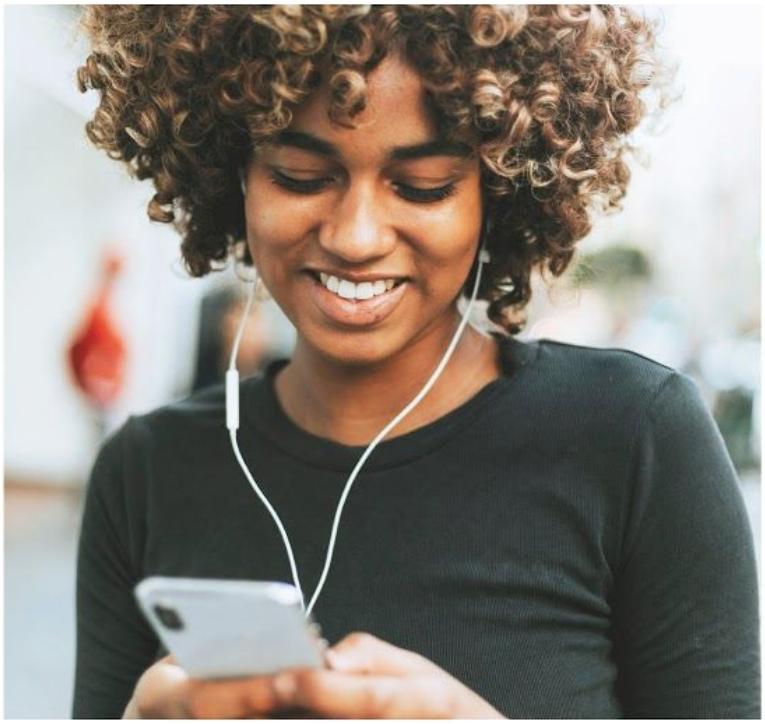
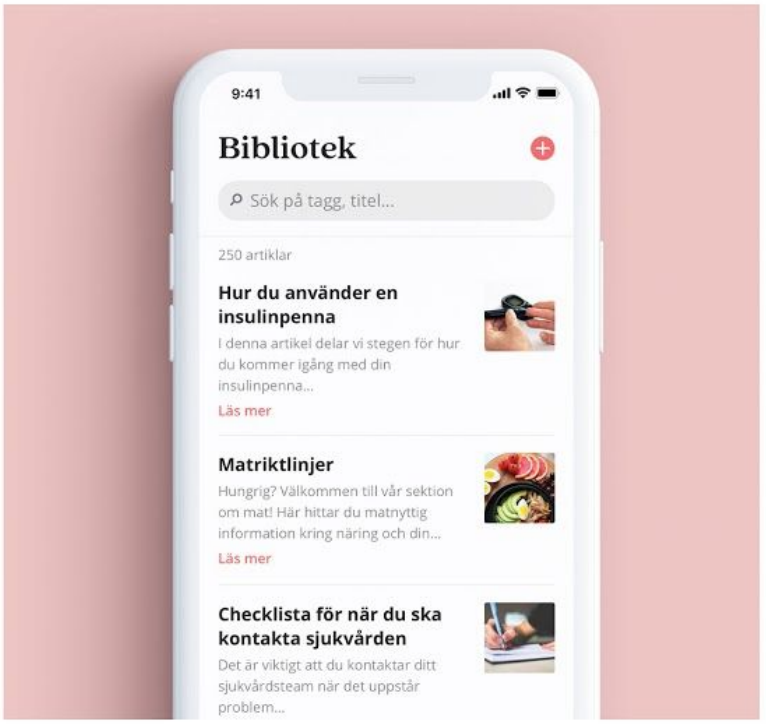
