INSTITUTO SUPERIOR DE ENGENHARIA DO PORTO
MESTRADO EM ENGENHARIA INFORMÁTICA




Adaptação de infraestrutura de interoperabilidade clínica ao Regulamento Geral de Proteção de Dados

MIGUEL ÂNGELO BOTELHO MONTEIRO
Outubro de 2019

POLITÉCNICO
DO PORTO

Instituto Superior de Engenharia do Porto

Adaptação de infraestrutura de interoperabilidade clínica ao Regulamento Geral de Proteção de Dados

Miguel Ângelo Botelho Monteiro

Dissertação para obtenção do Grau de Mestre em Engenharia Informática, Área de Especialização em Engenharia de Software

Orientador: Nuno Alexandre Pinto da Silva

Supervisor: André Filipe Roque Silva

Porto, outubro 2019

Declaração de confidencialidade

Nos termos do contrato de estágio curricular e do acordo de confidencialidade celebrado com a ALERT Life Sciences Computing, S.A ("ALERT"), o presente relatório é confidencial e poderá conter referências a invenções, *know-how*, desenhos, programas de computador, segredos comerciais, produtos, fórmulas, métodos, planos, especificações, projetos, dados ou obras abrangidos por direitos de propriedade industrial e/ou intelectual da ALERT. Este relatório poderá ser utilizado para efeitos de investigação e de ensino. Qualquer outro tipo de utilização está sujeito a autorização prévia e por escrito da ALERT.

Resumo

A evolução da era digital proporciona aos utilizadores um acesso à sua informação de um modo mais facilitado e conveniente através dos serviços/produtos das organizações que detêm a sua informação. Contudo, nos últimos anos, tem-se observado a falta de medidas de segurança na gestão da informação dos utilizadores, nas pequenas e grandes organizações, que originou vazamentos de informação pessoal e confidencial. Para combater estes incidentes, a União Europeia criou o Regulamento Geral de Proteção de Dados (RGPD) que define um conjunto de regras a serem respeitadas por todas as organizações, dentro ou fora da União Europeia, que façam tratamento sobre os dados pessoais de cidadãos residentes na União Europeia.

As instituições de saúde têm vindo a adotar Registos Clínicos Eletrónicos (EHR) com o objetivo de partilhar informação clínica entre si, promovendo o conceito de interoperabilidade clínica. Com a entrada em vigor do RGPD, é necessário garantir que a informação pessoal e clínica dos pacientes cumpra as imposições estabelecidas pelo RGPD. Sendo a ALERT uma organização que trabalha na área da saúde e tecnologias da informação, é fundamental que os produtos ALERT® estejam em cumprimento com o RGPD, de modo a que os pacientes estejam seguros da informação que é processada pelos produtos. Dito isto, a ALERT está a implementar processos no sentido de cumprir com as exigências do RGPD ao nível organizacional e dos seus produtos.

O ALERT® HIE é o produto de interoperabilidade clínica da ALERT. Este permite a partilha de informação clínica entre instituições que façam parte do seu domínio, como também a correlação de pacientes entre instituições de forma a melhorar os cuidados médicos prestados. Assim, o ALERT® HIE processa informação sensível e identificável dos pacientes das várias instituições, sendo fundamental que o produto esteja em cumprimento com as exigências do RGPD.

No sentido de respeitar estas exigências, este documento aborda uma análise dos requisitos necessários para que o produto cumpra o RGPD, um estudo de soluções existentes que permitirão responder aos requisitos identificados, novos conceitos de negócios provenientes do RGPD, adaptações necessárias nos processos de negócio, novos artefactos de desenho e a respetiva implementação no produto.

Os resultados obtidos através da experimentação ao algoritmo de correlacionamento de EHR de pacientes, permitiu aferir que quantos mais atributos forem utilizados maior será a precisão do algoritmo, no entanto, a sua cobertura irá descer significativamente devido aos possíveis erros de inserção que possam existir. Ao utilizar 6 atributos obteve-se uma precisão de 98,13% e uma cobertura de 87,55%, já com 14 atributos a precisão foi de 99,54% mas a cobertura de apenas 80,86%.

Palavras-chave: RGPD, Interoperabilidade clínica, Privacidade dos dados, Consentimento

Abstract

The evolution of the digital era gives users an easier and more convenient access to their information throughout services/products of the organizations that have their information. However, in recent years, there has been a lack of security measures in the management of user information in small and large organizations, which has resulted in leaks of personal and confidential information. In order to oppose these incidents, the European Union has established the General Data Protection Regulation (GDPR), which defines a set of rules to be respected by all organizations inside or outside the European Union, that treat personal data of residente european citizens.

In the past years, Health institutions have been adopting Electronic Health Records (EHR) in order to share clinical information with each other, promoting the concept of clinical interoperability. With GDPR's enforcement, it is necessary to guarantee the security of patient's personal and clinical information. Since ALERT is an organization inside the health and information technology area, it's fundamental that ALERT® products comply with the rules of GDPR, as they manage patient's sensitive information. For this reason, ALERT has been implementing processes in order to comply with GDPR requirements at the organizational level and regarding its products.

ALERT® HIE is ALERT's clinical interoperability product, that allows the share of clinical information between institutions that are part of its domain, as well as the correlation of patients in order to improve the healthcare. Therefore, as it processes patient's sensitive and identifiable information from the various institutions, it is fundamental that the product complies with GDPR requirements.

In order to respect these , this thesis approaches an analysis of the requirements necessary for the product to comply with the GDPR, along with a study of existing solutions that may help in the implementation of the identified requirements, new business concepts brought by GDPR, the necessary adaptations in the business process, new design artifacts and the respective implementation in the product.

The results obtained by the experimentation performed in correlation algorithm of patient's EHR, allowed to determine that the more attributes used, the greater the precision will be, however, the recall will decrease significantly due to the possible insertion error that may exist. The use of 6 attributes obtained an precision of 98,13% and a recall of 87,55%, while 14 attributes obtained a precision of 99,54% but the recall was only 80,86%.

Keywords: GDPR, Clinical interoperability, Data privacy, Consent

Agradecimentos

Em primeiro lugar quero agradecer à ALERT pela oportunidade de participar neste projeto. Obrigado a todos os seus colaboradores pelo suporte, ajuda e ambiente durante a elaboração da tese. Um obrigado especial aos engenheiros André Silva e Tiago Gonçalves que se mostraram sempre disponíveis e me apoiaram em todas as fases do projeto.

Agradeço ao ISEP por me ter acolhido nestes últimos cinco anos e especialmente ao Departamento de Engenharia Informática (DEI).

Agradeço a todos os docentes com que interagi durante a Licenciatura em Engenharia Informática(LEI) e no Mestrado em Engenharia Informática (MEI) por todos os conhecimentos transmitidos nas diversas uinidades curriculares. Um obrigado especial ao Professor Doutor Nuno Silva, por ter aceite ser meu orientador, pelas reuniões, esclarecimentos, conselhos, revisões e principalmente a sua disponibilidade e dedicação.

Agradeço à minha família por todo o apoio durante a minha vida, pois é graças a eles que tenho conseguido atingir os meus objetivos. Por último, quero agradecer à minha namorada Ana Machado, por todo o apoio durante os últimos cinco anos e espero continuar futuramente a alcançar a teu lado os objetivos que pretendemos.

Índice

Lista de Figuras

Lista de Tabelas

Lista de Extratos de Código

Acrónimos e Símbolos

Lista de Acrónimos

Acrónimo	Significado
API	Application programming interface
ATNA	Audit Trail and Node Authentication
EHR	Eletronic Health Record
HIE	Health Information Exchange
HSM	Hardware Security Model
HTTPS	Hypertext Transfer Protocol Secure
IHE	Integrating the HealthCare Enterprise
IoC	Inversion of Control
ISEP	Instituto Superior de Engenharia do Porto
ISO	International Organization for Standardization
JSON	JavaScript Object Notation
OID	Object Identifier
OIT	Oracle Index Text
Oracle TDE	Oracle Transparent Data Encryption
PHR	Personal Health Record
POI	Patient Other Identifier
QFD	Quality Function Deployment
REST	Representation State Transfer
RGPD	Regulamento Geral de Proteção de Dados
SGBD	Sistema de Gerenciamento de Banco de Dados
SO	Sistema Operativo
SSL	Secure Sockets Layer
TI	Tecnologia de Informação
UUID	Universally Unique Identifier
VTE	Vormetric Transparent Encryption
XACML	eXtensible Acess Control Markup Language
XDM	Cross-enterprise Document Media Interchange
XDR	Cross-enterprise Document Reliable Interchange
XDS	Cross Enterprise Document Sharing
XML	Extensible Markup Language

1 Introdução

Neste capítulo é apresentado o contexto, são identificados os problemas, os objetivos a atingir para a resolução dos problemas e a abordagem utilizada para alcançar os objetivos. Finalmente, é apresentada a estrutura do documento.

1.1 Contexto

Este trabalho foi desenvolvido no âmbito da unidade curricular do segundo ano, Tese/Dissertação/Estágio (TMDEI) do Mestrado em Engenharia Informática – área de especialização de Engenharia de *Software* do Instituto Superior de Engenharia do Porto (ISEP).

O projeto "Adaptação de infraestrutura de interoperabilidade clínica ao Regulamento Geral de Proteção de Dados", proposto pela ALERT, foca-se na adaptação do produto de interoperabilidade clínica, ALERT® HIE, ao novo Regulamento Geral de Proteção de Dados (RGPD) (Parlamento Europeu e Conselho, 2016).

As instituições de saúde têm vindo a adotar Registos Clínicos Eletrónicos (EHR – Eletronic Health Records), cuja estrutura hierárquica estabelecida pela ISO 13606 tem como objetivo a partilha de informação clínica entre entidades, promovendo assim a interoperabilidade clínica. Interoperabilidade clínica consiste na troca de informação clínica do paciente entre as diversas instituições independentemente da especialidade e especificidades de cada uma.

A adoção da interoperabilidade clínica por parte das instituições de saúde traz diversas vantagens aos cuidados de saúde modernos, tal como Benson e Grieve (2016, p. 3) descrevem:

> "Os cuidados de saúde modernos dependem de comunicação e trabalho em equipa. A evolução da interoperabilidade pode transformar a eficiência e eficácia dos serviços de saúde, providenciando informação onde e quando requerida, tornando as decisões mais

sólidas e rápidas, reduzindo o desperdício ao eliminar trabalho repetido e melhorando a segurança devido a serem cometidos menos erros."[1]

Existindo diversas instituições de saúde, cada uma com o seu sistema informático, implica heterogeneidade (nomeadamente protocolar, sintática, estrutural e semântica), entre sistemas informáticos, dificultando a existência da interoperabilidade entre instituições. Deste modo, é necessário encontrar soluções para resolver esta heterogeneidade.

Uma abordagem para alcançar a interoperabilidade consiste na criação de uma interface de comunicação que permita a troca de informação entre cada par de instituições, sendo que o número de ligações a estabelecer é dado pela seguinte fórmula:

$$Número\ de\ ligações\ bilaterais = \frac{n(n-1)}{2}$$

Assim, existindo 6 sistemas, é necessário implementar 15 interfaces; com 100 sistemas é necessário implementar 4950 interfaces (Benson and Grieve, 2016, p. 23). Se esta abordagem fosse adotada teria custos de desenvolvimento e manutenção inviáveis para alcançar a interoperabilidade clínica.

Outra solução é a criação de um ponto centralizado que permita o envio e a pesquisa de informação, sendo apenas necessário que este ponto centralizado desenvolva uma interface por cada sistema diferente e estes desenvolvam os mecanismos que permitam a comunicação com o ponto centralizado. Assim, o número de ligações a estabelecer entre n sistemas diferentes é n. Apesar de ser uma solução mais viável comparativamente à primeira apresentada, os custos de desenvolvimento e manutenção continuam a ser demasiado altos.

Portanto, é necessário encontrar uma solução que permita que os n sistemas diferentes possam comunicar com o ponto centralizado através de uma única interface. Para tal, é necessário adotar um padrão de partilha de informação. Assim, as instituições apenas necessitam de respeitar determinado padrão de troca de informação, de preferência definido por organizações especialistas da área.

O ALERT® *Health Information Exchange* (HIE) (ALERT Life Sciences Computing, 2018a) é o ponto centralizado desenvolvido pela ALERT com este propósito, e que permite a adoção de padrões de troca de informação clínica, tais como Health Level Seven International (Health Level Seven International [HL7], 2018a) e SNOMED International (SNOMED International, 2018a).

A evolução na área da informática acarreta riscos sobre fuga ou roubo de informação pessoal dos seus utilizadores, como também o uso indevido por parte das organizações que detêm a informação. No sentido de dar mais segurança e poder sobre os seus dados pessoais aos cidadãos europeus, foi criado em 27 de Abril de 2016 (aplicável a partir de 25 de Maio de 2018) o Regulamento Geral de a Proteção de Dados (RGPD), no qual todas as organizações/indivíduos dentro da União Europeia e fora que trabalhem com dados pessoais de cidadãos europeus que permitem a identificação direta ou indireta destes, têm de respeitar.

[1] Tradução Livre. No original "Modern healthcare depends on teamwork and communication. Improved interoperability can help transform the efficiency and effectiveness of health services, to provide information when required, facilitate quicker and more soundly based decision-making, reduce waste by cutting out repeated work, and improve safety due to fewer errors."

A informação de saúde dos pacientes é considerada informação sensível e o nível de sensibilidade irá depender de paciente para paciente. Este, para aceitar a partilha de informação entre instituições tem de estar confiante que a instituição de saúde irá garantir a confidencialidade e a integridade da sua informação pessoal e clínica, sendo que, para além disso, também deverá responsabilizar-se por qualquer violação na privacidade e segurança dos dados (Benson, 2012, pp. 72–73).

Segundo os princípios descritos no artigo 5° do RGPD (Parlamento Europeu e Conselho, 2016, pp. 35–36), para que um produto no mercado esteja em cumprimento com o RGPD, o tratamento realizado sobre os dados pessoais deve ser **lícito**, **leal** e **transparente** perante o cidadão europeu. Os dados pessoais, quando recolhidos, são para **finalidades determinadas**, **explícitas** e **legítimas**, sendo que estes devem ser **adequados**, **pertinentes**, **limitados** e **exatos** ao que é necessário. Além disso, deve ser garantida a **integridade** e **confidencialidade** dos dados pessoais durante o seu tratamento. Por fim, o responsável pelo tratamento é **responsável** por garantir o cumprimento dos princípios anteriormente mencionados, tendo que demonstrar esse cumprimento sempre que necessário.

1.2 Problema

Visto que o produto ALERT® HIE necessita de informação pessoal dos pacientes para processar transações, caso estas não estejam em conformidade com as atuais leis de privacidade e direitos dos cidadãos, pode trazer consequências legais e perda de credibilidade do produto. Como o RGPD é o atual regulamento europeu em vigor sobre os direitos de privacidade dos cidadãos, é do interesse da organização cumpri-lo de forma a respeitar as suas implicações, algo que, atualmente, não acontece por completo.

Após a análise extensa do RGPD, foram enumerados na Tabela 1 os requisitos do RGPD necessários para que o ALERT® HIE cumpra o RGPD. Apesar do produto já cumprir na totalidade alguns desses requisitos, (i) existem requisitos que ainda não são cumpridos na sua totalidade e (ii) existem ainda alguns requisitos que não são aplicáveis devido ao tipo de tratamento sobre que irá ser realizado.

Tabela 1 - Cumprimento do RGPD pelo ALERT® HIE

Requisitos	Cumprimento pelo ALERT® HIE
Consentimento	×
Acesso aos dados pessoais	✓
Retificar dados pessoais	✓
Apagamento dos dados pessoais	Não se aplica
Limitação do tratamento	✓
Notificação aos destinatários dos dados pessoais	✓/×
Portabilidade dos dados	✓
Oposição ao tratamento	Não se aplica
Oposição às decisões individuais automatizadas	×
Auditoria de eventos	✓/×
Cifragem	✓/×
Mecanismos de autenticação e autorização	✓
Disponibilidade	✓
Resiliência	✓

Na secção 3.1 são demonstradas as razões do estado definido para cada um dos requisitos identificados.

1.3 Objetivos

O objetivo deste projeto é resolver as limitações do ALERT® HIE no que diz respeito ao cumprimento do RGPD. Assim, e da análise da Tabela 1, identificam-se as seguintes adaptações necessárias ao ALERT® *Health I nformation Exchange* (HIE):

- Implementar funcionalidades relacionadas com o consentimento do paciente sobre a partilha da sua informação clínica;
- O paciente conseguir opor-se à decisão individual automatizada existente no produto;
- Desenvolver o processo de notificação aos destinatários a quem a informação dos pacientes foi comunicada;
- Atualizar o registo de auditoria, de modo a que o produto consiga demonstrar estar em conformidade com o RGPD;
- Atualizar os processos de cifragem, de modo a que garanta a confidencialidade da informação.

Na secção 3.1 são demonstradas as razões do estado definido para cada um dos requisitos identificados.

O cumprimento destes objetivos permitirá à ALERT garantir que o seu produto de interoperabilidade clínica respeita a informação pessoal e clínica dos seus pacientes segundo o RGPD.

1.4 Abordagem

Nesta secção é apresentada a abordagem que permitirá atingir os objetivos definidos:

- Interpretar o RGPD e identificar as necessidades que este implica;
- Investigar os conceitos sobre interoperabilidade clínica, HIE e privacidade dos dados;
- Estudar a solução existente e identificar os requisitos necessários para o cumprimento do RGPD;
- Apurar soluções que assistam na resolução dos problemas identificados;
- Análise de valor da adaptação para o cliente;
- Definição de novos conceitos de negócio, possíveis intervenientes e processos;
- Identificação dos requisitos para a resolução dos problemas identificados;
- Conceção de artefactos de desenho que possibilitem o debate e a resolução dos problemas identificados;
- Implementação dos requisitos funcionais identificados seguindo os artefactos de desenho;
- Desenvolvimento de casos de testes que permitam aferir que as funcionalidades desenvolvidas foram corretamente implementadas.

1.5 Motivações

Este projeto é motivado por diversos fatores, descritos nas secções seguintes.

1.5.1 Cultura organizacional ALERT

Em relação à cultura organizacional, a missão da ALERT é "melhorar a saúde e prolongar a vida, alcançar rentabilidade para benefício da sociedade e inspirar outros para a excelência através do nosso exemplo" (ALERT Life Sciences Computing, 2018b). Um dos valores da ALERT é o compromisso do desenvolvimento de *software* de qualidade e excelência, pois este lida com vidas humanas diariamente. A ALERT considera que a fórmula para o sucesso do seu *software* consiste na dupla verificação e inovação, como é demonstrado na Figura 1, deste modo serão minimizados os erros, promovendo o crescimento sustentado continuamente.

Figura 1 - Fórmula de sucesso da ALERT

1.5.2 Fatores de influência

Os fatores de influência fazem com que a organização tenha de se adaptar à medida que estes acontecem. No contexto deste projeto, os principais fatores de influência são:

- As capacidades organizacionais da ALERT;
- Os clientes dos produtos ALERT®;
- Organizações concorrentes;
- Fatores externos que influenciam a área de negócio da ALERT.

A ALERT, como uma organização que desenvolve *software* na área da saúde, necessita de estar sempre a par das novidades na área da saúde e da tecnologia. Como os seus produtos utilizam diversos padrões de nomenclatura e partilha da informação clínica, é necessário que a ALERT conheça o estado atual dos padrões que utiliza nos seus produtos, como também os possíveis padrões que possam estar a ser desenvolvidos de forma a que consiga responder a estas mudanças de negócio atempadamente. Deste modo, os produtos ALERT®, para terem valor no mercado, terão de estar sempre em conformidade com as mais recentes novidades.

O crescimento de uma organização, como a ALERT, está relacionado com o facto dos seus clientes reconhecerem o valor dos produtos ALERT® e utilizarem estes produtos para realizarem as suas tarefas do dia-a-dia, quer sejam em hospitais, clínicas privadas ou outras instituições de saúde. À data atual deste documento, os produtos ALERT® já se encontram em 12700 instituições espalhadas por 13 mercados globalmente (ALERT Life Sciences Computing, 2018c).

Existem cada vez mais soluções de *software* no mercado na área da saúde, o que implica uma competição entre os produtos ALERT® com os restantes concorrentes, quer a nível nacional como internacional. É importante que os produtos ALERT® consigam realizar todas as tarefas necessárias, no sentido de facilitar as atividades dos profissionais de saúde no dia-a-dia e ajudarem na saúde e bem-estar dos seus pacientes. Mas muitas vezes alguns dos clientes do *software* ALERT® já possuem produtos de outros concorrentes ou não têm os fundos ou a necessidade de investir em todos os produtos ALERT®, portanto é fundamental que os produtos ALERT® cumpram os padrões internacionais de forma a interligarem-se com os outros *softwares* concorrentes, como também que não estejam fortemente acoplados entre si.

Por fim, fatores de influência externos como a modificação da legislação em vigor sobre a saúde ou, no caso deste documento sobre a proteção de dados na União Europeia, num dos mercados em que a ALERT está inserida faz com que a ALERT tenha de estar atenta a estas possíveis alterações de modo a conseguir atempar-se às mudanças. A criação ou modificação de padrões

também poderá ter impacto nos produtos ALERT® e consequentemente afetar os clientes que utilizam estes produtos. Portanto, a ALERT fica com atenção máxima a estas possíveis influências externas, quer a nível nacional como internacional, de modo a conseguir responder efetivamente a estas.

