Rio PREFEITURA | RIOSAÚDE

CARTILHA DE BOAS PRÁTICAS

USO SEGURO DE APLICATIVOS DE MENSAGEM

Rio PREFEITURA | RIOSAÚDE

CARTILHA DE BOAS PRÁTICAS

USO SEGURO DE APLICATIVOS DE MENSAGEM

Rio de Janeiro • 2023

ÍNDICE

INTRODUÇÃO

Com a entrada em vigor da Lei Geral de Proteção de Dados (LGPD), as empresas precisam se adaptar a uma nova realidade a respeito da proteção dos dados pessoais. Nesta Cartilha de Boas Práticas do uso de aplicativos de trocas de mensagens instantâneas, apresentaremos orientações para utilização desses aplicativos de acordo com as melhores práticas.

Sabemos que muitos aplicativos (apps) são uma excelente ferramenta para se comunicar com agilidade. A troca de mensagens e o envio de arquivos de maneira simples e rápida são algumas das características que fizeram esses aplicativos serem bastante populares, sendo utilizados tanto para assuntos pessoais quanto de trabalho. No entanto, sabemos também que não são aplicativos corporativos, mas que temos a cultura de utilza-los em ambiente de trabalho em razão dessas facilidades mencionadas. Com isso, deve-se ter em mente que o uso sem a devida cautela, pode trazer uma série de riscos para o usuário e a empresa.

Pensando nisso, elaboramos esta cartilha com orientações e adaptações que devem ser realizadas pelos usuários nas empresas para utilização dos aplicativos de comunicação de forma mais segura e de acordo com as boas práticas.

CONCEITOS

A **Lei Geral de Proteção de Dados Pessoais** (LGPD - Lei nº 13.709/18) representa um importante avanço para o Brasil, pois garante maior controle dos cidadãos sobre suas informações pessoais.

Afinal, nossos dados revelam muito sobre nós, não é mesmo? Assim, sua proteção é indispensável.

Quando uma pessoa, ou um paciente, por exemplo, concede à unidade de saúde os seus dados pessoais espera que os mesmos sejam utilizados apenas para o fim consentido e que estejam protegidos contra quaisquer incidentes de violação de dados.

Na RioSaúde, a adequação à LGPD é tratada com seriedade, devendo estar presente em todas as etapas do nosso trabalho, desde um simples cadastro em uma vaga no site da empresa até às trocas de informações entre fornecedores, colaboradores e afins.

É importante ressaltar alguns conceitos para uma melhor compreensão da LGPD:

- **DADOS PESSOAIS:** são quaisquer tipos de dados que identifiquem uma pessoa ou permitam identificá-la. Em unidades de saúde são exemplos de dados pessoais comuns o nome e o telefone de pacientes.

- **DADOS PESSOAIS SENSÍVEIS:** são os que se referem a temas sensíveis vinculados a uma pessoa, tais como raça, etnia, religião, vida sexual e opinião política, dentre outros, bem como dados referentes à saúde, o que inclui os biométricos e genéticos.

- **TRATAMENTO:** toda operação realizada com dados pessoais, como as que se referem à coleta, classificação, utilização, acesso, processamento, arquivamento, armazenamento, compartilhamento, eliminação.

- **TITULAR DOS DADOS:** pessoa a quem se referem os dados pessoais que são objeto de tratamento.

- **FINALIDADE:** é o objetivo que a empresa deseja alcançar a partir de cada ato de tratamento dos dados pessoais.

- **INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS:** qualquer evento relacionado à violação na segurança dos dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, ou qualquer forma de tratamento de dados inadequada ou ilícita, que possam resultar em riscos para a privacidade e os direitos do titular.

- **ENCARREGADO DE DADOS PESSOAIS:** pessoa responsável por atuar como canal de comunicação entre a empresa, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD):** órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.
- **BANCO DE DADOS:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **BASE LEGAL:** hipóteses previstas na LGPD que autorizam o tratamento de dados pessoais.

