respeite a privacidade do usuário

Manter os interesses do titular dos dados em primeiro lugar, isto é, disponibilizar controles robustos para proteção de dados, notificando-o de maneira clara e oportuna, ao mesmo tempo que torna as configurações referentes à privacidade amigáveis.

Já o § 2º do artigo 46, da Lei Geral de Proteção de Dados Pessoais, determina que as medidas de que trata o caput deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

13. CONTROLES INTERNOS

A segurança da informação como parte de controles internos assegura a sustentabilidade e competitividade dos negócios.

Os benefícios de uma plataforma segura vão além de simplesmente garantir maior confiabilidade e respeitar a privacidade, ou criar proteção contra vazamentos de dados. Vantagens e benefícios econômicos surgem quando se adota segurança da informação como parte de controles internos, resultando em oportunidades de nivelar a competitividade com as demais empresas no mercado internacional.

É importante entender que o desenvolvimento econômico, tecnológico e a inovação estão presentes em empresas com visão de futuro focada no crescimento. De fato, em muitos ambientes a tecnologia é a espinha dorsal para o acesso e a interação direta de clientes, fornecedores, parceiros de negócios e colaboradores. Não é possível pensar em proporcionar uma experiência positiva sem pensar no ambiente e sua infraestrutura tecnológica de forma segura.

Implementação de *compliance* de segurança

São medidas necessárias. A palavra *compliance* pode ser traduzida como "conformidade" e é uma das bases da governança corporativa, item essencial a ser implementado. Faz parte de várias áreas, inclusive da tecnologia da informação, e na infraestrutura, quando adotado, eleva o grau de maturidade do ambiente de TI.

Devidamente alinhado com a estratégia da empresa, tem como foco criar um conjunto de boas práticas que podem ser usadas para aprimorar os resultados atingidos. Ao estabelecer regras e padrões, o *compliance* começa a fazer sentido e pode se tornar aliado na continuidade do negócio. A ausência de práticas de compliance podem sujeitar a organização a riscos, inclusive atrelados a multas elevadas.

O papel do time de TI é fundamental para o entendimento e ajuste de itens que norteiam o *compliance*, como normas de utilização do ambiente tecnológico e políticas de segurança da informação, os quais são pré-requisitos formais que dão embasamento para criação de algo aplicável. O objetivo alcançado no final pode ser maturidade do ambiente de tecnologia, confiabilidade, integridade, aumento nos lucros, mais vendas, mais clientes etc.

Criação de uma Política de Segurança da Informação (PSI)

O objetivo deste documento é definir as diretrizes de segurança da informação, garantindo que os recursos de tecnologia e as respectivas informações sejam usados de maneira adequada, conforme as normas internas da empresa, estabelecendo os princípios e as diretrizes, aprovado e divulgado por decisão da diretoria, a qual se torna um pilar de apoio e fomento das iniciativas necessárias ao alcance dos objetivos de segurança estabelecidos.

Um PSI visa preservar a integridade, confidencialidade e disponibilidade de todas as informações dos documentos recebidos, criados, emitidos, impressos e/ou reproduzidos no âmbito corporativo, incluindo informações em formato físico, eletrônico ou magnético, e informações que não são diretamente reveladas, tais como: informações técnicas, escopos de projetos, relatórios, ativos físicos e conteúdo gerado em decorrência das atribuições da função; além dos respectivos equipamentos de tecnologia da informação, utilizando-se de mecanismos de controles, boas práticas e procedimentos.

As diretrizes que poderão nortear a Política de Segurança da Informação podem se baseiam no Conjunto de Conceitos Dirigidos para Gestão de Tecnologia da Informação (Cobit), mantido pela Information Systems Audit and Control Association (Isaca); e Normas da família ISO/IEC 27000 (International Organization for Standardization / International Electrotechnical Commission) que apontam os padrões internacionais de boas práticas para gestão de segurança da informação, assim como requisitos mandatórios e recomendações; e na Lei Geral de Proteção de Dados Pessoais, que é a legislação brasileira que regula as atividades de tratamento de dados pessoais.

Criação de um Plano de Continuidade de Negócios (PCN)

Toda atividade de negócio está sujeita a interrupções; ter um Plano de Continuidade de Negócios fornece a capacidade de reagir adequadamente às interrupções operacionais enquanto se preserva a vida e protege o bem-estar, a segurança e a imagem da organização. O sucesso do plano depende principalmente de pessoas.

O Plano de Continuidade de Negócios pode ser elaborado internamente pela área de tecnologia em observância às diretrizes emanadas pela diretoria e às boas práticas no mercado, com objetivo traçar estratégias e planos de ação que garantam o funcionamento e a disponibilidade dos serviços essenciais de tecnologia da empresa durante uma crise técnica com falha massiva, ou durante um desastre que impeça a continuidade dos trabalhos até que ocorra a normalização da situação.

Entende-se por crise a interrupção prolongada dos serviços e por desastre uma situação relevante que gere indisponibilidade parcial ou total, como a ocasionada por incêndio, alagamento e inundação, vendaval, interrupção de energia, ataque de negação de serviço, ataque *hacker*, desabamentos e resultados de eventos diversos provocados pelo homem, intempéries ou problemas que limitem a capacidade de resposta imediata.

- Plano de Contingência
- Plano de Recuperação de Desastres
- Plano de Administração e Gerenciamento de Crise
- Plano Continuidade Operacional

Cada plano de ação pode conter premissas básicas a serem cumpridas durante a crise, que vão desde o funcionamento de sistemas primários até a forma como os porta-vozes lidarão com a imprensa, caso a crise atinja grande repercussão na opinião pública.

Backup e *restore*

A continuidade do negócio pode ser diretamente afetada quando a empresa não possui capacidade rápida de restaurar dados e informações. Um bom plano de continuidade do negócio prevê rotinas de *backup* claramente descritas, além disso, gestores estão habituados em buscar soluções de backup para garantir a recuperação após incidentes, mas fazer *backup* não é suficiente.

A capacidade de rápida recuperação de dados está diretamente ligada à continuidade do negócio.

Verificar e atestar o *backup* e a restauração dele pode garantir o funcionamento correto para a recuperação em caso de uma falha, invasão, incidente ou desastre; do contrário, pode causar perdas irreversíveis. Está associado diretamente aos dados e informações, muitas delas de caráter vantajoso e competitivo para o mercado e de vital importância para o bom funcionamento do negócio.

Planejamento de capacidade

Uma análise de capacidade e performance que responda a perguntas simples, como: “quanto temos em recursos disponíveis?”; ou “no próximo ano precisaremos contratar novos recursos?”.

Esse recursos são computacionais, fundamentais para garantir o andamento das operações, ou seja, uma visão para suportar o crescimento organizacional de forma escalável e a incorporação de novos negócios.

É um item que dá aos gestores condições de atuar precisamente nos problemas perceptíveis por usuários e agir com base em situações monitoradas.

Devido à ampliação contínua de banco de dados, relacionamentos entre sistemas, sincronização entre ambientes, processamento e espaço de armazenamento, analisar mensalmente os recursos de processamento, memória, espaço em disco e banco de dados da estrutura tecnológica é uma prática que dará à empresa uma visão a longo prazo de sua capacidade, inclusive pode nortear a quantidade de recursos a serem alocados em projetos durante determinados períodos.

Licenciamento e conformidade

Os crimes cibernéticos têm dimensões e criatividades tão grandes que a mineração de dados, mesmo que brutos, é de grande valia no mercado. Manter o licenciamento de softwares e a conformidade deles dentro da legalidade minimiza o risco da obtenção de informações por golpistas, algo comum em softwares ilegais.

As multas pelo não licenciamento adequado de softwares são altíssima.

As multas pelo não licenciamento são altíssimas, assim como há multas pelo licenciamento incorreto. Ao criar um item de compliance com foco no licenciamento, a organização poderá ter a percepção da empregabilidade correta das licenças, ajustar as de uso único ou coletivo, renovar e adquirir aquilo que realmente faz sentido ao trabalho e às rotinas diárias do pessoal, e até mesmo ajudar na compreensão para saber se o tipo de software é adequado para a utilização de determinada pessoa ou setor.

Há, portanto, um risco iminente em manter softwares ilegais. A qualquer momento a organização pode ser submetida a auditoria pela empresa fabricante ou licenciadora, ou receber ação judicial, e consequentemente arcar com prejuízo financeiro.

Relatório de antivírus, anti spam, *firewall* e ferramentas de monitoramento

Ao adotar uma rotina de análise de antivírus e demais ferramentas de monitoramento, a organização pode ter uma visão detalhada para implementar ações que os eliminem.

Esses relatórios normalmente também contêm detalhes sobre as ameaças, incluindo a listagem de computadores que relataram incidentes com vírus ou usuários que violaram as diretivas de proteção, ou seja, as regras.

Vivemos na era digital, nossa sociedade acessa a internet mais do que nunca, e não estamos imunes. Compliance não garantirá a inviolabilidade do ambiente, mas com ele poderão ser adotadas ações para minimizar impactos e reduzir os riscos.

Acesso administrativo, manutenção de contas, e-mails e grupos

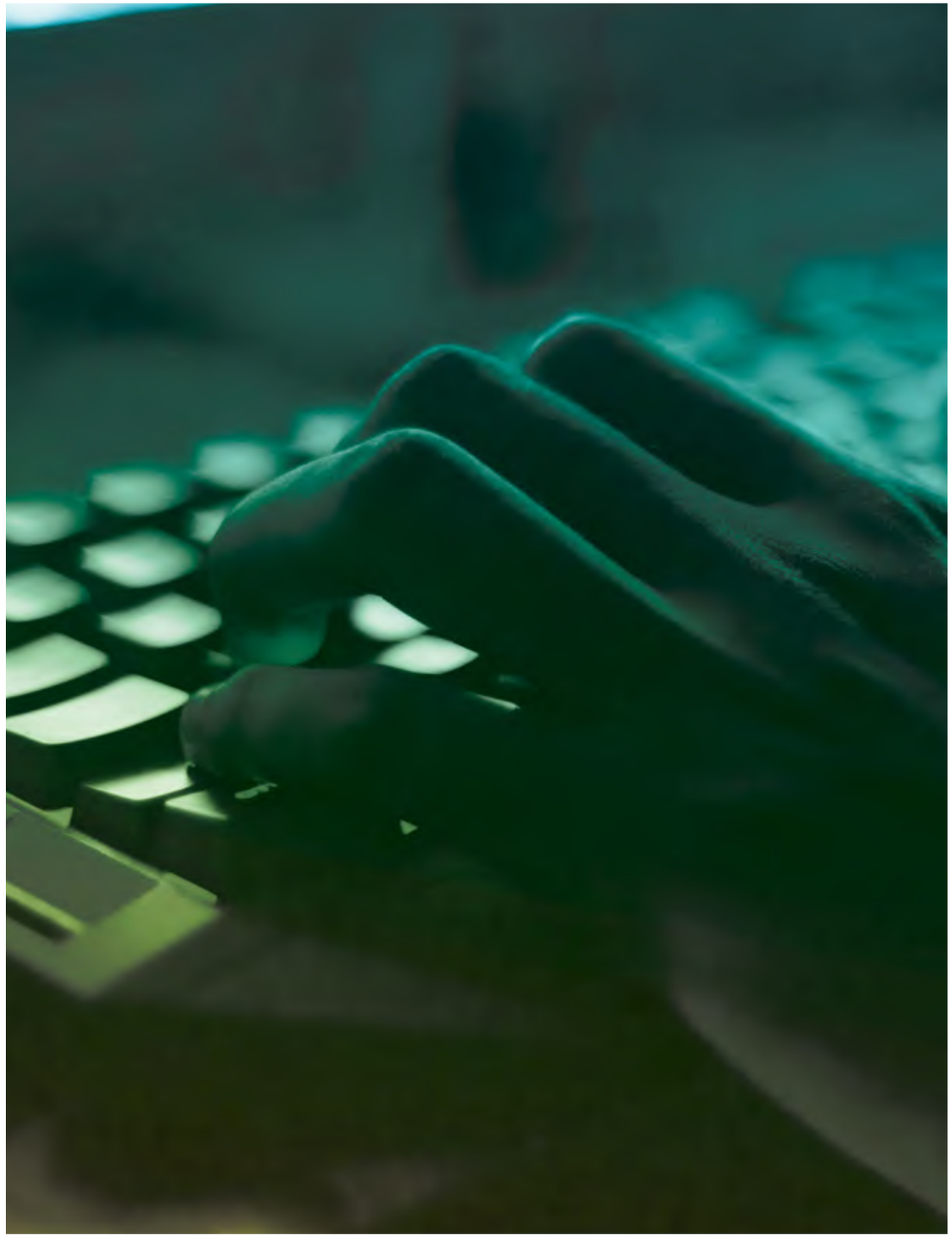
É imprescindível que se tenha um alinhamento técnico de atividades para garantir o registro mínimo de uma documentação de controle, pois este item envolve alto risco, levando a transações não autorizadas.

Em grandes empresas não é difícil encontrar exemplos em que o colaborador é desligado e a área de TI não é comunicada. Ora, se a TI é a provedora dos acessos, também os retira; quando não há um procedimento de revisão periódica de contas de usuários, a revogação de tais acessos é cumprida.

O adequado controle de acessos e contas é fundamental para a garantia da integridade e privacidade dos dados.

Usuários administradores locais têm permissões elevadas para alterar configurações em suas estações de trabalho. Administradores de domínio têm acesso ainda mais elevado, com permissões totais para alterar, incluir, excluir, modificar estações de trabalho, servidores, aplicativos e serviços.

Contas de usuários administradores que não são controladas, geridas e verificadas com certeza são portas de entrada para problemas. Essa rotina pode ajudar no controle de adequação, identificar colaboradores transferidos a outro departamento, mudanças de funções, além de demissões.