1.6 Estrutura do documento

No primeiro capítulo é feita uma contextualização do tema do documento, são identificados os problemas necessários a resolver de modo a que o ALERT® HIE cumpra o RGPD, os objetivos que se esperam alcançar, a abordagem utilizada para alcançar esses objetivos e as motivações para a realização deste projeto.

No segundo capítulo é levantado o atual estado da arte sobre conceitos importantes relacionados com o tema que o documento aborda, tais como:

- EHR;
- Interoperabilidade clínica;
- Privacidade dos dados.

Além disso, também são apresentadas as possíveis soluções a adotar que possibilitam a resolução dos problemas impostos pelo RGPD.

No terceiro capítulo são detalhadas as especificações de cada um dos requisitos identificados durante a secção 1.2, que posteriormente serão categorizados como requisitos funcionais e não funcionais através de um diagrama de casos de uso e por intermédio do modelo FURPS+ respetivamente. Além disso, são demonstradas através da técnica QFD as relações entre os requisitos identificados e é feita a análise funcional dos requisitos de forma a priorizá-los.

No quarto capítulo é feita a análise de negócio, que consiste na identificação dos principais conceitos de negócio com que se lida, que são apresentados por meio de um diagrama de modelo domínio, como também são ilustrados os possíveis intervenientes e os processos de negócio relevantes. Neste capítulo, também é efetuada uma apresentação arquitetural e tecnológica do produto, como também é apresentado o algoritmo de correlacionamento de pacientes.

No quinto capítulo, é feita uma análise das alternativas concetuais de forma a adotar as melhores soluções para resolver os requisitos identificados. Após a escolha das soluções são apresentados os diversos artefactos de desenho que explicam as decisões tomadas para a resolução dos problemas identificados, influenciados diretamente pelas soluções adotadas. São apresentados desenhos arquiteturais de alto e baixo nível, diagramas de sequência de requisitos funcionais relevantes e modelo relacional.

No sexto capítulo são apresentados extratos de implementação significativos, boas práticas de implementação adotadas e as principais motivações de algumas decisões tomadas durante a implementação.

No sétimo capítulo são definidos os objetivos, abordagem e preparação da experimentação ao algoritmo de correlacionamento de pacientes, como também são apresentados os resultados obtidos e avaliação dos mesmos.

Por último, no oitavo capítulo é feito um resumo de todo o trabalho implementado, identifica-se dos os objetivos alcançados e os que não o foram e os motivos de não se ter conseguido alcançar todos os objetivos. São também apresentadas sugestões de trabalho futuro.

2 Estado da arte

Neste capítulo é analisado o estado da arte sobre (i) EHR (Electronic Health Record), (ii) interoperabilidade clínica e (iii) a privacidade dos dados. São apresentadas possíveis soluções para resolver o problema de consentimento e a cifragem dos ficheiros da base de dados.

2.1 EHR

Os registos clínicos eletrónicos (EHR – Eletronic Health Record), segundo Dey, Ashour, Fong e Borra (2018, p. 354), são o principal componente que permite a gestão das operações dos hospitais após a sua adoção. Estes contêm uma coleção de informação do paciente no formato digitalizado, permitindo a partilha e a comunicação eficaz da informação sobre o paciente entre os profissionais dentro da mesma instituição e de outras instituições, com o objetivo de melhorar o serviço de saúde prestado aos pacientes. Benson e Grieve (2016, p. 25) complementam que os EHR são uma coleção de observações realizadas por profissionais de saúde sobre um paciente em particular. Nestas observações são também registadas o contexto da observação, quem fez, quando e onde, de forma a garantir a validade das observações.

2.1.1 Estrutura hierárquica

A *International Organization for Standardization* (ISO) elaborou um padrão para a estrutura hierárquica dos EHR, com o objetivo de partilhar informação clínica entre entidades, sendo esta documentada na ISO 13606 como pode ser observado na Figura 2.

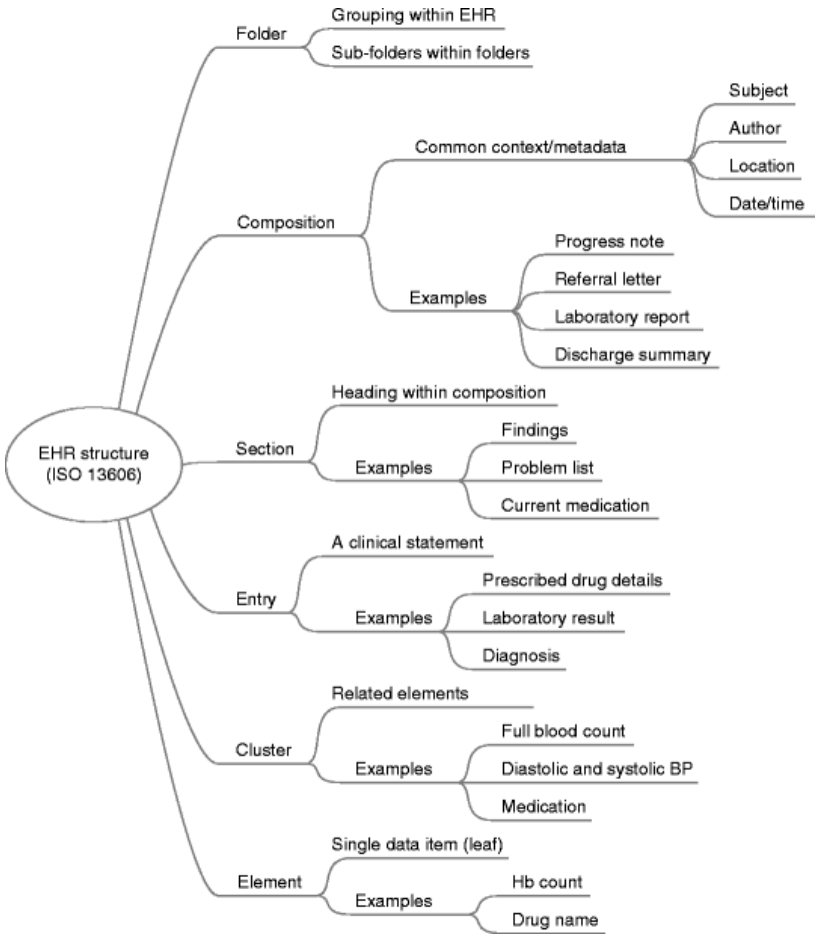


Figura 2 - Estrutura hierárquica do EHR ISO 13606 (Benson and Grieve, 2016, p. 26)

Como Benson e Grieve explicam (2016, p. 25), esta estrutura hierárquica está divida em diferentes categorias que estão interligadas entre si:

1. **Pasta** é o nível mais alto dentro da estrutura do EHR, esta permite a criação de uma estrutura de pastas e subpastas e agrupar composições dentro, possibilitando a divisão por episódio clínico, especialidade clínica, equipa de cuidados, período de tempo.

2. **Composição** é um conjunto de informação relacionado com uma consulta clínica, sessão ou documento, contendo sempre um conjunto de metadados desde o autor, paciente, data, hora e localização. Após a composição ser criada esta é imutável.

3. **Secção** é um grupo de declarações clínicas dentro de uma composição. Esta podem estar relacionadas com fatores de risco, diagnósticos, medicação, investigação.

4. **Declaração clínica** é a informação registada após uma observação, avaliação ou instrução. Exemplos de declarações clínicas são testes realizados ao paciente, sintomas problemas ou tratamentos.

5. **Grupo** é um conjunto de estrutura de dados, incluindo tabelas e gráficos. Elementos relacionados podem ser agrupados num grupo, como por exemplo a pressão arterial sistólica e diastólica.

6. **Elemento** é o nó folha dentro da estrutura do EHR, representando um valor único, e.g. pressão arterial sistólica, nome do medicamento, peso corporal.

2.1.2 Benefícios

Vários estudos demonstram que a adoção dos EHR por parte das instituições de saúde traz benefícios económicos às instituições como também as tornam mais eficazes e eficientes. Conforme um estudo realizado por Johnson, Pan e Walker (2004) a utilização de sistemas informáticos avançados na área da saúde poderá ajudar a poupar USD44.000.000.000 anualmente. Segundo uma estratégia de negócio para a adoção dos EHR na Irlanda, Carroll e Corbridge (2016) identificaram inúmeros benefícios da adoção dos EHR, sendo que alguns dos benefícios estão associados a mais que um resultado:

1. Melhorar a experiência do paciente;
2. Melhorar a segurança e cuidados do paciente;
3. Melhorar a eficiência do serviço de saúde.

2.1.2.1 Experiência do paciente

Na Figura 3 são apresentados benefícios na utilização de EHR segundo Carrol e Corbridge (Carrol and Corbridge, 2016).

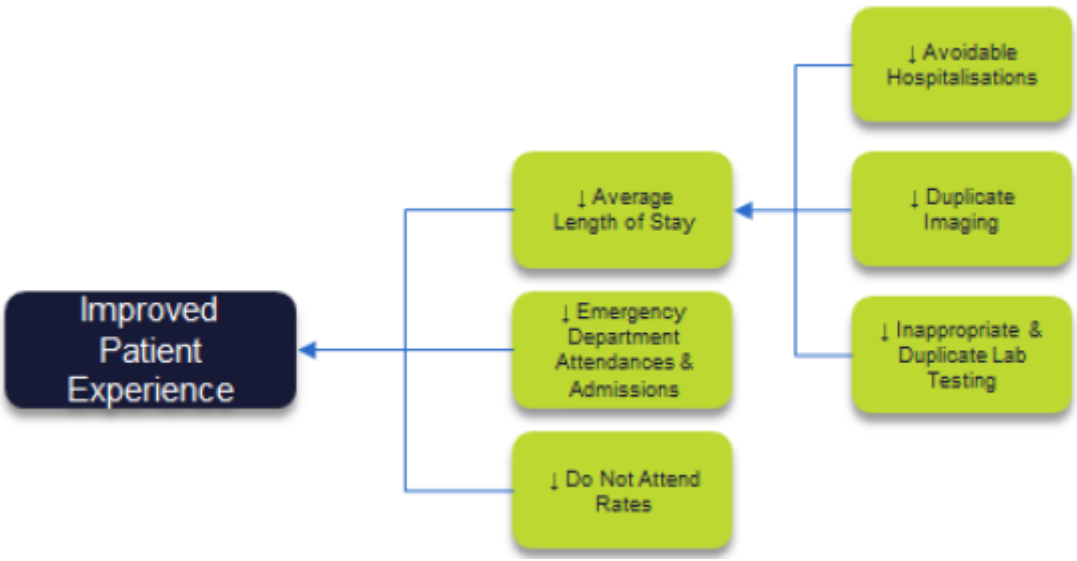


Figura 3 – Melhor Experiência do paciente (Carrol and Corbridge, 2016, p. 43)

Além destas o EHR tem outras funções que permitem melhorar a experiência do paciente, como por exemplo as prescrições eletrónicas. De acordo com uma análise feita a questionários sobre a utilização de prescrições eletrónicas nos EUA (Reddy and Aggarwal, 2015, p. 40), concluiu-se que:

- 92% dos pacientes estão felizes pelos seus médicos utilizarem as prescrições eletrónicas;

- 90% apontam que raramente ou ocasionalmente não têm as prescrições prontas quando vão à farmácia;
- 76% apontam que é mais fácil obter a medicação através da prescrição eletrónica;
- 63% reportam menos erros na medicação.

O EHR promove a educação e a participação dos pacientes na sua saúde, ao fornecer informação de acompanhamento, instruções de cuidados próprios, alertas para consultas de acompanhamento, explicações sobre as condições de saúde ao paciente através dos PHR[2], entre outros (Reddy and Aggarwal, 2015, p. 41).

Segurança e cuidados do paciente O EHR fornece informação sobre o paciente de uma forma precisa e estruturada, o que permite aos médicos identificar mais rapidamente e sistematicamente o problema correto a tratar. De acordo com Reddy e Aggarwal (2015, p. 40) os erros de medicação causam, em média, a morte de um paciente por dia e problemas de saúde a 1 milhão de cidadãos americanos anualmente. Os EHR permitem a integração com sistemas de suporte a decisões clínicas (CDSS – Clinical Decision Support Systems) permitindo assim prever e evitar a utilização de certos medicamentos devido a conflitos com outros medicamentos que o paciente possa estar a tomar, alergias que este tenha, ou mesmo a dosagem a utilizar do medicamento selecionado. Com isto, a segurança do paciente é melhorada e os cuidados de saúde são mais eficazes, como são apresentados na Figura 4.

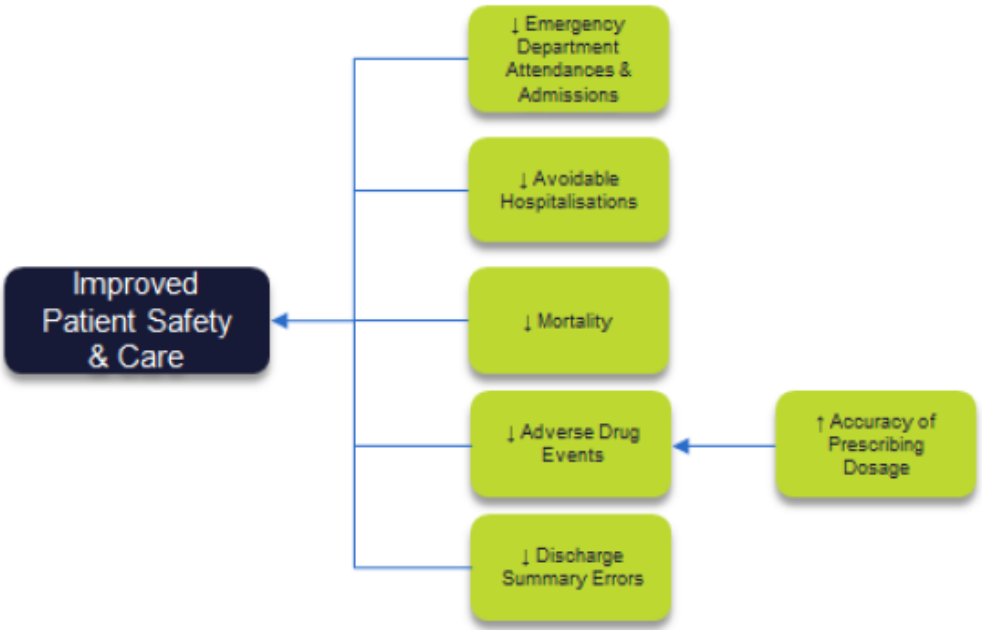


Figura 4 - Melhorar segurança e cuidados do paciente (Carrol and Corbridge, 2016, p. 44)

[2] Personal Health Record (PHR) é o registo clínico eletrónico geridos pelo paciente. Este, permite que o paciente tenha um papel ativo na sua saúde e consigam aceder aos resultados de um exame, prescrições, alergias e entre outros (Heart et al., 2017, p. 22).

2.1.2.2 Eficiência do serviço de saúde

A utilização de EHR permite diminuir diversos custos, como também tornar os processos de saúde mais eficientes. A redução mais drástica é na utilização de papel, tinteiros, canetas e tudo o resto que é necessário para gerir os registos em formato de papel. A informação, ao estar num formato digital, permite que os médicos tenham acesso à informação dos pacientes nos seus consultórios, sendo desnecessário o tempo desperdiçado ao armazenar, procurar e transportar os registos médicos do paciente. Ao armazenar exames digitalmente e partilhá-los com outras instituições, faz com que não seja necessário a duplicação dos mesmos, tornando os cuidados mais eficientes e diminuindo os custos da realização dos exames.

Segundo um questionário feitos a médicos dos EUA (Reddy and Aggarwal, 2015, p. 40) os resultados indicam que:

- 94% dos médicos indicam que o EHR faz com que os registos dos pacientes estejam sempre disponíveis;
- 88% reportam que o EHR produz benefícios na sua prática;
- 75% mencionam que o EHR permitiu fornecer ao paciente um melhor serviço médico.

Logo, a utilização de EHR faz com os cuidados de saúde sejam mais eficientes e permitam a diminuição de custos relacionados com o paciente, como também a gestão dos seus registos médicos, tal como a Figura 5 descreve.

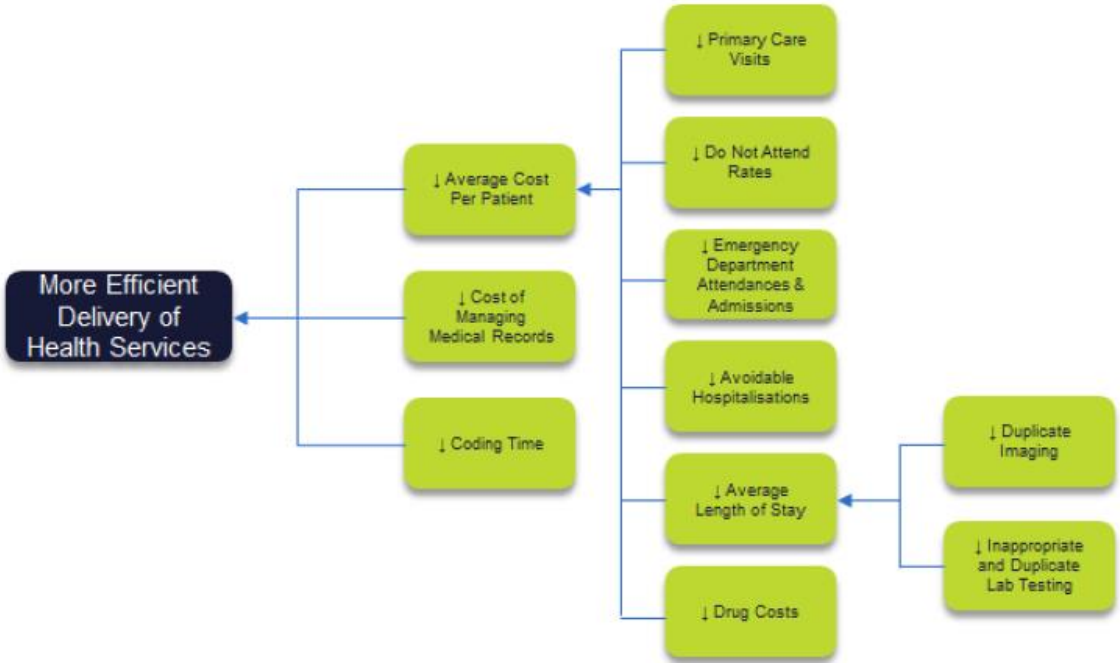


Figura 5 - Benefícios para melhorar a eficiência do serviço de saúde (Carrol and Corbridge, 2016, p. 45)

Portanto, a utilização de EHR permitem obter os benefícios acima mencionados, tornando os cuidados de saúde mais eficientes e eficazes, promovendo uma melhor gestão dos recursos.

2.2 Interoperabilidade clínica

Interoperabilidade segundo a organização IEEE (1990) consiste na "capacidade de dois ou mais sistemas ou componentes partilharem informação e utilizarem essa informação" [3]. Nas subsecções seguintes irão ser detalhados os tipos de interoperabilidade que existem a nível do negócio da saúde, as diferenças entre interoperabilidade e integração, serão enumerados alguns dos padrões clínicos mais reconhecidos globalmente, como também será apresentada a organização IHE que desenvolve perfis de integração para serem implementados em sistemas de interoperabilidade clínica.

2.2.1 Interoperabilidade

Benson e Grieve (2016, pp. 23–24) demonstram a explosão combinatória necessária para interligar diretamente n sistemas entre si através da equação:

$$Number\ of\ links = \frac{n(n-1)}{2}$$

Dado que para conectar 6 sistemas é necessário implementar 15 interfaces, para 100 sistemas é necessário implementar 4,950 interfaces devido ao facto de cada um destes ter as suas divergências dentro do seu modelo de negócio, como foi referenciado acima. Com este tipo de solução a interoperabilidade clínica seria muito dificilmente alcançável globalmente, logo a adesão a padrões por parte das organizações, independentemente do modelo de negócio, permitirá mais facilmente alcançar interoperabilidade entre sistemas. A Figura 6 demonstra os benefícios da adoção de padrões.