TIPOS DE APPS E FUNCIONALIDADES

WhatsApp: é um dos aplicativos de mensagens instantâneas mais populares do mundo. Permite que os usuários troquem mensagens de texto, imagens, vídeos, áudios e documentos. Oferece chamadas de voz e vídeo. Suporta grupos para troca de mensagens em um ambiente mais colaborativo.

Telegram: permite o envio de mensagens de texto, imagens, vídeos, áudios e documentos. Também oferece chamadas de voz e vídeo. Suporta grupos grandes e canais para comunicação em massa. Permite a criação de bots (abreviatura de robô) e integrações para uma variedade de funções.

Instagram: rede social que originalmente se concentrou no compartilhamento de fotos e vídeos. Posteriormente, passou a oferecer recurso de troca de mensagens entre usuários (via Direct). Também oferece a opção de chamadas de vídeo.

Facebook Messenger: permite que os usuários enviem mensagens de texto, façam chamadas de voz e vídeo, compartilhem fotos, vídeos e emojis, além de oferecer integração com o Facebook. Também permite conversas individuais e em grupo.

Gmail e Google Meet: o Gmail é um serviço de e-mail da Google, mas também permite a troca instantânea de mensagens através de chat. Os usuários podem enviar e-mails e mensagens pelo mesmo aplicativo. O Google Meet é uma plataforma de videoconferência integrada ao Gmail, permitindo chamadas de vídeo e áudio em tempo real.

Microsoft Teams: plataforma de comunicação e colaboração empresarial. Além de mensagens instantâneas, oferece recursos de videoconferência, compartilhamento de documentos e integração com outras ferramentas da Microsoft. É amplamente utilizado para comunicação e colaboração em ambientes de trabalho e equipes.

Esses aplicativos oferecem diversas funcionalidades de troca instantânea de mensagens. A escolha por um, no entanto, dependerá das necessidades, preferências e contexto de uso de cada pessoa. Além disso, é importante considerar a privacidade e a segurança ao escolher um aplicativo de mensagens, especialmente para conversas sobre temas sensíveis.

COMO AGIR

- Caso seja necessária a utilização de aplicativos no trabalho para trocas de mensagens (ex: Google Meet, WhatsApp, etc), lembre-se: ao finalizar a comunicação, exclua os dados pessoais coletados ou acessados.

- Caso use o WhatsApp como ferramenta de comunicação no trabalho, dê preferencia ao WhatsApp Business. Essa versão oferece funcionalidades específicas para atender as necessidades das empresas, como configuração de respostas automáticas e verificação empresarial.

- A criação de grupos não deve ser incentivada, mas em caso de justificada necessidade, o colaborador responsável por sua criação deve ter o cuidado de dar prévia ciência aos colaboradores e fornecedores que serão inseridos no grupo.

- O ideal é que ocorra o ingresso ativo dos participantes, ou seja, sem inclusão direta. Uma forma de estimular tal ingresso pelos próprios participantes é encaminhar um convite contendo link ou QR Code de acesso ao grupo, deixando ele optar por entrar ou não. Além disso, é importante que os grupos, criados com a finalidade de otimizar as rotinas internas, contenham em sua descrição suas regras e finalidades.

- Apenas uilize os aplicativos de comunicação não oficiais (ex.: WhatsApp, Telegram e afins) como último recurso para compartilhamento interno de dados pessoais.

- Dê prioridade:
  - E-mail corporativo;
  - Pastas no servidor local;
  - Sistemas de gestão interna utilizados.

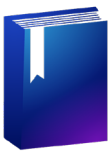
- Os colaboradores, quando desligados, devem ser prontamente removidos dos grupos de trabalho e daqueles onde são compartilhados dados pessoais controlados pela empresa.

- Não se deve reencaminhar a terceiros não autorizados mensagens contendo conteúdo corporativo sigiloso ou dados pessoais compartilhados nos grupos internos.

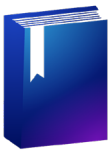
- Apenas o colaborador responsável pela criação do grupo deve ser seu administrador, controlando a inclusão e exclusão dos integrantes de acordo com as finalidades do grupo.