Política de senhas

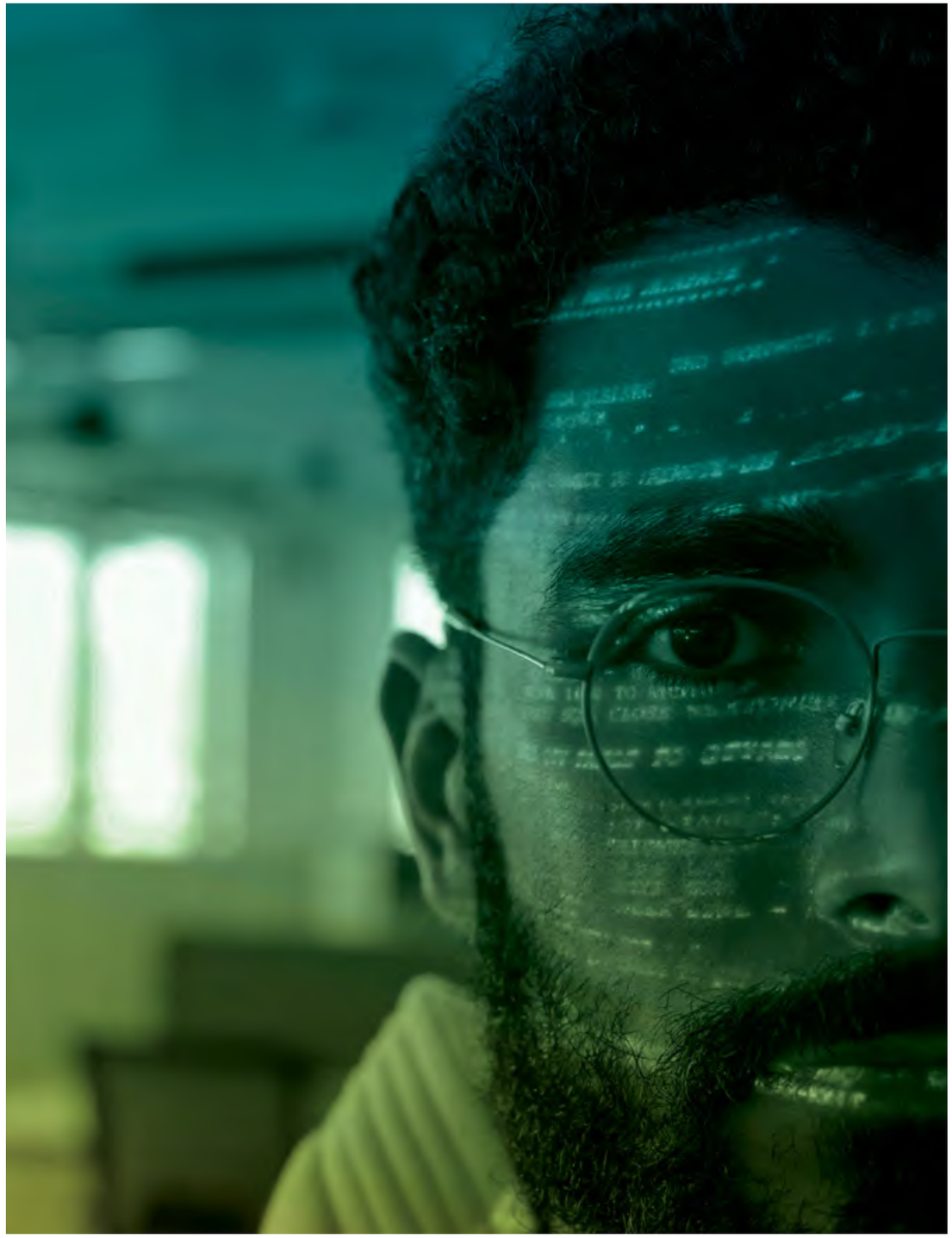
Um problema de segurança no computador ou uma senha simples pode colocar em risco a confidencialidade e integridade dos dados e arquivos armazenados. Ao obter acesso ao computador ou dispositivo, ele pode ser usado para prática de atividades maliciosas, como servir de repositório de dados fraudulentos, realizar ataques a outros computadores e dispositivos ou ainda propagar aplicativos e softwares maliciosos.

A Microsoft informa que "ao definir uma senha de conta de usuário para uma senha que contém menos de 15 caracteres, o Windows gera um hash da senha. Estes hashes são armazenados no banco de dados do gerenciador de contas de segurança ou no Active Directory".

Não se deve usar a mesma senha para todos os sites. Há gerenciadores que ajudam bastante.

O Windows geralmente armazena a senha em memória. Um programa malicioso, vírus ou cibercriminoso poderá descobrir a senha com maior facilidade se ela contiver menos de 15 caracteres. Adotar uma senha de no mínimo 15 caracteres, incluindo letras minúsculas, maiúsculas, números e símbolos, vai torná-la mais forte e mais difícil de descobrir.

Não se deve utilizar a mesma senha em todos os sites e acessos. A proteção das senhas é uma importante medida de segurança na internet. Existem aplicativos gerenciadores de senhas que ajudam bastante, assim como a maioria dos navegadores de internet disponibiliza funções que podem auxiliar na proteção.



Phishing e ações de engenharia social

Phishing é comum nas organizações. Em resumo, é uma tentativa de obtenção de informações, golpe, e é feito através de falsificação de comunicação eletrônica, como o e-mail.

Os criminosos mascaram campos, fazem o e-mail de origem parecer verdadeiro, mas na realidade é tudo uma enganação, falsificação. O e-mail de origem é outro, está mascarado e não aparece ao usuário de destino. A ousadia dos autores é tão grande que o título do e-mail faz sentido e o texto condiz com o trabalho diário. Se não houver atenção, cai-se no golpe.

A engenharia social é um meio eficaz para os criminosos, com um método de ataque em que uma pessoa mal-intencionada faz manipulação psicológica para induzir alguém a tomar ações específicas.

É importante não abrir anexos nem responder a e-mails dos quais não se tem certeza se realmente deveria recebê-lo.

Diferentemente de outros tipos de crimes, esse método não usa sistemas sofisticados ou softwares e aplicativos de última geração. O sucesso depende da relação estabelecida entre o criminoso, que tenta ganhar a confiança, e a vítima.

Geralmente, por meio de uma identificação falsa, o criminoso se passa por instituições, marcas famosas ou até pessoas de confiança da vítima para conseguir convencê-la a fornecer informações pessoais, baixar aplicativos com vírus ou abrir links maliciosos.

No meio digital, a engenharia social pode ser feita através de e-mails, mensagens, perfis falsos nas redes sociais ou mesmo por chamadas telefônicas. Esse tipo de estratégia é vantajosa para os criminosos, pois é mais fácil convencer pessoas a cederem seus dados do que descobri-las por meio de ataques tecnológicos.

Além disso, golpes que utilizam a técnica de engenharia social, como aqueles via WhatsApp, ainda têm a capacidade de "viralizar", impactando muitos outros usuários.

É importante não abrir anexos nem responder a e-mails dos quais não se tem certeza se realmente deveria recebê-lo, ou com conteúdo estranho que não condiz com o trabalho diário, ou que contenha no cabeçalho um endereço estranho.

Implantação de mecanismos de validação de duas etapas

Para contas em aplicativos e serviços na internet, usar apenas senhas pode não ser suficiente para proteção. Senhas podem ser facilmente descobertas através de páginas falsas, engenharia social, por observação se não forem bem-elaboradas, ou computadores e dispositivos infectados por vírus e softwares maliciosos.

A confirmação da identidade oficial do usuário pode ser fator adicional de proteção, como a verificação de duas etapas, um recurso opcional oferecido por diversos serviços na internet, como webmail, redes sociais, internet banking, armazenamento em nuvem e aplicativos.

Ativar uma segunda camada de verificação, como tokens por e-mail ou SMS, aumentam muito a segurança.

Estar em compliance e adotar medidas de segurança é estar orientado e adequado às boas práticas existentes na área de tecnologia.

Ao habilitar, a segurança da conta aumenta e consequentemente será mais difícil ser invadida, pois o invasor precisa saber a senha na primeira etapa e as informações da segunda etapa, por exemplo: respostas secretas para perguntas que só você sabe, códigos gerados por tokens, número PIN etc.

Normalmente se recebe a verificação da segunda etapa por e-mail, SMS ou chamada de voz. É um código individual criado pelo serviço e enviado apenas ao dono da conta.

É importante manter os dispositivos seguros, cadastrar senhas complexas, ter antivírus, manter o sistema operacional atualizado e logicamente ter o controle físico sobre os equipamentos.

Como iniciar?

Recomenda-se iniciar criando uma planilha simples com itens que devem ser verificados diariamente, semanalmente ou mensalmente; incluir um responsável pela verificação e determinar um local para os registros dessas verificações, análises, bem como apontamento das evidências e ações adotadas.

O monitoramento de informações dentro da empresa não é violação de privacidade e sim uma medida preventiva contra ações indevidas, ilegais, que vem de encontro ao respeito às leis e determinações muitas vezes externas a um empreendimento.

Estar em compliance e adotar medidas de segurança é estar orientado e adequado às boas práticas existentes na área de tecnologia.

CAPÍTULO**03**

PRESCRIÇÃO ELETRÔNICA E REGISTRO DE DISPENSAÇÃO VIA DIGITAL

1. INTRODUÇÃO

No contexto de atenção à saúde, a prescrição (ou receita) é um documento escrito que contém o ato do profissional de saúde, com instruções sobre o tratamento indicado para o paciente. Já a dispensação é o ato farmacêutico de aviar um ou mais medicamentos a um paciente, geralmente em resposta à apresentação de uma prescrição emitida por profissional legalmente habilitado. É durante a dispensação que o farmacêutico poderá informar e orientar sobre o uso adequado do produto.

75% das prescrições têm altas chances de equívocos interpretativos devido aos erros de grafia e à dificuldade de interpretação da letra do prescritor.

De modo geral, uma prescrição deve conter informações fundamentais e legíveis sobre o medicamento, como sua identificação adequada, dose, via e frequência de administração, duração do tratamento, data da prescrição, identificação do paciente e do profissional prescritor.

Uma pesquisa conduzida pela Agência Nacional de Vigilância Sanitária (Anvisa) e pela Organização Mundial de Saúde (OMS)[3] identificou que cerca de 75% das prescrições têm altas chances de equívocos interpretativos devido aos erros de grafia e à dificuldade de interpretação da letra do prescritor, seja na identificação do medicamento, seja na posologia. Do lado dos pacientes, apenas 50% deles utilizam remédios corretamente conforme orientação de receita, e para 30% o remédio prescrito não faz mais efeito por conta do uso incorreto feito no passado.

3 Pesquisa disponibilizada no site do Sistema Nacional de Auditoria do governo federal. Disponível em http://189.28.128.21/denasus/. Acesso em: 16 mar. 2022.

No mesmo sentido, de acordo com a *Klas Research*, empresa de pesquisas para área da saúde e tecnologia, 39% dos erros associados à medicação acontecem no momento da prescrição, tais como a utilização de medicamentos com interação medicamentosa, erros de posologia considerando aspectos pessoais do paciente e vias de administração inadequadas, entre outros.

O uso de softwares de prescrição e registros de dispensação eletrônica, além de ferramentas digitais, no contexto de atendimento digital em saúde e integração do jornada do paciente, pode reduzir esses desafios por meio de suas inúmeras vantagens:

- Maior segurança: as receitas digitais dificultam a incidência de alterações de receituário pós-emissão, a falsificação de receita e a dispensação irregular por meio de sua tecnologia e presença de assinatura digital.
- Melhor experiência para o prescritor: com a utilização de sistemas de suporte clínico, reduz-se a possibilidade de erros assistenciais.
- Melhor comunicação entre prescritor-paciente-dipensador: as receitas digitais impedem as confusões comuns de letras do prescritor pelo paciente e pelo dipensador durante a dispensação, por exemplo: troca de medicamentos que têm nomes, pronúncias ou embalagens parecidas e programas falhos de detecção de interação medicamentosa.
- Melhor experiência para pacientes crônicos: possibilita a renovação das receitas sob supervisão do profissional de saúde para medicamentos de uso contínuo.

As receitas digitais impedem as confusões comuns de letras do prescritor pelo paciente.

Em telemedicina, é importante que a discussão imponha não apenas digitalização dos processos existentes em papel, mas também a premissa seja o bom uso da tecnologia como grande aliada e geradora de ganhos à saúde pública e à organização do cuidado dentro do sistema de saúde.

Trata-se da transformação digital completa da gestão de saúde que possibilita a integração de dados clínicos e o histórico do paciente, reduzindo a burocracia e aumentando significativamente a segurança sanitária, rastreabilidade, adesão ao tratamento e segurança.

Mecanismos digitais e softwares de prescrição e de registro de dispensação eletrônica podem transformar essa realidade. As receitas digitais aumentam a segurança em relação ao processo prescritivo, uma vez que dificultam a incidência de alterações de receituário após a emissão, dificultam a falsificação de receita e a dispensação irregular. Com a utilização de sistemas de suporte clínico, reduz-se a possibilidade de erros assistenciais. A tecnologia, nesse contexto, atua como incentivadora da adesão ao tratamento pelo paciente, um dos fatores mais importantes na promoção da saúde da população. Ainda, tem papel considerável no processo de melhoria da comunicação profissional de saúde e paciente e pelo farmacêutico durante dispensação, por exemplo: troca de medicamentos que têm nomes, pronúncias ou embalagens parecidas e programas falhos de detecção de interação medicamentosa.

As tecnologias de prescrição e dispensação eletrônica, por seu caráter inovador e uso da tecnologia na geração de ganhos à saúde, ganharam importância durante a pandemia de coronavírus (SARS-Cov-2) como aliadas essenciais à telemedicina. Dos atendimentos

em telemedicina e da expansão tecnológica em saúde que vem acontecendo em diversos países destaca-se, por exemplo, que cerca de 73% dos países da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) já permitiam atendimento médico remoto em 2018 (OCDE, 2020). Contudo, foi a partir da pandemia relacionada ao coronavírus que esse modelo de atendimento remoto ganhou ainda maior tração e adoção pelos sistemas de saúde dos países. Estima-se que esses serviços cresçam cerca de 18% anualmente no mundo até o ano de 2027 (GLOBAL MARKET INSIGHTS, 2020).

Embora a telemedicina esteja disponível há anos em muitos países, também foi a partir da declaração da pandemia que houve importante aceleração desse modelo de atendimento. Agora, é um dos principais modelos de saúde digital utilizados no Reino Unido. Nos últimos anos, houve investimento maciço em uma estratégia digital first: visando melhorar o acesso ao cuidado, o paciente entra no sistema de saúde inglês, prioritariamente, por um atendimento digital. Esse modelo reduz desperdícios para os sistemas públicos de saúde, além de simplificar a jornada do paciente (SDB, 2021a).

Enquanto alguns não permitem prescrição de tratamentos de forma virtual, outros limitam-na para certos medicamentos

Porém, mesmo com a adoção mais ampla da telemedicina, assim como a legislação e regulação em alguns países, outros ainda não conseguiram acompanhar a tecnologia (ou apenas iniciaram o processo de implementação) e limitam algumas atividades de saúde em ambiente virtual. Enquanto alguns não permitem prescrição de tratamentos de forma virtual, outros limitam-na a certos medicamentos, como narcóticos. A lista de países com restrições para prescrição de medicamentos inclui Holanda, Espanha, Suíça, Índia, Indonésia, Japão, Filipinas, Taiwan e, infelizmente, Brasil[4].

4 Pesquisa 2021 Global Medical Trends – Resultados da América Latina.

Quando se analisa o caso brasileiro, constata-se que, assim como no cenário internacional, a pandemia foi catalisadora da viabilização e expansão da saúde digital e telemedicina. Desde o início de 2020, diversos setores da economia e, em especial, da saúde, enfrentam desafios estruturais para superar as dificuldades emergentes e continuar a prestação dos serviços essenciais. Todos precisaram se adequar à realidade pandêmica e, inequivocamente, o processo de digitalização em curso nos diversos setores públicos e privados oportunizou melhor enfrentamento a esse cenário.

Avançou-se em meses o que vinha sendo almejado há anos. A Lei nº 13.989/2020 garantiu e ampliou o acesso à assistência e à saúde em todo o país, por meio da permissão do uso da telemedicina durante a pandemia. Nesse mesmo cenário, foi aprovada a Lei nº 14.063/2020, que também possibilitou que documentos eletrônicos subscritos por profissionais de saúde fossem reconhecidos como válidos – incluindo as prescrições – desde que acompanhados de assinatura digital.