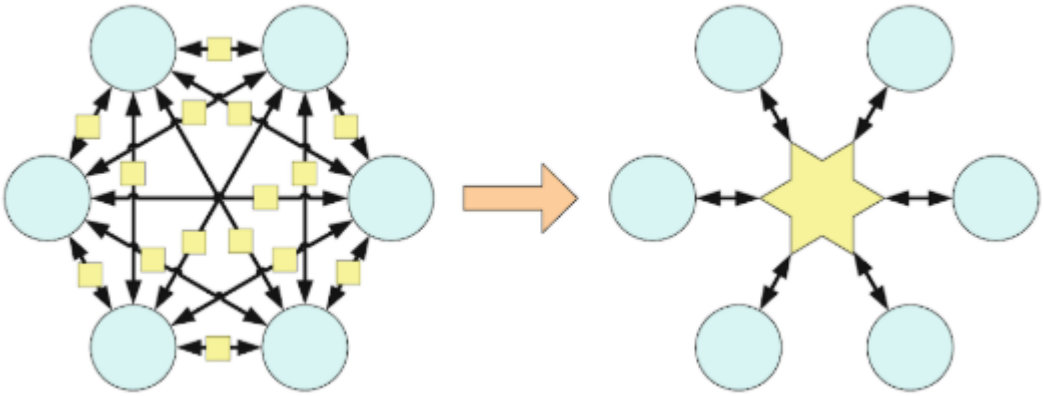


Figura 6- Benefícios na adoção de padrões (Benson and Grieve, 2016, p. 24)

A adesão por parte das organizações a padrões não significa que os seus sistemas se tornem interoperáveis imediatamente. Para tal é necessário que a implementação de cada padrão siga as especificações definidas como também que este seja reconhecido e implementado por outras organizações. Existem três características sobre padrões que influenciam diretamente a sua implementação por parte das organizações, como é enumerado em baixo:

[3] Tradução Livre. No original "ability of two or more systems or components to exchange information and to use the information's that has been exchanged"

1. **Disseminação** – descreve o quão utilizado é o padrão dentro da área de negócio. Quanto maior for a adoção por parte das organizações a um determinado padrão mais reconhecido este é, e certamente mais sistemas existirão com este tipo de padrão.

2. **Especificação** – relaciona-se com o âmbito do padrão. Quanto mais detalhada for a especificação de um padrão e este fornecer orientações sobre a sua implementação, maior será a adesão por parte das organizações.

3. **Compatibilidade** –consiste na compatibilidade deste com outras versões do mesmo padrão ou outros padrões. Quanto maior for a compatibilidade entre versões do mesmo padrão ou outros padrões, mais facilmente as organizações poderão interoperar (Stelzer et al., 2006, p. 16).

A Figura 7 mostra que quão mais fortes forem as características acimas mencionadas sobre um padrão e quanto maior for a adesão por partes das organizações a este padrão, mais flexível e reconhecido globalmente este se torna.

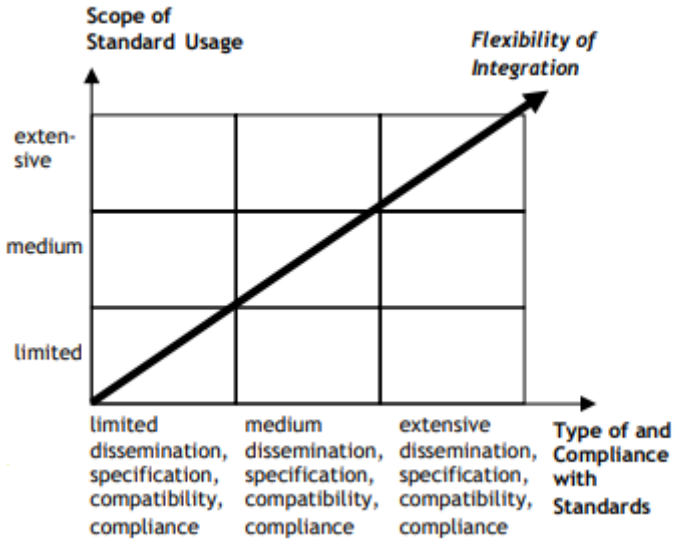


Figura 7 - Flexibilidade de integrações de padrões (Stelzer et al., 2006, p. 17)

Os padrões são aplicáveis a quatro camadas de interoperabilidade interligadas entre si:

1. Tecnológica
2. Informação
3. Humana
4. Institucional

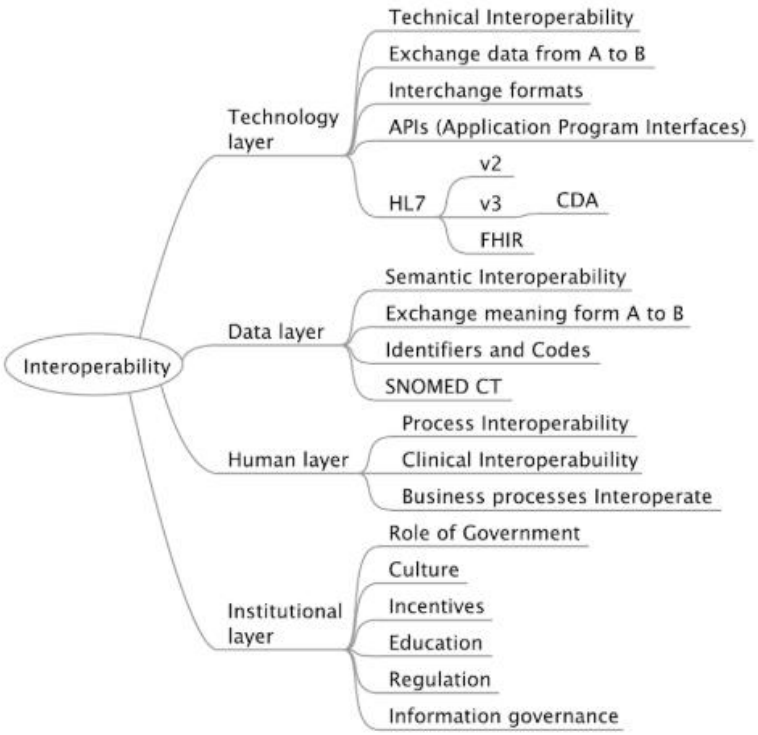


Figura 8 - Camadas de interoperabilidade (Benson and Grieve, 2016, p. 21)

Cada camada, como apresenta a Figura 8, engloba em si definições e os seus propósitos como também o tipo de interoperabilidade associado. Nas subsecções seguintes irão ser descritos os detalhes das camadas tecnológica, de informação e humana.

2.2.1.1 Interoperabilidade técnica

Benson e Grieve (2016, p. 20) consideram que interoperabilidade técnica consiste na troca de informação entre o sistema A e B, sendo que esta é independente da distância e do domínio dos sistemas. Para além disso não se interessa pelo significado da informação que está a ser partilhada.

A organização European eHealth Governance Initiave (eHGI) (2012, p. 1) considera que interoperabilidade técnica consiste na capacidade de duas ou mais aplicações partilharem informação entre si, conseguindo realizar uma tarefa de uma maneira apropriada e satisfatória, sem a necessidade de uma operação interveniente extra sobre a informação.

Segundo o Doutor Secundino Lopes (2016, p. 42) interoperabilidade técnica "… abrange as questões técnicas de ligação entre os sistemas, nomeadamente: interfaces, serviços de interligação, integração dos dados e serviços de segurança".

Com base nestes três significados apresentados sobre interoperabilidade técnica, pode-se considerar que esta consiste na partilha de informação entre dois ou mais sistemas diferentes, focando-se na parte técnica de como a informação é transmitida. Este tipo de interoperabilidade está dentro da camada tecnológica como é suportado pela Figura 8.

2.2.1.2 Interoperabilidade semântica

Como para interoperabilidade técnica, também existem diversas definições sobre interoperabilidade semântica. Para Benson e Grieve (2016, p. 21) interoperabilidade semântica significa que o remetente e o recetor interpretam a informação da mesma maneira e esta tem de ser inequívoca para não originar ambiguidades, permitindo assim que as diferentes aplicações consigam partilhar e utilizar essa informação.

Já a organização eHGI (2012, p. 1) considera que interoperabilidade semântica consiste na capacidade de garantir que a informação partilhada é inequivocamente entendida pelo recetor, quer este seja um sistema, serviço ou utilizador.

Interoperabilidade semântica, segundo o Doutor Secundino Lopes (2016, p. 42), está:

> "… relacionada com a necessidade de garantir que a informação trocada entre sistemas mantém o seu significado e é compreensível mesmo que utilizada por outra aplicação que não foi inicialmente desenvolvida para esta finalidade. Permite que os sistemas possam combinar os dados recebidos com outras fontes de informação."

Portanto é possível aferir que interoperabilidade semântica consiste na partilha de informação entre dois ou mais sistemas, em que estes consigam interpretar essa informação de forma a conseguirem utilizar esta nos seus processos internos. Este tipo de interoperabilidade insere-se dentro da camada de informação como suportado pela Figura 8.

2.2.1.3 Interoperabilidade de processos

O Doutor Secundino Lopes (2016, p. 41) cita que interoperabilidade de processos "… está relacionado com a ligação de processos internos de duas organizações de forma a criarem um processo comum". Já Benson e Grieve (2016, pp. 21–22) descrevem que interoperabilidade de processos traduz-se nos utilizadores de uma rede partilharem conhecimento entre si através das aplicações, trazendo valor para os utilizadores quando utilizam informação criada em diferentes aplicações.

Interoperabilidade clínica é um subconjunto da interoperabilidade de processos, sendo que esta é a possibilidade de dois ou mais profissionais clínicos em diferentes equipas de cuidados, trocarem informação sobre um paciente e prestarem o melhor tratamento possível (Benson and Grieve, 2016, p. 22).

Os processos de negócio de uma organização envolvem sempre utilizadores. A informatização destes processos tem o intuito de agilizar e facilitar os processos que anteriormente eram feitos manualmente. No final, a interoperabilidade de processos irá beneficiar os utilizadores do sistema, neste caso em estudo os profissionais de saúde, pois evitará duplicação, desperdício e erros. A interoperabilidade de processos e clínica inserem-se na camada humana como suportado pela Figura 8.

2.2.2 Diferenças entre interoperabilidade e integração

Interoperabilidade e integração de sistemas são dois conceitos que consistem na partilha/comunicação de informação entre sistemas. Apesar disso, estes têm as suas diferenças, como Kasunic e Anderson (2004, p. 15) explicam:

> "geralmente integração vai além da interoperabilidade envolvendo sempre um grau de dependência funcional entre sistemas. Enquanto que sistemas interoperáveis conseguem ser independentes, sistemas integrados perdem funcionalidades significativas se o fluxo de serviços for interrompido. Um conjunto de sistemas integrados devem ser necessariamente interoperáveis, mas sistemas interoperáveis não precisam de ser integrados."[4]

Integração de sistemas tem tanto efeitos positivos como negativos. Os efeitos positivos são o facto de ajudar na partilha de informação, agilizar os processos de negócio e também ajudar a unir componentes, mas a integração com componentes entre diversas organizações pode reduzir a flexibilidade e agilidade da organização, aumentando assim o seu acoplamento, sendo que quanto mais forte for o acoplamento entre sistemas de outras organizações menor será a probabilidade destes se alterarem. Esta situação é denominada por *Lock-in,* como Stelzer, Fischer e Nirsberger (2006, p. 1) mencionam.

Na Tabela 2 é apresentado um resumo das diferenças entre interoperabilidade e integração do ponto de vista técnico como também do ponto de vista organizacional.

Tabela 2 - Interoperabilidade versus Integração (Lopes, 2016, p. 44)

	Do ponto de vista técnico (sistemas, dados)	**Do ponto de vista organizacional**
Integração	**Fusão** de sistemas, serviços, ou produtos, num único sistema, serviço ou produto. Coordenação, coerência e unificação de sistemas	**Interdependência** entre organizações. **Integração** dos fluxos de informação.
Interoperabilidade	Interconexão entre sistemas. Coexistência, autonomia e federação de sistemas heterogéneos. Relacionada com os aspetos técnicos de comunicação, e partilha de serviços e dados entre	Desenvolvimento de capacidades e mecanismos de colaboração entre as organizações, grupos e pessoas. Relacionada com o alinhamento de processos de negócio, estruturas organizacionais, objetivos,

[4] Tradução livre. No Original "Integration is generally considered to go beyond mere interoperability to involve some degree of functional dependence. …While interoperable systems can function independently, an integrated system loses significant functionality if the flow of services is interrupted. An integrated family of systems must of necessity be interoperable, but interoperable systems need not be integrated.

	Do ponto de vista técnico (sistemas, dados)	Do ponto de vista organizacional
	as várias aplicações do sistema.	bases legais, culturas e métodos de trabalho.

2.2.3 Padrões clínicos

Interoperabilidade clínica consiste na troca de informação clínica do paciente entre diversas instituições independentemente da especialidade. Como existe mais que um sistema de saúde, e cada um tem o seu próprio modelo de negócio, uma solução para alcançar a interoperabilidade consiste na criação de um ponto centralizado que permita o envio da informação clínica do paciente e a pesquisa por esta quando necessário. Para alcançar isto é necessário a adoção de padrões por parte das organizações.

Nas subsecções seguintes serão apresentados alguns dos padrões globalmente reconhecidos por diversas organizações na área de interoperabilidade clínica.

2.2.3.1 HL7

Health Level Seven International (HL7) fundada em 1987, é uma organização com fins não lucrativos dedicada ao desenvolvimento de padrões, com o intuito de ajudar na troca, integração e partilha de informação eletrónicas de saúde que suporte a prática clínica e gestão. A sua visão é "um mundo no qual todos podem aceder e usar de forma segura a informação de saúde correta quando e onde precisam"[5] (HL7, 2018b).Desde a sua criação HL7 criou diversos padrões tais como:

1. HL7 *Version 2* (V2);
2. HL7 Version 3 (V3);
3. HL7 Clinical Document Achitecture (CDA®);
4. HL7 Fast Healthcare Interoperability Resources (FHIR®).

O HL7 V2 é um padrão de troca de mensagens, que suporta a maioria das interfaces de comunicação utilizadas na indústria de comunicação na saúde, reduz os custos de implementação e geralmente é compatível com as versões anteriores. Devido a estas características este padrão de comunicação é utilizado em 95% das instituições de saúde nos EUA e está implementado em 35 países (HL7, 2018c).

O HL7 V3 é um padrão de comunicação de informação através de conteúdos no formato XML. A HL7 criou este padrão para colmatar a flexibilidade do seu antigo padrão de comunicação, HL7 V2, sendo que este segue uma metodologia de comunicação baseada em modelos, produzindo as mensagens no formato XML (HL7, 2018d).

[5] Tradução Livre. No Original "*A world in which everyone can securely access and use the right health data when and where they need it".*

O HL7 CDA® tem por base as especificações do HL7 V3. Este define uma estrutura e semântica para a transmissão de documentos clínicos entre instituições e pacientes, sendo que a partilha dos documentos clínicos, tal como no HL7 V3, é feita no formato XML. O HL7 CDA® é adotado por HIEs globalmente, pois permite a interoperabilidade de documentos clínicos entre várias instituições (HL7, 2018e).

O HL7 FHIR® é o padrão de comunicação mais recente da organização HL7, baseando-se numa arquitetura RESTful. O FHIR® define inúmeros recursos (*Resources)* com o intuito de resolverem uma ampla variedade de problemas clínicos e administrativos. Para a transmissão de informação é possível utilizar o formato XML e JSON permitindo assim conectar-se a diferentes plataformas que estão a emergir no momento, e.g. aplicações móveis e cloud (HL7, 2018f).

Na Figura 9 é apresentada a linha do tempo da publicação das várias versões dos padrões acima referidos.

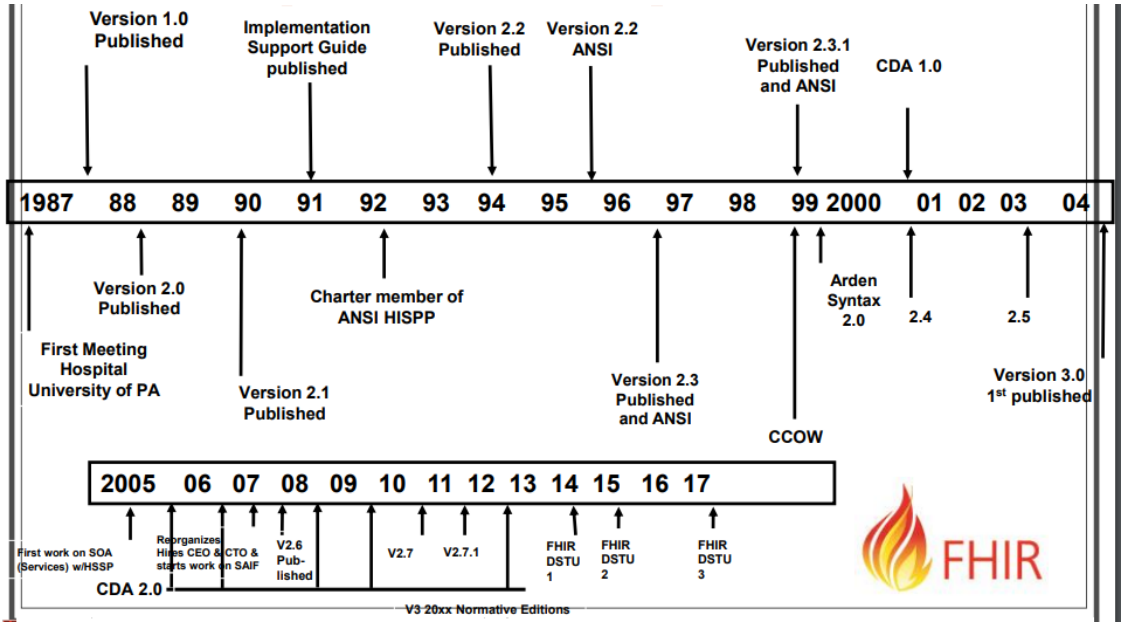


Figura 9 - Linha do tempo na publicação de padrões HL7 (Beebe, 2018, p. 38)

2.2.3.2 DICOM

Digital Imaging and Communications in Medicine DICOM® é um padrão internacional para a transmissão de informação sobre exames de imagem. Este padrão permite a transmissão entre os equipamentos que processam os exames de imagens e os sistemas de saúde clínica no formato DICOM, sendo assim um padrão adotado pelos fornecedores de equipamentos e as organizações que desenvolvem *software* (Digital Imaging and Communication in Medicine, 2018).

2.2.3.3 SNOMED International

Systematized Nomenclature of Medicine International (SNOMED International, 2018b) é uma organização sem fins lucrativos que detém, gere e desenvolve o padrão SNOMED CT. Este padrão tem como objetivo unificar a terminologia utilizada na partilha de informação de saúde através dos EHR. A SNOMED propõe que a:

"troca segura, precisa e efetiva de informação de saúde é fundamental para melhorar os cuidados de saúde globalmente. Neste sentido esforçam-se para determinar o melhor padrão global para terminologias na saúde, de forma a melhorar o SNOMEDCT e a segurança do paciente".[6]

2.2.3.4 ICD

International Classification of Dieases (ICD) é um padrão internacional, desenvolvido pela *World Health Organization* (WHO), para documentar um universo de doenças, distúrbios, lesões e outras condições relacionadas com saúde de forma a identificar as tendências e estatísticas relacionadas com saúde mundialmente. Para isso o padrão permite:

- Armazenar, pesquisar e analisar informação de saúde para ajudar os sistemas de apoio à decisão com base em evidências.
- Partilhar e comparar informações de saúde entre hospitais, regiões e países.
- Comparar informação entre diferentes períodos de tempo (World Health Organization, 2018).

2.2.4 IHE

Integrating the Healthcare Enterprise (IHE) é uma organização quem tem por objetivo melhorar a interoperabilidade clínica entre sistemas informáticos, promovendo a coordenação e integração de vários padrões como por exemplo a DICOM® e a HL7. A IHE reúne anualmente os utilizadores e desenvolvedores destes sistemas com os seguintes objetivos:

1. Definir novos casos de uso críticos para a partilha de informação;
2. Criar perfis de integração[7] com especificações detalhadas para resolver os casos de uso definidos, selecionando e otimizando padrões estabelecidos;
3. Promover a implementação das especificações detalhadas nos perfis de integração, por parte das organizações;
4. Testar os perfis de integração da IHE num evento cujo nome é Connectathon (IHE, 2018a).

[6] Tradução Livre. No original "The safe, accurate and effective exchange of health information is an essential foundation to improve healthcare around the world. We strive to determine the best global standards for health terminology and to engage with the global healthcare community to improve SNOMED CT and patient safety."

[7] Perfis de integração fornecem uma linguagem comum de forma a resolver as necessidades de integração entre softwares de saúde. Estes perfis oferecem aos desenvolvedores uma abordagem de implementação clara, com padrões de comunicação suportados pela indústria e cuidadosamente documentados, revistos e testados. Os perfis de integração são um ferramenta que permite reduzir, às organizações que implementam, a complexidade e custo de implementação de sistemas interoperáveis (IHE, 2019).

Dito isto, os perfis de integração existentes que possam incluir soluções para os problemas identificados deverão ser tidos em consideração, pois estas soluções serão implementadas por outras organizações promovendo assim a interoperabilidade entre produtos.

