TO TRANSLATE - Preview

editar

TO TRANSLATE - GENERAL INFORMATION

97%

Pré-visualização

TO TRANSLATE - Editing :	João de Macedo	**TO TRANSLATE - Status :**	Em progresso
TO TRANSLATE - Evaluation :	Nelson Gonçalves		
TO TRANSLATE - Validation :	João Aloísio		

TO TRANSLATE - Validation

Mapeamento de riscos

Gravidade de risco

Probabilidade de risco

- Medidas existentes ou planeadas
- Com as medidas corretivas implementadas
- Acesso (i)legítimo aos dados
- Modificação (in)desejada dos dados
- Desaparecimento dos dados

28/03/2020

TO TRANSLATE - Validation

Plano de ação

Visão geral

Princípios fundamentais

- Objetivos
- Base legal
- Dados adequados
- Precisão de dados
- Duração dos dados
- Informação para os titulares dos dados
- Obtenção do consentimento
- Direito de acesso e portabilidade de dados
- Direito à retificação e apagamento
- Direito à restrição e à oposição
- Subcontratação
- Transferências

Medidas existentes ou planeadas

- Cifrar os dados
- Autenticação

Riscos

- Acesso ilegítimo de dados
- Modificação indesejada de dados
- Desaparecimento de dados

Medidas Improváveis
Medidas Aceitáveis

Princípios fundamentais

Nenhum plano de ação registado.

Medidas existentes e planeadas

Nenhum plano de ação registado.

Riscos

Nenhum plano de ação registado.

TO TRANSLATE - Validation

TO TRANSLATE - DPO and data subjects opinion

TO TRANSLATE - No data to display.

Contexto

Visão geral

Qual é a finalidade de tratamento considerada no âmbito da análise?

O projeto proposto consiste no desenvolvimento de uma aplicação para o agendamento de consultas numa clínica. Nesta aplicação é possível agendar consultas, ver o histórico e resumo de consultas,

consultar as receitas médicas e ver o historial dos utentes.
Para os utentes se registarem na aplicação têm de indicar o seu nome completo, idade, data de nascimento, número de utente e password. Aos médicos são fornecidas credenciais para posteriormente associarem o seu nome, password e especialidade.

A clínica pode apagar a conta de um médico, no entanto a conta de um utente não poderá ser apagada. Portanto, este projeto proposto respeita os critérios 3 e 7 acima mencionados, pelo que seria necessário efetuar uma DPIA.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

É necessário garantir que os dados armazenados sejam confidenciais, onde ninguém os poderá aceder e que os dados inseridos serão apenas usados no contexto da aplicação.

Quais são as normas aplicáveis à finalidade de tratamento?

Para a cifragem dos dados a equipa de desenvolvimento sugere o uso de um dos standarts disponíveis.

Avaliação : Aceitável

Contexto

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Dados pessoais do utente:
- Nome completo
- Data de nascimento
- Número de utente de saúde
- Password
- Histórico de consultas
- Consultas agendadas

Dados pessoais dos médicos:
- Nome completo
- Especialidade
- Doentes

Dados processados:
- Histórico de consultas por utente
- Histórico de prescrições por consulta
- Consultas agendadas

Como funciona o ciclo de vida dos dados pessoais e dos processos inerentes?

Os dados são inseridos na aplicação pelos utentes e pelos médicos, sendo estes inseridos numa base de dados onde não é Possível eliminar informação relativamente aos utentes. A partilha de dados não será possível visto que os utentes apenas têm Acesso à sua informação, e os médicos apenas têm acesso à informação dos seus utentes. Os processamentos com mais riscos Associados são a inserção de informação pessoal e sensível dos utentes, bem como a gestão da mesma.

Quais são os ativos de informação utilizados na finalidade de tratamento?

Aplicação: JavaScript
Base de dados: MongoDB

Avaliação : Aceitável

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

O armazenamento dos dados da aplicação, tem como objetivo extrair dados para obter dados Estatísticos, como por exemplo, a frequência da clínica, o tipo de doenças mais comuns, relacionado Com as idades, as especialidades mais procuradas, etc.

Avaliação : Aceitável

Qual é o fundamento para tratamento de dados pessoais?

Cada utente aceita os termos da aplicação aquando a sua inscrição.