A Lei nº 14.063/2020, garantiu que documentos médicos eletrônicos fossem reconhecidos como válidos quando assinados digitalmente.

Dados levantados pela Saúde Digital Brasil (SDB) mostram que, entre 2020 e 2021, mais de 7,5 milhões de atendimentos foram realizados. Tão importante quanto o volume de consultas é o índice de resolutividade dos atendimentos, que foi de 91%, ou seja: os pacientes tiveram seu problema resolvido e não precisaram recorrer ao atendimento presencial (SDB, 2021b).

Inclusive, no momento de pandemia e isolamento social, as empresas do setor de saúde digital estavam prontas para rapidamente atuar, conectando-se entre si, entre redes de atendimento médicos, softwares de prescrição eletrônica e farmácias. Houve treinamento de médicos, farmacêuticos e gestores com vistas a possibilitar o tratamento mesmo em situação excepcional. O setor contribuiu, e ainda contribui, para ajudar pacientes que usam de medicação esporádica ou contínua, de modo que possam seguir seus tratamentos com menor risco de contato e contágio.

os benefícios da digitalização só serão possíveis com o envolvimento de todo o ecossistema de saúde

É nesse espírito de construção e colaboração das empresas do setor que reside a essência deste Manual de Boas Práticas. Tem-se a preocupação de que a utilização de princípios de telessaúde e da saúde digital em geral fomente e consolide de modo crescente, inovador e promissor aqueles que se propõem a se utilizar a prescrição eletrônica e os mecanismos de software para dispensação remota de medicamentos.

Assim, as diretrizes previstas neste manual destinam-se ao mercado como um todo aos interessados no tema e ao setor de saúde digital como um todo. Em especial, aos fornecedores de tecnologias e usuários de sistemas de prescrições e dispensações eletrônicas que tenham interesse em terem suas soluções no mais alto parâmetro de qualidade e adequação.

De fato, a utilização completa dos benefícios decorrentes da digitalização da saúde só será possível com o envolvimento de todo o ecossistema de saúde que nela se insere: empresas de tecnologia, empresas de saúde, governo, fiscalizadores, agências reguladoras, vigilâncias sanitárias, profissionais de saúde, hospitais, Sistema Único de Saúde (SUS), pacientes, farmácias e indústria farmacêutica.

2. OBJETIVO DAS DEFINIÇÃO DAS BOAS PRÁTICAS

Como entidade pioneira no setor de saúde digital, a SDB e seus associados se comprometem a ser referência em boas práticas na área. Como parte de suas atividades, inclui-se a discussão em grupo de trabalho para tratar melhores práticas e cenários regulatórios da prescrição e dispensação eletrônica.

O presente Manual tem como objetivo:

- Consolidar os princípios de atuação das empresas com vistas a superar eventuais preocupações no setor de saúde digital.
- Definir boas práticas sob a perspectiva de atuação setorial além da legislação específica hoje existente.
- Conscientizar sobre as possibilidades do bom uso da prescrição eletrônica e do registro de dispensação digital.
- Democratizar o conhecimento sobre saúde digital.

O objetivo da SDB é fomentar o cenário para uma melhor e mais completa e segura experiência digital para profissionais de saúde, pacientes e farmácias, eliminando a necessidade do uso de papel e desburocratizando o dia a dia das pessoas. A associação traz mais transparência na prescrição e dispensação de remédios, reduzindo significativamente os equívocos no aviamento de medicamentos e ampliando sensivelmente a adesão ao tratamento prescrito – justamente o maior gerador de gastos no setor da saúde.

3. PRINCÍPIOS E BOAS PRÁTICAS SOBRE PRESCRIÇÃO ELETRÔNICA E REGISTRO DE DISPENSAÇÃO VIA DIGITAL

3.1 Autonomia do profissional prescritor

Um dos princípios fundamentais no exercício dos profissionais de saúde prescritores é a sua autonomia em receitar tratamentos, prezando pela ética e pelo foco na melhor conduta para o paciente pautada por evidências. Conforme já reconhecido por conselhos profissionais em seus códigos de ética e pela literatura, o prescritor deve contemplar a saúde global do paciente, analisando seu contexto, sua condição de saúde e avaliar todas as vantagens e as desvantagens da prescrição e que considere a opção de menor risco para atingir a eficácia terapêutica desejada, isentando-se de conflito de interesse.

O prescritor deve contemplar a saúde global do paciente, analisando seu contexto, sua condição de saúde e avaliar todas as vantagens e as desvantagens da prescrição

Nesse cenário, as plataformas devem seguir esses padrões do ponto de vista legal e ético, minimizando conflitos de interesse e preservando a autonomia de prescrição do profissional sem restrições no recebimento e dispensação, desde que atendam aos requisitos das legislações aplicáveis, incluindo a de assinatura eletrônica, que garantem a segurança e validade jurídica dos documentos eletrônicos[5].

Além disso, as plataformas podem contribuir, por meio de suas ferramentas e sistemas adicionais, com informações e elementos de suporte à decisão com embasamento clínico. Isso sem induzimento por essas ferramentas à seleção de determinado item, respeitando-se o fato de que o ato de prescrição e criação de protocolos de tratamento é reservado aos profissionais de saúde.

5 A Lei nº 14.063/2020 dispõe sobre a os documentos e as assinaturas eletrônicas em questão de saúde pública e atualizou a Lei nº 5.991/1975.

Os profissionais de saúde que têm a prerrogativa de prescrever devem ter sempre a liberdade de fazê-lo, da mesma forma que precisam garantir qualidade técnica do diagnóstico e das prescrições prestadas sempre em benefício do paciente[6].

A prescrição é um documento com valor legal, pelo qual se responsabilizam aqueles que prescrevem, dispensam e administram os medicamentos, cujo objetivo é tornar claras as instruções aos pacientes e demais profissionais de saúde, garantindo a fidelidade da interpretação e a objetividade da informação.

3.2 Autonomia clínica do profissional de saúde no ato de dispensação

É fundamental que o processo de dispensação respeite a autonomia do farmacêutico e, muito além disso, reconheça a importância desse profissional para o uso correto e racional de medicamentos e a adesão ao tratamento.

O farmacêutico tem o importante papel de validar as informações das prescrições de medicamentos antes da dispensação observando os aspectos técnicos e legais dos receituários, reduzindo possíveis erros de escrita, dosagem, indicação e interação medicamentosa. Ou seja, o farmacêutico é mais uma linha de defesa do paciente contra erros no tratamento.

Na adesão terapêutica, tem o papel de orientar o paciente para o correto uso dos medicamentos prescritos, reforçando a importância de seguir as instruções de uso, esclarecendo quanto ao manuseio adequado dos produtos e à correta administração bem como atuando no combate à automedicação.

É preciso avançar com ferramentas que possibilitem melhorias nos sistemas de dispensação, facilitem o registro e ajudem no próprio atendimento farmacêutico. As plataformas poderão ser fonte de informações técnicas para

6 OSÓRIO DE CASTRO CGS, PEPE VLE. Nota técnica: Prescrição de medicamentos. ENSP/ Fiocruz, Rio de Janeiro, 2011.

decisões referentes à intercambialidade na dispensação ou em outras etapas da assistência à saúde desses profissionais, por exemplo, como as interconsultas.

Nesse cenário, as ferramentas e tecnologias empregadas no processo de prescrição eletrônica (e-prescription) não devem substituir a atuação do farmacêutico como profissional responsável pela dispensação de medicamentos e orientação ao tratamento. Antes, devem valorizar, reconhecer e empoderar esse profissional. Para isso, as plataformas devem contribuir para orientação legível e compreensível do que foi recomendado pelo prescritor, assim como trazer orientações para validação de prescrições, com checagem de veracidade e conformidade de acordo com a legislação.

3.3 Autonomia e empoderamento do paciente

O paciente tem direito de participar, com autonomia, do seu cuidado, o que significa que ele pode participar de processos de tomada de decisão compartilhada com os profissionais de saúde sobre seu cuidado (BRITO; KUNNEMAN; MONTORI, [2017]). Isso garante que ele consiga ponderar riscos e benefícios, podendo optar ou não pelo tratamento sugerido pelo profissional de saúde.

Nesse processo, ele também é o responsável, por exemplo, pela escolha do estabelecimento farmacêutico por meio do qual deseja acessar o tratamento prescrito. Essa abordagem designa ao paciente um lugar de empoderamento e informação, em que ele é um agente ativo e responsável pela própria saúde.

As plataformas eletrônicas devem ser aliadas do processo para que o paciente receba informações claras sobre o tratamento e os protocolos que estão sendo receitados.

É importante notar que empoderar o paciente é dar subsídios para decisões e prosseguimento nas adesões após orientações oferecidas durante a consulta. Isso se soma à prerrogativa e responsabilidade do profissional prescritor para indicação da melhor prática terapêutica. Deve-se reforçar que o paciente irá receber documentos com a identificação, em que constará o tratamento indicado e a posologia (a própria prescrição).

Nesse contexto, as plataformas eletrônicas devem ser aliadas do processo para que o paciente receba informações claras sobre o tratamento e os protocolos que estão sendo receitados. Elas também devem garantir a validade e conformidade da prescrição para que possa ser dispensada em qualquer estabelecimento farmacêutico assegurando a autonomia do paciente na escolha sobre qual canal gostaria de acessar ou de onde adquirir o tratamento

receitado. Ainda, essas tecnologias podem contribuir e fornecer informações sobre os canais disponíveis de acesso e dispensação do tratamento prescrito, sempre deixando a cargo do paciente a escolha de em qual estabelecimento deseja acessar o tratamento.

3.4 O uso racional de medicamentos

O uso racional de medicamentos é um conceito guarda-chuva reconhecido pela OMS e observado pelo Ministério da Saúde que engloba diversas estratégias para que a prescrição, a dispensação e o uso de tratamentos ocorram de forma adequada e segura ao paciente, com menor custo e amplo acesso pela sociedade. Esse conceito tem importância sistêmica, não só pelo cuidado do indivíduo, mas também pelas consequências para o sistema de saúde, do ponto de vista de saúde pública e de custos de tratamentos feitos de forma irregular ou inapropriada. Ele se alia às noções de segurança do paciente na medida em que engloba discussões relacionadas ao uso abusivo de medicamentos, à falsificação e ao acesso indevido a fármacos, principalmente de medicamentos controlados regulados pela vigilância sanitária.

As plataformas eletrônicas devem contribuir para o uso racional de medicamentos e, para isso, são norteadas pelo suporte a todos os envolvidos na cadeia do cuidado de profissionais de saúde, como farmacêuticos, médicos, biomédicos e enfermeiros, além de gestores e órgãos de vigilância sanitária, assim como na jornada de tratamento do paciente.

As plataformas eletrônicas devem contribuir para o uso racional de medicamentos

Do ponto de vista sanitário e de saúde pública, as plataformas devem ter como prioridade contribuir para a rastreabilidade e da segurança na circulação de medicamentos no sistema de saúde. Nesse sentido, devem promover a digitalização aliada à

As plataformas eletrônicas devem ser aliadas do processo para que o paciente receba informações claras sobre o tratamento e os protocolos que estão sendo receitados.

integração com órgãos reguladores, buscando maior controle sobre a veracidade das informações e verificação da dispensação de substâncias controladas, evitando possíveis fraudes e erros que colocariam em risco os pacientes.

Considerando os atores individuais ao longo da jornada de tratamento, as plataformas devem prezar pelo cuidado e suporte ao paciente, ao prescritor e ao farmacêutico por orientações claras na plataforma. Assim, quando possível, deve prestar suporte para uso da ferramenta. Sob a ótica do uso racional de medicamentos, as plataformas também devem oferecer informação e orientações clínicas da forma mais clara possível, prezando pela legibilidade e inclusão de ferramentas que trazem segurança da informação com baixo risco de extravios, como pode ocorrer no caso de documentos físicos.

Com relação ao prescritor, prioriza-se a agilidade e assertividade das ferramentas para que possibilitem o suporte clínico relacionado às informações acerca do tratamento. Para o farmacêutico, por fim, as plataformas devem buscar maior controle e rastreabilidade da origem da receita, respeitando a legislação de segurança de informação e proteção de dados, trazendo informações que forneçam maior segurança ao ato da dispensação do medicamento, em especial os controlados e antibióticos.

4. ÉTICA E COMPLIANCE DAS EMPRESAS DO SETOR

As empresas ou órgãos que oferecem ou se utilizam de plataformas de prescrição e registro de dispensação de medicamentos de forma eletrônica são responsáveis por realizar serviço relacionado à saúde pública e tratar dados sensíveis. Essas empresas devem se comprometer com os mais altos padrões éticos e legais, visando à segurança sanitária, do paciente e da informação, e à repressão de atos de corrupção.

As empresas, por meio do diálogo setorial, também devem sempre procurar a atualização das normas que conferem maior segurança ao prescritor, paciente e farmacêutico e possibilitam melhorias e inovações tecnológicas que tragam benefícios para o ecossistema de saúde.

Os provedores de prescrição digital devem se comprometer com os mais altos padrões éticos e legais, visando à segurança sanitária, do paciente e da informação, e à repressão de atos de corrupção.

Nesse sentido, as relações com órgãos reguladores, agentes de governo e demais atores do setor devem ser pautadas na ética e integridade, assim como promover avanços tecnológicos que garantam acesso seguro a medicamentos e assistência à saúde no sistema de saúde público e privado, observando as boas práticas descritas neste Manual.

5. VISÃO DE FUTURO

A SDB promove da atuação totalmente digitalizada de emissão,controle e fiscalização das prescrições e registros de dispensação eletrônicos

As diretrizes aqui definidas têm como objetivo superar eventuais entraves nas discussões sobre o uso da prescrição e dispensação eletrônica para todos os tipos de receitas, inclusive aquelas que dependem de suporte do poder público regulamentar, como notificações de receita (talonários azuis e amarelos), além de retinoides e talidomida.

A SDB é um propagador da atuação totalmente digitalizada de emissão, controle e fiscalização das prescrições e registros de dispensação eletrônicos. Por isso, a entidade quer incentivar e contribuir para que os órgãos de vigilância sanitária possam se apropriar dessa tecnologia para aprimorar suas atividades em um setor que conte com uma experiência totalmente remota desde a prescrição até o acesso ao tratamento.

A experiência digital vem mudando a forma de organizar os sistemas de saúde em todo o mundo. Países como Suécia (INERAA), Canadá (Canada Health Infoway), Reino Unido (NHS Digital), Estados Unidos (Office of the National Coordinator), Austrália (Digital Health Agency of Australia) estão há anos investindo na estrutura dos seus modelos organizacionais, serviços e sistema em saúde com a finalidade de garantir através da tecnologia a atenção à saúde e a continuidade do cuidado.

Seguindo os exemplos internacionais, a SDB vislumbra um futuro que permita uma experiência totalmente digital no sistema de saúde brasileiro e, consequentemente, o maior acesso ao cuidado do paciente em todas as etapas da jornada em seu tratamento, em ambiente remoto ou físico.

