Política de Privacidade do Aplicativo Sob Controle

Privacidade
Na Roche Diabetes Care Brasil Ltda. ("Roche Diabetes") é uma empresa altamente comprometida com a privacidade e proteção dos dados dos indivíduos que confiam suas informações à nós. Saiba que usamos os seus dados de maneira consciente e transparente!
Por isso, é muito importante que você entenda por que e como nós iremos tratar os seus dados quando você acessa Software Sob Controle ("Aplicativo").
Na Roche Diabetes estamos empenhados em proteger as suas informações pessoais. Esta Política de Privacidade descreve os tipos de informações pessoais que a Roche pode coletar; os meios pelos quais a Roche pode coletar, utilizar ou compartilhar as suas informações pessoais; as medidas adotadas pela Roche para proteger as suas informações pessoais; e as opções que você possui no que diz respeito ao uso das suas informações pessoais.

Consentimento
Sempre que fornecer dados utilizando o Aplicativo, você estará concordando com os termos desta Política, incluindo sobre a prática de coleta, utilização, uso, armazenamento, retenção e compartilhamento com terceiros das informações fornecidas no aplicativo.

Caso você seja o responsável que insere os dados do Paciente, antes da inserção dos dados no Aplicativo, você deve colher o consentimento do Paciente.

Utilização
Este aplicativo destina-se a profissionais de saúde, operadores da área saúde e público exclusivamente indicado por estes e residentes no Brasil em geral (pacientes).

Identidade e detalhes de contato do Controlador dos Dados Pessoais
Segundo a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – "LGPD"), a Roche Diabetes, juntamente com o Cliente que está provendo este Aplicativo a você são considerados "Controlador" dos seus Dados Pessoais. Se após a leitura desta Política você ainda tiver qualquer dúvida, ou por qualquer razão precisar se comunicar conosco para assuntos envolvendo os seus Dados Pessoais, você pode entrar em contato:

- pelo e-mail: rdc.privacidadedados@roche.com
- por escrito (pelo correio):Roche Diabetes Care Brasil Ltda
Rua Dr. Rubens Gomes Bueno, n. 691, 2 andar
Várzea de Baixo - São Paulo - SP
04730-903 - Brasil
- pelo SAC: 0800 77 20 126

Relação de Subcontratados
A subcontratação para os fins do presente Processamento de Dados deverá ser entendida como significando serviços que se referem diretamente à prestação do serviço principal e neste caso, a empresa BLACKBEAN TECHNOLOGIES LTDA. é a operadora deste Aplicativo.
Isso não inclui serviços auxiliares, como serviços de telecomunicação, serviços postais/de transporte, serviços de suporte ao usuário e de manutenção ou a alienação de portadores de dados, bem como outras medidas para garantir a confidencialidade, disponibilidade, integridade e flexibilidade do hardware e software de equipamentos de processamento de dados.
Os seus dados pessoais são rigorosamente limitados com quem compartilhamos e não são vendidos a terceiros para benefícios comerciais. Os dados pessoais podem ser compartilhados com terceiros fornecedores para fornecer a você produtos Accu-Chek®,

quando autorizado, e com os terceiros fornecedores de serviços em nuvem, que no caso específico é a DigitalOcean, Inc. Os terceiros e subcontratados obedecem a esta Política de Privacidade.

Escopo geográfico e prazo de armazenamento
O objeto do processamento de dados pessoais contratualmente acordado está limitado ao território brasileiro e os dados poderão ser armazenados em banco de dados fora do território brasileiro, no momento sendo armazenado nos Estados Unidos.
Os dados pessoais do Aplicativo poderão ser armazenados por até 10 (dez) anos para fins exclusivos de compartilhamento de dados pessoais cadastrais pelas autoridades administrativas que detenham competência legal para a sua requisição, para fins de cumprimento de obrigação legal, contratual e/ou regulatória.
Toda e qualquer transferência de dados pessoais obedecerá a Lei Geral de Proteção de Dados.