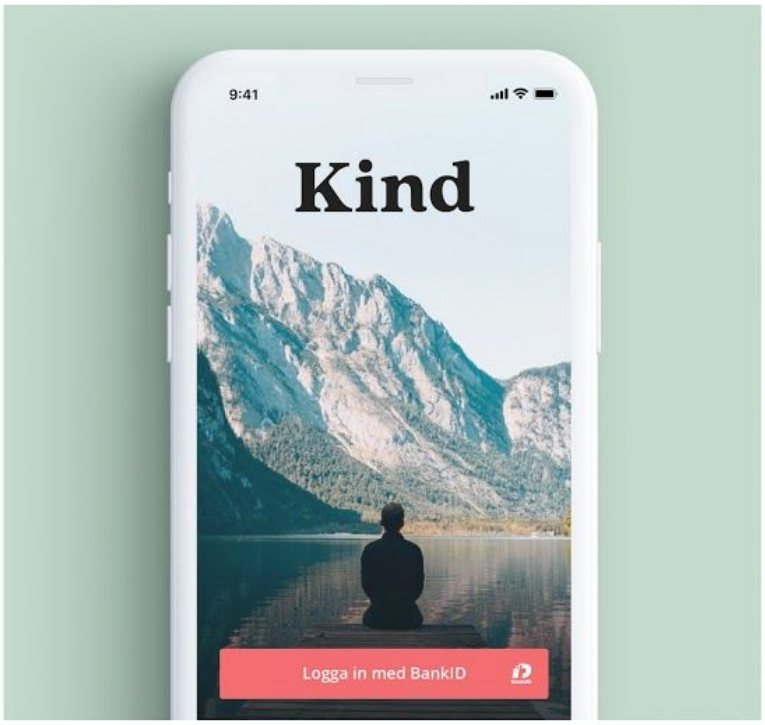
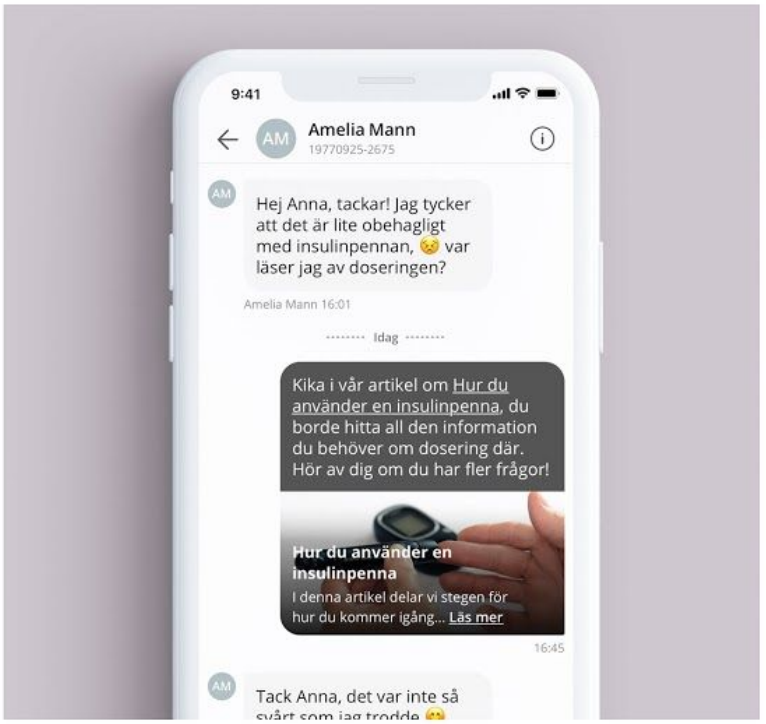