A entidade acredita na evolução dos sistemas de saúde em que o papel seja recurso e não mais requisito para o acesso à assistência à saúde e que possibilite ao paciente a experiência totalmente remota desde a prescrição até o acesso ao tratamento, quando possível e necessário. Assim como outros setores, entende-se que o futuro permitirá que os sistemas informatizados trarão de forma sistêmica e atualizada dados cruciais para gestores, fiscalizadores e reguladores, possibilitando a adoção de melhores políticas e práticas relacionadas à segurança, com rastreabilidade no acesso a medicamentos.

Para isso, o sistema de saúde deve estar cada vez mais preparado, integrado e interoperável em um fluxo inteiramente digitalizado, desde a originação dos documentos médicos, em clínicas, serviços de saúde e hospitais até a dispensação nas farmácias, e também os órgãos de vigilância sanitária na validação e no controle da veracidade das prescrições.

A digitalização dos controles pode representar grande avanço para a vigilância sanitária

Há pontos que devem ser aprofundados e desenvolvidos por todo o ecossistema para garantir o acesso seguro ao tratamento de pacientes. Adotar como premissa a digitalização dos controles pode representar grande avanço para a vigilância sanitária e para o sistema de saúde, reduzindo burocracias para os profissionais de saúde, a iniciativa privada e o setor público.

Esses avanços perpassam pelo trabalho ativo e em conjunto com os atores do setor para a derrubada de barreiras relacionadas à infraestrutura e conectividade no país; atualização das normas que possibilitem o uso responsável de tecnologias; assim como a educação e conscientização plena dos gestores, profissionais de saúde e pacientes sobre o potencial e os benefícios das prescrições eletrônicas.

CAPÍTULO**04**

INTE-ROPE-RABILI-DADE

1. SOBRE A ELABORAÇÃO DESSE DOCUMENTO

O objetivo é, em primeira mão, trazer clareza sobre o tema de interoperabilidade no setor de saúde e ser apoio para implementação de projetos de interoperabilidade.

Este documento é uma iniciativa da Saúde Digital Brasil (SDB), que, em conjunto com seus associados, formou times multidisciplinares de especialistas nos temas, os quais, a partir de suas experiências e práticas do setor privado e público, construíram este material. O objetivo é, em primeira mão, trazer clareza sobre o tema de interoperabilidade no setor de saúde e ser apoio para implementação de projetos de interoperabilidade.

O documento contém conceitos e diretrizes gerais para a implementação das melhores práticas de interoperabilidade de dados em saúde, alinhando diretrizes do Ministério da Saúde a iniciativas em andamento no Brasil e no mundo, tanto nos setores público como no sistema privado.

2. CONCEITUAL

O que é interoperabilidade

O termo "interoperabilidade" foi definido nos anos 1990 pela IEEE como "Habilidade de dois ou mais sistemas ou componentes de trocar informações e usar a informação que foi trocada"[1]. Essa definição se aplica a sistemas de informação de qualquer setor, incluindo o setor da saúde.

O Ministério da Saúde trouxe a definição da academia de computação e definiu que "A interoperabilidade pode ser entendida como uma característica que se refere à capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente"[2].

Os padrões de interoperabilidade devem garantir que a informação seja compreendida tanto pelo receptor quanto pelo emissor.

Em ambas as definições, interoperabilidade vai além de uma simples integração sistêmica de dados, e a SDB reforça que o conceito deve viabilizar a troca de informações de forma que a informação seja compreendida pelo receptor e usada por ele, garantindo a eficácia no contexto em que é aplicada. Portanto é característica dessa troca de informações sistêmica "via interoperabilidade" a aplicação de padrões, que devem garantir a compreensão semântica da informação por parte do emissor e do receptor.

1 http://www.jhi-sbis.saude.ws/ojs-jhi/index.php/jhi-sbis/article/viewFile/502/268
2 https://www.gov.br/governodigital/pt-br/governanca-de-dados/interoperabilidade

A interoperabilidade em saúde

Não diferente dos demais setores, com o avanço da tecnologia, a informatização dos centros de cuidado e o avanço das técnicas médicas e dispositivos médicos, mais do que nunca se torna necessário o uso da interoperabilidade para conectar todos os pontos de cuidados e seus dados. Assim, tem-se uma visão única e histórica da trajetória de cuidados de um cidadão, viabilizando a tomada de decisão clínica, a eficácia na gestão de saúde e até mesmo a eficiência do setor, evitando desperdícios, como repetição de exames de image e/ou análises clínicas por exemplo.

Uma visão única e completa da trajetória de cuidados do paciente evita desperdícios e viabiliza a tomada de decisão clínica com segurança e assertividade.

Tais avanços estão contextualizados no conceito de saúde digital, e a SDB, como a maior Associação de prestadores e fomentadores de serviço dessa área no Brasil, traz uma visão histórica de como o tema interoperabilidade vem sendo conduzido e quais deveriam ser as boas práticas a serem adotadas na sua aplicação, respeitando as questões regulatórias, de segurança de informação e privacidades de dados.

3. VISÃO GERAL DE INTEROPERABILIDADE NO SETOR DE SAÚDE

Interoperabilidade é um dos temas-chaves relacionados à saúde digital, área de conhecimento e práticas estabelecida pela Organização Mundial de Saúde (OMS) que preconiza o uso de recursos tecnológicos para produzir e disponibilizar informações confiáveis sobre o estado de saúde de um indivíduo, para quem precisa, no momento em que precisa, promovendo saúde para todos e em todos os lugares, incluindo práticas de telemedicina, telessaúde e saúde móvel.

Em 22 de junho de 2017, na Resolução CIT nº 19, é declarada no Brasil a estratégia de saúde digital, orquestrada pelo Ministério da Saúde através do DataSUS. A estratégia foi elaborada a partir de boas práticas estabelecidas e declaradas pela OMS no Pacote de Ferramentas da Estratégia Nacional de e-Saúde (National eHealth Strategy Toolkit) e União Internacional das Telecomunicações (UIT). A resolução abrange toda a estratégia digital, considerando itens já preconizados na Política Nacional de Informação e Informática em Saúde de 2015 (PNIS), como fatores básicos sobre digitalização dos sistemas de saúde, pois se sabe que o Prontuário Eletrônico do Paciente (PEP) ainda não é uma realidade, assim como processos de operação nas unidades de saúde, fluxo de atendimento e governanças de recursos.

A temática de interoperabilidade é destacada como elemento imprescindível para uma gestão de saúde de alto nível.

Posteriormente, o Ministério da Saúde fortaleceu ainda mais a estratégia de saúde digital publicando os documentos de Plano Diretor de Tecnologia da Informação e Comunicação 2019-2021 (PDTIC) e a Estratégia de Saúde Digital para o Brasil 2020-2028 (ESD28), publicada pela Portaria GM/MS nº 3.632, de 21 de dezembro de 2020. O Ministério da Saúde, pela Portaria nº 2.073/2011, regulamentou i uso de padrões de interoperabilidade em saúde nos níveis municipais, estaduais e federal, para instituições dos setores público e privado de saúde.

Em 28 de maio de 2020, o Ministério da Saúde instituiu, por meio da Portaria GM/MS nº 1.434, a Rede Nacional de Dados em Saúde (RNDS) como plataforma nacional de interoperabilidade de dados em saúde, com todos os componentes e diretrizes para sua implementação.

Nota-se que, em todos os documentos, a temática de interoperabilidade é destacada como elemento imprescindível para uma gestão de saúde de alto nível, principalmente considerando o estágio atual e as fragilidades do setor, em que temos o setor fragmentando, com uma diversidade de sistemas de informações, com diferentes fornecedores, protocolos e vocabulários, falta de padronização, ausência de sistemas informatizados e processos de coleta de dados.

A SDB recomenda que a temática se torne urgente na pauta e no planejamento das empresas do setor público e privado de saúde, e que as iniciativas para sua adoção sejam iniciadas o quanto antes. É importante a priorização de pautas que antecedem a interoperabilidade em si, que dizem respeito à preparação de uma rede de atendimento informatizada, pautada por boas práticas assistenciais e padronização de dados, principalmente fazendo uso de PEP, regularizado como o responsável pela guarda de dados dos pacientes.

4. DIRETRIZES DE INTEROPERABILIDADE EM SAÚDE

A SDB, como entidade representativa dos prestadores de serviço de telessaúde do Brasil, tem por objetivo através de suas publicações a construção de referências em boas práticas no cenário de mercado da saúde digital brasileira.

Este documento estabelece padrões mínimos com os quais as empresas signatárias se comprometem a realizar sua prática de seus negócios, permitindo o compromisso com a qualidade e entrega de valor no setor de saúde digital do Brasil, trazendo previsibilidade aos investidores e excelência no atendimento aos pacientes.

As diretrizes da OMS e do Ministério da Saúde evidenciam a necessidade de evolução dos sistemas de saúde para fins de interoperabilidade.

Entendemos não ser possível hoje se desenhar um horizonte de saúde digital sem a governança de dados mínima orientada por um prontuário único, que permite ao proprietário dos dados – no caso, o paciente – transitar suas informações e a coordenação de seu cuidado pelo sistema de saúde.

É consenso entre os associados o respeito às normas internacionais e a construção de um cenário de negócios que permita a interoperabilidade internacional de dados conforme sugerido pela estratégia de saúde digital da OMS, nos esforços de garantir a todo cidadão acesso e privacidade dos seus dados de saúde.

As diretrizes da OMS e do Ministério da Saúde evidenciam a necessidade de evolução dos sistemas de saúde para fins de interoperabilidade. Além da melhoria da gestão de saúde do cidadão e da comunidade como um todo, inclusive da sustentabilidade do setor de saúde, é importante destacar que, para setores privados, estar aderente a padrões de interoperabilidade traz uma série de benefícios estratégicos e comerciais, possibilitando a parceria de empresas que têm interesses em comum em gestão de saúde baseada em valor, que, além de proporcionar um melhor serviço ao indivíduo, conseguem atuar na redução de custos e desperdícios, com foco principal em ações preventivas.

A gestão de saúde baseada em valor merece seu destaque como motivadora da interoperabilidade, já que sua aplicação na essência só se torna possível a partir da integração de sistemas e a troca de dados. O termo *value-based healthcare* foi definido por Michael Porter como: "*Value-based healthcare* é uma iniciativa de reestruturação dos sistemas de saúde em todo o mundo, cujo objetivo global é ampliar o valor para os pacientes, conter a escalada de custos e oferecer mais conveniência e serviços aos clientes". A partir da definição de Porter, e considerando o cenário de alto custo do setor, a interoperabilidade torna-se, mais do que motivadora, imprescindível para a mudança de paradigma da saúde nacional.

Aqui são descritas questões importantes que impulsionam, auxiliam e direcionam os interessados na adoção de digitalização do sistema de saúde com finalidades interoperáveis. Não serão abordadas neste documento questões de troca de dados para fins financeiros. Este documento focará a interoperabilidade de dados clínicos para gestão de saúde e a visão longitudinal do indivíduo.

A SDB entende que o tema interoperabilidade é amplo e tem questões particularmente técnicas e complexas, porém traz aqui uma visão de macrotemas importantes, direcionadores, que devem ser considerados na sua adoção. Os textos não são exaustivos mas trazem pistas e conceitos que podem ser aprofundados pelos leitores interessados.

4.1. Fluxo de dados

Interoperabilidade, por conceito, fala de sistemas integrados. Para tanto, é importante que os sistemas estejam integrados de forma **bidirecional**, gerando e consumindo dados através de **protocolos** que padronizam e facilitam a implementação da comunicação dos sistemas. Deve ser de comum acordo entre prestadores de serviços e cidadão a troca de dados, para que todos os envolvidos na cadeia de troca de informações se beneficiem.

4.2. Arquitetura de implementação

A interoperabilidade viabiliza uma visão unificada e histórica de saúde de um indivíduo, reunindo dados coletados em qualquer ponto do sistema de saúde, seja público ou privado, seja privado ou publico, integrando todos os níveis e serviços de atenção à saúde.

A implementação da interoperabilidade se dá por meio de um conjunto de sistemas, padrões e tecnologias. É possível que cada entidade implemente sua própria plataforma ou decida utilizar o serviço de terceiros, que por sua vez podem entregar partes do que compreende como interoperabilidade ou uma plataforma completa. É relevante no início da adoção estabelecer um desenho de arquitetura conceitual de troca de informações. É importante considerar na escolha da solução o contexto em que uma empresa está inserida e os motivadores da interoperabilidade (por exemplo, uma única unidade de saúde que deve enviar dados ao governo). Abaixo descreveremos três tipos de adoção de interoperabilidade:

REPOSITÓRIOS MÚLTIPLOS E INDIVIDUALIZADOS é possível implementar a interoperabilidade de forma que todos os sistemas enviem dados e recebam dados de outros provedores, gerando cada um sua própria visão de dados. Nesta implementação, cada sistema deverá ter uma interface para integrar dados em um protocolo padrão (entrada e saída de dados) e poderá criar um repositório que centralizará as informações próprias e as recebidas

de parceiros. Neste caso há grande duplicidade e redundância, já que todos os sistemas possuem dados de todos os sistemas, gerando inclusive problemas de manutenção dos mesmos, podendo levar a inconsistências. Além disso, a maioria dos sistemas hoje é utilizada para registros eletrônicos de dados clínicos, os PEP (Prontuário Eletrônico do Paciente), que são de tecnologias proprietárias e restritas para recepção de dados externos, tornando inviável essa implementação.

É importante considerar na escolha da solução o contexto em que uma empresa está inserida e os motivadores da interoperabilidade.

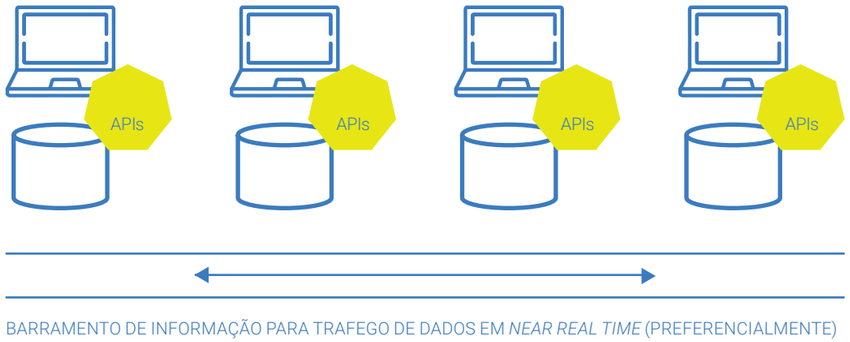
INTEGRAÇÃO EM TEMPO REAL outra forma de implementação é a troca de dados em tempo real; ou seja, a cada solicitação de visualização de dados de um paciente, todos os sistemas conectados processam os dados e respondem ao requisitante. Para essa implementação, exige-se um alto nível de sofisticação de integração sistêmica, com nível de maturidade dos protocolos e tecnologias avançadas, mesmo assim, torna quase impossível o acesso simultâneo a todos os pontos ao mesmo tempo, preservando o intervalo de resposta para obter os dados. No contexto atual, essa adoção não é aplicável.

