



HEALTHBIT

Política de Privacidade e
Proteção de Dados



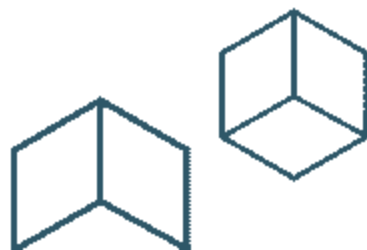
1.

Introdução



Introdução

A HealthBit – Inteligência em Saúde, com o intuito de estabelecer suas diretrizes de privacidade e proteção de dados em prol dos usuários de suas tecnologias e de todos os titulares dos dados por ela recepcionados, publica a presente “Política de Privacidade e Proteção de Dados”, a fim de esclarecer como são utilizadas as informações por nós obtidas, de forma clara e objetiva.





2.

Definições



Definições

Consideram-se para os fins da presente Política de Privacidade e Proteção de Dados os seguintes conceitos:

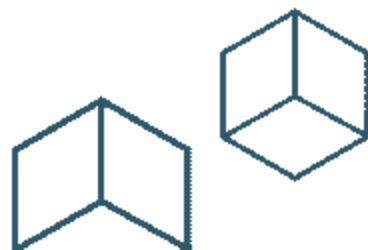
- **Usuário:** todos aqueles que possuem acesso aos sistemas da HealthBit, sejam colaboradores, clientes ou terceiros.
 - **Titular de Dados:** pessoa a quem se referem os dados pessoais tratados na HealthBit.
 - **Dado Pessoal:** qualquer informação relacionada a pessoa natural identificada ou identificável.
 - **Dado Pessoal Sensível:** dado pessoal que verse sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.
 - **Dado anonimizado:** dado incapaz de proporcionar a identificação de titular, a partir da remoção de informações por meios técnicos razoáveis.
 - **Dado criptografado:** dado que somente pode ser acessado mediante o conhecimento de chave criptográfica, em razão da realização de procedimento técnico de codificação.
 - **Tratamento:** qualquer operação envolvendo dados pessoais, tais como: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
 - **Controlador(a):** pessoa física ou jurídica responsável pelas decisões referentes ao tratamento de dados pessoais e dados pessoais sensíveis.
 - **Operador(a):** pessoa física ou jurídica que realiza operações de tratamento em nome do Controlador(a).
-





Definições

- **Agentes de Tratamento:** Controlador(a) e Operador(a) de dados.
 - **Encarregado (Data Protection Officer):** pessoa física ou jurídica responsável pela intermediação entre o controlador de dados, titulares e Autoridade Nacional de Proteção de Dados.
 - **Relatório de Impacto à Proteção de Dados Pessoais:** documentação elaborado pelo Controlador de dados, que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos aos direitos dos titulares, bem como medidas e mecanismos de mitigação de risco.
 - **Consentimento:** manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada e previamente informada.
 - **Bases Legais de Tratamento:** possibilidades autorizadoras para o tratamento de dados pessoais e dados pessoais sensíveis expressamente previstas na Lei Geral de Proteção de Dados, nos artigos 7º e 11, respectivamente.
 - **Equipe de Privacidade e Proteção de Dados:** comitê formado por membros das equipes de Desenvolvimento e TI, Dados, Jurídico, Compliance, Recursos Humanos e Administrativo, a fim de organizar, criar diretrizes e monitorar o correto uso de dados pessoais e dados pessoais sensíveis no ambiente de atuação da HealthBit.
 - **Banco de Dados:** conjunto de dados pessoais estabelecido em um ou em vários locais, em suporte eletrônico ou físico, devidamente estruturado.
 - **Servidor:** computador remoto que responde solicitações via internet, podendo armazenar dados.
 - **Transferência Internacional de Dados:** transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro.
-





3.

Atuação da HealthBit



Atuação da HealthBit

Para cumprir nossa missão junto aos clientes, a HealthBit atua ora como Controladora e ora como Operadora de dados pessoais e dados pessoais sensíveis, com o objetivo de prestar os serviços contratados da forma mais completa, utilizando o mínimo necessário para tanto.

Os processos e sistemas da HealthBit, conforme determinado na Política de Segurança da Informação, devem ser estruturados em conformidade com a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados, cumprindo com os requisitos mínimos de segurança técnica e boas práticas de segurança corporativa pela legislação exigidos.

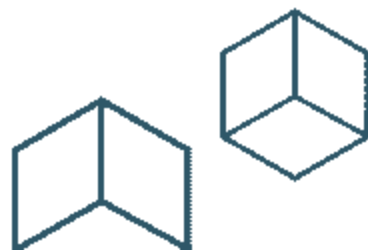
Os contratos envolvendo tratamento de dados pessoais e dados pessoais sensíveis da HealthBit devem ter sua finalidade e resultados descritos, devendo também os clientes e parceiros moverem esforços para conformidade com a lei. Todos os contratos que posicionem a HealthBit como Operadora de dados devem ser reanalisados até a vigência da Lei Geral de Proteção de Dados, para que as obrigações decorrentes do acordo junto à empresa cliente estejam em conformidade com a nova legislação.

