

TO TRANSLATE - Preview

TO TRANSLATE - GENERAL INFORMATION

100%

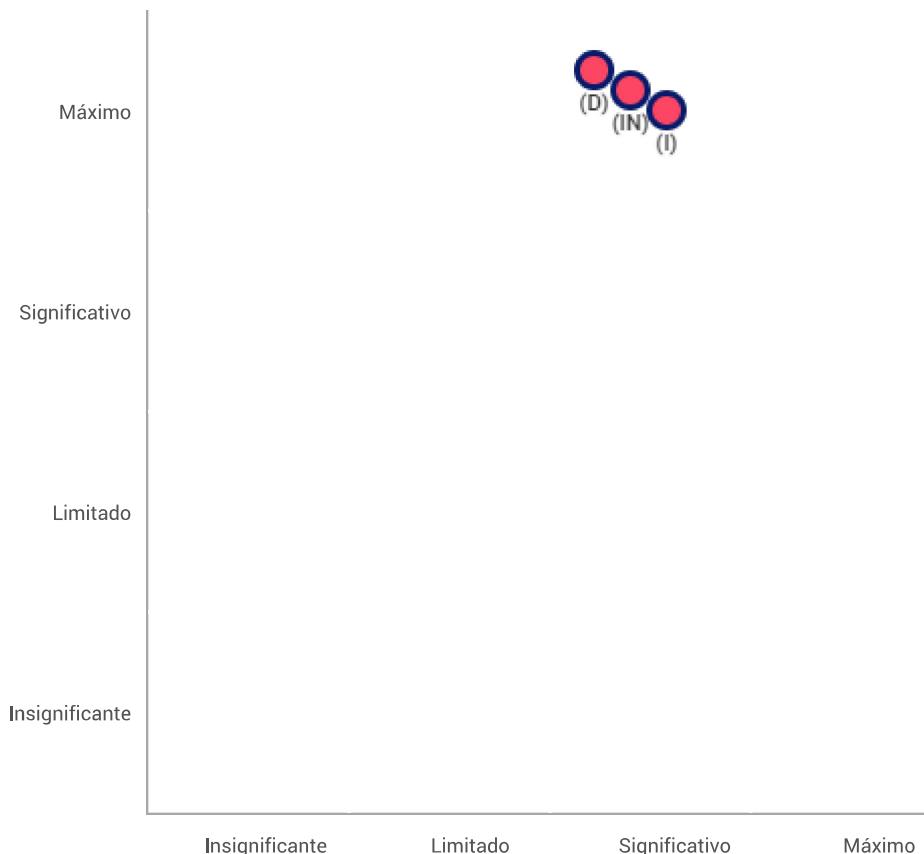
Pré-
visualização

TO TRANSLATE - Editing :	Marco Couto	TO TRANSLATE - Status :	Validação Essinada
TO TRANSLATE - Evaluation :	Joana Ribeiro		
TO TRANSLATE - Validation :	Paulo Mendes		

TO TRANSLATE - Validation

Mapeamento de riscos

Gravidade de risco



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

Probabilidade de risco

26/03/2020

TO TRANSLATE - Validation

Plano de ação

Visão geral

Princípios fundamentais	Medidas existentes ou planeadas
Objetivos	Encriptação e pseudominimização de dados
Base legal	Autenticação
Dados adequados	
Precisão de dados	
Duração dos dados	
Informação para os titulares dos dados	
Obtenção do consentimento	Acesso ilegítimo de dados
Direito de acesso e portabilidade de dados	Modificação indesejada de dados
Direito à retificação e apagamento	Desaparecimento de dados
Direito à restrição e à oposição	
Subcontratação	
Transferências	

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

Nome do DPO

App de consulta médica

Opinião do DPO

O tratamento pode ser implementado de forma correta.

Procura da opinião de partes interessadas

A opinião das partes em questão foi solicitada.

Opiniões de partes interessadas

Pacientes, Especialistas

Status de pessoas em questão

O tratamento deve ser implementado.

Opiniões de partes interessadas

O tratamento pode ser implementado dado as pesquisas em pacientes e especialistas.

Contexto

Visão geral

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

O projeto tem como objetivo o desenvolvimento de uma aplicação para uma marcação de consultas médicas por parte dos especialistas bem como a adição de medicação. Os pacientes podem sempre verificar qualquer alteração que possa ter sido feita bem como o seu histórico.

As credenciais de registo são introduzidas pelo paciente para a sua inscrição em que o especialista fornece um código de ativação.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

É necessária a garantia de que os dados preenchidos não são fornecidos a terceiros e que esses dados só são utilizados pela aplicação.

Quais são as normas aplicáveis à finalidade de tratamento?

Utilização da pseudominimização e da encriptação de dados que são relevantes por parte do paciente ou do especialista.

Avaliação : Aceitável

Contexto

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Os dados pessoais dos pacientes: nome completo, nome de utilizador, password, idade, número de utente de saúde, número do cartão de cidadão, NIF, endereço eletrónico, especialista associado (médico de família).

Os dados pessoais dos especialista: nome completo, nome de utilizador, password, especialização, número de utente de saúde dos pacientes que possui, posto de saúde.