REPOSITÓRIO CENTRALIZADO sabendo das limitações das práticas acima, é uma boa prática a adoção de uma arquitetura de dados centralizados, que preconiza um **repositório central de dados**. Nessa arquitetura todos os sistemas enviam seus dados para o repositório central, que deve ser capaz de receber os dados, armazená-los, padronizá-los numa linguagem de comum entendimento e disponibilizá-los, preservando questões de segurança e privacidade de dados. Na adoção desse tipo de arquitetura, deve-se considerar o objetivo principal, o interesse do paciente e da gestão de saúde, e portanto os repositórios de saúde devem ser **não exclusivos**.

ARQUITETURA HÍBRIDA na arquitetura híbrida é possível implementar para alguns dados a centralização e para outros a busca em sistemas proprietários em tempo real, desde que o sistema esteja apto a compartilhar dados através do protocolo padrão de interoperabilidade.

A seguir será apresentada uma arquitetura padrão com componentes mínimos de interoperabilidade.

Provedores e Consumidores de informação



Sobre o repositório de dados, é importante que se tenha determinações propostas, reguladas e monitoradas por **agências regulatórias** como ANS, SUS, ISO de sistemas de saúde, Anvisa, ANPD. Atualmente ainda não se tem uma definição sobre o conceito de repositório único de saúde, bem como troca de dados. A RNDS mostrou que tem grande potencial para isso, porém é atualmente uma via de mão unidirecional de informações, recebendo dados do setor privado e ainda não os compartilhando.

4.3. Registro Eletrônico de Saúde (RES)

Como discutido anteriormente, a arquitetura de centralização de dados vem sendo aplicada em âmbito nacional, internacional no setor público e privado. Conceitualmente, para essa centralização de dados, estabelece-se a denominação de "RES". O Registro Eletrônico de Saúde (RES) é um sistema cuja premissa é a centralização da padronização de dados de saúde. Nele são armazenados dados clínicos e histórico de condutas. Estas informações armazenadas num repositório único viabilizam a gestão integral do paciente e a continuidade do cuidado.

A premissa é que esse repositório esteja conectado a diversos sistemas de saúde que através de protocolos de comunicação pré-estabelecidos trocam informações, tanto para registrar dados no RES quanto para consumir dele, viabilizando que o fluxo de dados seja bidirecional. A RNDS é um exemplo de implementação de RES.

4.4. Modelos de informações em saúde

Para que a troca de dados seja efetiva, é importante considerar o contexto da informação conforme momento e local em que foi obtida, e por isso é importante considerar padrões e modelos informacionais no momento da interoperabilidade de dados.

Os modelos de informações em saúde devem ser o ponto de partida para qualquer projeto de implementação de interoperabilidade. É preciso conhecer o contexto do sistema de saúde e os processos nos quais os dados estão envolvidos, bem como poder descrever os dados de saúde através da representação humana e conceitual. Uma vez representados conceitualmente esses dados, com todos os seus elementos, estruturais e semânticos, é possível avançar nas questões de interoperabilidade.

Para que a troca de dados seja efetiva, é importante considerar o contexto da informação conforme momento e local em que foi obtida.

Podemos citar como exemplo uma cirurgia em ambiente hospitalar, em que temos diversos dados sendo gerados. Cada local onde o procedimento ocorre gera dados diferentes que precisam ser conceituados. Assim, em qualquer outra unidade hospitalar, haverá o mesmo conhecimento sobre aquela informação. Como exemplo podemos citar o conceito de Sumário de Alta ou do Classificação Internacional de Doenças (CID).

A definição de modelos de informação facilita e garante a interoperabilidade de dados no nível semântico e sintático.

Dentro do conceito de modelos de informações de saúde, é importante considerar o conceito de arquitetura de documentos clínicos – CDA. Esse padrão estabelece como os dados de saúde são agrupados/agregados

para que seja possível realizar a troca de dados sem ruptura de contexto.

O Ministério da Saúde definiu alguns documentos clínicos, que visam consolidar informações relevantes do ponto de vista clínico para que seja possível continuar o cuidado. Exemplos de documentos clínicos:

- **REGISTRO DE ATENDIMENTO CLÍNICO** registro de dados essenciais preenchido pelos profissionais de saúde durante uma consulta de atenção primária, especializada ou domiciliar.
- **SUMÁRIO DE ALTA** compêndio dos principais registros realizados durante um período de internação.
- **REGISTRO DE IMUNIZAÇÃO** registro dos evento de vacinação com informações de lote e data da imunização.
- **SUMÁRIO DE DISPENSAÇÃO DE MEDICAMENTO** registro dos medicamentos dispensados aos pacientes, com detalhes de lote, fabricante, etc.

Como referência nacional e internacional na modelagem de dados clínicos para o setor de saúde, o OpenEHR especifica os modelos de informações em saúde e seus domínios. Ele representa de forma bem completa e estruturada os conceitos clínicos e também faz menção a terminologias, tema

O Ministério da Saúde estabelece como padrão de arquitetura de documento clínico o HL7 CDA e, para a definição do RES, o modelo de referência OpenEHR.

que será abordado posteriormente. A grande vantagem do OpenEHR é que esta instituição agrega uma comunidade de profissionais que participam ativamente da sua especificação, mantendo-a sempre atualizada. É uma excelente referência para entender o conceito informacional e a organização dos dados clínicos, base para interoperabilidade.

Visando a interoperabilidade semântica nacional, o Ministério da Saúde, através da Portaria nº 2.073, de 31 de agosto de 2011, estabelece como padrão de arquitetura de documento clínico o HL7 CDA e para a definição do RES, o modelo de referência OpenEHR.

Na RNDS, documento técnico publicado em 05/11/2019, o Ministério da Saúde também informa a utilização do OpenEHR como padrão semântico dos documentos trocados.

4.5. Dados mínimos

Além da complexidade sistêmica e processual da interoperabilidade de dados em saúde, é importante considerar os desafios relacionados à diversidade de dados, sistemas e padrões de qualidade de informações. Adotar como premissa o conceito de "dados mínimos" garante que o projeto possa focar entidades e dados principais para atingir os fins desejados. A interoperabilidade completa de todo o prontuário precisa ser analisada, pois muitas vezes a continuidade do serviço assistencial não requer todos os dados de uma internação, por exemplo.

Para fins de redução da fragmentação dos sistemas de saúde, o Ministério da Saúde estabeleceu na Resolução CIT nº 6/2016 o Conjunto Mínimo de Dados (CMD). O decreto de 29/11/2017 determina sua implantação, e a Resolução CIT nº 34/2017 atualiza o modelo informacional. O CMD é voltado a dados administrativos, clínicos-administrativos e clínicos:

- **I – ADMINISTRATIVOS** são aqueles relacionados com a gestão de recursos dos estabelecimentos de saúde que prestam assistência, tais como humanos, materiais ou financeiros;
- **II – CLÍNICO-ADMINISTRATIVOS** são aqueles relacionados com a gestão dos pacientes, enquanto usuários dos estabelecimentos de saúde; e
- **III – CLÍNICOS** são aqueles relacionados ao estado de saúde ou doença dos indivíduos, expressos em diagnósticos, procedimentos e tratamentos realizados. (RESOLUÇÃO CIT Nº 6, DE 25/08/2016)

É prudente que todo projeto de interoperabilidade declare dados mínimos a serem interoperáveis, com foco no valor gerado para os sistemas de saúde local e profissionais envolvidos no processo, bem como para o paciente. O projeto de interoperabilidade deve garantir a evolução da completude de dados de forma iterativa e no tempo. Um "Mapa de Dados" e um roadmap de evolução baseado em valor são exemplos de documentos importantes a serem gerados.

4.6. Protocolos de troca de dados | comunicação

Para agilizar e facilitar a troca de dados entre os diversos serviços e sistemas envolvidos no setor de saúde, é imprescindível a adoção de um protocolo padrão de troca de informações.

O INSTUTUTO HL7 – Health Level Seven é a organização responsável por desenvolver padrões e especificações de troca de mensagens entre diferentes sistemas de saúde. O protocolo HL7 é internacional e foi criado para troca de dados de saúde, clínicos e administrativos. Diversas versões já foram publicadas e as versões mais recentes estão em pleno uso. A primeira nunca se popularizou, e a versão 2.4 do HL7 é amplamente utilizada para troca de dados entre equipamentos de análises clínicas dos hospitais e núcleos de operação de exames e sistemas de LIS, através de comunicação socket.

O protocolo HL7 é internacional e foi criado para troca de dados de saúde, clínicos e administrativos. Diversas versões já foram publicadas e as versões mais recentes estão em pleno uso.

Para a interoperabilidade entre sistemas que vão além dos limites internos das unidades de saúde, o protocolo HL7 V3 foi desenvolvido em 2005, já com uma abordagem disruptiva, orientado a objeto, utilizando princípios de UML e com foco em interoperabilidade semântica.

Para apoiar toda a estratégia de dados, o HL7 V3 estabelece o RIM, o modelo de informação de referência para dados clínicos, administrativos e financeiros.

O Ministério da Saúde, através da Portaria nº 2.073, de 31 de agosto de 2011, após várias iniciativas, decreta como padrão de troca de informação a tecnologia Web Service SOAP em XML e para resultados e solicitações de exames o padrão HL7 V3.

Além do HL7 V3, o padrão de documentos clínicos CDA foi implementado, com a finalidade de "Encapsular" os dados clínicos em Documentos, para que a informação interoperada não perdesse contexto.

O padrão HL7 V3, por utilizar SOAP (tecnologia em desuso), não é mais utilizado atualmente, e o mercado está seguindo para a adoção do HL7 V4, conhecido como HL7 FHIR, que utiliza padrão Restfull para troca de dados.

O HL7 FHIR – Fast Health é um padrão totalmente novo em comparação com as versões anteriores. Ele tem como objetivo implementar, por meio de um conceito resumido de recursos, uma troca de dados de forma facilitada e mais rápida entre as instituições.

O FHIR permite através da representação de seus módulos (recursos) interoperar 80% dos casos clínicos, viabilizando também a extensão de recursos para casos específicos.

Já existem diversas aplicações e servidores desenvolvidos para a utilização e validação do protocolo. A documentação é pública, facilitando o trabalho dos desenvolvedores e sua adoção como protocolo Rest de troca de dados.

Com o lançamento da RNDS em maio de 2020, o protocolo HL7 FHIR foi estabelecido como protocolo padrão de interoperabilidade pelo Ministério da Saúde e já está sendo adotado para troca de dados de imunizações e resultados de exames para diagnóstico de covid-19 entre empresas do setor público e privado.

A SDB recomenda a utilização do protocolo HL7 FHIR para troca de dados entre entidades de saúde, públicas e privadas.

O protocolo FHIR está sendo amplamente utilizado no setor, principalmente para troca de dados, porém existem empresas que também estão utilizando o padrão para persistência e armazenamento de dados no RES. Apesar do protocolo ter sido apresentado para a comunidade como uma simplificação, é de difícil implementação, exigindo profissionais especializados escassos no mercado.

A SDB recomenda a utilização do protocolo HL7 FHIR para troca de dados entre entidades de saúde, públicas e privadas.

4.7. Semântica, padrões de dados, terminologias, vocabulários e ontologias

O termo “interoperabilidade” carrega em si um conceito que por sua vez eleva o nível das integrações de dados. Mais do que integrar dados, interoperar significa viabilizar que a mensagem trocada seja compreendida no nível semântico e dentro do seu contexto pelo receptor, e considerando as diversidades de sistemas geradores de dados, com diferentes formatos e padrões individuais, é importante que se adote um padrão comum de algumas informações a serem trocadas, denominadas terminologias.

O Protocolo FHIR pode ser configurado para utilizar terminologias na troca de dados. Caso não se tenha um padrão público, comum a todas a todos, cada entidade pode “especificar” o seu padrão proprietário.

A seguir descrevemos algumas terminologias adotadas no nível nacional

CID (CLASSIFICAÇÃO INTERNACIONAL DE DOENÇAS) está atualmente na versão 10. Com essa padronização é possível classificar a condição de saúde de um paciente que apresenta algum quadro de diagnóstico de doença.

LOINC (LOGICAL OBSERVATION IDENTIFIERS, NAMES AND CODES) regulamenta os nomes e códigos de resultados laboratoriais e observações clínicas.

ICPC (INTERNATIONAL CLASSIFICATION FOR PRIMARY CARE) contém a classificação internacional de cuidados primários utilizada nos registros clínicos, principalmente de médicos de família.

O Protocolo FHIR pode ser configurado para utilizar terminologias na troca de dados. Caso não se tenha um padrão público, comum a todas a todos, cada entidade pode “especificar” o seu padrão proprietário.

Terminologias são o coração da interoperabilidade, portanto a adoção delas seguindo padrões públicos é de suma importância.

CIF (CLASSIFICAÇÃO INTERNACIONAL DE FUNCIONALIDADE, INCAPACIDADE E SAÚDE) rege a classificação dos resultados e das condições relacionadas à saúde.

SNOMED CT (SYSTEMATIZED NOMENCLATURE OF MEDICINE – CLINICAL TERMS) classifica um evento de saúde com todas as variáveis que o compõem.

TUSS/TISS padrão utilizado para interoperabilidade com sistemas de saúde suplementar, para contas médicas e visão administrativa e financeira. Destaca-se nesse padrão a nomenclatura TUSS, que codifica procedimentos executados, desde atendimentos, exames, cirurgias e até mesmo materiais e medicamentos.

DICOM padronização de dados utilizada para troca e armazenamento de imagens de diagnóstico.

ISBT 128 padronização de etiquetas de produtos relativos ao sangue humano, de células, tecidos e produtos de órgãos.

Visando a interoperabilidade semântica nacional, o Ministério da Saúde, através da Portaria nº 2.073, de 31 de agosto de 2011, estabelece como padrão de codificação de termos clínicos a terminologia SNOMED-CT, DICOM para representação de exames de imagem e LOINC (Logical Observation Identifiers Names and Codes) para codificação de exames laboratoriais. Além dos padrões citados, foram estabelecidos CID, CIAP-2, TUSS e CBHPM. Na RNDS, manteve-se a orientação para uso de LOINC para envio de dados de covid-19 e utilizou-se um padrão próprio do sistema GAL para amostras laboratoriais.

Para padronização de terminologias, recomenda-se a utilização de servidores de terminologias. No caso da RNDS, é empregado o https://simplifier.net/ para os casos de notificações covid-19 com padrões adotados para os itens:

- Exames LOINC
- Divisão Geográfica do Brasil
- Resultado qualitativo do Exame
- Subgrupo da Tabela SUS
- Tipo de Amostra Biológica
- Tipo de Estabelecimento de Saúde
- Grupo de Atendimento
- Via de Administração
- Classificação Brasileira de Ocupações – CBO
- Estratégia de Vacinação
- Exames do GAL
- Raça | Cor
- Imunobiológico
- Local de Aplicação
- Dose de Vacina
- Tipo de Documento
- Etnia Indígena

EXEMPLOS

- https://simplifier.net/redenacionaldedadosemsaude/~resources?category=CodeSystem
- https://simplifier.net/redenacionaldedadosemsaude/~resources?category=ValueSet

Apesar de termos algum avanço, ainda se tem um grande trabalho na manutenção das bases e construção de bases públicas de terminologias inexistentes, como é o caso de dados base de dados de medicamentos.