Serão observados os princípios da necessidade, adequação, qualidade dos dados, livre acesso ao titular, segurança, transparência, prevenção, finalidade e não discriminação, além da garantia a confidencialidade, integridade e disponibilidade dos dados.

Além disto, o tratamento deve ser feito com a coleta mínima de dados, visando resultado compatível com a finalidade da coleta e utilizando, sempre que possível, meios técnicos e administrativos para proteção de dados pessoais de acessos indevidos ou situação de tratamento inadequada.

Sempre que possível, serão utilizados meios de anonimização e criptografia, a fim de garantir a transferência segura, tão somente dos dados necessários.

Na presente Política de Privacidade e Proteção de Dados foi descrito todo o ciclo de vida dos dados recebidos e/ou coletados pela HealthBit, conforme abaixo trazido.





4.

Recebimento dos Dados



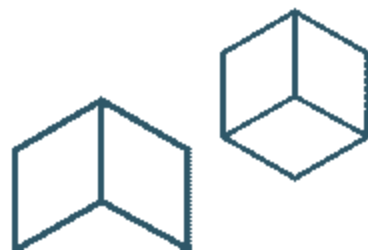
Recebimento dos Dados

Em razão da necessidade de coleta de dados pessoais e dados pessoais sensíveis para realização de suas funções contratualmente ajustadas, a HealthBit recebe de seus clientes ou diretamente dos titulares os dados a serem utilizados em sua atuação, sempre com o devido enquadramento às bases legais autorizadoras do tratamento de dados expressamente previstas na Lei Geral de Proteção de Dados brasileira.

Desta forma, para o recebimento de arquivos pela HealthBit é criado um “portal” específico para cada cliente, uma aplicação cuja finalidade é exclusivamente o recebimento de dados. Este “portal” é hospedado em servidor na infraestrutura da Healthbit na Microsoft Azure, e toda transmissão de arquivos é feita via conexão segura pelo protocolo HTTPS.

O envio de arquivos no portal é realizado pelo controlador dos dados. O “portal” criptografa os arquivos recebidos e os disponibiliza ao funcionário responsável da Healthbit para download. O acesso de funcionários é especificado na criação do “portal”, de modo que apenas os funcionários responsáveis pelo cliente empresa em questão possuem acesso ao “portal” e a capacidade de fazer download dos dados e descriptografá-los.

Os servidores da HealthBit ficam localizados em ambiente estrangeiro que respeita a legislação de proteção de dados brasileira, realizando-se transferência internacional de dados da HealthBit para a empresa Microsoft Azure, havendo contrato de hospedagem com as devidas especificações do serviço.





5.

Inserção e Armazenamento



Inserção e Armazenamento dos Dados

No papel de Operadora ou Controladora de dados, a Healthbit utiliza aplicações hospedadas em servidores Microsoft Azure para realização de suas operações, através de transferência internacional de dados. Especificamente, as aplicações utilizam banco de dados MySQL Server e MongoDB.

Os bancos de dados são protegidos por senha e armazenam os dados de forma criptografada. Para cada empresa cliente da Healthbit é utilizada uma instância própria de banco de dados ("database").

O acesso direto ao banco de dados é restrito aos responsáveis técnicos da Equipe de Desenvolvimento e TI, que podem fazê-lo apenas via conexão segura criptografada usando suas chaves pessoais e intransferíveis. Além disto, os responsáveis em questão assinam Termo de Confidencialidade e Sigilo junto à HealthBit, garantindo a correta utilização e gerência das informações.

A inserção, visualização e operação dos dados a funcionários e clientes, quando devidamente autorizados, é feita via aplicação, que implementa as restrições de acesso definidas em contrato. Além disto, os acessos somente são concedidos mediante a assinatura de Termo de Cessão de Acesso e Confidencialidade, que estabelece o dever de sigilo e proteção de dados disponíveis no sistema pelos usuários.

A inserção de dados nos sistemas é feita por um funcionário da Healthbit habilitado para trabalhar com dados da empresa cliente específica, com a devida assinatura de termo de sigilo. O envio de arquivo para inserção é feito via aplicação, que insere as informações no banco de dados e exclui o arquivo do servidor, de modo que os dados existam apenas no banco de dados ("database") da empresa cliente em questão.

Somente são inseridos e armazenados no sistemas os dados que possuem a devida base legal autorizadora de tratamento, seja para que a HealthBit figure como Controladora ou como Operadora de dados.

A HealthBit pode, entretanto, manter armazenados os dados necessários para cumprimento de obrigação legal, pelo prazo que a respectiva legislação exigir a guarda dos mesmos.