Os dados armazenados e processados: históricos de doenças, relatórios, medicação.

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

Os dados são inseridos pelos pacientes, pelos especialistas, e pelo gerente do posto médico a nível informático. São armazenados numa base de dados onde não se removem os dados dos pacientes. Os dados mais pessoais são importantes de serem armazenados de forma segura.

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

A aplicação utilizada é o Javascript e a base de dados é a MySQL.

Avaliação : Aceitável

Princípios fundamentais

Proporcionalidade e necessidade

A finalidade de tratamento é específica, explícita e legítima?

O armazenamento dos dados tem como objetivo a extração de dados estatísticos para saber informações concretas como a frequência do paciente ao posto médico, as doenças mais comuns em geral bem como a medicação.

Avaliação : Aceitável

Qual é o fundamento para tratamento de dados pessoais?

Os pacientes e os especialistas que se registam na aplicação autorizam para que os seus dados sejam utilizados para fim estatísticos.

Avaliação : Aceitável

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

Nos pacientes os dados utilizados para autenticação são o nome de utilizador, a password e o código de ativação. A nível informativo é introduzido o seu nome completo, idade, número de utente de saúde, número do cartão de cidadão, NIF, morada. Os históricos são colocados para fins de estatísticas tais como medicação, frequência de adesão ao posto médico. A nível informativo são utilizados os relatórios dos especialistas.

Nos especialistas (médicos de família) são utilizados dados de autenticação como o nome de utilizador, password. A nível informativo o seu nome completo, a sua morada, o seu posto médico. A nível informativo os pacientes que aborda.

Avaliação : Aceitável

Os dados pessoais estão atualizados e são fidedignos?

Sim. Os dados são alterados em caso de engano e é tudo alterado de forma fidedigna.

Avaliação : Aceitável

Qual é o prazo da conservação dos dados?

A conservação de dados é permanentes a partir do momento que o paciente consente ao registar na aplicação.

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?

A partir do momento do registo, os pacientes são notificados via endereço eletrónico para utilizarem a sua conta.

Avaliação : Aceitável**Como é obtido o consentimento dos titulares de dados?**

A partir do momento do registo dos seus dados.

Avaliação : Aceitável**Como é garantido o acesso e portabilidade de dados pessoais?**

O acesso e portabilidade dos dados pessoais é trocado entre paciente e o seu especialista.

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

A atualização pode ser feita a qualquer momento por parte do especialista ou do paciente.

Avaliação : Aceitável**Como é garantida a limitação do tratamento dos dados pessoais pedido pelo titular dos mesmos?**

Os pacientes podem aceitar ou não os termos de utilização.

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

Não é aplicado.

Avaliação : Aceitável**No caso de transferência de dados fora da União Europeia, os dados são adequadamente protegidos?**

Esta aplicação era ser um desenvolvimento para Portugal pelo que fora de União Europeia será irrelevante a utilização.

Avaliação : Aceitável

RISCOS

Medidas planeadas ou existentes

Encriptação e pseudominização de dados

Utilização destas normas para segurança dos dados.

Avaliação : Aceitável**Autenticação**

Autenticação dos dados introduzidos.

Avaliação : Aceitável

RISCOS

Acesso ilegítimo dos dados

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

Terceiros que queiram obter informação de um paciente.

Quais são os principais ameaças que poderiam levar ao risco?

Aceder à password e, consequentemente, aos dados pessoais do paciente.

Quais são as fontes de risco?

Mau desenvolvimento da aplicação.

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

Autenticação, Encriptação e pseudominização de dados

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

Máximo, Risco elevado.

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

Significante, Alta probabilidade.

Avaliação : Aceitável

RISCOS

Modificação indesejada dos dados

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

Terceiros que queiram obter informação de um paciente.

Quais são as principais ameaças que poderiam levar ao risco?

Aceder à password e, consequentemente, aos dados pessoais do paciente.

Quais são as fontes de risco?

Mau desenvolvimento da aplicação.

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

Encriptação e pseudominização de dados, Autenticação

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

Máximo, Gravidade elevada.

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

Significante, Comprometimento dos dados.

Avaliação : Aceitável

RISCOS

Desaparecimento de dados

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

Terceiros que queiram obter informação de um paciente.

Quais são as principais ameaças que poderiam levar ao risco

Aceder à password e, consequentemente, aos dados pessoais do paciente.

Quais são as fontes de risco?

Mau desenvolvimento da aplicação.

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

Encriptação e pseudominização de dados, Autenticação

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

Máximo, Muito grave caso aconteça.

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

Significante, Roubo de dados e informações do utente.

Avaliação : Aceitável

RISCOS

Visão geral dos riscos

Impactos potenciais

Terceiros que queiram obter...

Ameaças

Aceder à password e, conseq...

Acesso ilegítimo dos dados

Gravidade : Máximo

Probabilidade : Significativo

Fontes

Mau desenvolvimento da apli...

Medidas

Autenticação

Modificação indesejada dos dados

Encriptação e pseudominizaç...

Gravidade : Máximo

Probabilidade : Significativo

Desaparecimento de dados

Gravidade : Máximo

Probabilidade : Significativo