O tema interoperabilidade e terminologias para a frente de prescrição eletrônica ainda é tabu. Não existe uma regulamentação nacional a respeito de padrões de interoperabilidade para dispensações medicamentosas. Também não se tem padrão definido para prescrições de exames. Recomenda-se o uso do LOINC, porém o grande desafio é a regionalização da nomenclatura de exames, seja na questão da língua, pois o LOINC está em inglês, seja no regionalismo, já que o mesmo exame pode ter nomes diferentes no Brasil. Como alternativa, hoje se utiliza muito o padrão TUSS para nomenclatura nacional, mas esse cadastro foi criado para fins comerciais, é genérico e não representa

unitariamente a especificação técnica dos exames a serem realizados. Criou-se, por volta de 2010, no Brasil, um padrão chamado MEDINC, que seria o LOINC brasileiro correlacionado ao LOINC internacional e a TUSS brasileira, que atendida à granularidade ideal para prescrição de exames. O trabalho era de grande valia, entretanto não foi continuado de forma pública. Algumas empresas nacionais utilizaram a sua última publicação e evoluíram o padrão de forma individual. A SDB recomenda a revitalização/resgate do MEDINC, de forma que alguma entidade pública ou privada possa ser responsável pela sua atualização e distribuição, tornando-se o padrão adotado para prescrições digitais.

Para medicamentos, existe um material que representa a iniciativa de padronização de fármacos proposto pelo SBIS / HL7 Brasil (https://br-pharmacy.gointerop.com/fhir/toc.html) e outra iniciativa em andamento é da OBM, na criação de uma lista padronizada de medicamentos, CMED, que por sua vez não é completa e não representa a granularidade necessária para interoperabilidade, o que pode ocasionar grandes riscos caso tenha uma não associação ao medicamento correto. O mercado de prescrições eletrônicas é novo, composto por startups que usam inclusive como diferencial competitivo suas bases cadastrais.

O SNOMED-CT também precisa ser evoluído para sua ampla utilização. Alguns sites do ministério da saúde trazem isso como pauta: http://www.spms.min-saude.pt/ e www.sns.gov.pt/.

Como orientação, a SDB sugere a utilização das terminologias citadas acima já estabelecidas e definidas pelo Ministério da Saúde. Para os termos ainda não padronizados, sugere-se a intervenção e de alguma frente que possa regulamentar, podendo ser a ANS ou algum órgão do Ministério da Saúde em conjunto com as entidades privadas. Terminologias são o coração da interoperabilidade, portanto a adoção delas seguindo padrões públicos é de suma importância. Fugir de padrões obrigará a existência de "de-paras", que são grandes causas de ineficiência e erros no setor.

4.8. Cadastros nacionais de identificação

Para o sucesso da implementação de interoperabilidade, mais do que as questões de terminologias apresentadas anteriormente, é importante cuidar da identificação única dos "atores" no processo de saúde. Primeiro do paciente, como figura central do cuidado, e do qual os dados representam as condições e evoluções clínicas. O paciente precisa ter uma identificação única e padronizada, considerando as regras regulatórias nacionais, para que a transmissão de seus dados seja feita de modo a identificá-lo como único no sistema que o recebe, e o RES ter uma visão histórica de todos os seus dados independente da unidade de tratamento de saúde pela qual passou. Além da padronização dos dados dos pacientes, todo profissional de saúde, sendo um cidadão, também precisa estar devidamente identificado.

O paciente precisa ter uma identificação única e padronizada.

O Ministério da Saúde estabeleceu o CNS para identificação de cidadãos e profissionais de saúde – Base Estratégica do Sistema Nacional de Informação em Saúde.

O uso do CPF para cidadãos nascidos no Brasil é uma alternativa, considerando que os recém-nascidos já saem da maternidade com o registro, porém é importante considerar que essa não é a realidade nas localidades extremas e em locais menos desenvolvidos, e que por lei a utilização do sistema de saúde não obriga o uso do CPF, somente de um documento de identificação com foto.

Cada entidade deve procurar criar seus MPI (Master Patient Index), preferencialmente utilizando diretrizes do Ministério da Saúde e regulações locais para identificação única dos indivíduos, a fim de que se possa identificar unicamente os cidadãos que passam pelos sistemas de saúde e que possam interoperar seus dados.

No caso da RNDS para notificação de Covid-19, é obrigatório o envio de dados utilizando o CNS como chave de identificação do paciente que realizou o exame.

O paciente precisa ter uma identificação única e padronizada, para que a transmissão de seus dados seja feita de modo a identificá-lo como único no sistema.

Ainda não se tem regularizado o padrão a ser utilizado para estrangeiros, mas sugere-se a utilização de Registro Nacional Migratório (RNM) ou Registro Nacional de Estrangeiros (RNE).

Além da identificação de cidadãos e profissionais de saúde, é importante identificar o estabelecimento de saúde onde o evento de saúde ocorreu. Indica-se a utilização do CNES, que regulamenta os estabelecimentos, inclusive os vínculos dos profissionais de saúde com o estabelecimento. É uma boa prática para inclusive aumentar a qualidade de dados e evitar possíveis fraudes na troca de informações.

A SDB recomenda a utilização de chave única para pacientes, profissionais de saúde e unidades de saúde. Para o paciente, sugere-se utilizar os cadastros nacionais de pessoas nacionais e estrangeiras estabelecidos pelo governo, o CPF para nascidos no Brasil. A não utilização de CPF não pode ser critério para exclusão do paciente do sistema de saúde, então deve-se adotar políticas ou chaves únicas temporárias para que esse paciente não seja desprezado no processo e que possa ser "evoluído" para um cadastro único a partir de políticas de governança de dados, tema que será apresentado na sequência. Para profissionais de saúde, recomenda-se o cadastro do CNS, que por sua vez está vinculado ao cadastro de CBO - Código Brasileiro de Ocupação (especialidades) e CNES (estabelecimentos).

4.9. Governança de dados em saúde

Os itens acima descrevem a importância dos padrões de dados e do uso de terminologias, porém a realidade é que os sistemas têm baixa qualidade de dados, inviabilizando muitas vezes associações e tráfego das informações. Para isso, sugere-se que, com o programa de interoperabilidade, implemente-se um programa de governança e qualidade de dados, que deve cuidar dos processos e qualidades de dados desde o seu nascedouro, nos prontuários de saúde, por exemplo. O time de governança de dados também deve ser responsável por definir regras de qualidade e padrões de tratamento de dados a serem implementados na camada de troca e persistência de dados, bem como por criar um programa de análise e tratamento de inconsistência para garantir que 100% dos registros clínicos sejam interoperáveis.

É importante considerar que, para uma coleta assertiva do dado, no momento e contexto correto, será necessário fazer mudanças nos processos assistenciais. A governança de dados deve caminhar de mãos dadas com os processos assistenciais e, ainda que sejam necessárias mudanças de processos, não podem gerar ônus na operação e experiência de profissionais de saúde. Destaca-se aqui um problema já muito explorado que é a tentativa de digitalização e criação de campos estruturados para o preenchimento de prontuários

4.10. A Lei Geral de Proteção de Dados Pessoais no Brasil, o direito à portabilidade dos dados pessoais e a segurança da informação

Recentemente, em 18 de setembro de 2020, com a entrada em vigor da Lei Geral de Proteção de Dados Pessoais (o "Pessoais" faz parte do nome da lei, embora sua inicial não conste da sigla) (Lei nº 13.709, de 14 de agosto de 2018 – "LGPD"), a proteção das informações pessoais e os dados de saúde passaram a ser regulamentados por um sistema jurídico unificado, em âmbito nacional, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade do titular dos dados.

O Sistema Europeu foi a principal inspiração para a elaboração da legislação brasileira, tomando-se por base os fundamentos do Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation – GDPR), adotado na União Europeia, desde que entrou em vigor, em 25 de maio de 2018.

A LGPD tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade do titular dos dados.

Isto posto, no Brasil, assim como na legislação europeia, os dados de saúde foram categorizados como sensíveis pela LGPD (art. 5º, II), merecendo maior atenção e proteção do legislador quanto ao tratamento de dados realizados pelo setor da saúde, como, por exemplo, as informações constantes do prontuário médico, os resultados de exames laboratoriais, as informações sobre pesquisa clínica, os quais deverão estar em consonância com as disposições previstas nos arts. 7º e 11, de forma a atender e resguardar os direitos dos titulares pacientes garantidos pela nova legislação.

Para assegurar o cumprimento da LGPD, é fundamental que, além da observância das bases legais que autorizam o tratamento de dados sensíveis durante todo o seu ciclo de vida, sejam observados padrões de segurança da informação pelos serviços e sistemas mediante a implementação de contro-

les gerenciais, técnicos e administrativos para reduzir danos prováveis, perda, modificação ou acesso não autorizado aos dados, considerando-se os seguintes fatores: i) identificação do risco; ii) implementação de controles e medidas para mitigar o risco; iii) a rastreabilidade e avaliação do risco.

As informações de saúde são consideradas sensíveis e tratadas de modo diferenciado pela LGPD.

No Brasil, para os controles de segurança da informação, as normas reconhecidas internacionalmente publicadas pela Organização Internacional de Normatização (ISO) e pela Comissão Eletrônica Internacional (IEC), considerando os domínios de controle ISO/IEC 27001, têm sido adotadas por estabelecimentos de saúde para implementar, operar, monitorar, revisar e gerir a segurança da informação (SGSI). A ISO/IEC 27701, extensão da ISO/IEC 27001, também passou a ser objeto de implementação para definição de processos de proteção de informações pessoais em uma base contínua e evolutiva, norma específica para gerenciamento de segurança da privacidade do titular.

Outro modelo de referência para o Brasil que tem sido adotado por estabelecimentos de saúde como boas práticas em privacidade e segurança da informação é a Lei de Portabilidade e Responsabilidade dos Planos de Saúde (HIPAA – Health Insurance Portability and Accountability Act, EUA), criada para modernizar o fluxo de informações de saúde e estabelecer como as informações de dados pessoais mantidas em todos os setores da saúde devem ser protegidas contra fraude e roubo, entre outras regulamentações para as transações eletrônicas de saúde.

Portanto, serviços e sistemas que tratam dados pessoais sensíveis, ou seja, dados de saúde, deverão atender aos comandos da LGPD, a fim de manter a privacidade, integridade, auditabilidade, autenticação do usuário, assinatura eletrônica e guarda dos documentos e informações, resguardando os direitos dos proprietários da informação, ou seja, os indivíduos.

O Direito à Portabilidade (LGPD, art. 11, parágrafo 4º) é uma das importantes novidades trazidas pela nova legislação de proteção de dados. Ao conferir maior garantia ao titular sobre o controle dos seus dados, ampliou seus direitos em relação a outras leis, inclusive as de livre concorrência no mercado. Considerando que, o "dono" do dado pessoal é o próprio titular, ficou assegurado ao titular o direito de levar seus dados, de forma facilitada e para onde quiser, sendo a portabilidade parte dos mecanismos de acesso, modificação, exclusão, transferência ou processamento (por si ou por terceiros) de seus próprios dados.

A LGPD define o direito à portabilidade de dados como a transferência dos dados para outro prestador de serviço ou produto, mediante solicitação expressa do titular, sujeito ao sigilo comercial e industrial, nos termos da regulamentação da ANPD (LGPD, art. 18, V).

O art. 40 da LGPD atribuiu à ANPD a competência para dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, com a observância dos princípios da necessidade e transparência.

Há de se destacar, neste ponto, que a LGPD vedou expressamente a comunicação ou uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, com exceção para as hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados (art. 11., parágrafo 4º), e para permitir a portabilidade de dados quando solicitada pelo titular (art. 11., parágrafo 4º, I), ou para transações financeiras e administrativas resultantes do uso e da prestação dos referidos serviços (art. 11., parágrafo 4º, II). No entanto, há expressa proibição às operadoras de planos privados de assistência à saúde que o

O Direito à Portabilidade (LGPD, art. 11, parágrafo 4º) é uma das importantes novidades trazidas pela nova legislação de proteção de dados.

tratamento de dados de saúde seja realizado para a prática de seleção de riscos na contratação de qualquer modalidade, e/ou para a contratação e exclusão de beneficiários (art. 11., parágrafo 5º).

Para que o direito à portabilidade seja efetivamente garantido ao titular, será necessário estabelecer padrões e normas. A segurança, mencionada no art. 40, deverá ser uma das primeiras preocupações dos agentes de tratamento, tendo em vista que qualquer sistema ou interface que permita o acesso a dados pessoais deverá ser revestido de controles de segurança para inibir o acesso não autorizado aos dados pessoais lá armazenados.

Outro ponto sensível com relação à segurança será a identificação do titular que se apresenta e faz a solicitação de portabilidade de suas informações. A falha do controlador nessa identificação poderá acarretar num incidente de segurança relacionado aos dados, cujos prejuízos são incalculáveis para o titular, dependendo da informação vazada ou compartilhada indevidamente, além da possibilidade de aplicação de sanções pela ANPD.

Quanto aos padrões de interoperabilidade, sob a ótica do direito de portabilidade do titular, será necessário que os sistemas informatizados consigam processar as informações portadas entre eles, sob pena de não se dar efetividade a essa garantia legal ao titular de dados.

A portabilidade tem impactos na responsabilidade dos agentes de tratamento dos dados pessoais. Ao realizar a portabilidade de um controlador para outro, os dados podem deixar de existir junto ao controlador que os enviou, transferindo a responsabilidade, naquele mesmo ato, ao controlador que os recebeu. A atenção deverá ser redobrada nesse sentido, visto que o direito à portabilidade não necessariamente pressupõe a exclusão automática dos dados pelo

As dificuldades para a portabilidade e a interoperabilidade dos dados podem surgir se eles forem armazenados em formatos proprietários.

controlador que os detinha, sujeito ao cumprimento de prazos mínimos legais para retenção dos dados, ainda que contrariamente à vontade do titular.

As dificuldades para a portabilidade e a interoperabilidade dos dados podem surgir se eles forem armazenados em formatos proprietários. Nesse contexto, é provável que todos os sistemas de armazenamentos de dados pessoais que estiverem em conformidade com a Lei Geral de Proteção de Dados Pessoais estarão aptos a atender aos padrões de interoperabilidade regulamentados pela Autoridade Nacional de Proteção de Dados.

4.11. LGPD & privacidade

A privacidade deverá ser observada desde a concepção no desenvolvimento de sistemas, conforme determina expressamente a LGPD. A "*privacidade by design*" impõe a incorporação da privacidade durante todo o ciclo de vida no tratamento dos dados, desde o estado inicial até o descarte, levando-se em conta sete princípio básicos: i) ser proativo, não reativo; preventivo, não corretivo; ii) adotar a privacidade como padrão; iii) adotar a privacidade integrada na concepção do produto ou do serviço embarcado na tecnologia; iv) funcionalidade total -saldo positivo, não zero a zero; v) segurança de ponta a ponta durante todo o ciclo de vida; vi) visibilidade e transparência; vii) respeito pela privacidade do usuário;

A SDB recomenda que as soluções de interoperabilidade possam estar aderentes às questões de privacidade de modo que o titular de dados possa exercer todos os seus direitos.

