Política de Privacidade

A presente aplicação é um sistema protótipo desenvolvido com o objetivo de otimizar a gestão dos recursos hospitalares existentes, promovendo uma alocação mais eficiente e eficaz dos recursos.
Considerando que a solução desenvolvida e a utilização do sistema envolvem a manipulação e o processamento de diversos dados, incluindo dados sensíveis, é essencial que todos os utilizadores compreenderem como esses dados serão tratados, protegidos e utilizados. Neste sentido, o presente documento visa esclarecer os procedimentos e práticas adotadas no tratamento de dados pessoais, garantindo que todas as operações sejam realizadas em conformidade com o Regulamento Geral de Proteção de Dados (RGPD) – Regulamento (UE) 2016/679, assegurando a proteção dos direitos dos titulares dos dados.

Dados Pessoais Recolhidos

Durante a utilização da aplicação e para a prestação dos seus serviços, serão recolhidos dados pessoais, sendo estes tratados de acordo com as finalidades específicas da plataforma. Para o correto funcionamento do sistema e para assegurar a prestação dos serviços da aplicação, serão recolhidos e tratados os seguintes dados pessoais dos utilizadores:

- Username
- Função (Role)
- Email
- Nome Completo
- Data de Nascimento
- Gênero
- Número do Registo Médico
- Informações de Contacto
- Condições Médicas/Alergias
- Contacto de Emergência
- Histórico de Consultas
- Número de Licença
- Identificador de Pedido de Operação
- Identificação do Paciente
- Identificação do Médico

Os dados recolhidos estão organizados nas seguintes categorias:

Dados de Identificação Pessoal: informações que permitem a identificação direta de um indivíduo, como paciente, médico ou membro do staff.

Dados de Contato: informações que possibilitam entrar em contato com um utilizador, como email e número de telefone.

Dados de Identificação do Sistema: informações necessárias para o registo e autenticação de utilizadores no sistema.

Dados de Saúde: informações relacionadas à saúde dos pacientes, classificadas como sensíveis e sujeitas a proteções adicionais.

Dados de Operações e Agendamentos: informações relativas à organização e gestão de operações e consultas dos pacientes.

Em conformidade com as finalidades para as quais a aplicação foi desenvolvida, os dados pessoais serão tratados de forma adequada, para garantir o normal funcionamento da plataforma.
Assim, os dados pessoais serão submetidos aos seguintes tratamentos:

Recolha de dados: A recolha de dados é realizada para integrar o utilizador no sistema, permitindo que forneça as informações necessárias para a utilização das funcionalidades da aplicação

Conservação dos dados: Os dados são armazenados para garantir a integridade e continuidade do funcionamento da plataforma, permitindo a prestação dos serviços solicitados.

Processamento dos dados: O processamento dos dados tem como finalidade garantir a execução eficiente das funcionalidades do sistema.

Partilha dos dados: A partilha de dados com terceiros ou entidades externas é realizada apenas quando exigido ou estritamente necessário, como, por exemplo, para atender ao interesse do paciente em casos de transferências para outros centros de saúde por exemplo.

Restrição de acesso aos dados: O acesso aos dados é restrito com o objetivo de proteger a privacidade dos utilizadores e garantir que apenas pessoas autorizadas possam aceder aos dados.

Utilização dos dados: Os dados recolhidos são utilizados para viabilizar os serviços fornecidos pela aplicação, atendendo às necessidades dos utilizadores e aos objetivos da plataforma

Atualização dos dados: A atualização dos dados visa garantir que a informação é sempre precisa e atualizada, assegurando que todas as funcionalidades e ações são realizadas com base em dados corretos.

Eliminação dos dados: Os dados são eliminados quando o utilizador solicita ou quando não são necessários para as finalidades para as quais foram recolhidos.

Armazenamento de dados: O armazenamento dos dados tem como finalidade preservar o histórico do utilizador e das operações realizadas, garantindo a continuidade do serviço.

Os dados são recolhidos com as seguintes finalidades:

- Permitir a criação de uma conta de utilizador no sistema, garantindo que cada utilizador tem uma identificação única para aceder à plataforma e utilizar os seus serviços.
- Permitir a comunicação entre o utilizador e a plataforma, para enviar notificações, alertas sobre agendamentos e atualizações importantes. Também serve como meio de recuperação de conta e autenticação.