Avaliação : Aceitável

Os dados pessoais recolhidos são adequados, relevantes e limitados para o propósito de tratamento realizado (princípio da minimização de dados)?

Utentes:
- Nº de utende: Autenticação
- Password: Autenticação
- Nome completo: Informativo
- Data de nascimento: Informativo
- Idade: Estatístico
- Histórico de consultas: Estatístico
- Histórico de prescrições: Estatístico
- Histórico de doenças: Estatístico
- Resumo das consultas: Informativo
- Especialidade: Marcação de consultas

Médicos:
- Nome de utilizador: Autenticação
- Password: Autenticação
- Nome completo: Informativo
- Especialidade: Marcação de consultas
- Utentes associados: Informativo

Avaliação : Aceitável

Os dados pessoais estão atualizados e são fidedignos?

Os médicos podem alterar as informações das doenças dos utentes, mudar as prescrições, como a sua especialidade, se for esse o caso.

Avaliação : Aceitável

Qual é o prazo da conservação dos dados?

Os dados tem um tempo de vida ilimitado, excetuando os dados removidos em relação aos médicos.

Avaliação : Aceitável

Princípios fundamentais

Controlos para proteger os direitos pessoais dos titulares dos dados

Como é que os titulares dos dados são informados sobre o tratamento dos seus dados?

Aquando da sua incrição na aplicação, aceitando os termos.

Avaliação : Aceitável

Como é obtido o consentimento dos titulares de dados?

Aceitando os termos e resgitando-se na aplicação

Avaliação : Aceitável

Como é garantido o acesso e portabilidade de dados pessoais?

Tanto os médicos como os utentes conseguem aceder aos seus dados sempre que quiseres, através da aplicação.

Avaliação : Aceitável

Como é garantida a atualização/retificação e apagamento dos dados pessoais pedida pelo titular dos mesmos?

Os médicos podem atualizar as suas informações, assim como os utentes.

Avaliação : Aceitável

Como é garantida a limitação do tratamento dos dados pessoais pedido pelo titular dos mesmos?

Aquando do registo na aplicação, os utentes podem discordar com os termos de utilização.

Avaliação : Aceitável

As obrigações dos subcontratantes são claramente identificadas e reguladas por contrato ou outro ato normativo?

Não se aplica.

Avaliação : Aceitável

No caso de transferência de dados fora da União Europeia, os dados são adequadamente protegidos?

Não acontece porque esta aplicação apenas está disponivel para clínicas em Portugal.

Avaliação : Aceitável

Riscos

Medidas planeadas ou existentes

Cifrar os dados

Uma medida de segurança desta aplicação passa por cifrar todos os dados inseridos na base de dados, garantido a sua confidencialidade.

Avaliação : Aceitável

Autenticação

Apenas quem tem credenciais de acesso consegue entrar na aplicação. Cada utente e médico tens as duas únicas credenciais de acesso.

Avaliação : Aceitável

Riscos

Acesso ilegítimo dos dados

Quais poderiam ser os principais impactos nos dados dos titulares se o risco ocorrer?

Acesso a dados confidenciais e sensiveis por parte de terceiros

Quais são os principais ameaçasque poderiam levar ao risco?

Acesso s credenciais dos utilizadores.

Quais são as fontesde risco?

Atividade humana no desenvolvimento da aplicação.

Quais são os controlos identificados que contribuem para abordar o risco?

Como estimas a gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados?

Significante

Como estimas a probabilidade de risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Significante

Riscos

Modificação indesejada dos dados

Quais poderiam ser os impactos nos dados dos titulares se o risco ocorrer?

Modificação dos dados dos utentes

Quais são as principais ameaças que poderiam levar ao risco?

Acesso aos dados dos utentes

Quais são as fontesde risco?

Atividade humana no desenvolvimento da aplicação.

Quais são os controlos identificados que contribuem para abordar o risco?

Cifrar os dados, Autenticação

Como estimas a gravidade do risco, especialmente de acordo com impactos potenciais e controlos planeados?

Significante

Como estimas a probabilidade do risco, especialmente em relação a ameaças, fontes de

risco e controlos planeados?

Insignificante

Riscos

Desaparecimento de dados

Quais são os principais impactos nos dados dos titulares se o risco ocorrer?