A SDB recomenda que as soluções de interoperabilidade possam estar aderentes às questões de privacidade de modo que o titular de dados possa exercer todos os seus direitos. Como pilar desses direitos, o consentimento de dados deve ser implementado em todas as pontas do processo e com total transparência para o titular, que deverá ter ciência sobre o tráfego/compartilhamento e a finalidade de uso dos seus dados.

A depender da finalidade do uso da informação, a tutela da saúde tem soberania sobre a questão de necessidade de consentimento do paciente. Em condições de extremo risco de morte, o profissional de saúde pode ter acesso a todo histórico de saúde de um determinado paciente sem que o mesmo tenha consentido. É importante que as soluções de interoperabilidade estejam aptas para viabilizar esse controle de acesso a dados.

4.12. LGPD, PEP e RES

O prontuário médico, assim definido pela Resolução nº 1638/2002, do CFM (art. 1º), é um documento único constituído por um conjunto de informações, sinais e imagens registradas de conhecimento do histórico de saúde do paciente, e de assistência a ele prestada, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo, de caráter legal, sigiloso e científico.

Tradicionalmente, os prontuários eram corporificados em arquivos em papel. Com a evolução das formas digitais e magnéticas, os prontuários passaram a ser em suporte digital. O Conselho Federal de Medicina, através das Resoluções CFM nº 1.639/2002, 1.821/2007 (conforme alterada) e 2.218/2018, passou a regulamentar normas técnicas referentes à digitalização e ao uso dos Sistemas Informatizados para a Guarda e Manuseio dos Documentos dos PEP, e dos Sistemas de RES, elevando os patamares de conformidade – NGS1 – Nível de Garantia de Segurança 1, e NGS2 – Nível de Garantia de Segurança 2, quanto à observância do caráter sigiloso, da privacidade e da segurança das informações.

Importante destacar, ainda, que a Lei nº 13.787, de 27 de dezembro de 2018, regulamentou a digitalização e utilização de sistemas informatizados para os prontuários de pacientes, tendo estabelecido, no tocante à manutenção dos registros médicos, após decorrido o prazo mínimo de 20 anos a partir do último registro, os prontuários, independentemente de sua forma de armazenamento, em suporte de papel e os digitalizados, poderão ser eliminados. Alternativamente à eliminação, o prontuário poderá ser devolvido ao paciente, observados, em qualquer caso, a proteção da intimidade e o sigilo das informações.

Os dados pessoais e sensíveis de pacientes tratados em PEP e em bases de dados estruturadas em RES deverão obedecer aos princípios que regem as atividades do tratamento de dados pessoais, conforme disposto no art. 6º da LGPD.

O Princípio da Finalidade (LGPD, art. 6º, I) dispõe sobre o propósito do tratamento de dados, devendo ser legítimo, específico, explícito e informado ao titular.

O Princípio da Finalidade (LGPD, art. 6º, I) dispõe sobre o propósito do tratamento de dados, devendo ser legítimo, específico, explícito e informado ao titular. Neste aspecto, é importante estabelecer termos de aditamento aos prontuários que informem a sua integração em bases de dados mais amplas e da eventual utilização dos dados para estudos científicos e análise estatísticas com a finalidade de aplicação em estudos de saúde, dada a condição de anonimato e vedada a utilização comercial. O desrespeito dos limites das finalidades informadas ao titular viola, ainda, o princípio da adequação (LGPD, art. 6º, II) e o da limitação ao tratamento mínimo (LGPD, art. 6º, III).

O Princípio da Garantia de Acesso e Controle do Titular Sobre os seus Dados (LGPD, art. 6º, IV) dispõe sobre o direito dos titulares em ter "consulta facilitada e gratuita" aos dados e a forma como são tratados, considerando que tais dados deverão ser de qualidade (LGPD, art. 6º, V). O Princípio da Transparência (LGPD, art. 6º, VI) impõe aos agentes de tratamento a disponibilização de informações "claras, precisas e facilmente acessíveis" sobre a realização do tratamento, resguardados os segredos industrial e comercial. Nesse aspecto, é importante que os sistemas estejam aptos a conferir acesso aos prontuários e sobre o próprio tratamento realizado.

Por fim, os Princípio da Proteção, Segurança, Prevenção, Não Discriminação e Responsabilização e Prestação De Contas (LGPD, art. 6º, VII a X) visam proteger os titulares contra acessos não autorizados e de situações

acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, bem como contra o uso discriminatório ou abusivo. Neste sentido, os sistemas deverão adotar medidas técnicas e administrativas aptas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, mediante a implementação de controles gerenciais para identificação, mitigação e rastreabilidade das informações em todo o ciclo de vida dos dados, a fim de garantir a confidencialidade, integridade e disponibilidade ao titular.

As bases legais para tratamento de dados pessoais previstas no art. 7 (I a X), da LGPD, são relevantes para o tratamento de dados na área da saúde.

Deve ser informado ao titular paciente, inclusive, e em especial, o compartilhamento dos dados com outros profissionais da mesma clínica, do mesmo hospital ou do mesmo plano de saúde.

No tocante ao consentimento (art. 5º, XII), poderá ser considerada boa prática a obtenção de consentimento de PEP e a inclusão dos dados em outras bases, com e sem anonimização, tendo em vista que as funções dos prontuários médicos são diversas, e deve ser informado ao titular paciente, inclusive e em especial, o compartilhamento dos dados com outros profissionais da mesma clínica, do mesmo hospital ou do mesmo plano de saúde.

Para fins sanitários, é permitido pela LGPD a realização do tratamento dos dados sem o consentimento do seu titular, quando necessário para a proteção da vida e da incolumidade do titular ou de terceiros, em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridade sanitária. No tocante à tutela da saúde, é importante ressalvar que o tratamento de dados do titular sem o seu expresso consentimento tem incidência apenas para os procedimentos realizados por profissionais da saúde que apresentem regularidade formal do exercício de atividade de acordo com o órgão regulatório de cada profissão. Nesses casos, não está autorizado o tratamento de dados em favor de terceiros.

Por fim, é importante destacar que o legítimo interesse do controlador (LGPD, art. 10) poderá fundamentar tratamento de dados pessoais para

finalidades legítimas, consideradas a partir de situações concretas, preservados os direitos e as liberdades fundamentais do titular, em casos de apoio e promoção de atividades do controlador, proteção do exercício regular dos direitos do titular ou para a prestação de serviços que o beneficiem. Nessas hipóteses, há expressa previsão legal (parágrafo 2º, art. 10), que somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados. Os dados de saúde (e outros dados sensíveis) não podem ser tratados com base no legítimo interesse.

Ainda sobre a aplicabilidade da LGPD em PEP e RES, o Código de Ética Médica (alterado pela Resolução nº 2.217 c.c. Resoluções CFM nº 2.222/2018 e 2.226/2019) prevê, em seu art. 87, a obrigatoriedade de elaboração de prontuário pelo médico para a finalidade específica da criação de um registro médico e do histórico do paciente. Os efeitos do consentimento do paciente serão relevantes para eventual responsabilização dos limites do consentimento, da informação e do esclarecimento fornecido pelo profissional. Sendo assim, a importância do consentimento, nesses casos, é mitigada pelos aspectos legais e regulatórios determinantes ao médico, de acordo com a finalidade, a adequação e o tratamento mínimo (LGPD, art. 11, II, "a" – não se exige o consentimento em caso de obrigações legais e regulatórias).

Somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

O controlador deverá ter o mapeamento do tempo de guarda dos dados pessoais tratados. Independentemente de qualquer pedido do titular, o controlador deverá ter seus processos bem definidos de exclusão de dados pessoais, de acordo com o art. 6º, III, da LGPD, os quais devem, de fato, ser excluídos após o término do seu tratamento. Para tanto, cada atividade de tratamento de dados identificada pelo controlador deverá ter a previsão de prazo máximo de retenção, após o qual os dados devem ser excluídos ou anonimizados.

4.13. A importância das agências regulatórias

A interoperabilidade é necessária para o avanço da saúde digital e saúde 4.0. Empresas públicas e privadas já estão se movimentando para criar sua estratégia de interoperabilidade, porém dois temas são cruciais para os avanços e requerem o direcionamento regulatório:

1 DADOS PADRONIZADOS | TERMINOLOGIAS | PADRÕES em relação a padrão de dados, as terminologias precisam avançar e, por serem "compartilhadas", é necessário atuação de alguma agência regulatória para a sua governança, ainda que se tenha a participação de entidades privadas e públicas na sua confecção. As bases de terminologias precisam estar disponíveis e serem atualizadas conforme o avanço do setor, porque novas formas de se fazer medicina surgem, precisando nascer regularizadas e interoperáveis (ex.: novos devices precisam ser aprovados pela Anvisa e padrões de interoperabilidade deveriam ser um critério para entrada no mercado).

2 DIRETRIZES DE ACESSO A DADOS estamos na era da informação e sua posse traz poder e vantagens competitivas. A cultura de compartilhamento de dados, princípio e fim de interoperabilidade, ainda não é uma prática no setor, que, apesar de querer avançar para estratégias de *value based* ainda se sente ameaçado pela perda de poder com o compartilhamento de dados. Além das questões estratégicas, questões de interesses e ética precisam ser consideradas, principalmente tratando-se de dados de saúde. As entidades reguladoras precisam estar presentes e criar meios para atuar na governança do compartilhamento e uso de dados, impedindo, por exemplo que, as operadoras ou verticalizadas utilizem-se de dados clínicos para geração de produtos que podem discriminar ou inviabilizar o acesso à saúde para uma parcela dos cidadãos.

As entidades reguladoras precisam estar presentes e criar meios para atuar na governança do compartilhamento e uso de dados.

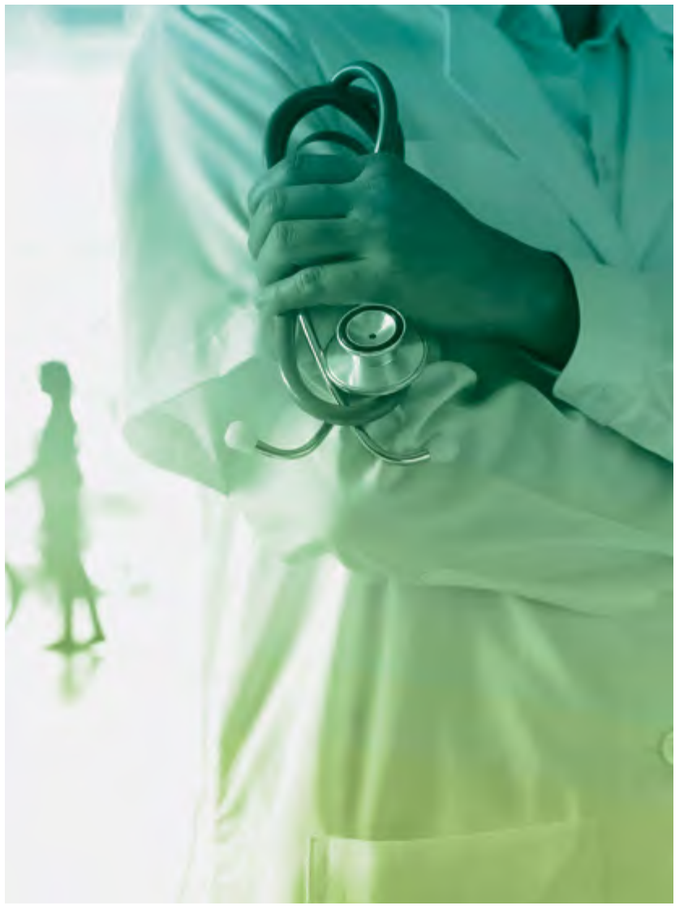
As agências regulatórias Anvisa, ANS, ANPD e iniciativas do Ministério da Saúde em conjunto com organizações não governamentais têm um papel fundamental no avanço da interoperabilidade e precisam progredir nas questões de governança de terminologias, padrões e processos de governança, assim como diretrizes de acesso a dados clínicos.

4.14. Centralização e portabilidade de dados

Reconhecemos a propriedade e a privacidade dos dados em saúde como direito humano de todos os cidadãos. Assim sendo, a portabilidade de dados deve respeitar sempre o interesse primeiro do cidadão, e como direito essencial à liberdade de compartilhar ou não, de ter por parte de seus operadores o compromisso público de guarda e transferência de forma oportuna e estruturada que permita a imediata continuidade de seus cuidados em saúde.

A SBD tem o compromisso de fortalecer e apoiar toda iniciativa de criação de repositórios de informação em saúde, reconhecendo a RNDS como instrumento indispensável e de grande relevância na construção de um sistema de saúde mais justo e democrático no Brasil, da mesma forma como nos posicionamos contra a construção de qualquer monopólio da informação em saúde no Brasil.

Considerando as garantias legais estabelecidas no art. 170 da Constituição Brasileira que definem como princípio constitucional a livre iniciativa, e os fundamentos que disciplinam a proteção de dados no território nacional previstos no art. 2º da LGPD, tais como a proteção à privacidade de dados, a autonomia sobre a consulta e o uso de dados em saúde como princípio de direito humano, a SDB que a centralização compulsória e exclusiva não pode ser unicamente destinada a apenas um repositório.



A associação entende que é fundamental a garantia à livre iniciativa privada na construção, na manutenção e no desenvolvimento de repositórios de informações em saúde no Brasil, sem a qual não será possível alcançar todas as dimensões necessárias à governança de dados em saúde no país, bem como à cooperação com organismos internacionais da forma recomendada pela OMS, de forma oportuna e ágil como as que são exigidas em eventos de emergência de saúde pública.

A construção deste conjunto do registro de dados em saúde deve permitir não apenas o registro dos profissionais médicos, mas também o de todos os profissionais envolvidos no cuidado, bem como os fornecedores da cadeia de suprimentos, e essencialmente dos registros a serem feitos pelo próprio paciente, por registro de voz, gráfico, escrito ou aquele imputado por meio de dispositivos que captam dados do paciente e gravam os essenciais em seu registro pessoal.

A prática de troca e intercâmbio de dados deve ser feita de maneira bidirecional sem a qual é impossível a construção de um registro único e de conteúdo progressivamente crescente de informações, bem como a coordenação do cuidado em saúde. Assim, essa entidade assume o compromisso público de fomentar a integração e cooperação no intercâmbio de dados mediante a autorização de seus proprietários, os cidadãos.

É fundamental a garantia à livre iniciativa privada na construção, na manutenção e no desenvolvimento de repositórios de informações em saúde no Brasil.

As iniciativas das empresas signatárias desta associação se comprometem a estruturar suas unidades de negócio de maneira a manter sua base de Registro de Dados em Saúde dentro de uma governança em que seja respeitada toda a legislação de dados e nas previsões do art. 11, IV, parágrafo 1º.

