Informação PIA

PIA
Aplicação para marcação de consultas no posto médico

Nome do autor
João Sousa

Nome do assessor
Francisco Araújo

Nome do validador
Gonçalo Raposo

Data de criação
18/04/2019

Contexto

Visão geral

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

O projeto aqui apresentado consiste no desenvolvimento de uma aplicação para a marcação de consultas num posto médico, que permite aos utentes, para além do agendamento de consultas, ter acesso ao histórico de consultas realizadas, bem como as prescricões médicas receitadas em cada consulta e um breve resumo sobre as suas consultas, onde consta o que foi falado.

As credenciais para os médicos são disponibilizados pelo respetivo posto médico em que trabalha, enquanto os utentes tem que registar na aplicação e indicar nome completo, nome de utilizador, idade, data de nascimento, posto médico que frequentam, doenças, password. Por outro lado os médicos tem apenas a si associado nome completo, nome de utilizador, passowrd, posto médico atual e os respetivos utentes a si associados.

Os postos médicos podem apagar a conta de um médico, caso este mude de estabelecimento, sendo neste caso gerado novas credencias pelo novo estabelecimento frequentado. Os utilizadores uma vez registados na aplicação não podem nunca apagar a sua conta.

Quais são as responsabilidades inerentes ao tratamento de dados pessoais?

É necessário garantir que os dados armazenados não serão pratilhados com terceiros, isto é, nenhuma identidade exterior à equipa de desenvolvimento e que os dados inseridos são apenas usados no contexto da aplicação.

Deve-se ainda cifrar os dados aramzenados.

Quais são as normas aplicáveis à finalidade de tratamento?

Para a cifragem dos dados a equipa de desenvolvimento sugere o uso de um dos standards diposníveis.

Avaliação : Pendente

Dados, processos e ativos de suporte

Quais são os dados pessoais tratados?

Dados pessoais do utente:
-Nome completo
-Nome de utilizador
-Data de Nascimento
-Idade
-Posto médico frequentado
-Doenças
-Password

Dados pessoais dos médicos:
-Nome Completo
-Nome de utilizador
-posto médico atual
-Doentes a si associados

Dados processados:
-Histórico de consultas do utente
-Histórico de doenças
-Histórico de prescições para cada consulta
-Resumo das consultas

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

Os dados serão inseridos na aplicação pelos utentes (informações pessoais, agendamento de consultas), pelo gerente do posto médico (informação relativa ao médico) e pelo médico (informação relativa às consultas). Todos os dados inseridos na aplicação serão armazenados numa
base de dados, sendo que não é possível a remoção de utentes. Não haverá também partilha dos
dados com terceiros, uma vez que cada utente tem acesso apenas à sua informação e os médicos
tem apenas acesso às informações 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

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 estatísticos, de por exemplo, a frequência com que se vai ao posto médico, que tipo de consultas são. Serve ainda para extrair dados estatísticos de quais as doenças mais comuns nos cidadãos portugueses, quais os medicamentos mais receitados para cada doença específica bem como quais os médicos mais requisitados

Qual é o fundamento para tratamento de dados pessoais?

Cada utente a quando do registo na aplicação, autoriza a que os seus dados sejam utilizados para tratamento estatístico.

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

Utentes:
-Nome de Utilizador : Autenticação
-Password : Autenticação
-Nome completo: Informativo
-Data de nascimento: Informativo
-Idade : Estatístico
-Histórico de doenças: Estatístico
-Histórico de consutlas: Estatístico
-Histórico de prescrições: Estatístico
-Resumo das consultas : Informativo
-Posto médico frequentado : Marcação de consultas

Médicos:
-Nome de utilizador : Autenticação
-Passowrd : Autenticação
-Nome completo : Informativo
-Posto médico autal : Maracação de consultas
-Utentes associados : Informativo

Os dados pessoais estão atualizados e são fidedignos?

A qualquer momento, tanto os utentes como os médicos podem mudar as suas informações pessoais, como por exemplo, a adição de novas doenças, atualização da idade, atualização do posto médico, entre outras.

Qual é o prazo da conservação dos dados?

Os dados dos utentes tem um tempo de vida ilimitado, ficando para sempre armazenados e não podendo haver a eliminação dos mesmos. Quanto aos médicos os seus dados podem ser apagados quando o mesmo muda de posto médico.

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 quando do registo na aplicação, todos os utentes são avisados para os usos das informações que colocarão na aplicação.

Como é obtido o consentimento dos titulares de dados?

Após a atuenticação na aplicação.

Como é garantido o acesso e portabilidade de dados pessoais?

Os utentes e os médicos conseguem ter acesso aos seus dados, uma vez que a aplicação terá uma página com o perfil do utente/médico

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

A qualquer altura tanto os médicos como os utentes podem atualizar as suas informações na página do perfil dos mesmos.

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

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

As obrigações dos subcontratrantes são claramente identificadas e regulados por contrato ou outro ato normativo?

Não se aplica.

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

Como a aplicação apenas funcionará no território português, não existe intenção da nossa parte de transferir os dados para fora da União Europeia

Riscos

Medidas planeadas ou existentes

Cifrar os dados

Uma media de segurança da nossa aplicação passa por cifrar todos os dados inseridos na mesma, de maneira a terceiros não terem acesso à informação de qualquer utente.