Guia de segurança



Kind

Kind está disponível a ambos profissionais da saúde e pacientes em todo o mundo. Segurança é nossa prioridade número 1. Nós preservamos seus dados pessoais estritamente confidenciais. Este documento resume todas as nossas medidas de segurança para garantir um alto nível de proteção em nossos aplicativos.

Encriptação

A Kind usa a criptografia em trânsito e em repouso. Isso significa que seus dados são criptografados do seu dispositivo (telefone e navegador) para nossa infraestrutura nos quais nossos discos também são criptografados.

Em trânsito

Para criptografar o tráfego em trânsito, utilizamos o HTTPS. Esse sistema é realizado através da combinação dos comandos chamados “Secure Sockets Layer” (SSL) e “Transport Layer Security” (TLS). Os dados enviados de um cliente, seja pela web ou por um aplicativo móvel, são emitidos por uma conexão HTTPS, a qual é protegida por um certificado SSL de 2048 bits.

Em repouso

Quando alguma informação como: dados pessoais, mensagens, anexos, entre outros for enviada do cliente para nossa infraestrutura a mesma será armazenada de maneira segura na AWS utilizando padrões de criptografia. Os dados armazenados nos volumes, o disco E/S e os instantâneos criados são todos criptografados. As chaves de

criptografia (EBS) “Elastic Block Storage” e (S3) “Simple Storage Service” utilizam o algoritmo AES-256 e são inteiramente gerenciadas e protegidas pela infraestrutura de gerenciamento de chaves da AWS, por meio da “AWS Key Management Service” (AWS KMS).

Acesso

Trabalhamos com o princípio de privilégios reduzidos em toda a organização Kind. Isso significa que a cada funcionário é dado apenas o acesso necessário para executar suas tarefas. Na AWS, isso se traduz em níveis de permissões mais detalhadas usando o (AWS IAM) “Identity and Access Management”. Cada novo usuário precisa configurar o mecanismo (MFA) “Multi Factor Authentication”, um multiplo fator de autenticação antes de conseguir executar qualquer ação na plataforma. Isso adiciona um nível maior de segurança, pois mesmo com o nome de usuário e a senha, um hacker, por exemplo, não terá acesso a nossa infraestrutura.

Um sistema “bastion” foi também implantado para isolar nossa plataforma de internet. Isso significa que nenhum banco de dados ou arquivo pode ser recuperado através da internet sem acesso ao sistema “bastion”. Nosso sistema “bastion” é protegido por um par de chaves RSA criptografado de 2048 bits e uma restrição de IP. Dessa forma, alguém fora de nossa organização não poderá acessar nossa infraestrutura, ainda que essa pessoa tenha credenciais válidas.

Todo acesso à nossa infraestrutura é feito através do CloudTrail e do VPC FlowLogs. O CloudTrail fornece dados de atividades da API,

revelando assim a identidade de quem faz a chamada API, o horário da chamada API, a origem do endereço IP, os parâmetros da solicitação e os elementos de resposta retornados pelo serviço da AWS. Em caso de qualquer atividade suspeita um alarme é acionado e enviado aos nossos administradores para revisão.

Separação de dados

A fim de manter seus dados pessoais como: mensagens e anexos seguros, nós os separamos completamente dos dados do aplicativo. Utilizamos IDs genéricos para correlacionar dados entre nossos diferentes serviços, não utilizamos nomes de usuários tampouco e-mail. Na eventualidade de um dos nossos bancos de dados ser comprometido, não haveria a possibilidade de relacionar a informação vazada a um indivíduo específico.

Cópia de segurança / alta disponibilidade

Fazemos backup de nosso aplicativo diariamente. Esses backups são criptografados utilizando o algoritmo AES-256 e são totalmente gerenciados e protegidos pela infraestrutura de gerenciamento de chaves da AWS, por meio da “AWS Key Management Service” (AWS KMS).

Nossa infraestrutura é altamente disponível pois abrange várias zonas de disponibilidade da AWS. As zonas de disponibilidade consistem em um ou mais centro de dados discretos, cada um com energia, rede e conectividade redundantes, gerenciados em

instalações separadas. No caso de haver a interrupção de uma zona de disponibilidade todo o tráfego será redirecionado para as zonas de disponibilidade restantes, reduzindo assim o impacto ao cliente.