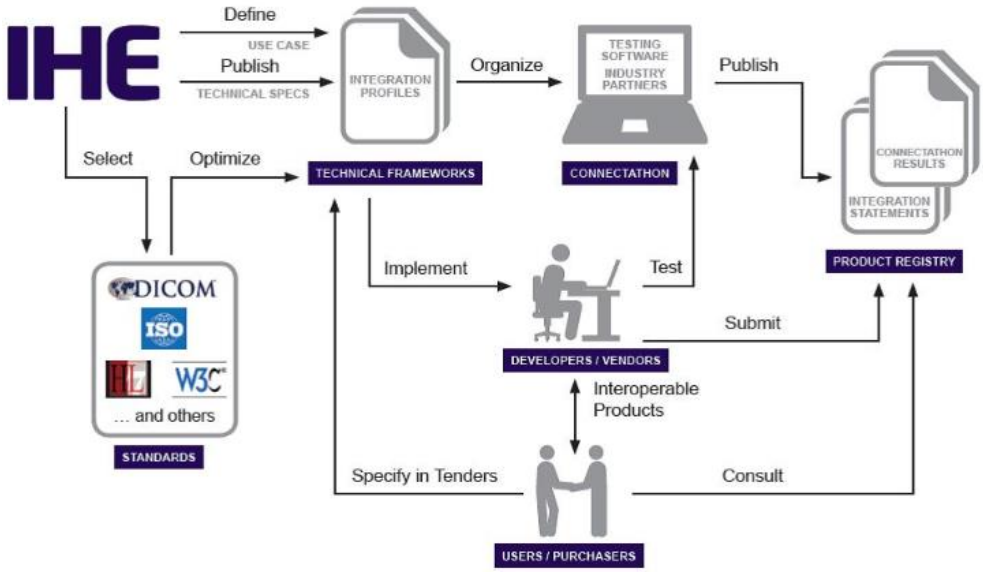


Figura 10 - Processo IHE (IHE, 2018a)

A Figura 10 representa o processo desde a conceção até à publicação final dos perfis de integração. Estes são definidos para ajudar a resolver problemas de interoperabilidade em vários domínios na saúde, desde: Cardiologia; Dentária; Oftalmologia; Infraestrutura Tecnológica de Informação; Patologia e Medicina Laboratorial; entre outros (IHE, 2018b). O produto de interoperabilidade clínica da ALERT encontra-se dentro do domínio de Infraestrutura Tecnológica de Informação.

Os perfis de integração poderão estar num dos cinco estados apresentados na Figura 11.

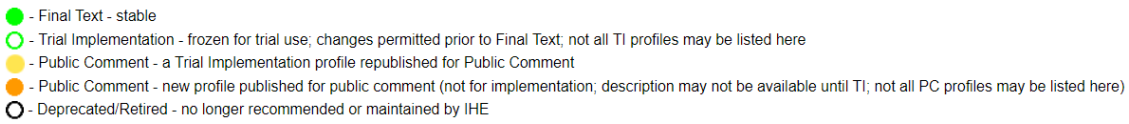


Figura 11 - Possíveis estados dos perfis de integração (IHE, 2018c)

2.3 Privacidade dos dados

O roubo, fuga ou divulgação de informação pessoal ocorre em muitos os setores de negócio (InfoWatch Analytics Center, 2017), sendo que a área da saúde apresenta um risco elevado devido à temática da partilha de informação clínica dos pacientes. Um estudo realizado por John Jiang da *Michigan State University* aponta para 1,800 ocorrências de fugas de informação de saúde no período de 2009 a 2016 nos EUA (Michigan State University, 2017). Outro estudo realizado pelo mesmo autor e Ge Bai identifica que 53% das fugas são devidas a causas internas, dos quais 25% são por falta de mecanismos de controlo de acesso ou divulgação, como se comprova na Figura 12 (Michigan State University, 2018).

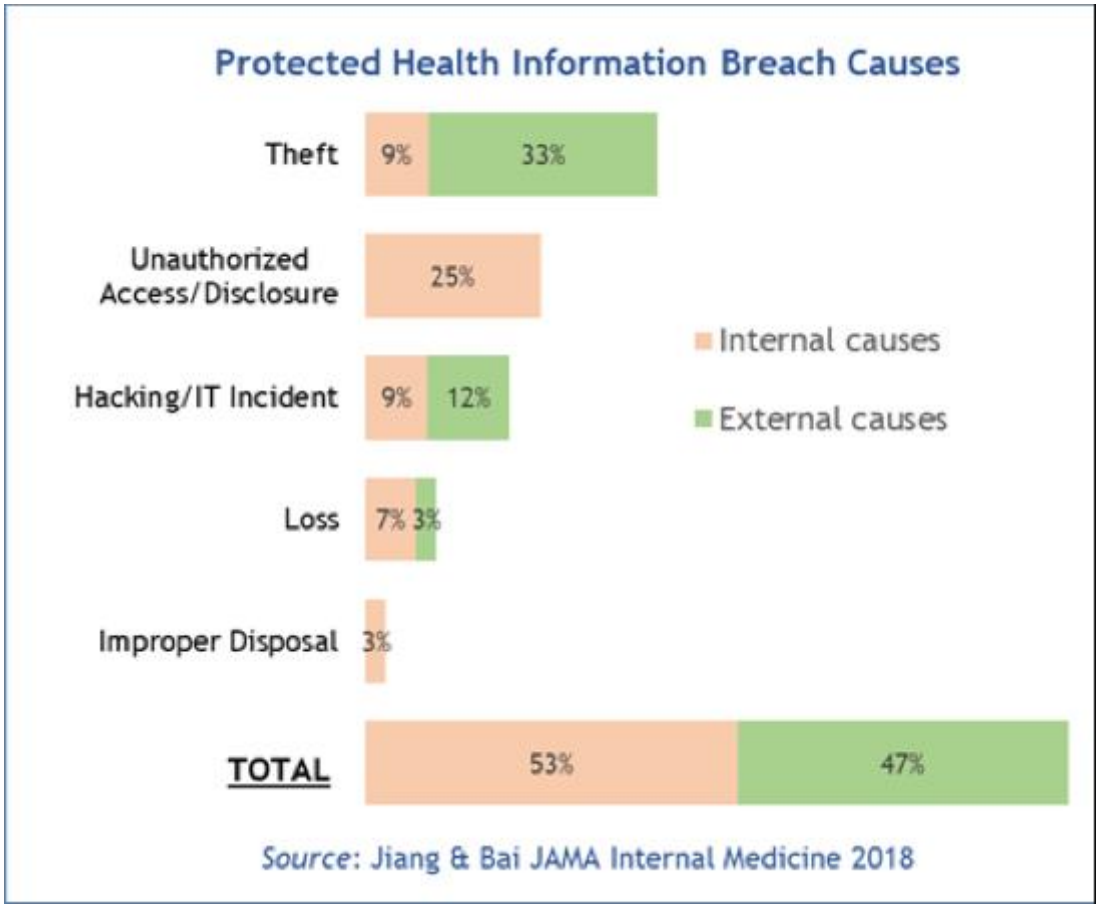


Figura 12 - Causas de fuga de informação nos EUA (Michigan State University, 2018)

Kenneth Bamberger e Deidre Mulligan (2011) afirmam que a:

> "A privacidade está para a era da informação como o ambiente estava para a era industrial. O uso indevido da informação é semelhante à má gestão dos recursos ambientais no início da era industrial. E todos iremos pagar este custo se não corrigirmos desde já…"[8]

O Regulamento Geral de Proteção de Dados veio colmatar as deficiências sobre a privacidade dos dados pessoais dos cidadãos europeus substituindo a diretiva 95/46/CE (Parlamento Europeu e Conselho, 1995), trazendo mais responsabilidades aos responsáveis pelo tratamento de dados pessoais. Na seguintes subsecções serão apresentadas as diferenças, dos principais temas relevantes para este documento, sobre a antiga diretiva e o novo Regulamento Geral de Proteção de Dados.

[8] Tradução Livre. No Original "privacy is to the information age what the environment was to the industrial age. You know, it's our big impact on our environment to misuse data in a way that environmental resources were misused earlier in the industrial age. And we'll be paying this cost if we don't get this right now…"

2.3.1 Dados pessoais

Dados pessoais são todos os dados que permitam a identificação direta ou indireta, em especial por referência a um identificador.

A diretiva 95/46/CE e o RGPD têm a mesma definição para dados pessoais, apenas tendo sido acrescentados mais alguns dados como é possível visualizar na Tabela 3.

Tabela 3 - Definição dados pessoais na Diretiva 95/46/CE e no RGPD

Dados Pessoais	Diretiva 95/46/CE	RGPD
Dados Identificáveis	• Nome • Número de identificação	• Nome • Número de identificação • Dados de localização • Identificadores por via eletrónica
Elementos específicos	Identidade: • Física • Fisiológica • Psíquica • Económica • Cultural ou social	Identidade: • Física • Fisiológica • Genética • Mental • Económica • Cultural ou social

2.3.2 Tratamento de dados pessoais

O tratamento de dados pessoais é qualquer operação realizada sobre os dados pessoais dos titulares, sejam estas operações efetuadas por meios automatizados ou não. A Tabela 4 apresenta o que é considerado tratamento de dados pessoais na diretiva 95/46/CE e no RGPD.

Tabela 4 - Tratamento de dados na diretiva 95/46/CE e no RGPD

Diretiva 95/46/CE	RGPD
• Recolha • Registo • Organização • Conservação • Adaptação ou alteração • Recuperação • Consulta • Utilização • Comunicação • Difusão • Bloqueio • Comparação ou interconexão • Apagamento ou destruição	• Recolha • Registo • Organização • Estruturação • Conservação • Adaptação ou alteração • Recuperação • Consulta • Utilização • Divulgação • Difusão • Comparação ou interconexão • Limitação • Apagamento ou destruição

2.3.3 Tratamento de categorias especiais de dados pessoais

Tanto a diretiva 95/46/CE como RGPD enumeram um grupo de categorias específicas que proíbem o seu tratamento, sendo que o RGPD e a diretiva 95/46/CE apresentam algumas exceções que permitem o seu tratamento. Estas exceções no RGPD são enumeradas no ponto 2 do artigo 9° e na diretiva no ponto 2 do artigo 8°. A Tabela 5 apresenta as categorias especiais adicionadas pelo RGPD em comparação com a diretiva.

Tabela 5 - Categorias especiais entre diretiva 95/46/CE e o RGPD

Diretiva 95/46/CE	**RGPD**
• Origem racial ou étnica • Opiniões políticas • Convicções religiosas • Filosóficas • Filiação Sindical • Saúde • Vida sexual	• Origem racial ou étnica • Opiniões políticas • Convicções religiosas • Filosóficas • Filiação Sindical • Saúde • Vida sexual • Orientação sexual • Dados genéticos • Dados biométricos

2.3.4 Consentimento

Os titulares dos dados pessoais necessitam de dar o seu consentimento para que estes dados possam ser utilizados para o tratamento em questão. O RGPD especifica mais um atributo complementar sobre a definição de consentimento em relação à Diretiva 95/46/CE como é apresentado na Tabela 6.

Tabela 6 - Diferenças sobre consentimento na Diretiva 95/46/CE e RGPD

Diretiva 95/46/CE	**RGPD**
• Livre • Específico • Informado	• Livre • Específico • Informado • Explícito

Ao contrário da Diretiva 95/46/CE, o RGPD (Parlamento Europeu e Conselho, 2016, p. 37) apresenta no artigo 7° as condições aplicáveis ao consentimento. Este artigo menciona que quando o tratamento dos dados pessoais, por parte do responsável pelo tratamento, for realizado com base no consentimento, este deve demonstrar que o titular dos dados o deu. O pedido de recolha do consentimento por parte de uma declaração escrita, que apresente também outros assuntos, deve ser feito de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Por fim, o responsável pelo tratamento dos dados deve garantir que o titular poderá retirar o consentimento a qualquer momento sem qualquer restrição, sendo este informado deste direito quando fornece o seu consentimento.

2.3.5 Princípios do tratamento de dados pessoais

Os responsáveis pelo tratamento de dados pessoais devem seguir os princípios relativos ao tratamento de dados pessoais enumerados pela lei atual em vigor sobre a proteção de dados. Na Diretiva 95/46/CE este princípio é apresentado no artigo 5°, já no RGPD é apresentado no artigo 6°.

Ambas as leis concordam que o tratamento dos dados pessoais deve ser feito de forma leal e lícita, mas o RGPD considera que é necessário haver transparência sobre o tratamento como também o responsável pelo tratamento deve garantir a integridade e confidencialidade dos dados.

2.3.6 Recolha de informação

A recolha de informação pessoal pode ser feita pessoalmente com o titular dos dados ou não, devendo o responsável pelo tratamento facultar a informação e os direitos que o titular deve conhecer, como é descrito nos artigos 10° e 11 da diretiva 95/46/CE e nos artigos 13° e 14° do RGPD. A Tabela 7 apresenta a informação que o titular dos dados tem direito a receber por parte do responsável pelo tratamento em cada uma das leis sobre a proteção de dados.

Tabela 7 - Informação a facultar na recolha de informação pelo titular na diretiva 95/46/CE e RGPD

Diretiva 95/46/CE	**RGPD**
• Identidade do responsável pelo tratamento e eventualmente o seu representante • Finalidades do tratamento • Destinatários ou categorias de destinatários • Existência do direito de acesso aos dados • Existência do direito de retificar os dados	• Identidade do responsável pelo tratamento e eventualmente o seu representante • Contactos do encarregado da proteção de dados • Finalidade do tratamento dos dados bem como fundamento jurídico para o tratamento • Destinatários ou categorias de destinatários • Prazo de conservação dos dados (ou critérios para determinar o prazo) • Retificar consentimento Apresentar reclamação a uma autoridade de controlo

O RGPD agora obriga o responsável pelo tratamento de informar o titular por quanto tempo este vai conservar os dados, como é mencionado na Tabela 7, mas caso não consiga informar por quanto tempo irá conservar a informação, o responsável deve mencionar quais os critérios que utiliza para determinar esse prazo.

A diferença entre a informação ser recolhida presencialmente ou não é apenas o tempo em que o responsável tem para informar o titular das informações apresentadas acima. Quando for recolhido presencialmente o responsável terá de informar o titular imediatamente. Caso seja feito remotamente, segundo o RGPD, o responsável terá o mais tardar um mês para comunicar

esta informação, exceto se a informação pessoal se destinar para fins de comunicação, caso em que deverá ser feita na primeira comunicação ou deverá comunicar esta informação na divulgação a um destinatário da informação.

2.3.7 Direitos dos titulares

Os titulares dos dados pessoais possuem direitos sobre os seus dados pessoais. Estes direitos na diretiva 95/46/CE são apresentados nos artigos 12°,14° e 15° já no RGPD são apresentados nos artigos 15°, 16°, 17°, 18°, 20°, 21° e 22°. O RGPD em comparação com a diretiva 95/46/CE, definiu melhor os direitos já existentes na diretiva. A Tabela 8 demonstra os direitos que as duas leis sobre a proteção de dados oferecem.

Tabela 8 - Direitos dos titulares dos dados pessoais na diretiva 95/46/CE e RGPD

Diretiva 95/46/CE	**RGPD**
• Aceder aos dados pessoais • Retificar os dados pessoais • Apagar os dados pessoais • Bloqueio • Receber notificação com informação de a quem os dados foram transmitidos Não ficar sujeito a nenhuma decisão com base no tratamento automatizado	• Aceder aos dados pessoais • Retificar os dados pessoais • Apagamento dos dados pessoais (“direito a ser esquecido”) • Opor ao tratamento • Não ficar sujeito a nenhuma decisão com base no tratamento automatizado • Limitar o tratamento Portabilidade dos dados

A limitação do tratamento e a portabilidade dos dados foram os dois novos direitos que os cidadãos europeus ganharam com o RGPD. O primeiro permite ao titular dos dados limitar o tratamento dos seus dados pessoais nas seguintes situações:

1. Os dados pessoais não estarem corretos;

2. O tratamento for ilícito e o titular dos dados propuser a limitação em vez da eliminação;

3. O responsável não precisar dos dados, mas o titular necessita para efeitos de declaração, exercício ou defesa de um direito num processo judicial (Parlamento Europeu e Conselho, 2016, p. 44);

O direito sobre a portabilidade dos dados permite aos cidadãos europeus obter todos os dados pessoais que lhes digam respeito fornecidos a um responsável, num formato estruturado, de uso corrente e de leitura automática, sendo que este pode transmitir esses dados a outro responsável sem que o primeiro o possa impedir se o tratamento for realizado por meios automatizados. Caso o titular dos dados queira exercer este direito, este poderá pedir que os dados sejam transmitidos diretamente entre os responsáveis sempre que exista esta compatibilidade de enviar e receber a informação.

2.4 Abordagens para o consentimento

O consentimento do paciente permite que o tratamento sobre a sua informação pessoal e clínica seja lícito, de acordo com o artigo 6° do RGPD (Parlamento Europeu e Conselho, 2016, pp. 36–37). Além disso, o consentimento deve ser manifestado pelo paciente de forma livre, específica, informada e explícita, consoante o artigo 4° nº11 do RGPD (Parlamento Europeu e Conselho, 2016, p. 34).

O produto ALERT® HIE de momento não tem qualquer funcionalidade relacionada com o consentimento do paciente, o que implica que este não possa realizar tratamento sobre informação pessoal de um cidadão europeu. Nas subsecções seguintes serão apresentadas possíveis soluções, de modo a que o tratamento efetuado sobre a informação pessoal do paciente seja transparente perante o mesmo, visto que é necessário segundo o artigo 12° do RGPD (Parlamento Europeu e Conselho, 2016, pp. 39–40), e este ao consentir torne o tratamento lícito.

Com a finalidade de avaliar cada uma das soluções, serão utilizados 4 diferentes critérios:

1. Compreensão e decisão das políticas de privacidade do consentimento, i.e. a capacidade de a solução permitir que a(s) política(s) de privacidade do consentimento estejam num formato legível para os pacientes e estes possam consentir às políticas de privacidade que desejarem;

2. Integração no produto, i.e. consiste na avaliação da eficácia e eficiência de implementação/integração da solução no produto como também a sua manutenibilidade, assim como a sua flexibilidade e adaptação à infraestrutura atualmente utilizada no produto;

3. Integração com o sistema de auditoria de eventos, i.e. consiste na avaliação da eficácia e eficiência de integração da solução adotada com o componente responsável por auditar as transações existentes no produto;

4. Conformidade com padrões de interoperabilidade, i.e. consiste na avaliação da conformidade da solução com padrões de interoperabilidade, promovendo assim a interoperabilidade do produto e do consentimento, caso seja necessário.

2.4.1 BPPC

O *Basic Patient Privacy Consents* (BPPC) é um perfil de integração da organização IHE, que permite ao domínio de afinidade do HIE definir um conjunto de políticas de privacidade necessárias para realizarem o tratamento sobre a informação do paciente. Cada política de privacidade é associada a um OID[9], que permite às instituições que têm acesso ao domínio de afinidade, identificar inequivocamente a política de privacidade (IHE, 2017).

[9] OID é um identificador único global criado por uma autoridade registadora, existindo diversas formas de representar OIDs. A HL7 na sua representação utiliza uma *string* numérica, e.g 2.16.840.1.113883. Independentemente da estrutura utilizada no OID, esta segue uma estrutura em árvore em que o elemento mais à esquerda representa a raiz e o mais à direita representa o nó folha (HL7, 2019).

Este perfil de integração integra dois atores. O criador de conteúdos é responsável por publicar os documentos de consentimento do paciente para o HIE. Já o consumidor de conteúdos deverá verificar a existência do(s) documento(s) de consentimento de modo a confirmar se é possível realizar o tratamento sobre a informação pessoal e clínica do paciente.

2.4.1.1 Compreensão e decisão sobre as políticas de privacidade do consentimento

O BPPC não determina as políticas de privacidade que devem existir, ficando isso ao critério do domínio de afinidade que implementa este perfil e consoante a situação de negócio. Portanto, o domínio de afinidade apenas tem de definir as políticas de privacidade num formato legível e associar um OID a cada uma dessas políticas (IHE ITI Technical Committee, 2018a, p. 195). Na Figura 13 é apresentado um exemplo de política de privacidade.

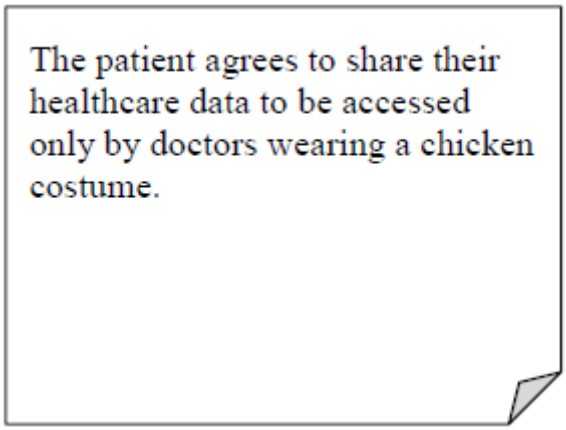


Figura 13 - Exemplo de política de privacidade (IHE ITI Technical Committee, 2018a, p. 195)

Após o domínio de afinidade definir as políticas de privacidade, estas serão apresentadas ao paciente, de modo a que este tenha conhecimento sobre as políticas de privacidades existentes, podendo consentir a todas ou a um conjunto destas. Assim o tratamento realizado será transparente perante o paciente, como foi mencionado ser necessário na secção 2.4.

O paciente, ao consentir a uma política de privacidade, desencadeia a criação de um documento do tipo "*Patient Privacy Policy Acknowledgment Document*" que irá conter o OID da política de privacidade e o ID do paciente. A criação e a publicação deste documento pelo criador de conteúdos no HIE, garante que o paciente deu o seu consentimento à política de privacidade selecionada. Assim, quando o consumidor de conteúdos necessitar de uma determinada política de privacidade para realizar tratamento sobre a informação do paciente, apenas precisa de encontrar o documento de consentimento dessa política de privacidade associado ao paciente, para validar que este deu o seu consentimento perante a política de privacidade em questão.