Como e porque tratamos os seus Dados Pessoais
Neste Aplicativo, podemos solicitar Dados Pessoais sobre você. Exemplos de Dados Pessoais que podemos coletar que o identificam de forma direta incluem seu nome, CPF, CNS, e-mail, genitor(a), unidade de atendimento, sexo, endereço completo, telefone de contato, data de nascimento, faixa de diabetes, tipo de insulina, data do diagnóstico, resultado de exame, peso e altura e também é possível anexar qualquer tipo de anexo.
As informações pessoais são processadas quando você cria a sua conta no aplicativo Sob Controle. Processamos dados inseridos no monitor de glicemia da marca Accu-Chek®, bem como a frequência com que você usa o monitor e os valores com horários, metas de glicose e insumos fornecidos. Também coletamos informações pessoais se você solicitar o serviço de suporte ao cliente Accu-Chek®.
Nós tratamos os seus Dados Pessoais nos nossos Sites por diversas razões, incluindo para gerar relatórios, estatísticos, para um melhor tratamento ou gerenciamento dos insumos fornecidos. Importante ressaltar que os dados pessoais inseridos por você, tais como nome, idade e endereço, devem ser fidedignos e não são alterados por nós e refletirão conforme forem coletados.

Também informamos que os dados poderão ser compartilhados, de modo anonimizado, com empresas do Grupo Roche, para fins estatísticos

Atualizações
Esta Política de Privacidade poderá ser atualizada a qualquer momento e você será informado.

Medidas Técnicas e Organizacionais
1. **Confidencialidade**
   - Controle de Acesso Físico
     Nenhum acesso não autorizado às instalações de processamento de dados, por exemplo: cartões magnéticos ou com chip, chaves, itens eletrônicos para abertura de portas, equipe de segurança de entrada e/ou serviços de segurança da instalação, sistemas de alarme, Sistemas de vídeo/CCTV.
     Pessoas não autorizadas estarão impedidas de obter acesso físico às instalações, edifícios ou salas onde estejam localizados os sistemas de processamentos de dados que processam e/ou usam Dados Pessoais.
     Medidas de segurança para a Nuvem:
     - Controles de segurança física incluem, entre outros, controles de perímetro como cercas, muros, equipe de segurança, circuito fechado de televisão, sistemas de detecção de intrusos e outros meios eletrônicos.
     - O acesso físico é rigorosamente controlado, tanto no perímetro quanto em pontos de entrada no edifício, e inclui, entre outros, equipe de segurança profissional que utiliza circuito fechado de televisão, sistemas de detecção de intrusos e outros meios eletrônicos. A equipe autorizada deverá passar por uma autenticação

de dois fatores no mínimo duas vezes para acessar os andares de centro de dados. Pontos de acesso físico a locais de servidores serão gravados por uma câmera de circuito fechado de televisão (CCTV), conforme definido na Política de Segurança Física do Centro de Dados da DigitalOcean, Inc. Os Mecanismos de Segurança Física serão revisados por auditores externos independentes durante auditorias para conformidade com nosso SOC, PCI DSS, ISO 27001 e FedRAMP.

2. **Integridade**
   - Controle de Transferência de Dados
     Nenhuma leitura, cópia, alteração ou supressão não autorizada de dados com transferência ou transmissão eletrônica, por exemplo: codificação, redes virtuais privadas (VPN), assinatura eletrônica.
     O protocolo SSL sobre HTTP para garantir a comunicação por meio de Internet não confiável é usado nessa solução.

O acesso aos ambientes de produção é realizado por SSH através de chave criptografada público-privada.

   - Controle de Entrada de Dados
     A verificação, independentemente de se e por quem os dados pessoais são inseridos em um sistema de processamento de dados, será alterada ou apagada, por exemplo: registro, administração de documento.
     A Roche Diabetes implementou um sistema de registro para inserção, modificação e supressão de dados. Esses registros de rastreabilidade incluem acesso do usuário, tipo de acesso e arquivo/registro acessado, dentre outros detalhes.
     A Roche Diabetes implementou a validação de inserção de dados em campos de informações que aceitam a inserção de informações de usuários, incluindo controles de segurança acima de validações de informações lógicas de negócios.
     Validações lógicas de negócios incluem, entre outras: nenhuma área obrigatória estar faltando, formato e extensão de controle das áreas que aceitam inserção.
     Controles de autorização também estão em vigor, de forma que a validação verifique que cada usuário cadastrado tem direito de praticar um ato no sistema.