- Identificar a função de cada utilizador dentro do sistema e consequente acesso a diferentes funcionalidades e dados.
- Identificar o utilizador de forma personalizada, de forma a garantir a prestação de serviços de forma precisa e clara, bem como para associar corretamente os dados ao utilizador.
- Garantir que o sistema possa fornecer serviços adequados à faixa etária do utilizador e cumprir requisitos legais relacionados a tratamentos médicos e consentimento, especialmente em casos de menores de idade.
- Fornecer um atendimento médico mais personalizado, com base nas necessidades específicas de saúde de cada utilizador, além de poder ser usado para personalizar as comunicações e interações no sistema.
- Identificar de forma única cada paciente dentro do sistema, associando-os ao seu histórico médico, exames realizados e tratamentos recebidos
- Permitir a comunicação direta com o utilizador, garantindo que é possível entrar em contato com o mesmo por diferentes meios.
- Garantir que o sistema e os profissionais de saúde possam fornecer cuidados adequados e seguros ao utilizador, levando em consideração suas condições durante tratamentos e intervenções médicas.
- Garantir que, em caso de emergência médica, o utilizador tem um contato adicional, permitindo uma ação rápida e eficaz.
- Garantir a continuidade dos cuidados de saúde, permitindo aos médicos e outros profissionais da saúde aceder ao histórico clínico do paciente para oferecer um atendimento mais eficaz.
- Validar a qualificação dos profissionais de saúde, garantindo que apenas quem está habilitado pode desempenhar as suas funções dentro da plataforma.
- Garantir que as operações agendadas sejam corretamente associadas ao paciente e ao médico responsável.
- Garantir que os dados de cada paciente sejam corretamente associados às suas informações médicas e de operação
- Associar corretamente as operações e consultas aos profissionais responsáveis.

Prazos de conservação de dados pessoais na aplicação

No caso de a conta ser encerrada automaticamente ou no caso de o próprio utilizador eliminar permanentemente a sua conta, determinados dados são mantidos no sistema.

Dados de Conta do Utilizador (Username, Nome, Role, Contacto de emergência):
Devem ser mantidos enquanto o utilizador tiver uma conta ativa no sistema. Após a desativação da conta, esses dados podem ser eliminados dentro de um prazo de 6 meses de modo a permitir a reativação da conta ou verificação de atividades passadas relacionadas ao acesso.

Informações de Contato (Email, Telefone):
Devem ser mantidas de forma associada ao histórico médico, garantindo que seja possível comunicar com o paciente mesmo que este não esteja ativo no sistema.

Isto é relevante no caso de ser necessário fornecer atualizações relacionadas a exames, tratamentos, ou para tratar de situações decorrentes do histórico médico. Assim, estes dados devem ser conservados por um período de 5 anos.

Dados de Identificação Pessoal (Nome Completo, Data de Nascimento, Gênero):
Devem ser mantidos enquanto o utilizador está ativo no sistema e até 5 anos após desativação da conta, de modo a conseguir identificar um paciente caso seja necessário.

Dados Médicos e Histórico (Histórico de Consultas, Condições Médicas, Número de Registo Médico, Identificador de Paciente e Médico):
Os dados relacionados ao histórico de saúde serão mantidos por um período de 5 anos após a última interação do paciente com o sistema. A retenção dessas informações é obrigatória para garantir a rastreabilidade das intervenções e operações médicas realizadas. Além disto permite e facilita investigações futuras que possam ser essenciais para a saúde do paciente, mesmo quando este já não se encontre ativo no sistema.

Armazenamento de Dados Arquivados (Histórico de Operações, Género, Data de nascimento):
Estes dados devem ser mantidos por um período de 10 anos, desde que anonimizados, para fins estatísticos, históricos ou legais.

Em conformidade com o Regulamento Geral de Proteção de Dados (RGPD), deve haver estabelecido um plano de ação estruturado para lidar com violações de dados. Os procedimentos consistem nos seguintes passos:

1. **Identificação e Contenção**
   O primeiro passo é identificar o tipo de violação que ocorreu e implementar ações imediatas para conter o incidente, mitigando os impactos de forma eficaz.

2. **Avaliação da situação**
   Após a contenção e resolução inicial do problema, é crucial realizar uma avaliação do incidente. Esta etapa envolve identificar que dados foram comprometidos, determinar os utilizadores afetados, e avaliar os potenciais riscos que podem surgir, como roubo de identidade, prejuízos financeiros, ou danos à privacidade. Esse diagnóstico permite compreender a gravidade da situação e tomar medidas proporcionais para mitigar os impactos.

3. **Notificação às Autoridades Competentes**
   Em conformidade com o RGPD, é obrigatório notificar a Comissão Nacional de Proteção de Dados (CNPD) sobre a violação. Esta comunicação é essencial para garantir a transparência, permitir que a autoridade supervisora monitore a situação e tome medidas adicionais, se necessário.

4. **Informar os Titulares dos Dados**
   Sempre que a violação representar um risco elevado aos direitos e liberdades dos utilizadores, os titulares dos dados afetados devem ser notificados. A comunicação deve incluir informações claras sobre o incidente, os dados comprometidos e as ações tomadas para mitigar os impactos.

5. **Medidas Corretivas e Prevenção**
   Após o incidente, é fundamental identificar as causas da violação e implementar medidas corretivas para evitar reincidências. Isso pode incluir reforço das políticas de segurança, adoção de criptografia, monitorização contínua e autenticação multifatorial.