Desaparecimento de todo o historial médico

Quais são as principais ameaças que poderiam levar ao risco

Falta de backup dos dados

Quais são as fontesde risco?

Atividade humana no desenvolvimento da aplicação.

Quais são os controlos identificados que contribuem para abordar o risco?

Cifrar os dados

Como estimas a gravidade de risco, especialmente de acordo com impactos potenciais e controlos planeados?

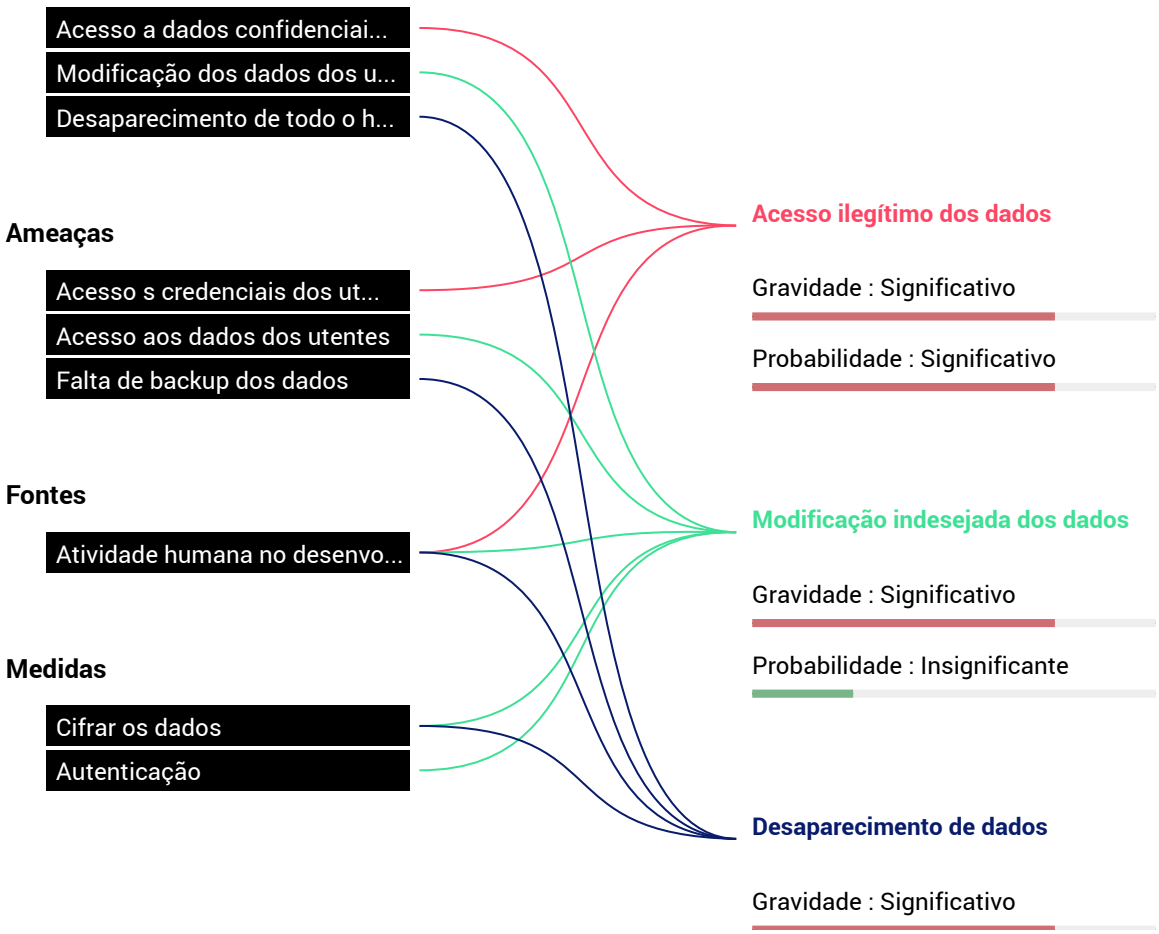
Significante

Como estimas a probabilidade do risco, especialmente em relação a ameaças, fontes de risco e controlos planeados?

Insignificante

Riscos

Visão geral dos riscos



Probabilidade : Insignificante