3. **Disponibilidade e Flexibilidade**
   - Controle de Disponibilidade
     Dados Pessoais serão protegidos contra destruição ou perda acidental ou não autorizada.
     <u>Medidas Gerais quando usada Nuvem:</u>
     - A Roche Diabetes implementa processos de backup regulares para oferecer a restauração de negócios cruciais, de acordo com a estratégia de backup,
     - A Roche Diabetes usa suprimentos de energia ininterrupta (por exemplo: UPS, pilhas, geradores, etc.) para proteger a disponibilidade de energia aos centros de dados.
     - A Roche Diabetes definiu planos de contingência comercial para processos cruciais aos negócios, e poderá oferecer estratégias de recuperação de desastres para serviços cruciais aos negócios.

     <u>Medidas Específicas para Operações quando usada Nuvem:</u>
     - O aplicativo é protegido com arquitetura de segurança específica, seguindo a defesa no princípio de profundidade
       - Firewall do perímetro em configuração de alta disponibilidade. Somente conceder acesso a entradas permitidas para o aplicativo
       - O design do aplicativo permite alta disponibilidade e flexibilidade
       - A infraestrutura é monitorada em termos de disponibilidade e desempenho
       - Monitoramento de segurança específico e processo de administração de incidentes em vigor

- A Roche Diabetes utiliza processos de backup regulares para prover a restauração de sistemas cruciais aos negócios conforme e quando necessário. É realizado backup de toda a infraestrutura de produção diariamente (por meio de snapshots) e os snapshots são guardados por 30 dias, já os snapshots criados manualmente ficam armazenados até a exclusão do operador.

4. **Procedimentos para testes, determinação e avaliação regulares**

- Administração de Proteção de Dados;
  Existe uma estratégia de defesa multicamadas como uma proteção contra modificações não autorizadas.
  Especificamente, a Roche Diabetes usa o seguinte para implementar as seções de controle e medidas descritas acima. Em particular:
  - Firewalls;
  - Centro de Monitoramento de Segurança;
  - Backup e recuperação;
  - Testes de penetração interna e externa;
  - Codificação de dados em trânsito e em repouso

- Administração de Resposta a Incidentes;

  Os aplicativos da Roche Diabetes e infraestrutura subjacente são monitorados 24 horas por dia, 7 dias por semana, para detectar eventos de segurança ou incidentes em potencial. Um processo de administração de incidentes de segurança está em vigor para garantir:
  - A ativação da resposta a incidentes, e que as medidas corretas sejam tomadas, comunicações lançadas, etc.
  - Ajuda para se recuperar rápida e eficientemente de incidentes de segurança, minimizar perda ou furto de informações e interrupção de serviços
  - Uso de informações obtidas durante o manuseio do incidente para melhor se preparar para o manuseio de futuros incidentes e para oferecer uma proteção maior para sistemas e dados
  - Início de medidas corretivas (e redução de taxa de repetição) e medidas preventivas para impedir que isso ocorra.

  Caso dados pessoais estejam envolvidos no incidente de segurança, o Processo de Violação de Dados Pessoais da Roche Diabetes será ativado, e o Diretor de Proteção de Dados, notificado, a fim de ativar as atividades exigidas pela legislação vigente, ou seja, comunicação às autoridades ou Titulares de Dados, quando necessário.
- Proteção de Dados por Design e Inadimplemento
  De acordo com a confidencialidade de dados de saúde, a Roche Diabetes designou a Plataforma em conformidade com princípios de proteção de dados, como minimização de dados, codificação de dados, e está comprometida em manter e aperfeiçoar continuamente os níveis de segurança e privacidade com medidas técnicas e organizacionais apropriadas, projetadas de maneira efetiva e a fim de cumprir as exigências da LGPD e proteger os direitos de Titulares de Dados.
  Espontaneamente, apenas dados pessoais que sejam necessários para cada finalidade específica do processamento são processados, envolvendo a quantidade de dados pessoais coletados, a extensão de seu processamento, o período de seu armazenamento e sua acessibilidade.