A portabilidade de dados é um direito do titular, e ainda não está regulamentada pela ANP ou pelo Ministério da Saúde. Esse tema precisa estar em pauta para que as soluções de interoperabilidade implementem funcionalidades que viabilizem essa operação. A HIPPA, lei norte-americana, pode servir de inspiração para questões de segurança e portabilidade de dados.

4.15. *Data home* em saúde

Entendemos que a centralização dos dados em saúde é essencial para a garantia do intercâmbio seguro e construtivo dos dados em saúde, da mesma forma que compreendemos que, respeitado o interesse público e de livre iniciativa, não deve existir monopólio dos dados em saúde no Brasil e, assim como a RNDS, deve ser reservada a qualquer iniciativa – privada ou privada – a possibilidade de estruturação de unidades de negócio que tenham como atividade econômica o compartilhamento de arquivos eletrônicos protegidos de informações de saúde entre duas ou mais entidades não filiadas, em benefício e mediante o consentimento do titular dos dados, nos termos em que prevê a lei.

Essas instituições são aqui denominadas como Organizações de Intercâmbio de Dados em Saúde (OIDS).

5. FATORES IMPORTANTES NA ADOÇÃO DE INTEROPERABILIDADE

1. A estratégia deve ser apoiada por *sponsors* de tecnologia, gestão estratégica e gestão do corpo clínico. O projeto é complexo, longo e de custo alto, por abranger disciplinas médicas, técnicas e processuais que vão além da tecnologia.

2. A estratégia de desenvolvimento de sistema é pautada em processos e experiência dos usuários e entrega de valor. Visão de dados mínimos considerando o contexto do usuário – local, infraestrutura disponível e tráfego de informações, tempo disponível para prestação e registros, dispositivo disponível (PC, mobile, smartphone). Considerar que menos é mais e que muita informação não é sinônimo de melhor precisão no cuidado, informação certa, no tempo certo. Deve-se priorizar as informações relevantes para a operação e estratégia de cuidado adotada no momento corrente.

3. A estratégia de desenvolvimento de projetos deve usar metodologias ágeis, entregando valor de forma iterativa, priorizando a maturidade dos sistemas envolvidos, do time de desenvolvimento e a capacidade da ponta de absorver mudanças processuais para consumo de novos dados.

4. Deve-se ter uma equipe multidisciplinar atuando no projeto de forma orquestrada.

5. Deve-se seguir padrões e boas práticas preconizados pelo Ministério de Saúde e órgãos competentes direcionadores e reguladores.

6. Temas de governança de cadastros, padronização de dados, infraestrutura e processos deverão caminhar juntos na implementação do projeto.

6. CONCLUSÃO

A adoção da interoperabilidade depende de diversas frentes que precisam fazer parte de um plano de estratégia de saúde digital, desde a informatização dos sistemas de saúde até a educação e o engajamento dos profissionais no uso correto dos sistemas informatizados de saúde, como prontuários eletrônicos e sistemas de gestão hospitalares.

A interoperabilidade e a informatização não garantem melhorias e boas práticas de gestão e assistência, então é imprescindível que no projeto estratégico de saúde digital estejam contempladas revisões e adequações de processos e diretrizes de cuidados, considerando a visão integrada e longitudinal do paciente

Ainda é um desafio a complexidade da implementação técnica de sistemas robustos e complexos em dados de saúde, considerando também o custo de projetos que devem incluir recursos computacionais caros e mão de obra

A adoção da interoperabilidade depende de diversas frentes que precisam fazer parte de um plano de estratégia de saúde digital

A interoperabilidade visa melhorar toda a experiência de saúde de toda a população, saudáveis e doentes, dos profissionais de saúde e de gestores de saúde, no âmbito operacional, tático e estratégico.

O Ministério da Saúde estabeleceu planos robustos para avanços na saúde digital, com metas e objetivos até 2028, que consideram a integração dos setores público e privado não só na troca de dados mas como também de serviços, pautados pelo Programa do Connect SUS, em que a RNDS materializa em sistema informacional a plataforma de integração e centralização de dados e serviços de saúde.

Apesar de o plano nacional estar estruturado na RNDS, é preciso considerar o cenário político e econômico do país e que mecanismos de financiamento são necessários para o avanço no setor público. É preciso considerar também o momento único que estamos vivendo na economia das healthtechs e startups de saúde, e nesse cenário o setor privado precisa criar mecanismos para, a partir das diretrizes do Ministério da Saúde, e padrões mínimos possam desenvolver seus sistemas digitais de saúde interoperáveis, viabilizando no futuro a integração de serviços e dados de saúde com todos os players do mercado privado e do setor público.

Este documento dá pistas para que as iniciativas do setor privado tenham uma base sólida comum, e diretrizes para o desenvolvimento de seus sistemas digitais e de interoperabilidade em saúde, viabilizando que o Ecossistema de Saúde Digital aconteça da forma mais fluida possível.

Lembramos que a interoperabilidade visa melhorar toda a experiência de saúde de toda a população, saudáveis e doentes, dos profissionais de saúde e de gestores de saúde, no âmbito operacional, tático e estratégico.

REFE-
RÊN-
CIAS
BIBLIO-
GRÁFI-
CAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 29/05/2022.

CAVOUKIAN, Ann. Privacy by Design. The 7 Foundational Principles. Disponível em: https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf. Acesso em 29/05/2022.

CFM. RESOLUÇÃO CFM Nº 2.314/2022. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2022/2314_2022.pdf. Acesso em 29/05/2022.

CFM. RESOLUÇÃO CFM Nº 2.299/2021. Disponível em: https://sistemas.cfm.org.br/normas/arquivos/resolucoes/BR/2021/2299_2021.pdf. Acesso em 28/03/2021.

CIS CONTROLS. CIS Controls v7. Disponível em: https://www.cisecurity.org/controls/v7. Acesso em 29/05/2022.

CIS CONTROLS. CIS Controls v8. Disponível em: https://www.cisecurity.org/controls/v8. Acesso em 29/05/2022.

ISO. ISO/IEC 27001:2013. Disponível em: https://www.iso.org/standard/54534.html. Acesso em 29/05/2022.

ISO. ISO/IEC 27003:2017. Disponível em: https://www.iso.org/standard/63417.html. Acesso em 29/05/2022.

ISO. ISO/IEC 27004:2016. Disponível em: https://www.iso.org/standard/64120.html. Acesso em 29/05/2022.

ISO. ISO/IEC 27005:2018. Disponível em: https://www.iso.org/standard/75281.html. Acesso em 29/05/2022.

AGUIAR, Geysa; DA SILVA, Lourival Alves; FERREIRA, Marco Antônio Magalhães. Ilegibilidade e ausência de informação nas prescrições médicas: fatores de risco relacionados a erros de medicação. **Revista Brasileira em Promoção da Saúde**, v. 19, n. 2, p. 0, 2006.

BRASIL. Ministério da Saúde. **Contribuições para o uso racional de medicamentos**. 2021. Volume I. Disponível em: https://www.gov.br/saude/pt-br/assuntos/saude-de-a-a-z/u/arquivos/contribuicoes-para-o-uso-racional-de-medicamentos.pdf. Acesso em 29/05/2022.

BRASIL. Ministério da Saúde. **Estudo de modelos internacionais de governança em saúde digital**. 2021b. Disponível em: https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/ModelosinternacionaisdeGovernanaemSadeDigital.pdf. Acesso em 29/05/2022.

BRITO, Juan P.; KUNNEMAN, Marlene; MONTORI, Victor M. **Tomada de decisão compartilhada**. [202-]. Disponível em: https://stg-bestpractice.bmj.com/info/pt/mbe-toolkit/pratique-mbe/tomada-de-decisao-compartilhada/. Acesso em 29/05/2022.

GIMENES, Fernanda Raphael Escobar et al. Influencia de la redación de la prescripción médica en la administración de medicamentos en horarios diferentes al prescripto. **Acta Paulista de Enfermagem**, v. 22, n. 4, p. 380-384, 2009.

MADRUGA, Célia Maria Dias; SOUZA, Eurípedes Sebastião Mendonça. **Manual de orientações básicas para prescrição médica**. 2. ed. rev. e amp. Brasília: CRM-PB/CFM, 2011. Disponível em: https://portal.cfm.org.br/images/stories/biblioteca/cartilhaprescrimed2012.pdf. Acesso em 29/05/2022.

OCDE. **Bringing healthcare to the patient**: an overview of the use of Telemedicine in OECD countries. 2020. Disponível em: https://www.oecd-ilibrary.org/social-issues-migration-health/bringing-health-care-to-the-patient_8e56ede7-en. Acesso em 29/05/2022.

OSÓRIO DE CASTRO CGS, PEPE VLE. **Nota técnica: Prescrição de medicamentos**. ENSP/Fiocruz, Rio de Janeiro, 2011.

WTW. **Pesquisa 2021 Global Medical Trends – Resultados da América Latina**. Willis Tower Watson. Disponível em https://www.wtwco.com/-/media/WTW/Insights/2020/11/pesquisa-2021-global-medical-trends.pdf. Acesso em 29/05/2022.

SDB. **Benchmarking revela que países referência em saúde no mundo liberam que primeiras consultas sejam realizadas à distância**. 2021a. Disponível em: https://saudedigitalbrasil.com.br/publicacoes/benchmarking-revela-que-paises-referencia-em-saude-no-mundo-liberam-que-primeiras-consultas-sejam-realizadas-a-distancia/. Acesso em 29/05/2022.

SDB. **Entidade aponta que telemedicina salvou mais de 75 mil vidas entre 2020 e 2021**. 2021b. Disponível em: https://saudedigitalbrasil.com.br/publicacoes/entidade-aponta-que-telemedicina-salvou-mais-de-75-mil-vidas-entre-2020-e-2021/. Acesso em 29/05/2022.

VRIES, T. P. G. M. et al. **Guia para a boa prescrição médica**. Porto Alegre: ArtMed, p. 67-71, 1998. Disponível em: https://pesquisa.bvsalud.org/bvsms/resource/pt/mis-18925. Acesso em 29/05/2022.

LEGISLAÇÃO

- Lei nº 5.991, de 17 de dezembro de 1973.
- Lei nº 14.063, de 23 de setembro de 2020.
- Lei nº 13.021, de 8 de agosto de 2014.
- Lei nº 13.989, de 15 de abril de 2020.
- Lei nº 6.360, de 23 de setembro de 1976.
- Lei Geral de Proteção de Dados.
- RDC nº 96, de 17 de dezembro de 2008.
- Portaria nº 344, de 12 de maio de 1998.
- Código de Ética Médica.
- Código de Ética Farmacêutica.
- Lei no. 13.709, de 14 de agosto de 2018
- Resolução CFM 2.299, de 26 de outubro de 2021
- Resolução CFM 2.314, de 05 de maio de 2022

http://fhir.org/

https://restfulapi.net/

http://aps.saude.gov.br/ape/esus/manual_3_2/introdutorio

http://aps.saude.gov.br/ape/informatizaaps

http://bvsms.saude.gov.br/bvs/saudelegis/cit/2017/res0019_13_07_2017.html

http://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html

http://cnes.datasus.gov.br/

http://openehr.org.br/

http://www.ans.gov.br/images/stories/Interecoes_com_ANS/Apresentacao_CSS/css_93_apresentacao_registro_eletronico.pdf

http://www.ans.gov.br/prestadores/tiss-troca-de-informacao-de-saude-suplementar

http://www.campogrande.ms.gov.br/cartadeservicos/artigos/links-e-terminologia-em-saude/

http://www.providersedge.com/ehdocs/ehr_articles/health_info_exchange_business_models.pdf

http://www.sbmfc.org.br/wp-content/uploads/media/file/CIAP 2/CIAP Brasil_atualizado.pdf (CIAP)

http://www.snomed.org/

http://www2.datasus.gov.br/DATASUS/index.php?area=060203 (CID-10)

https://bvsms.saude.gov.br/bvs/IIIfis/pdf/Rogerio_Sugai.pdf

https://bvsms.saude.gov.br/bvs/publicacoes/estrategia_saude_digital_Brasil.pdf

https://bvsms.saude.gov.br/bvs/saudelegis/gm/2011/prt2073_31_08_2011.html

https://conjuntominimo.saude.gov.br/#/

https://datasus.saude.gov.br/faq/informacoes-tecnicas/

https://hapifhir.io/

https://loinc.org/

https://mobileapps.saude.gov.br/portal-servicos/files/f3bd659c8c8ae3ee966e575fde27eb58/bc79b5cd9a740fec75045a23d19a67d6_3m802imji.pdf

https://rnds.saude.gov.br/

https://rnds-guia.saude.gov.br/docs/rnds/tecnologias/

https://slideplayer.com.br/slide/11912242/

https://www.conasems.org.br/

https://www.conasems.org.br/wp-content/uploads/2019/02/Estrategia-e-saude-para-o-Brasil-1.pdf

https://www.conass.org.br/resolucoes-cit/

https://www.conass.org.br/wp-content/uploads/2016/12/RESOLUCAO-N_6_16.pdf (CMD – Conjunto Mínimo de Dados)

https://www.gov.br/ans/pt-br/arquivos/assuntos/prestadores/padrao-para-troca-de-informacao-de-saude-suplementar-tiss/padrao-tiss/padrao_tiss_componente_organizacional_202104.pdf

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guia-boas-praticas-lgpd

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital

https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/a-estrategia-brasileira

https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/EstrategiaesaudeparaoBrasil_CIT_20170604.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/EstratgiaeSadeparaoBrasil.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/PlanodeAoMonitoramentoeAvaliao.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/PlanoDiretordeTecnologiadaInformaoeComunicao.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital/a-estrategia-brasileira/PolticaNacionaldeInformaoeInformtica.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/AesparaaAdequaodaRNDSLGPD24.06.2020.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/ApresentaodaReunioTcnicaRNDSLanamentoemAlagoas12.11.2019.pdf

https://www.gov.br/saude/pt-br/assuntos/saude-digital/material-de-apoio/material-de-apoio

https://www.gov.br/saude/pt-br/assuntos/saude-digital/monitoramento-e-avaliacao-da-esd/monitoramento-e-avaliacao-da-esd

https://www.who.int/docs/default-source/documents/gs4dhdaa2a9f352b0445bafbc79ca799dce4d.pdf

ASSOCIADOS

Conexa

DASA

DOC24

Docway

ALBERT EINSTEIN
SOCIEDADE BENEFICENTE ISRAELITA BRASILEIRA

saúde iD

L2D SAÚDE DIGITAL

memed

mevo

PRORADIS

Receita Digital

sabin MEDICINA DIAGNÓSTICA

Starbem CUIDANDO DA SUA SAÚDE

Teladoc HEALTH

TopMed SAÚDE DIGITAL

Tuinda Care

unio digital

ViBe saúde

Saúde Digital Brasil

11 97818 4456

CONTATO@SAUDEDIGITALBRASIL.COM.BR

IMPRENSA@SAUDEDIGITALBRASIL.COM.BR

REDES SOCIAIS: SAUDEDIGITALBRASIL