Autenticação

Para entrar na aplicação é preciso o uso de credências pessoais e únicas relativas a cada utente/médico

Acesso ilegítimo dos dados

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

Acesso aos dados dos utentes por parte de terceiros

Quais são os principaisameaçasque poderiam levar ao risco?

Acesso à password dos utentes/médicos,.

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

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, Se houvesse a cifrar dos dados, era difícil a qulaquer pessoa aceder ou alterar os dados.

Desaparecimento de dados

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

Desparecimento de todo o historial médico dos utentes.

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

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
- Informação para os titulares dos 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.

Visão geral dos riscos

Impactos potenciais

- Acesso aos dados dos utente...
- Modificação dos dados dos u...
- Desparecimento de todo o hi...

Ameaças

- Acesso à password dos utent...
- Acesso aos dados dos utentes
- Falta de backup dos dados

Fontes

- Atividade humana no desenvo...

Medidas

- Cifrar os dados
- Autenticação

Acesso ilegítimo dos dados

Gravidade : Significativo

Probabilidade : Significativo

Modificação indesejada dos dados

Gravidade : Significativo

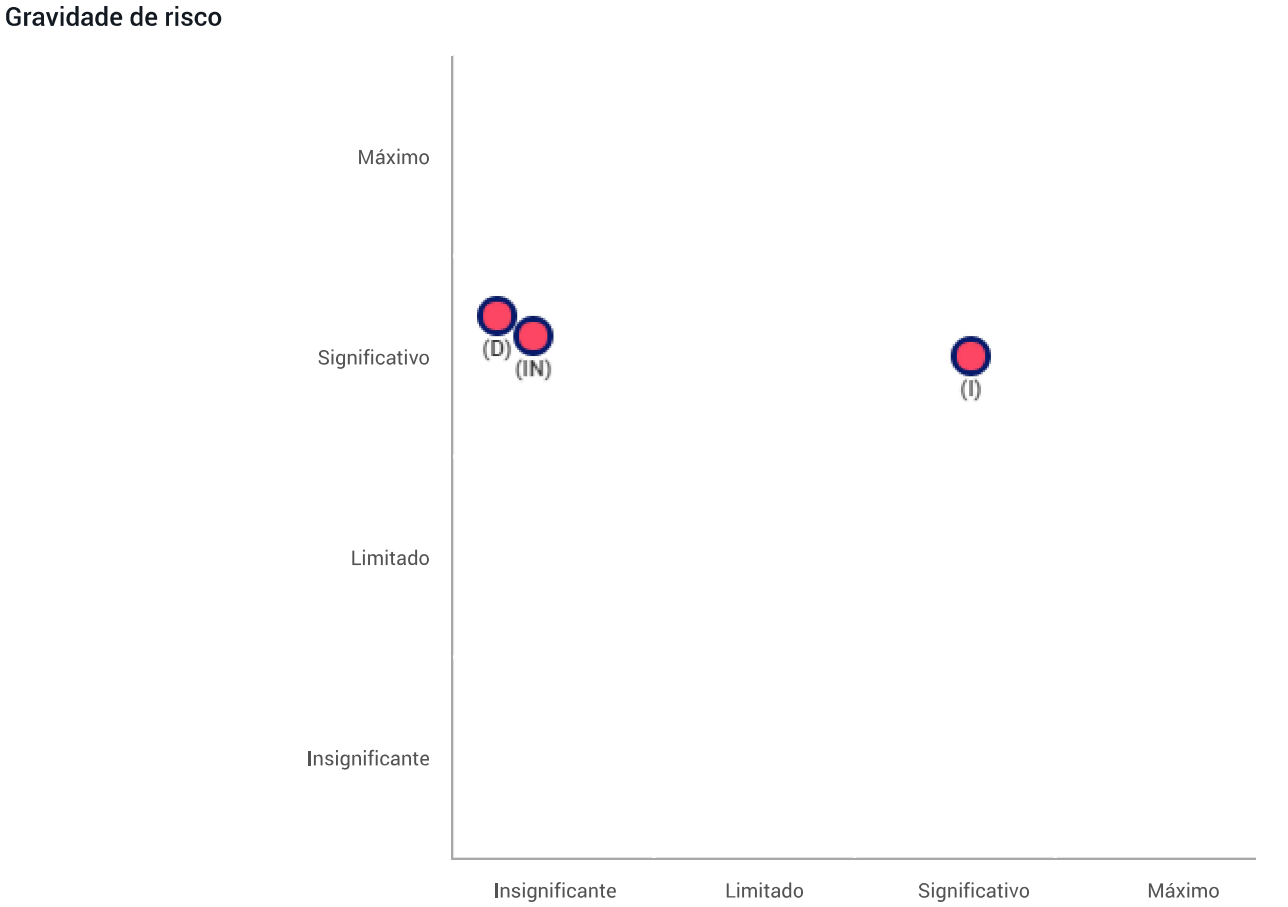
Probabilidade : Insignificante

Desaparecimento de dados

Gravidade : Significativo

Probabilidade : Insignificante

Mapeamento de riscos



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

18/04/2019