2.4.1.2 Integração no produto

Conforme foi mencionado anteriormente, a definição de políticas de privacidade é elaborada pelo domínio de afinidade, tendo o paciente apenas a possibilidade de aceitar ou rejeitar estas políticas. Isto retira flexibilidade de escolha ao paciente, pois, por exemplo, o paciente não consegue decidir com quais instituições pretende partilhar a sua informação dentro do domínio

de afinidade. Logo, o BPPC permite que o paciente escolha com quais políticas de privacidade deseja consentir, mas não tem opções sobre as preferências do paciente.

Este perfil de integração, segundo a informação disponibilizada pela IHE ITI Technical Committee (2018a, pp. 194–294), depende de um dos seguintes perfis de integração: XDS, XDR ou XDM da IHE.

O ALERT® HIE já implementa um conjunto de perfis de integração da IHE, sendo o XDS um destes perfis. Também implementa padrões de comunicação, nomenclatura e arquitetura de documento internacionalmente reconhecidos, sendo o HL7 CDA® um exemplo deste último tipo de padrão, que por sua vez é utilizado no documento de consentimento do BPPC. Logo, o produto já tem as condições necessárias para que este perfil de integração seja facilmente implementado.

Este perfil de integração da IHE não tem qualquer implicação sobre tecnologias necessárias para a sua implementação, referindo apenas que o documento de consentimento está no formato do padrão HL7 CDA®. Dito isto, a implementação deste perfil não terá qualquer impacto nas tecnologias atualmente utilizadas no produto, apresentadas na subsecção 4.3.2.

2.4.1.3 Integração com o sistema de auditoria de eventos

Como mencionado na subsecção 3.1.10, o responsável pelo tratamento é responsável por comprovar o cumprimento do RGPD, sendo necessário garantir que todo o tratamento realizado sobre informação dos pacientes é registada de modo a conseguir-se provar que o tratamento foi efetuado de forma lícita. O BPPC consegue integrar com o perfil de integração ATNA[10], já implementado no produto, cuja responsabilidade é auditar os eventos processados nos diversos perfis de integração que se integram com este.

2.4.1.4 Conformidade com padrões de interoperabilidade

Como foi dito anteriormente, esta solução utiliza o padrão arquitetural a nível de documento clínico o HL7 CDA®, pelo que a utilização desta solução será vantajosa para garantir a interoperabilidade de consentimentos pelas instituições que pertencem ao domínio de afinidade.

2.4.2 APPC

O *Advanced Patient Privacy Consent* (APPC) é um perfil de integração da organização IHE, que descreve a semântica necessária para guardar, gerir e comunicar o consentimento do paciente entre instituições e organizações de forma mais refinada, por comparação com o perfil de integração BPPC (cf. 2.4.1). Tal como o BPPC, os atores do sistema do APPC são o criador de conteúdo e o consumidor de conteúdo, como foi explicado na subsecção 2.4.1.

[10] O perfil de integração *Audit Trail and Node Authentication* (ATNA) da IHE permite auditar os fluxos das transações existentes num HIE, de forma a comprovar a sua conformidade com as leis de segurança e privacidade (Integrating the Healthcare Enterprise, 2018d).

2.4.2.1 Compreensão e decisão sobre as políticas de privacidade do consentimento

O BPPC permite ao paciente decidir sobre o consentimento a um conjunto de políticas de privacidade previamente definidas pelo domínio de afinidade do HIE. O APPC possibilita ter um número de políticas de privacidade personalizáveis, proporcionando ao paciente uma escolha mais fina, como por exemplo, poder decidir com quem e qual informação pretende partilhar.

Em consequência do documento de consentimento gerado estar no formato XACML, o documento não é legível pela maior parte dos humanos. Apesar disso, este documento deve conter um campo cujo nome é "*Description*", que contemplará a descrição do conteúdo do documento de consentimento, em texto simples, como é possível visualizar na Figura 14.

De acordo com a IHE ITI Technical Committee (2018b, p. 31), como o campo "*Description*" está limitado na capacidade de representação do conteúdo do consentimento, os criadores de conteúdo podem criar um documento separado que contenha a representação legível do documento de consentimento. Este documento pode ser do formato do documento de consentimento do BPPC, mais precisamente HL7®CDA, PDF, ou outro formato apropriado. O criador de conteúdo deve registar esta representação legível como um documento separado e adicionar uma associação de transformação (XFRM) sobre este documento ao documento de consentimento do perfil de integração do APPC.

Ao contrário do perfil BPPC, o APPC foi criado de forma a permitir uma escolha mais fina sobre com quem o paciente quer partilhar a sua informação. Segundo a IHE ITI Technical Committee (2018b, pp. 13–14):

> "este perfil permite dar escolhas aos pacientes mais fina, ao criarem regras de acesso que adicionam restrições por cima das políticas de privacidade previamente definidas. Um paciente pode não querer dar permissão de acesso a todos os médicos aos seus documentos clínicos, portanto pode limitar a política de privacidade para apenas se aplicar a uma organização específica."[11]

[11] Tradução Livre. No original "This profile allows Patient Privacy Policy Domain to give patients choices that are more granular by creating access rules that add constraints on top of the rules defined in an underlying Patient Privacy Policy. A patient may not want to give all physicians access to her clinical documents and may therefor limit the Patient Privacy Policies to only apply to a specific healthcare provider organization"