6.

Eliminação dos Dados



Eliminação dos Dados

A HealthBit procede com a exclusão de dados pessoais e dados pessoais sensíveis sempre que ocorre a finalização de algum contrato de prestação de serviço junto a empresas clientes, colaboradores (respeitados os períodos onde é obrigatória a manutenção em decorrência de obrigação legal), a pedido do titular ou quando não houver base legal autorizadora para manutenção das informações em seus bancos de dados.

Adota-se, desta forma, um procedimento técnico para garantir a total exclusão dos dados armazenados nas hipóteses acima colocadas.

Tal procedimento é executado por um dos responsáveis técnicos da Equipe de Desenvolvimento e Tecnologia da Informação, e consiste na execução dos comandos necessários para exclusão total do banco de dados ("database") específico do cliente, como por exemplo "DROP DATABASE <nome do banco de dados da empresa>".

Todos os procedimentos de exclusão são devidamente registrados em arquivo. O registro deve conter quais dados foram excluídos, os responsáveis técnicos, data e horário, os comandos realizados e as saídas obtidas.

O titular ou empresa cliente correspondente é devidamente notificado da eliminação, com o devido comprovante da exclusão e uma declaração formal da HealthBit sobre o procedimento realizado.

Caso o pedido de eliminação seja feito por titular de dado, não havendo nenhuma base legal que autorize a manutenção dos dados, será adotado procedimento similar. Os titulares podem entrar em contato com a HealthBit para realizar qualquer requisição através do endereço eletrônico contato@healthbit.com.br ou juridico@healthbit.com.br.





7.

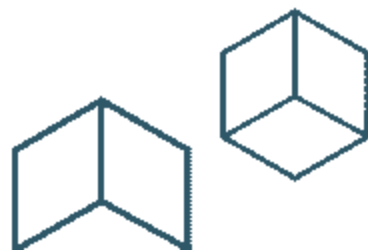
Utilização dos Dados



Utilização dos Dados

A HealthBit compromete-se a:

- a) Somente efetuar o tratamento de dados pessoais e dados pessoais sensíveis, na posição de controladora ou operadora de dados, quando devidamente enquadrados nas bases legais trazidas pelos artigos 7º e 11 da LGPD, respectivamente, e em total consonância com a finalidade e necessidade de utilização dos mesmos, levando-se em consideração o quanto contratualmente ajustado junto aos clientes e titulares de dados.
 - b) Não divulgar, sem autorização, os dados sob sua guarda, recebidos para execução dos serviços contratados pelos clientes, adotando políticas e procedimentos técnicos que garantam a proteção das informações.
 - c) Executar os procedimentos constantes na Política de Segurança da Informação, a fim de garantir a proteção de dados.
 - d) Cumprir com todas as determinações da Lei Geral de Proteção de Dados.
 - e) Elaborar Relatórios de Impacto à Proteção de Dados;
 - f) Agir em total consonância com as determinações do Controlador de dados, quando atuar na posição de Operadora.
-





Utilização dos Dados

Os usuários dos sistemas da HealthBit devem:

- a) Seguir as determinações da presente Política de Privacidade e Proteção de Dados e das Diretrizes de Ética e Conduta da HealthBit.
 - b) Cumprir as regras de utilização dos sistemas, não auxiliando terceiros a corromper ou invadir os sistemas da HealthBit, para qualquer finalidade, sob pena de responsabilização cível e criminal, de acordo com a legislação cabível.
 - c) Não disponibilizar acesso a terceiros, para quaisquer finalidades, sob pena de responsabilização de acordo com a legislação cabível.
 - d) Zelar pela segurança e proteção dos dados, agindo de acordo com as instruções passadas em treinamentos realizados pela HealthBit.
 - e) Reportar aos responsáveis da Equipe de Desenvolvimento e TI quaisquer falhas ou problemas durante a utilização dos sistemas.
-





8.

Vigência e Validade



Vigência e Validade

A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado e podendo ser revista a qualquer momento, sempre que necessário.

Todos os nossos funcionários, executivos, prestadores de serviços, consultores, fornecedores em geral e parceiros devem seguir e respeitar as diretrizes de privacidade ora publicadas, sem distinções ou exceções, nos moldes estipulados neste documento.





9.

Disposições Finais



Disposições Finais

A publicação da presente Política de Privacidade e Proteção de Dados presta-se para firmar publicamente o compromisso da HealthBit em garantir a correta gestão dos dados pessoais e dados pessoais sensíveis aos quais tem acesso, a fim de zelar pelos direitos dos titulares e de seus clientes.

A HealthBit cumpre e zela pela privacidade e proteção dos dados de seus clientes desde sua fundação, assumindo o compromisso de adequação à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados em todas as suas esferas de organização e atuação.





Obrigado

HEALTHBiT