- Em respeito à imagem, evite o compartilhamento de fotos de colaboradores nos grupos corporativos sem prévia autorização.

QUER SABER MAIS? ACESSE OS LINKS ABAIXO:



Política de Privacidade da RioSaúde
https://riosaude.prefeitura.rio/wp-content/uploads/sites/66/2023/06/politica-de-privacidade-lgpd.pdf



Política de Uso e Divulgação da Informação
https://riosaude.prefeitura.rio/wp-content/uploads/sites/66/2023/09/Politica-de-Divulgacao-da-Informacao-RioSaude-2023.pdf

10 PASSOS PARA UTILIZAÇÃO SEGURA DE APLICATIVOS

1. IDENTIFICAÇÃO E CLASSIFICAÇÃO DOS DADOS

Antes de compartilhar qualquer informação via aplicativos é fundamental identificar os tipos de dados envolvidos, como nome, prontuário, histórico médico, exames, etc. Classifique esses dados de acordo com sua sensibilidade.

2. USO DE CRIPTOGRAFIA

Certifique-se de que o aplicativo de mensagens que você está usando oferece criptografia de ponta a ponta para proteger os dados durante a transmissão.

3. SEGURANÇA DOS DISPOSITIVOS MÓVEIS

As informações pessoais de usuários, pacientes, colaboradores, parceiros ou fornecedores da organização armazenadas em dispositivos móveis devem ser protegidas contra acessos indevidos, compartilhamento ou divulgação não autorizada.

Caso utilize aplicativos pessoais de comunicação (ex.: WhatsApp particular, Telegram, afins) para acesso ou coleta de dados pessoais de pacientes, fornecedores ou colaboradores, certifique-se de ativar o recurso de confirmação em duas etapas, que constitui uma camada extra de proteção e mantém os dados relativamente em segurança.

PARA ATIVAR O RECURSO DE CONFIRMAÇÃO EM DUAS ETAPAS, SIGA ESTES PASSOS:

WhatsApp
Configuração > Conta > Confirmação em duas etapas.

Telegram
Configurações > Privacidade e Segurança > Verificação em duas etapas

4. MANTER CONVERSAS PRIVADAS

Evite compartilhar informações de pacientes em grupos de trocas de mensagens dos aplicativos. Mantenha as conversas privadas, limitando o acesso apenas às pessoas diretamente envolvidas no tratamento do paciente.

5. SENHAS E AUTENTICAÇÃO

Proteja o acesso ao seu dispositivo e ao aplicativo de mensagens com senhas sigilosas ou autenticação biométrica para evitar acessos não autorizados.

6. EVITE ENVIAR DADOS SENSÍVEIS

Evite o envio de dados altamente sensíveis, como números de seguro social ou informações de cartão de crédito por meio dos aplicativos de trocas de mensagens.

7. USO DE MENSAGENS TEMPORÁRIAS

Alguns dos aplicativos permitem uso de mensagens temporárias que desaparecem após um determinado período. Essa opção pode ser útil para proteger a privacidade dos pacientes.

8. ATUALIZAÇÃO DE SOFTWARE

Mantenha os aplicativos e o sistema operacional do seu dispositivo sempre atualizados para garantir a segurança.

9. ARMAZENAMENTO ADEQUADO

Evite o armazenamento de mensagens em dispositivos ou serviços de backup não seguros. Isso pode representar um risco para a segurança dos dados.

10. TREINAMENTO DOS PROFISSIONAIS

Garanta que todos os profissionais de saúde envolvidos na troca de informações via aplicativos estejam devidamente treinados em questões de privacidade e segurança de dados.

CONDUTAS QUE DEVEMOS EVITAR

Para além das regras relacionadas à Lei Geral de Proteção de Dados (LGPD), ao comunicar-se com titulares de dados pessoais em nome da RioSaúde é necessário evitar alguns padrões de conduta, como por exemplo os descritos abaixo:

- Se negar a realizar ou a prestar atendimento usuários e pacientes,

fornecedores e/ou parceiros, quando solicitado, ou abandonar a interação sem qualquer justificativa.