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet PolicySetId="urn:uuid:e3585197-9e3d-4ca3-9583-4540a3a5b64b"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-
overrides"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:hl7="urn:hl7-org:v3" xmlns="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xsi:schemaLocation="urn:oasis:names:tc:xacml:2.0:policy:schema:os    ihe-appc-xacml-combined-
schema-1.0.xsd">
  <Description>The patient agrees to grant access to the identified facility. The extent of access is
defined by the referenced policy. </Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
          <AttributeValue                                DataType="http://www.w3.org/2001/
XMLSchema#anyURI">urn:oid:2.999.2.1.1.35</AttributeValue>
          <SubjectAttributeDesignator                    DataType="http://www.w3.org/2001/
XMLSchema#anyURI" AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization-id" />
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch MatchId="urn:hl7-org:v3:function:II-equal">
          <AttributeValue DataType="urn:hl7-org:v3#II">
            <hl7:InstanceIdentifier root="2.999.1.1.1" extension="78901234"/>
          </AttributeValue>
          <ResourceAttributeDesignator                   DataType="urn:hl7-org:v3#II"
AttributeId="urn:ihe:iti:ser:2016:patient-id"/>
        </ResourceMatch>
      </Resource>
    </Resources>
  </Target>
  <PolicySetIdReference> urn:example:policy:extensive-access</PolicySetIdReference>
</PolicySet>
```

Figura 14 - Documento de Consentimento APPC (IHE ITI Technical Committee, 2018b, pp. 32–33)

2.4.2.2 Integração no produto

Esta solução é muito mais flexível do que o perfil BPPC, pois o paciente poderá personalizar o seu consentimento, dependendo das políticas de privacidade que o domínio de afinidade permitir que sejam personalizáveis. Possíveis personalizações que este perfil abrange são as restrições de privacidade por episódio clínico, por instituição de saúde e período de validade do documento de consentimento (IHE ITI Technical Committee, 2018b, p. 14).

O APPC, conforme a informação disponibilizada pela IHE ITI Technical Commitee (2018b, pp. 25–26), depende de outros perfis de integração, tais como: XDS, XDR e XDM. O ALERT® HIE já implementa um conjunto de perfis de integração da IHE, sendo o XDS um destes perfis. O facto do ALERT® HIE não utilizar de momento o formato XACML, dificulta a sua implementação numa primeira fase. Portanto, é possível concluir que o produto já tem algumas das condições necessárias para a implementação deste perfil, mas esta não deverá ser tão fácil quanto a do perfil BPPC, devido ao tipo de formato utilizado no documento de consentimento do paciente, bem como a possível personalização das políticas de privacidade por parte dos pacientes. Esta flexibilidade deverá certamente requerer mais esforço na sua implementação e manutenção.

Quanto à adaptação do APPC à infraestrutura existente, não existe qualquer implicação sobre tecnologias necessárias para a implementação deste perfil. Dito isto, a implementação deste perfil não terá qualquer impacto nas tecnologias e infraestrutura atualmente utilizadas no ALERT ® HIE.

2.4.2.3 Integração com sistema de auditoria de eventos

O APPC, como o BPPC, também permite integração com perfil ATNA da IHE, sendo possível, deste modo, manter só um componente responsável por auditar os eventos que processem informação pessoal e clínica do paciente(IHE ITI Technical Committee, 2018b, p. 25).

2.4.2.4 Conformidade com padrões de interoperabilidade

O APPC, como foi mencionado anteriormente, utiliza o formato XACML para representar as regras impostas pelo paciente nas políticas de privacidade personalizáveis. O XACML é um padrão da organização OASIS (2003), que descreve uma linguagem de política como também uma linguagem para decisões de controlo de acesso, sendo que estas linguagens são ambas representadas em XML.

2.4.3 Consent2Share

O *Consent2Share* é um produto de *software* de código aberto, da organização FEI Systems (2018a), que permite aos pacientes determinar, através de um processo de consentimento *online*, que informação clínica estes querem partilhar e com quais instituições de saúde. Esta solução permite que o paciente faça a gestão dos seus consentimentos, permitindo a sua criação, edição e eliminação. O paciente poderá criar mais que um consentimento dependendo da informação clínica que quer partilhar com as diversas instituições.

Esta solução adota uma arquitetura baseada em micro serviços, tornando a solução altamente escalável e resiliente (FEI Systems, 2018b).

2.4.3.1 Compreensão e decisão sobre as políticas de privacidade do consentimento

O Consent2Share tem um portal que permite aos pacientes inscritos acederam ao seu perfil, que por sua vez dispõe de diversas funcionalidades. Uma das funcionalidades é a criação de consentimentos eletronicamente, de modo a autorizar a partilha de informação entre várias instituições de saúde. Durante a criação do consentimento, o paciente decide quais os intervenientes que podem partilhar a sua informação e com quem, que tipo de informação clínica podem partilhar, qual o propósito da partilha e durante quanto tempo o consentimento é válido. Os consentimentos também poderão ser criados pelas instituições de saúde, mas é necessário que o paciente aceda com as suas credenciais no portal do paciente e aceite o consentimento (FEI Systems, 2017a, pp. 30–52).

A criação do consentimento de partilha de informação é apresentada numa interface gráfica de fácil utilização e legível por qualquer utilizador. Na atual versão, o produto suporta a língua inglesa e espanhola. Contudo, sendo o Consent2Share um produto de código aberto, deverá ser possível implementar qualquer outra linguagem para a tradução dos conteúdos, de modo a que seja legível por todos os possíveis utilizadores (FEI Systems, 2017b).

2.4.3.2 Integração no produto

Os mecanismos de autenticação e autorização no produto ALERT® HIE, como mencionado na subsecção 3.1.11, são ao nível da instituição. O Consent2Share, para além de possibilitar a criação de consentimentos apenas selecionando as instituições que fazem parte destes mecanismos, também permite que seja feito a nível de utilizador, sendo para isso necessário que o ALERT® HIE evoluísse o seu mecanismo de autenticação e autorização para o nível do utilizador.

Segundo a informação do *website* oficial do Consent2Share, este produto consegue integrar-se com sistemas já existentes do tipo EHR ou HIE, através do padrão de comunicação HL7 FHIR®. De qualquer modo, o tipo de consentimento que este abrange não é, de todo, o mais interessante para solucionar o problema existente, pois o consentimento desta solução apenas abrange o consentimento do paciente sobre a partilha de informação entre instituições, mas o RGPD implica que o consentimento do paciente também compreenda outras categorias de tratamento de dados pessoais, tais como as mencionadas na subsecção 3.1.1.

Na subseção 4.3.2 são mencionadas as tecnologias atualmente utilizadas no produto ALERT® HIE. O Consent2Share tem uma grande variedade de tecnologias, desde o uso de Angular JS, Node.JS, HTML5, CSS3, Java, MySQL, Docker, entre outros (FEI Systems, 2018b). Esta grande variedade de tecnologia e sendo uma solução baseada em micro serviços poderão ter um impacto significativo nos custos de monitorização. Já a sua instalação não deverá ter grande impacto nos custos associados, devido ao facto de ser possível utilizar as imagens[12] de cada micro serviço e por meio destas criar contentores[13] que irão executar os micro serviços, disponibilizado pela tecnologia Docker.

2.4.3.3 Integração com o sistema de auditoria de eventos

Segundo a documentação arquitetural do Consent2Share (FEI Systems, 2018c), este produto contém um componente responsável por auditar os eventos sobre o consentimento. A adoção desta solução implicaria que o produto ALERT® HIE tivesse dois componentes diferentes para monitorizar os acessos e tratamento efetuado em cada uma das aplicações, o que implicaria um separação da responsabilidade de auditoria de eventos do produto. Porém, existe a possibilidade de integrar o Consent2Share com o sistema de auditoria do ALERT® HIE, mas isto também traria impactos negativos devido ao facto de a codificação das mensagens ser definida nos perfis de integração da IHE, de modo a obter a interoperabilidade das mensagens caso seja necessário.

2.4.3.4 Conformidade com padrões de interoperabilidade

De acordo com a documentação do repositório do Consent2Share (FEI Systems, 2018b), o documento de consentimento do paciente, com as suas decisões de partilha de informação, serão transformadas num documento no formato XACML, que conterá as regras de acesso definidas pelo paciente.

[12] Imagens em Docker são representadas por ficheiros do tipo Dockerfile que permitem armazenar todas as dependências necessárias para a execução de uma aplicação (Docker, 2017).
[13] Contentores em Docker são instâncias executáveis de uma imagem que utilizam o kernel do sistema operativo onde são executados, de modo a obter melhor eficiência e reduzindo os custos (Docker, 2018).

2.4.4 Avaliação das soluções

Na Tabela 9 é apresentada uma classificação entre os diferentes critérios definidos e as soluções analisadas. As classificações variam entre os valores de 1 a 4 consoante os objetivos que serão pretendidos que a solução atinja, em que 1 representa uma fraca relação entre os objetivos da solução e o critério, 2 representa uma relação intermédia, 3 representa uma relação forte e 4 representa uma relação muito forte.

Tabela 9 - Avaliação geral das soluções apresentadas para o consentimento

Critérios	BPPC	APPC	Consent2Share
Compreensão e decisão sobre as políticas de privacidade do consentimento	4	3	2
Integração no produto	2	3	1
Integração com o sistema de auditoria de eventos	4	4	2
Conformidade com padrões de interoperabilidade	4	4	2

Nas subsecções seguintes serão justificados os motivos das classificações atribuídas a cada solução em cada um dos critérios definidos.

2.4.4.1 Compreensão e decisão sobre as políticas de privacidade do consentimento

Considerando o primeiro critério de avaliação, precisamente o de "Compreensão e decisão sobre as políticas de privacidade do consentimento", o BPPC é a melhor solução que cumpre este critério pois permite a definição de políticas de privacidade de forma legível e o paciente pode consentir apenas às políticas de privacidade que desejar.

O APPC apresenta uma relação forte, visto ter uma forma de associar um documento legível ao documento de consentimento e permitir a personalização das políticas de privacidade pelo paciente. No entanto, não existe informação referente ao formato utilizado para apresentação das políticas de privacidade, o que é um fator a ter conta pois é necessário que o paciente consiga entender as políticas de privacidade.

O Consent2Share apresenta uma relação intermédia com este critério, devido ao facto de o consentimento que este abrange apenas estar relacionado com a partilha de informação entre instituições de saúde, no entanto, é necessário que a solução adotada abranja diversas categorias de tratamento, como é mencionado na subsecção 3.1.1. Apesar de esta solução satisfazer a compreensão do paciente e a sua decisão com quem este quer partilhar a sua informação, não abrange os outros os critérios necessários.

2.4.4.2 Integração no produto

Consoante o segundo critério, mais propriamente o de "Integração no produto", o BPPC apresenta uma relação intermédia, pois apesar de o produto estar preparado para se integrar facilmente com este perfil de integração e este não afetar as tecnologias utilizadas nem a infraestrutura, o BPPC peca na sua flexibilidade e evolução da solução futuramente, visto que as políticas de privacidade definidas pelo domínio de afinidade são estáticas, apenas permitindo que o paciente possa consentir ou não a estas.

O APPC apresenta uma relação forte devido à sua flexibilidade, personalização das políticas de privacidade por parte dos pacientes e possível evolução que esta solução permite. Não afeta as tecnologias e infraestrutura utilizadas atualmente no produto. Como já foi mencionado anteriormente, o ALERT® HIE já implementa alguns dos perfis de integração que o APPC depende, facilitando assim a sua implementação. O facto do ALERT® HIE não utilizar de momento a semântica do XACML, dificulta a sua implementação numa primeira fase, mas o maior custo deverá estar associado aos custos de manutenção da solução devido à possível personalização das políticas de privacidade.

Quanto ao Consent2Share, este apresenta uma fraca relação neste critério devido ao facto de o consentimento não abranger todas as categorias de tratamento necessárias para resolver o problema de consentimento existente no ALERT® HIE, como foram mencionadas na subsecção 3.1.1, faz com que os custos de implementação e manutenção para resolver este problema não sejam os mais apreciados.

2.4.4.3 Integração com o sistema de auditoria de eventos

Quanto ao terceiro critério, mais concretamente o de "Integração com o sistema de auditoria de eventos", o BPPC e o APPC apresentam uma relação muito forte com este critério em virtude de serem perfis de integração da organização IHE, facilmente integram-se com o perfil de integração ATNA, onde este último tem como responsabilidade estabelecer medidas de segurança de modo a garantir a confidencialidade, a integridade da informação e a responsabilidade do utilizador/instituição (IHE, 2018d), critérios importantes para o cumprimento do RGPD mencionados na secção 1.1.

Já a solução Consent2Share apresenta uma relação intermédia, pois apresenta já um componente responsável por auditar os eventos associados ao consentimento da solução. Contudo o mais interessante seria que a solução conseguisse ser integrada com o sistema de auditoria atual, de modo a ter só um componente responsável pela auditoria. Porém, existe a possibilidade de integrar o Consent2Share com o sistema de auditoria do ALERT® HIE, mas também não é de todo uma solução positiva pelas razões apresentadas na subsecção 2.4.3.3.

2.4.4.4 Conformidade com padrões de interoperabilidade

Por último, relativamente ao quarto critério "Conformidade com padrões de interoperabilidade", tanto o BPPC como o APPC apresentam uma relação muito forte, devido a serem perfis de integração da IHE e utilizarem formatos interoperáveis para registarem o seu consentimento. Portanto ao partilhar os documentos de consentimento e as políticas de privacidade com outros HIE que implementem um destes perfis, deverá ser possível estes entenderem o conteúdo e aplicarem as regras impostas pelo paciente.

Quanto ao Consent2Share, apesar de utilizar o formato XACML para representar as regras de consentimento definidas pelo paciente, não é garantido que ao partilhar este tipo de documento com outros HIE, estes consigam entender e respeitar as regras definidas dentro do documento de consentimento.

2.5 Abordagens para cifragem da base de dados

Segundo o artigo 32° do RGPD (Parlamento Europeu e Conselho, 2016, p. 51), os responsáveis pelo tratamento devem aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança ao risco. Conforme é referido na subsecção 3.1.11, os ficheiros de base de dados do ALERT® HIE apenas estão protegidos pelo formato proprietário da Oracle. Contudo, não chega para garantir a segurança da informação dos pacientes em caso de furto digital ou físico dos ficheiros da base de dados.

Nesta secção serão apresentadas possíveis soluções que que permitem garantir a segurança necessária para o cumprimento do RGPD, sem que comprometa a lógica de negócio existente na base de dados. Além disso, é necessário ter em conta a compatibilidade com outras opções existentes que o produto pode já utilizar na base de dados (e.g. Oracle RAC[14]), dependendo dos requisitos do cliente na instalação do produto.

2.5.1 Tipos de cifragem

Dentro da camada de base de dados existem dois tipos de cifragem possível (Mogull and Lane, 2019, pp. 6–7):

- Cifragem transparente, consiste na cifragem dos conteúdos da base de dados como um todo. Este processo é transparente para os utilizadores e aplicações que utilizam a base de dados, como também não afeta a lógica de negócio existente dentro das aplicações e da base de dados. Este tipo de cifragem é maioritariamente utilizado quando se pretende prevenir a divulgação de informação sensível através de ameaças externas. Existem duas alternativas para este tipo de cifragem:
    - Uso de funcionalidades nativas dentro do motor da base de dados;
    - Uso de soluções terceiras que cifram a informação a nível do sistema de ficheiros do SO em que a base de dados está a ser executada.

  A desvantagem deste tipo de cifragem é que apenas protege a informação de ameaças externas, pois os utilizadores que tenham credenciais de acesso à base de dados poderão consultar a informação como se esta não estivesse cifrada.

- Cifragem por utilizador/informação, o consiste na cifragem da informação mais sensível dentro de uma coluna ou tabela da base de dados. O objetivo desta cifragem é proteger

[14] Oracle Real Application Clusters (RAC) é uma opção do produto de base de dados da Oracle que permite obter alta disponibilidade desta, através da ligação de vários servidores entre si aumentando o poder computacional, mas os utilizadores finais e aplicações continuam a ver a base de dados como um só (Oracle, 2019d).

a divulgação de informação sensível, como também separar a responsabilidades dos utilizadores que têm credenciais de acesso à base de dados. A desvantagem deste tipo de cifragem é a possível necessidade de realizar alterações de lógica dentro das aplicações e base de dados. Portanto, neste tipo de cifragem apenas se cifra o conteúdo mais sensível, de forma a minimizar as alterações necessárias a realizar e o impacto no desempenho da base de dados.

Com o intuito de resolver o problema acima mencionado, nas subsecções seguintes serão apresentadas soluções que utilizam o tipo de cifragem transparente, pois este tipo de cifragem não tem impacto sobre a lógica de negócio existente na base de dados, que é um dos objetivos devido ao algoritmo de correlacionamento de pacientes existente neste.

2.5.2 Oracle TDE

O Oracle *Transparent Data Encryption* (TDE) é uma solução da organização Oracle (2016a) que permite cifrar a informação sensível armazenada nas colunas das tabelas da base de dados ou nos *tablespace*[15]. Esta solução permite que a informação fique decifrada de forma transparente para os utilizadores e aplicações que tenham acesso à base dados. O TDE garante que a informação fica ilegível, de modo que não a informação não é utilizável nos casos em que os ficheiros de base de dados são furtados digitalmente ou fisicamente.

O TDE possibilita a cifragem por coluna das tabelas da base de dados ou pelo *tablespace*, como foi mencionado acima, mas as alternativas arquiteturais utilizadas são semelhante. O TDE utiliza uma arquitetura em duas camadas de chaves de cifragem, em que cada *tablespace*/coluna utiliza uma chave para cifrar e decifrar o seu conteúdo e depois esta chave é cifrada pela chave mestre que pode ser armazenada dentro da *Oracle* Wallet[16] ou num HSM[17] (Oracle, 2016a). Na Figura 15 é demonstrado a arquitetura do TDE aplicado à cifragem por *tablespace*.

[15] O *tablespace* é um contentor lógico de armazenamento que pode estar associado a um ou mais ficheiros físicos, em que se pode associar a quota de espaço em memória que este pode utilizar, realizar *backups* da informação e importar ou exportar o *tablespace* para outras instâncias da base de dados (Oracle, 2015b).

[16] *Oracle* Wallet é um contentor cifrado apenas acedido através de uma palavra-passe, este permite armazenar credenciais de autenticação, chaves mestre do TDE e certificados (Oracle, 2019e).

[17] *Hardware Security Module* (HSM) é um módulo responsável por operações de criptografia, desde gestão de chaves, partilha de chaves, cifragem, entre outros… É construído sobre *hardware* especializado tendo um SO focado em segurança, a interface de acesso através de uma rede é limitada, esconde e protege ativamente material criptográfico (Smirnoff, 2017).

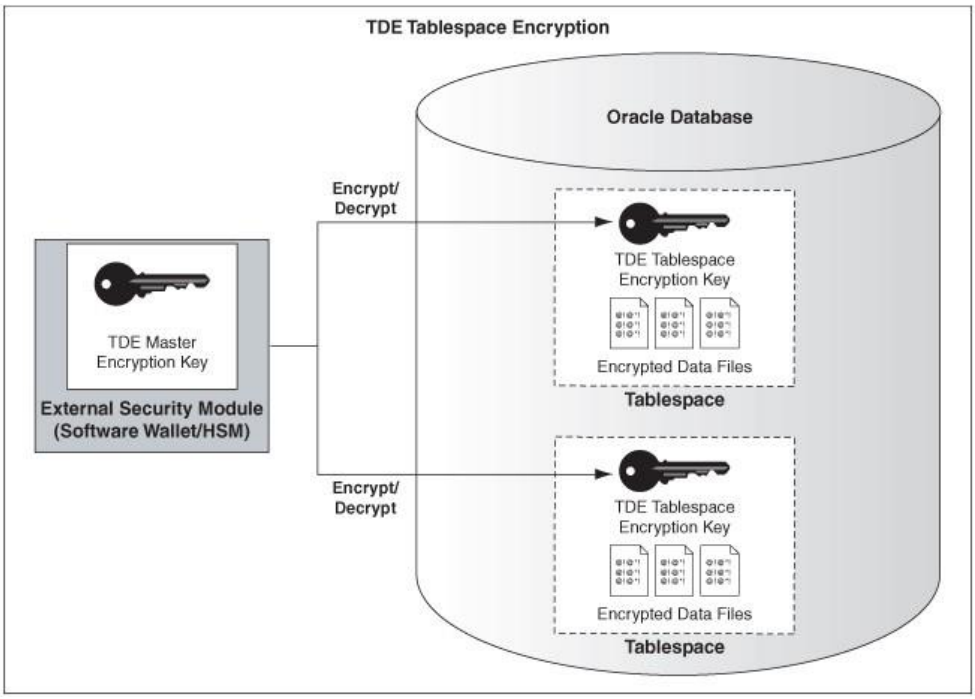


Figura 15 - Arquitetura de cifragem do TDE (Oracle, 2016a)

O TDE tem dois algoritmos de cifragem que utilizam chaves do tipo simétrica:

- o *Triple Data Encryption Standard* (3DES) em que o tamanho da chave de cifragem é de 168 *bits;*
- o *Advanced Encryption Standard* (AES) em que a chave de cifragem poderá ter tamanhos entre 128, 192 e 256 *bits* (Oracle, 2016a).

Ambos os algoritmos de cifragem disponíveis operam no modo *Cipher Block Chaining*[18] (CBC) (Oracle, 2016b).

As vantagens identificadas pela Oracle na utilização do TDE são:

- Garante que a informação sensível está segura em caso de furto dos ficheiros de base de dados;
- Não é necessário criar funções de cifragem e decifragem;
- Os utilizadores de base de dados ou aplicações não precisam de saber que a informação que estão a aceder está cifrada;
- Aplicações não tem de modificar para gerir a cifragem da informação;
- A gestão das chaves é independente das aplicações e dos utilizadores.

[18] O *Cipher Block Chaining* (CBC) é um método de cifragem que protege contra os ataques de blocos cifrados repetidos, através da criação de dependência com bloco anterior cifrado com o bloco por cifrar, sendo assim criado uma dependência com todos os blocos procedentes para a sua decifragem (Oracle, 2016c).

2.5.3 VTE

O *Vormetric Transparent Encryption* (VTE) é uma solução da organização Thales eSecurity (2018) que permite cifrar os ficheiros de base de dados a nível do sistema de ficheiros. Esta solução, comparativamente à Oracle TDE, é heterogénea pois é compatível com múltiplas bases de dados e SO diferentes. O VTE apenas disponibiliza o AES como algoritmo de cifragem.

O VTE (Thales eSecurity, 2018, pp. 8–12) disponibiliza diversas opções na sua instalação. A instalação mínima requer a implantação do agente VTE no servidor e a instalação de dois *Vormetric Data Security Manager* (DSM) de modo a assegurar a alta disponibilidade do serviço. O agente VTE é responsável por realizar as seguintes tarefas:

- Cifrar;
- Decifrar;
- Controlar os acessos aos ficheiros;
- Auditar os acessos à informação.

Já o *Vormetric Data Security Manager* (DSM) é responsável pelo armazenamento das políticas de acesso e as chaves simétricas ou assimétricas de cifragem. Também disponibiliza diversos tipos de interface para a gestão destas funcionalidades:

- Web GUI;
- CLI;
- SOAP;
- REST.

2.5.4 Avaliação das soluções

A Tabela 10 é apresenta as diferenças entre as soluções anteriormente analisadas sobre a cifragem da base de dados.

O TDE suporta dois tipos de algoritmos de cifragem, o 3DES e o AES, já o VTE só apresenta o algoritmo AES para cifrar a sua informação.

Apesar do algoritmo de cifragem ser importante, a forma como a chaves de cifragem são armazenadas é ainda mais importante, pois é através destas que se consegue cifrar e decifrar a informação. O TDE como solução nativa apresenta o Oracle Wallet para armazenar a chave mestre de cifragem, apesar de também ter compatibilidade com HSM. A desvantagem do Oracle Wallet é que este é armazenado dentro do mesmo servidor em que a base de dados é executada. Porém, como está cifrado e apenas é acedido através de uma palavra-passe, o risco de possível fuga de informação é baixo. Já o VTE apresenta o DSM que permite a gestão das chaves de cifragem remotamente, o que permite gerir diversas bases de dados através deste único componente.

O TDE, como foi dito anteriormente, tem duas opções de cifragem. A cifragem por coluna das tabelas é compatível a partir da versão base de dados Oracle 10g, já a cifragem por *tablespace* só é compatível pela Oracle 11g, o que significa que existe uma incompatibilidade com versões anteriores. Já o VTE, como é instalado sobre o sistema de ficheiros do SO, é independente das versões e o tipo de base de dados, como também permite a cifragem de ficheiros não estruturados (e.g. PDF), o que pode ser interessante no ponto de vista de negócio.

Tabela 10 - Diferenças entre o Oracle TDE e o VTE

Funcionalidades/Soluções	TDE	VTE
3DES	✓	×
AES	✓	✓
Gestão de chaves cifragem remotamente	×	✓
Compatibilidade com outros tipos de base de dados	×	✓

Resumidamente, o VTE é melhor em termos de compatibilidade com outras bases de dados relacionais e não relacionais, como também a gestão de chaves de cifragem para várias bases de dados em servidores diferentes. Contudo como o ALERT® HIE apenas utiliza base de dados relacionais da Oracle e atendendo às necessidades da organização, o Oracle TDE permite responder satisfatoriamente ao problema identificado.

3 Engenharia de Requisitos

Neste capítulo apresenta-se (i) uma análise dos requisitos do RGPD, apresentados na secção 1.2, enunciando o seu grau de cumprimentos pelo ALERT® HIE, o que permite (ii) a enunciação dos requisitos funcionais e não funcionais do sistema.

3.1 Análise de requisitos

As subsecções seguintes analisam cada um dos requisitos constantes no RGPD e o nível de suporte/provimento pelo ALERT® HIE.

3.1.1 Consentimento

3.1.1.1 Requisito

Para que o tratamento dos dados pessoais seja considerado lícito, é necessário que o tratamento esteja de acordo com uma das alíneas enumeradas dentro do artigo 6° nº 1 do RGPD (Parlamento Europeu e Conselho, 2016, pp. 36–37). O consentimento do cidadão é uma das alíneas que permite o tratamento lícito dos dados pessoais, devendo este ser dado de forma livre, clara e explícita. O cidadão pode retirar a qualquer momento o consentimento, como é descrito no artigo 7° do RGPD (Parlamento Europeu e Conselho, 2016, p. 37).

Quanto ao consentimento de menores de idade, este só é valido se estes tiverem pelo menos 16 anos de idade. Quando este não cumprir a idade mínima, é necessário garantir o consentimento pelo titular das responsabilidades parentais, de acordo com o artigo 8° do RGPD (Parlamento Europeu e Conselho, 2016, p. 37-38). Os Estados-Membros poderão dispor uma idade inferior desde que esta não seja inferior a 13 anos de idade.

3.1.1.2 Análise

O ALERT® HIE não tem qualquer funcionalidade que permita guardar e retirar o consentimento do paciente. Dito isto, é necessário prover uma solução de consentimento que abranja as seguintes categorias de tratamento de dados pessoais:

- Recolha – consiste na recolha da informação pessoal do paciente para um formato digital;
- Registo – baseia-se na persistência da informação do paciente;
- Conservação - representa o período em que os dados estarão persistidos;
- Consulta – consiste no acesso à informação do paciente;
- Adaptação ou alteração – atualização da informação do paciente;
- Divulgação – consiste na partilha da informação do paciente com terceiros;
- Apagamento ou destruição – baseia-se na eliminação da informação pessoal do paciente;
- Limitação – a informação pessoal continua armazenada, mas não é utilizada em qualquer tipo de tratamento.

Portanto, a implementação terá de abranger estas categorias de modo a que o tratamento efetuado sobre a informação do paciente seja lícito.

3.1.2 Acesso aos dados pessoais

3.1.2.1 Requisito

O RGPD, segundo o artigo 15° (Parlamento Europeu e Conselho, 2016, p. 43), permite que o cidadão europeu obtenha, do responsável pelo tratamento, a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e o acesso aos mesmos.

3.1.2.2 Análise

Este requisito está implementado no ALERT® HIE, pois os pacientes conseguem aceder à sua informação pessoal através do MyALERT® ou outro produto PHR (Personal Health Record) de outra organização, ou até mesmo por meio de uma instituição de saúde que esteja dentro do domínio do ALERT® HIE à sua informação pessoal.

3.1.3 Retificação dos dados pessoais

3.1.3.1 Requisito

Segundo o artigo 16° do RGPD (Parlamento Europeu e Conselho, 2016, p. 43), o titular dos dados tem o direito de retificar os seus dados pessoais inexatos que lhe digam respeito.

3.1.3.2 Análise

Esta funcionalidade já é possível através do uso do produto MyALERT® que permite a edição dos dados pessoais. Após o paciente editar os seus dados pessoais, estes serão persistidos no ALERT® HIE.

3.1.4 Eliminação dos dados pessoais

3.1.4.1 Requisito

Conforme o artigo 17° do RGPD (Parlamento Europeu e Conselho, 2016, pp. 43–44), o titular dos dados tem o direito a ser esquecido. Por outras palavras, dispõe do direito de apagar os dados pessoais, que lhe digam respeito, quando o solicita. O titular dos dados pessoais só pode exercer este direito quando uma das seguintes opções se verifica:

- Os dados pessoais deixam de ser necessários para a finalidade que motivou a sua recolha e tratamento;
- O titular dos dados pessoais retira o seu consentimento (cf. 3.1.1);
- Os dados pessoais foram tratados ilicitamente (cf. 3.1.1);
- O titular dos dados pessoais seja menor de idade.

3.1.4.2 Análise

Como o ALERT® se posiciona no domínio da saúde, os profissionais de saúde necessitam que a informação esteja disponível de forma a tomarem as devidas precauções necessárias na realização de tratamentos, permitindo melhorar a qualidade e segurança dos mesmos. O ALERT® HIE, sendo um produto que permite agrupar as informações/documentos relacionados com o paciente num só sítio, para possível consulta posteriormente, permite que a informação esteja sempre disponível.

Dito isto, é do entender do autor deste documento que os dados pessoais do paciente não podem ser eliminados por questões de qualidade e segurança dos cuidados de saúde. Este argumento é fundamentado pelo artigo 17° nº3 alínea C do RGPD que referencia o artigo 9° alínea I, em que este último refere que o tratamento de dados de saúde é lícitio, desde que sejam tomadas as medidas adequadas e específicas que salvaguardem os direitos de liberdade do titular dos dados, em particular o sigilo profissional (Parlamento Europeu e Conselho, 2016, p. 38,43).

3.1.5 Limitação do tratamento

3.1.5.1 Requisito

De acordo com o artigo 18° do RGPD (Parlamento Europeu e Conselho, 2016, pp. 44–45), o titular dos dados tem o direito de limitar o tratamento efetuado sobre os seus dados pessoais quando se aplicar uma das seguintes situações:

- O titular contestar a exatidão dos dados pessoais;
- O tratamento dos dados pessoais for ilícito e o titular dos dados solicitar a limitação do tratamento (cf. 1.2.1).

O responsável pelo tratamento é responsável por notificar o titular dos dados pessoais antes de ser anulada a limitação.

3.1.5.2 Análise

O ALERT®HIE tem uma funcionalidade que permite desativar a informação pessoal do paciente, pelo que esta funcionalidade poderá ser transposta para a limitação do tratamento de modo a resolver este requisito.

3.1.6 Notificação aos destinatários

3.1.6.1 Requisito

Consoante o artigo 19° do RGPD (Parlamento Europeu e Conselho, 2016, p. 45), o responsável pelo tratamento deverá notificar todos os destinatários a quem os dados foram comunicados, das alterações efetuadas pelo paciente quando este exerce um dos direitos mencionados nas subsecções 3.1.3, 3.1.4 e 3.1.5, salvo se a comunicação se revelar impossível ou implicar um esforço desproporcionado. Se o paciente requisitar, o responsável pelo tratamento deverá fornecer as informações dos destinatários a quem os dados foram comunicados.

3.1.6.2 Análise

Atualmente, o produto apenas permite obter os destinatários a quem os dados pessoais do paciente foram comunicados.

3.1.7 Portabilidade dos dados

3.1.7.1 Análise

De acordo com o artigo 20° do RGPD (Parlamento Europeu e Conselho, 2016, p. 45), o paciente poderá exercer o seu direito de portabilidade de dados devido ao facto de estar previsto o tratamento ser realizado com base no consentimento do titular dos dados. O responsável pelo tratamento deverá fornecer ao titular os dados pessoais que tem em sua posse num formato estruturado, de uso corrente e leitura automática. O titular também terá o direito de que os

dados sejam automaticamente transmitidos para outro responsável de tratamento sempre que tal seja tecnicamente possível.

O RGPD, no ponto 68 (Parlamento Europeu e Conselho, 2016, p. 13), aconselha que "… os responsáveis pelo tratamento de dados deverão ser encorajados a desenvolver formatos interoperáveis que permitam a portabilidade dos dados".

3.1.7.2 Análise

O ALERT® HIE, sendo uma solução que permite a transmissão de informação clínica entre instituições e HIE, implementa padrões de comunicação e terminologias de saúde médica reconhecidos mundialmente, tais como HL7 e SNOMED CT. Posto isto, já é possível fornecer ao paciente os seus dados num formato interoperável.

Quanto à questão da transmissão automática com outro responsável, sendo o ALERT® HIE um produto que que não tem interação direta com os pacientes, este não deverá assumir a responsabilidade da transmissão, mas, quando muito, deverá ter a opção de exportar a informação do paciente num formato interoperável.

Dito isto, o ALERT® HIE já cumpre este requisito.

3.1.8 Oposição

3.1.8.1 Requisito

A oposição ao tratamento dos dados pessoais por parte do titular dos dados, segundo o artigo 21° (Parlamento Europeu e Conselho, 2016, pp. 45–46), só é possível quando o tratamento for realizado em exercício de uma das seguintes possibilidades:

- Interesse público;
- Autoridade pública;
- Necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento;
- Para fins que não sejam aqueles para os quais os dados pessoais foram recolhidos;
- Quando os dados pessoais forem tratados para efeitos de comercialização.

3.1.8.2 Análise

Como está previsto que o tratamento sobre os dados pessoais seja realizado com o consentimento do paciente, este consequentemente perde o direito de oposição ao consentir o tratamento. De qualquer forma, o paciente poderá retirar o seu consentimento a qualquer momento, o que implicará o cessamento do tratamento, como foi mencionado na subsecção 3.1.1.1.

3.1.9 Oposição às decisões individuais automatizadas

3.1.9.1 Requisito

Consoante o artigo 22° do RGPD (Parlamento Europeu e Conselho, 2016, p. 46), o titular dos dados tem o direito de não ficar sujeito a nenhuma decisão automatizada que possa produzir efeitos na sua esfera jurídica ou que o afete significativamente.

3.1.9.2 Análise

O ALERT® HIE incorpora uma funcionalidade que permite correlacionar dados de pacientes armazenadas em diferentes instituições num só. Com a entrada em vigor do RGPD, é necessário garantir que o paciente está de acordo com esta decisão (correlação) automatizada. Caso o paciente não esteja de acordo, esta decisão (correlação) terá de ser feita manualmente por um ser humano.

3.1.10 Auditoria de eventos

3.1.10.1 Requisito

O RGPD afirma no nº2 do artigo 5° (Parlamento Europeu e Conselho, 2016, p. 36), que o responsável pelo tratamento deve ser responsável por comprovar o seu cumprimento com este regulamento. De modo a conseguir comprovar que a solução está em cumprimento, é necessário haver um registo do tratamento efetuado sobre a informação do paciente, de forma a se conseguir provar que o tratamento foi efetuado de forma lícita. Além disso, os acessos aos ambientes de produção dos clientes também devem ser auditados, de modo a provar-se os motivos de acesso e os problemas resolvidos.

3.1.10.2 Análise

O ALERT® HIE implementa o perfil de integração ATNA, da organização Integrating the Healthcare Enterprise (Integrating the Healthcare Enterprise [IHE], 2018d), que tem como objetivo auditar os eventos dos outros perfis de integração. Os eventos auditados seguem regras específicas de formato nas mensagens, definidas dentro dos outros perfis de integração, de modo a promover a interoperabilidade deste conteúdo, caso seja necessário. Dito isto, caso não existam perfis de integração que promovam uma solução aos requisitos necessários implementar, para que o produto esteja em cumprimento com o RGPD, terá que se implementar um novo formato de mensagem para estes requisitos. Contudo apenas a organização ALERT conseguirá entender o conteúdo da mensagem.

Quanto à questão de auditoria de acesso aos ambientes de produção do ALERT® HIE nos clientes, existe um processo formal onde o cliente abre um problema na plataforma JIRA da ALERT. No sentido de resolver o problema colocado pelo cliente, um dos colaboradores de suporte da ALERT terá de aceder remotamente ao ambiente do cliente, sendo que, para tal, terá de registar o motivo de estar a aceder (identificando o ID do problema criado pelo cliente), o período que estará conectado ao ambiente e a sua identificação, que é obtida através do utilizador autenticado.

O ALERT® HIE já implementa auditoria nas suas transações como também nos possíveis acessos à base de dados dos clientes. Contudo devido às possíveis alterações necessárias a realizar e à implementação de novos requisitos, poderá ser necessário auditar estas novas alterações de modo a comprovar o cumprimento com o RGPD.

3.1.11 Cifragem e Mecanismos de autenticação e autorização

3.1.11.1 Requisito

Conforme o artigo 32° do RGPD (Parlamento Europeu e Conselho, 2016, pp. 51–52), o responsável pelo tratamento dos dados pessoais deve aplicar as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco. A cifragem dos dados pessoais identificáveis do paciente é uma forma de assegurar a segurança dos seus dados e a sua identidade. Esta deverá ser feita quer ao nível da base de dados como também durante a transmissão de informação entre componentes cliente/servidor. Os mecanismos de autenticação e autorização também são um mecanismo de segurança que garantem a autenticidade dos utilizadores e verificam se estes têm autorização para aceder à informação pessoal.

3.1.11.2 Análise

Todas as comunicações efetuadas no produto são com base no protocolo de comunicação HTTPS, sendo utilizado o processo de autenticação em duas fases (SSL *two way authentication*) em que o cliente e servidor partilharão entre si o seu certificado e a cadeia de certificados até à autoridade certificadora. A lista de autoridades certificadoras em que cada interveniente confia, a distância de confiança configurada dentro de cada um e a distância do certificado do interveniente ao da autoridade certificadora, são os fatores que permitem verificar se os intervenientes confiam na ligação que estão a estabelecer (Clark and van Oorschot, 2013). Caso os certificados sejam válidos, eles partilharão uma chave de cifragem que utilizarão para cifrar e decifrar a informação durante a transmissão. Estes certificados também são utilizados como mecanismos de autenticidade ao nível da instituição. O mecanismo de autorização está incorporado ao nível do documento clínico, pelo que o médico, ao partilhar um documento clínico no ALERT® HIE, pode escolher com quais das instituições, dentro do domínio do produto, quer partilhar o documento.

Quanto ao acesso dos pacientes através de produtos do tipo PHR, como por exemplo o MyALERT®, é necessário que o paciente insira as suas credenciais de acesso, de forma a comprovar a sua identidade. Após a confirmação de autenticidade e autorização do paciente é garantido o acesso à informação pessoal e clínica.

O produto utiliza uma base de dados do tipo relacional da organização Oracle (2019a), sendo utilizados os mecanismos de segurança nativos desta. O SGBD Oracle não cifra nativamente a informação da base de dados, apesar de que os ficheiros de base de dados são armazenados num formato proprietário que não permite que a informação seja lida por outros programas (Oracle, 2015a). Ainda assim, existe um risco elevado de divulgação de informação se os ficheiros de base de dados forem furtados digitalmente ou fisicamente, pois apesar de não se conseguir ler diretamente dos ficheiros, é possível obter informação sensível quando os ficheiros são lidos por outra instância do SGBD da Oracle (Atil, 2016; Hall, 2019).

A solução de cifragem deverá ser transparente à utilização da base de dados, pois existe muita lógica dentro desta que necessita de ter a informação decifrada de forma a obter o resultado pretendido. Um exemplo é o correlacionamento de pacientes entre instituições de saúde, pois este utiliza algoritmos de grau de semelhança na informação demográfica, de forma a apurar se são ou não o mesmo paciente. Se a informação estiver cifrada, este algoritmo não conseguirá calcular a semelhança, comprometendo o resultado final deste. Outro requisito é continuar a permitir a pesquisa abertas, nomeadamente (i) por expressões regulares (e.g. SELECT * from Paciente WHERE Paciente.name LIKE "S*") ou (ii) em intervalos (e.g. SELECT * from Paciente WHERE Paciente.CorDosOlhos in ("azul", "verde")).

Resumidamente, o ALERT® HIE já implementa os mecanismos de segurança necessários para proteger a informação dos seus pacientes a nível aplicacional, bem como a nível de base de dados estão implementados os mecanismos de autenticação e auditoria de modo a proteger a informação dos pacientes. Contudo, as possíveis ameaças externas são um fator a ter em conta, sendo necessário encontrar uma solução que permita cifrar o conteúdo da base de dados sem que comprometa a lógica de negócio existente.