- Ser irônico(a), sarcástico(a) ou desrespeitar, com palavras ofensivas, causando constrangimento.

- Fazer comentários inapropriados, debochados insultuosamente, utilizando-se de palavras ofensivas e discriminatórias acerca da educação, formação, classe social, orientação sexual, raça, etc.

- Depreciar, desonrar ou difamar a organização, usuários e pacientes, fornecedores, colaboradores ou realizar críticas a atendimentos anteriores.

- Repassar informações inexistentes ou incorretas em relação a exames, diagnósticos, serviços ou qualquer outra informação que cause impactos ou prejuízos, sejam eles financeiros ou de reputação, para o cliente ou para a organização.

- Conduzir ou direcionar a interação ou o atendimento para assuntos pessoais.

- Enviar mensagens que possam comprometer a imagem e reputação da empresa perante os usuários, pacientes, parceiros e a comunidade em geral acarretando em prejuízo moral e financeiro.

- Expor, armazenar, distribuir, editar ou gravar material sexualmente explícito ou qualquer outro considerado ilegal através do uso dos recursos computacionais da rede corporativa, inclusive em canais de comunicação não oficiais (ex.: WhatsApp, Telegram).

- Executar programas que tenham como finalidade a decodificação de senhas, o monitoramento da rede, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

- Repassar números ou códigos de verificação solicitados por alguém via ligação ou qualquer outro dispositivo.

- Baixar e executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados à rede corporativa.

- Repassar informações sigilosas tais como resultados de indicadores, exames, informações sobre outros pacientes, etc. a pessoas não autorizadas.

PONTOS DE ATENÇÃO

- **ANTES DE CRIAR UM GRUPO COM FUNCIONÁRIOS, PARE E PENSE**

  Avalie se é necessário usar o aplicativo para encaminhar as demandas para a **equipe**. Se achar que sim, a recomendação é alinhar com eles sobre a criação do grupo. Dessa maneira, haverá uma maior aceitação dos colaboradores sobre o uso da ferramenta, o que é fundamental para aumentar a produtividade e evitar conflitos.

- **EVITE DISCUTIR ASSUNTOS NÃO RELACIONADOS AO AMBIENTE DE TRABALHO**

  É comum abordar temas diferentes do assunto principal do grupo. Mas evite ao máximo essa prática, já que foge da finalidade da criação do grupo, podendo despertar desinteresse de alguns participantes e prejudicar a comunicação de temas que, de fato, são centrais a todos.

- **EVITE ABREVIAÇÕES E EMOJIS**

  O uso de abreviações deve ser evitado para facilitar o entendimento do conteúdo das mensagens. Seja claro e objetivo na comunicação.
  A utilização de emojis deve ser restrita e feita com moderação. O melhor é usá-los apenas em ocasiões específicas (parabenizar alguém pelo aniversário ou mostrar que ficou satisfeito com uma resposta, por exemplo).

- **ESTEJA ATENTO AO VAZAMENTO DE INFORMAÇÕES**

  Não compartilhe com terceiros assuntos abordados no grupo. As informações corporativas devem ser mantidas no âmbito institucional. Um dado divulgado de maneira equivocada pode prejudicar os resultados de uma empresa.

- **ATENÇÃO AOS COLABORADORES DESLIGADOS DA EMPRESA**

  É de suma importância a constante revisão e remoção de pessoas desligadas da empresa de grupos de WhatsApp, e-mail e outros meios de comunicação que sejam eventualmente utilizados no âmbito corporativo. Isso assegura a confidencialidade das informações e a manutenção do controle de acesso aos recursos institucionais

- **BOM SENSO É FUNDAMENTAL**

  Utilizar os recursos disponíveis com inteligência é uma maneira de evitar problemas. Os apps de mensagens podem ser grandes aliados na comunicação profissional. **USE COM ATENÇÃO E RESPONSABILIDADE!**

Rio
PREFEITURA

RIOSAÚDE

RioSaudeOficial