3.1.12 Disponibilidade e Resiliência

3.1.12.1 Requisito

Segundo o artigo 32° do RGPD (Parlamento Europeu e Conselho, 2016, pp. 51–52), o responsável pelo tratamento deverá garantir não só a confidencialidade e integridade dos dados, mas também a disponibilidade e resiliência permanente do sistema. Como o produto se insere na área da saúde é fundamental que as possíveis falhas de *software* que possam acontecer não tenham impacto na usabilidade e disponibilidade do produto, devido ao facto de estas poderem afetar diretamente a saúde de um paciente.

3.1.12.2 Análise

O produto ALERT® HIE está preparado para ser executado em N instâncias, sendo que, normalmente, quando é instalado no cliente, é executado em pelo menos duas instâncias, de modo a permitir que o produto continue disponível caso uma das instâncias falhe.

De forma a aumentar a resiliência do produto, a ALERT conta com uma equipa de suporte que vigia as possíveis falhas que possam acontecer nos clientes, de forma a conseguir responder de forma atempada aos possíveis problemas que possam ocorrer e analisar possíveis padrões que possam causar estes erros. Ao aceder remotamente aos ambientes dos clientes, os colaboradores da ALERT passarão por um mecanismo de auditoria de forma a auditar a razão do acesso, explicado na subsecção 3.1.10.

3.2 Requisitos de sistema

Nesta secção são apresentados os requisitos funcionais e não funcionais que a solução deverá atingir.

3.2.1 Estruturação dos requisitos

Após a identificação dos requisitos necessários para o cumprimento do RGPD e a respetiva análise de modo a apurar o cumprimento do ALERT® HIE, durante a secção 3.1, na Tabela 11 são apresentados novamente os respetivos requisitos mas separando-os em requisitos funcionais e não funcionais.

Tabela 11 - Transformação dos requisitos do RGPD em requisitos funconais ou não funcionais

Requisitos de negócio	Cumprimento pelo ALERT® HIE	Requisito funcional	Requisito não funcional
Consentimento	✗	X	-
Acesso aos dados pessoais	✓	-	-
Retificar dados pessoais	✓	-	-
Apagamento dos dados pessoais	Não se aplica	-	-
Limitação do tratamento	✓	-	-
Notificação aos destinatários dos dados pessoais	✓/✗	-	X
Portabilidade dos dados	✓	-	-
Oposição ao tratamento	Não se aplica	-	-
Oposição às decisões individuais automatizadas	✗	X	-
Auditoria de eventos	✓/✗	-	X
Cifragem	✓/✗	-	X
Mecanismos de autenticação e autorização	✓	-	X
Disponibilidade	✓	-	X
Resiliência	✓	-	X

3.2.2 Funcionais

Os requisitos funcionais demonstram as funcionalidades que os atores envolvidos poderão usufruir da solução construída. Os principais atores do sistema são:

- Administrativo;
- Médico;
- Paciente.

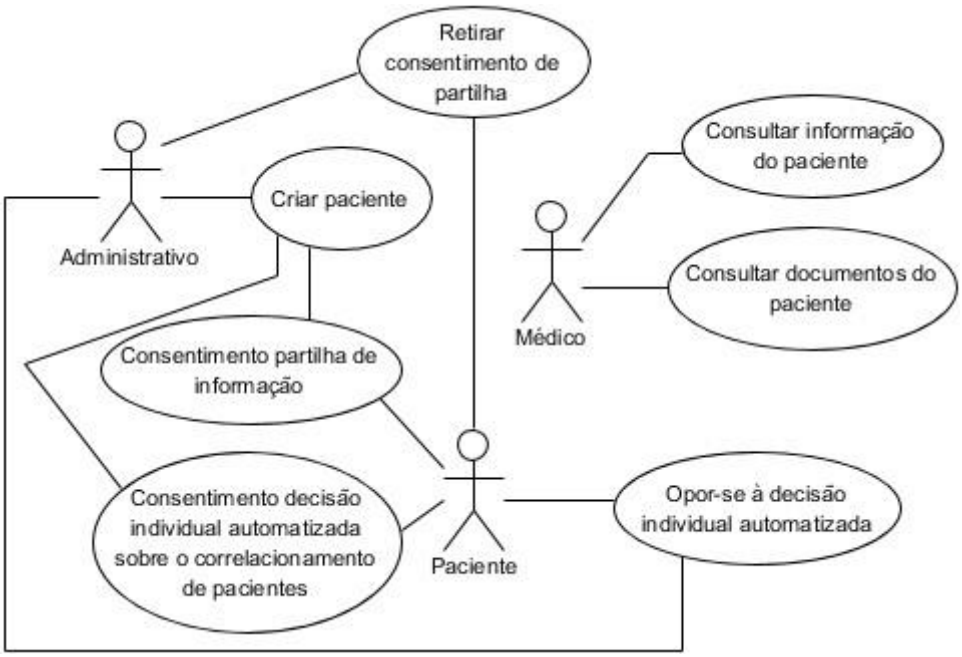


Figura 16 - Diagrama de casos de uso

O diagrama de casos de uso, representado na Figura 16, apresenta os requisitos funcionais identificados necessários para a adaptação do ALERT® HIE ao RGPD, sendo que alguns dos requisitos funcionais identificados já estão implementados, apenas tendo de sofrer uma reengenharia devido às alterações necessárias para o cumprimento do RGPD, nomeadamente:

- Criar Paciente – devido a ser necessário ter o consentimento do paciente para realizar tratamento sobre os seus dados pessoais;

- Consultar informação do paciente – devido a ser necessário verificar se o paciente consentiu que os seus dados pessoais fossem partilhados.

3.2.3 Não funcionais

Ao longo do documento foram especificados requisitos não funcionais, sendo que alguns estão diretamente identificados no RGPD enquanto que outros estão indiretamente. Dito isto, a Tabela 12 apresenta os requisitos não funcionais impostos pelo RGPD e os que a ALERT espera obter na solução final, segundo o modelo de FURPS+. FURPS+ é um acrónimo em que **F** significa funcionalidade, **U** usabilidade, **R** (*reliability*) confiabilidade, **P** (*performance*) desempenho, **S** suportabilidade e por último o símbolo **+** significa outro conjunto de critérios tais como restrições de desenho, implementação, interface, físicas e legais.

Tabela 12 - Requisitos não funcionais segundo modelo FURPS+

Classificação FURPS+	Requisito não funcional
Funcionalidade	Auditoria da aplicação
Funcionalidade	Cifragem da informação pessoal do paciente
Funcionalidade	Notificação aos destinatários

Classificação FURPS+	Requisito não funcional
Confiabilidade	Licitude do tratamento
Confiabilidade	Integridade da informação
Confiabilidade	Disponibilidade da aplicação
Confiabilidade	Resiliência da aplicação
Confiabilidade	Confidencialidade da aplicação
Confiabilidade	Responsabilidade da aplicação
Suportabilidade	A solução deverá conseguir ser executada em n instâncias, em que n>1
+ Legal	Cumprimento do RGPD
+ Interoperável	Solução deverá continuar a permitir a interoperabilidade
+ Implementação	Tecnologias: Java e base de dados relacional Oracle

3.3 Correlação e priorização dos requisitos

Nas subsecções seguintes será apresentado o correlacionamento entre os requisitos do cliente e as características técnicas do produto através da técnica QFD, bem como a identificação das principais funcionalidades que dão valor ao produto e a sua priorização através de uma análise funcional.

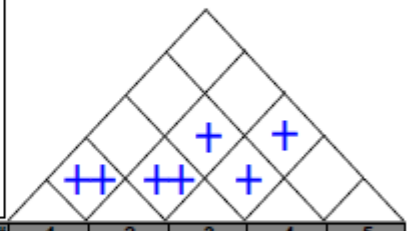
3.3.1 QFD

O *Quality Function Deployment* (QFD), é uma técnica criada em 1972 num estaleiro da Mitsubishi na cidade de Kobe, tendo sido desenvolvida ao longo dos últimos anos com o intuito de criar produtos de melhor qualidade que irão ter em conta as necessidades dos clientes. A sua descrição gráfica contempla dois eixos:

- O eixo vertical enumera os requisitos que o cliente pretende obter no produto/serviço;
- O eixo horizontal enumera as características técnicas do produto que darão resposta a estes requisitos.

Cria-se assim uma matriz, vulgarmente denominada “a casa da qualidade”, que descreve a relação entre cada um dos requisitos do cliente com as características técnicas do produto (Warwick Manufacturing Group, 2007). Além disso, por cima da matriz é possível visualizar o “telhado” da casa, que permite averiguar as relações entre as características técnicas do produto. A casa da qualidade relativa ao projeto em causa é representada na Figura 17.

Legend		
⊖	Strong Relationship	9
O	Moderate Relationship	3
▲	Weak Relationship	1
++	Strong Positive Correlation	
+	Positive Correlation	
—	Negative Correlation	
▼	Strong Negative Correlation	
▼	Objective Is To Minimize	
▲	Objective Is To Maximize	
X	Objective Is To Hit Target	



Row #	Max Relationship Value in Row	Relative Weight	Weight / Importance	Demanded Quality (a.k.a. "Customer Requirements" or "Whats") / Quality Characteristics (a.k.a. "Functional Requirements" or "Hows")	1 Políticas de privacidade	2 Consentimento	3 Autorização	4 Auditoria	5 Cifragem
				Column #	1	2	3	4	5
				Direction of Improvement: Minimize (▼), Maximize (▲), or Target (x)	X	X	X	X	X
1	9	25,0	25,0	Licitude do tratamento	⊖	⊖		O	
2	9	20,0	20,0	Integridade da informação			⊖	O	O
3	9	20,0	20,0	Confidencialidade da informação	▲	O	⊖		⊖
4	9	15,0	15,0	Responsabilidade				⊖	O
5	9	20,0	20,0	Oposição a decisões individuais automatizadas	O	⊖		O	
				Target or Limit Value	Suportado	Suportado	Suportado	Suportado	Suportado
				Difficulty (0=Easy to Accomplish, 10=Extremely Difficult)	2	7	5	3	4
				Max Relationship Value in Column	9	9	9	9	9
				Weight / Importance	305,0	465,0	360,0	330,0	245,0
				Relative Weight	17,9	27,3	21,1	19,4	14,4

Figura 17 - Casa da qualidade

Foram definidos pelo cliente cinco requisitos necessários para que o produto esteja em cumprimento com RGPD (cf. Subsecções 3.2.2 e 3.2.3):

- **Licitude do tratamento,** com uma importância de 25%, devido ao facto do paciente ter conhecimento sobre o tratamento que irá ser aplicado à sua informação pessoal e clínica;

- **Integridade da informação,** com uma importância de 20%, pois é necessário garantir a integridade da informação do paciente;

- **Confidencialidade da informação,** com uma importância 20%, visto que é necessário garantir que só os utilizadores a quem o paciente consentiu o acesso conseguem aceder à informação deste;

- **Responsabilidade,** com uma importância de 15%, uma vez que é importante registar os eventos de auditoria de forma a conseguir comprovar o cumprimento do produto perante o RGPD;

- **Oposição às decisões individuais automatizadas,** com uma importância de 20%, pois o paciente pode opor-se a decisões automatizadas como é descrito no artigo 22° do RGPD.

Também existem cinco características técnicas que permitem responder aos requisitos definidos pelo cliente (cf. Subsecções 3.2.2 e 3.2.3), sendo estas:

- As **políticas de privacidade** permitem definir que tipo de tratamento é realizado pelo produto. Esta característica está acopolada com os requisitos da licitude do tratamento e da oposição às decisões individuais automatizadas;

- O **consentimento** permite que o produto realize tratamento sobre a informação pessoal do paciente. Esta característica está acopolada aos requisitos de licitude, confidencialidade e oposição às decisões individuais automatizadas;

- O mecanismo de **autorização** verificará se o paciente deu autorização para o tratamento da sua informação, através do consentimento do paciente. Esta característica fica acopolada aos requisitos de integridade e confidencialidade da informação;

- A **auditoria** permite demontrar a licitude do tratamento realizado, ficando acopolado a quase todos os requisitos do cliente excepto a confidencialidade da informação;

- A **cifragem** irá garantir a confidencialidade da informação das possíveis ameaças externas, ficando acopolada aos requisito de integridade e confidencialidade da informação, como também ao de responsabilidade pelo tratamento.

Em relação ao correlacionamento entre as características técnicas do produto:

- As **políticas de privacidade** têm uma relação muito forte com o consentimento, pois este depende das políticas existentes;

- O **consentimento** tem uma relação muito forte com a autorização, pois é no consentimento que vão estar as regras de autorização de acesso definidas pelo paciente. Além disso, tem uma relação forte com a auditoria de forma a averiguar a integridade do documento de consentimento;

- A **autorização** tem uma relação forte com a auditoria e a cifragem, pois (i) a auditoria permite comprovar que não houve acessos à informação pessoal do paciente por utilizadores não autorizados, e (ii) só os utilizadores registados poderão visualizar o conteúdo decifrado.

3.3.2 Análise funcional

A análise funcional consiste na identificação das funcionalidades que dão mais valor ao produto. A Tabela 1 apresenta os requisitos necessários para que o produto ALERT® HIE esteja em cumprimento com o RGPD. Após a identificação dos requisitos, todas as funcionalidades, exceto as que não se aplicam ou já estão em cumprimento, são transpostas para um diagrama de árvore. Este diagrama decompõe os requisitos hierarquicamente de forma a realçar as funcionalidades principais que estão no topo e os requisitos necessários para que possa ser cumprido.

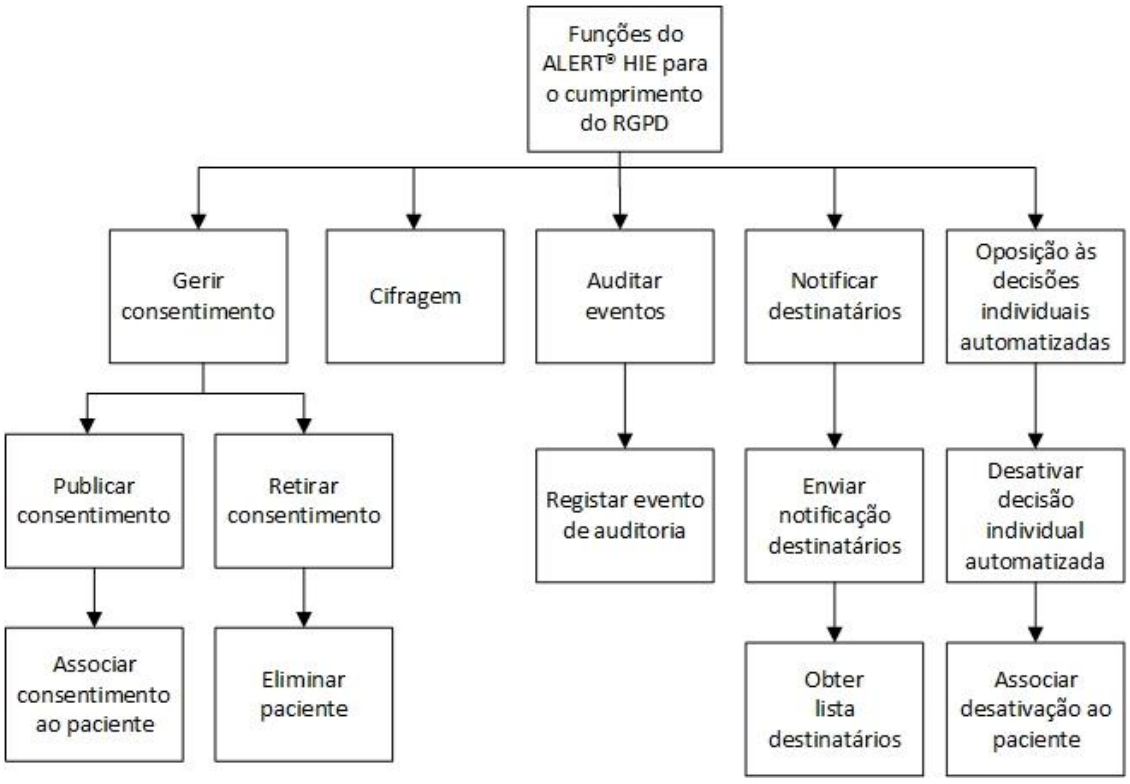


Figura 18 - Diagrama de árvore com as funções necessárias para o cumprimento do RGPD

Através da Figura 18, é possível averiguar que é necessário implementar 5 funcionalidades, de modo a que o produto esteja em cumprimento com o RGPD, sendo estas:

1. Gerir consentimento do paciente;

2. Cifragem;
3. Auditar eventos;
4. Notificar destinatários;
5. Oposição às decisões individuais automatizadas.

Após a identificação das funcionalidades, o próximo passo é classificar o seu nível de importância e prioridade, adotando a comparação entre pares como é ilustrado na Figura 19. Este método compara as funcionalidades entre si e atribui uma pontuação em cada comparação. Depois de todas as comparações estarem realizadas, é feito o somatório de todas as pontuações respetivas a cada funcionalidade. No final é possível verificar qual é a funcionalidade que tem maior prioridade e importância e as menos importantes por ordem decrescente. A pontuação varia entre 1 a 3, sendo que 1 ponto significa que é pouco mais importante, 2 pontos significa que a função é significativamente mais importante e por fim 3 pontos significa que é muito mais importante.

Figura 19 - Comparação de funcionalidades em pares

Ao analisar a Figura 19 conclui-se que as funcionalidade são prioritizadas da seguinte forma:

1. “gerir consentimento” com 8 pontos, devido ao facto de todo o tratamento realizados (cf. subsecção 3.1.1.2) ser dependente do consentimento do paciente, como foi descrito na subsecção 3.1.1;

2. “cifragem” com 6 pontos, visto que é fundamental para garantir a confidencialidade e integridade da informação das ameaças externas;

3. “auditoria de eventos” com 3 pontos, pois permite comprovar que o produto está em conformidade com o RGPD, conforme foi descrito na subsecção 3.1.10;

4. “oposição às decisões individuais automatizadas” com 2 pontos, visto que é necessário garantir que o paciente esteja consciente das decisões individuais automatizadas existentes na solução e se este está de acordo ou não com estas decisões;

5. “notificação dos destinatários” com 0 pontos, devido a esta funcionalidade não pôr em causa o princípio da privacidade dos dados.

4 Análise de Sistema

Neste capítulo são apresentados os principais conceitos de negócio, os processos de negócio que utilizam estes conceitos e os seus intervenientes. Também é apresentado o *software* ALERT® HIE sob um ponto de vista de base do projeto, mais concretamente a sua arquitetura, tecnologia e o algoritmo de correlacionamento de pacientes que toma decisões automáticas.

4.1 Conceitos de negócio

O diagrama de modelo de domínio permite ilustrar os principais conceitos de negócio e as suas relações, como é apresentado na Figura 20. O **HIE** faz parte de um **domínio de afinidade**, sendo este constituído por diversas **instituições de saúde**. O **HIE** processa diversos tipos de **transações** em que cada uma poderá desencadear um ou mais **eventos de auditoria**. As transações poderão envolver vários conceitos desde a **informação demográfica do paciente**, **identificação do paciente** e **documentos.** No HIE, um **paciente** poderá ter mais que uma **informação demográfica** e **identificação,** pois estas estão associadas à **instituição de saúde** que desencadeou o processo de criação do **paciente**, sendo também necessário para que se consiga correlacionar o mesmo **paciente** com identificações diferentes em **instituições** distintas.

Com a entrada em vigor do RGPD, é necessário ter o **consentimento do paciente** para se realizar tratamento sobre a informação pessoal do mesmo, conforme foi explicado na subsecção 3.1.1. Para tal, é necessário que o paciente consinta às **políticas de privacidade** criadas pelo **domínio de afinidade** e que este consentimento seja armazenado através de um ou mais **documentos de consentimento**. O paciente terá apenas um **documento de consentimento raiz** que referenciará os outros **documentos de consentimento.**

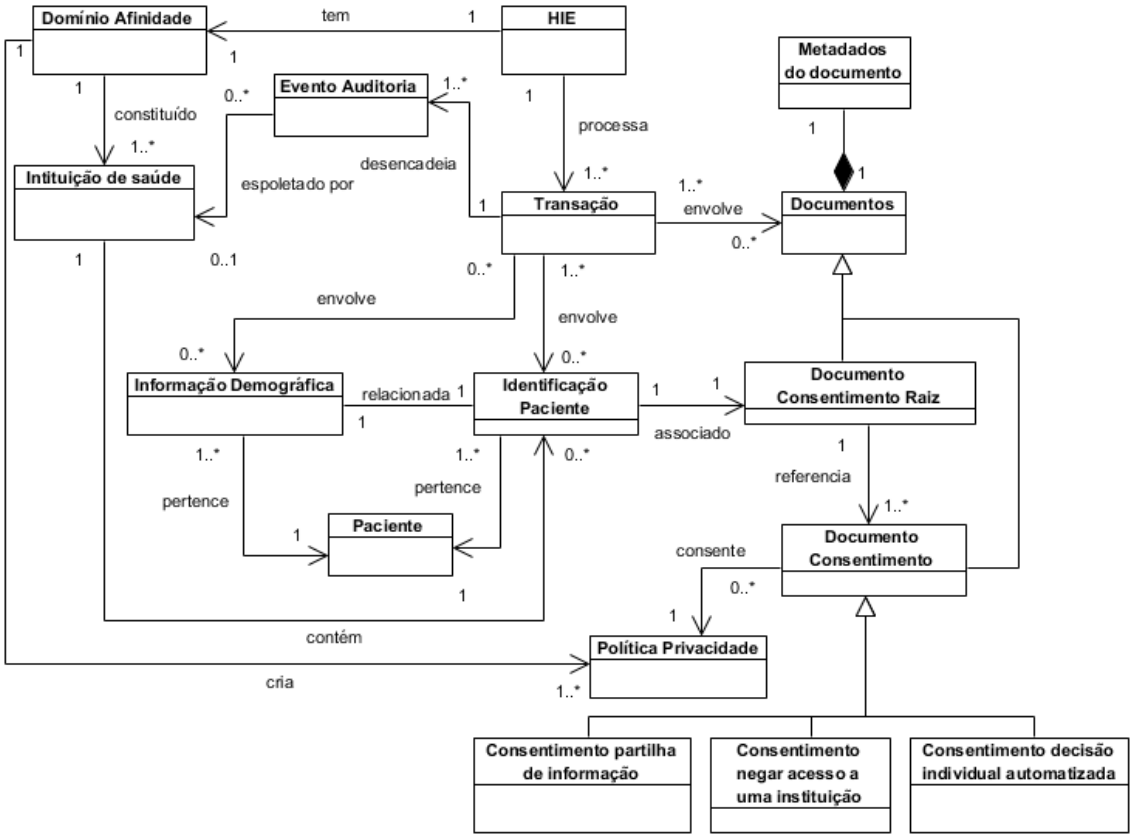


Figura 20 - Modelo de domínio relevante para o projeto

4.2 Processos e intervenientes

Nesta secção serão apresentados os processos que após a introdução do RGPD sofreram alterações, assim como os intervenientes que participam nestes processos. De modo a representar os processos de negócio, utilizar-se-á a modelação *Business Process Model and Notation* (BPMN), que facilita a comunicação entre os profissionais relacionados com os processos de negócio e os profissionais que implementam estes processos de negócio (Object Management Group, 2011, p. 21).

Existem cinco intervenientes sobre a adaptação do produto ALERT® HIE ao RGPD, sendo estes:

1. Paciente;
2. Administrativo da instituição;
3. Médico da instituição;
4. Administrador do HIE na instituição;
5. ALERT® HIE.

4.2.1 Processo de negócio da partilha de consentimentos do paciente

Na Figura 21 é apresentado um processo de negócio exemplificativo, que não representa necessariamente o processo de negócio que irá ser implementado nas instituições de saúde. Com este processo de negócio pretende-se dar uma contextualização ao leitor sobre a visita de um paciente a uma instituição de saúde, focando-se mais concretamente na criação do paciente e partilha do consentimento.

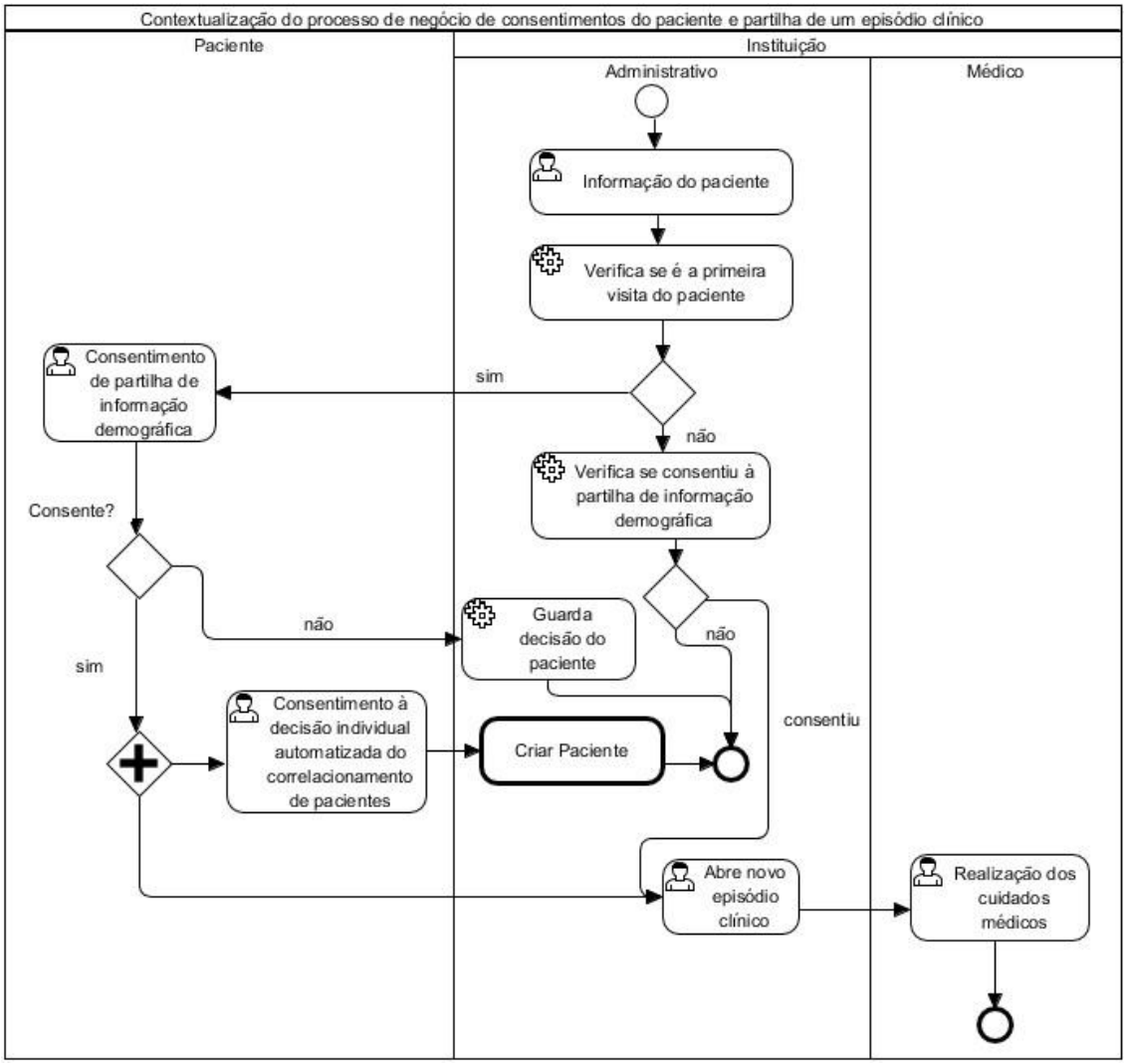


Figura 21 - Processo de negócio exemplificativo dos consentimentos do paciente na partilha de informação demográfica e episódio clínico

Como é possível aferir através da análise da Figura 21, quando o paciente visita uma instituição de saúde é recebido primeiramente pelo administrativo que irá perguntar pelos seus dados demográficos e a razão da sua deslocação à instituição de saúde. Após o paciente indicar os seus dados pessoais, o administrativo verifica se o paciente já visitou antes a instituição de saúde. No cenário do paciente nunca ter visitado a instituição de saúde, o administrativo questiona o paciente se quer partilhar a sua informação demográfica no HIE e explica as vantagens. Caso o paciente não consinta a partilha, o fluxo de visita do paciente continua sem

interferência com o HIE, apenas sendo registado no sistema da instituição a decisão do paciente. Em caso contrário, o paciente irá ser questionado se quer consentir também à decisão individual automatizada sobre o correlacionamento de pacientes entre instituições. Posteriormente, é criado o paciente no HIE a que a instituição está conectada. Na hipótese de o paciente já ter visitado a instituição de saúde, o administrativo apenas verifica se este já consentiu à partilha da sua informação demográfica e procede com o processo de negócio.

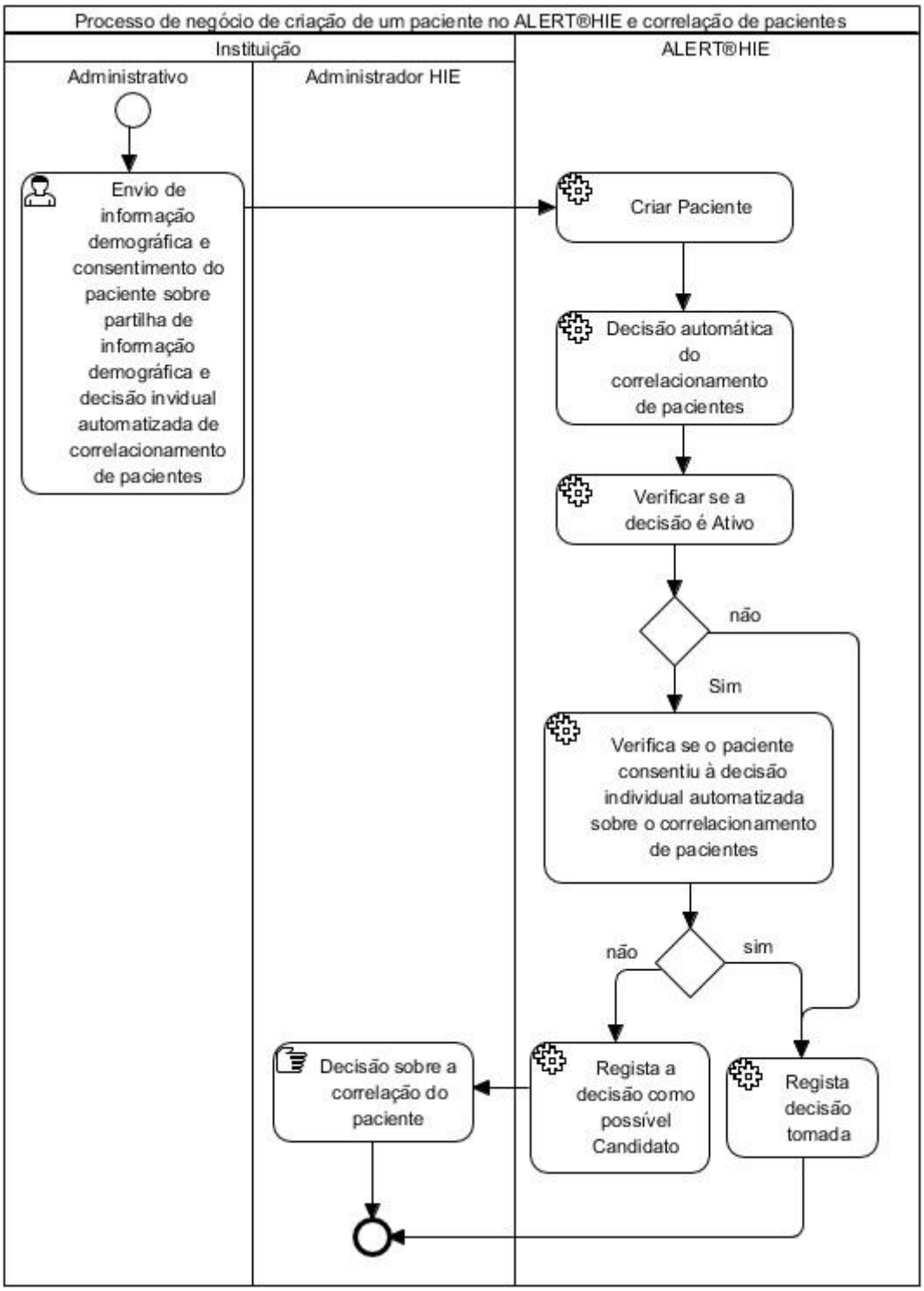


Figura 22 - Processo de negócio da criação de um paciente no ALERT®HIE e correlação de informação de pacientes

O administrativo ao obter o consentimento do paciente, partilha com o ALERT® HIE a informação demográfica e os documentos de consentimento relacionados com o paciente.

Ao receber a informação do paciente é criado um novo paciente sendo associado à intituição que enviou a informação. Depois, é espoletado o processo de correlacionamento de paciente entre instituições, em que primeiramente o sistema tentará correlacionar o paciente criado com todos os outros e tomará as respetivas decisões. Após tomar as decisões, verificara-se-á para cada decisão se esta é do tipo Ativo. Caso seja, é necessário verificar se os pacientes consentiram à decisão individual automatizada e, caso contrário, é registada a decisão. Ao verificar o consentimento dos pacientes à decisão individual automatizada, a decisão tomada pelo algoritmo é registada. Senão, a decisão é alterada para possível Candidato, sendo que a decisão final recairá sobre o administrador do HIE da instituição. O fluxo de criação do paciente e correlacionamento é descrito no processo de negócio da Figura 22.

4.2.2 Processo de negócio dos direitos do paciente do RGPD

O paciente tem duas opções para exercer os seus direitos sobre o ALERT® HIE no que toca ao RGPD:

1. Visitar uma instituição de saúde que faça parte do domínio do ALERT® HIE;

2. Aceder através de uma aplicação PHR, como por exemplo o MyALERT®.

Na Figura 23 é apresentado o processo de negócio exemplificativo, que pretende demonstrar a visita de um paciente a uma instituição de saúde quando este quiser exercer um dos seus direitos, dando-se foco no direito da portabilidade dos dados e o de retirar consentimento. No sentido de garantir que o paciente possa exercer os seus direitos na instituição de saúde que visitou, é necessário primeiramente garantir que existe o consentimento da partilha da informação demográfica do paciente, só depois o paciente poderá exercer qualquer um dos direitos mencionados na referentes ao RGPD. Na Figura 23 é possível aferir o processo a cima detalhado.

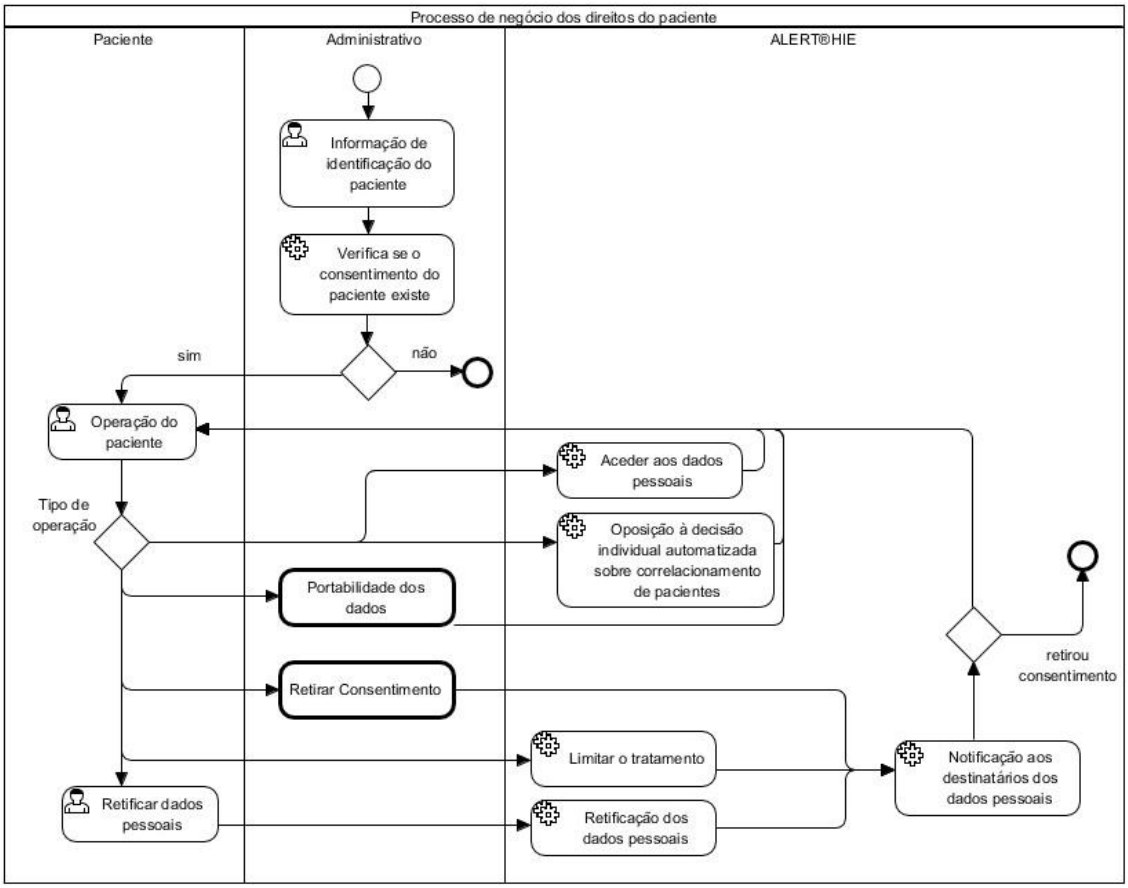


Figura 23 - Processo de negócio dos direitos do paciente sobre o RGPD

O paciente, ao exercer o direito da portabilidade dos dados, desencadeará dois subprocessos, dos quais um terá o objetivo de obter o contacto do responsável pelo tratamento a quem o paciente quererá comunicar a informação, e o outro terá como intuito obter toda a informação do paciente existente dentro do ALERT® HIE num formato interoperável. Após este dois subprocessos estarem concluídos é possível continuar o fluxo de negócio, sendo da responsabilidade do administrativo/instituição de saúde fazer a comunicação dos dados pessoais ao responsável pelo tratamento, como foi descrito na subsecção 3.1.7. Este fluxo pode ser verificado na Figura 24.

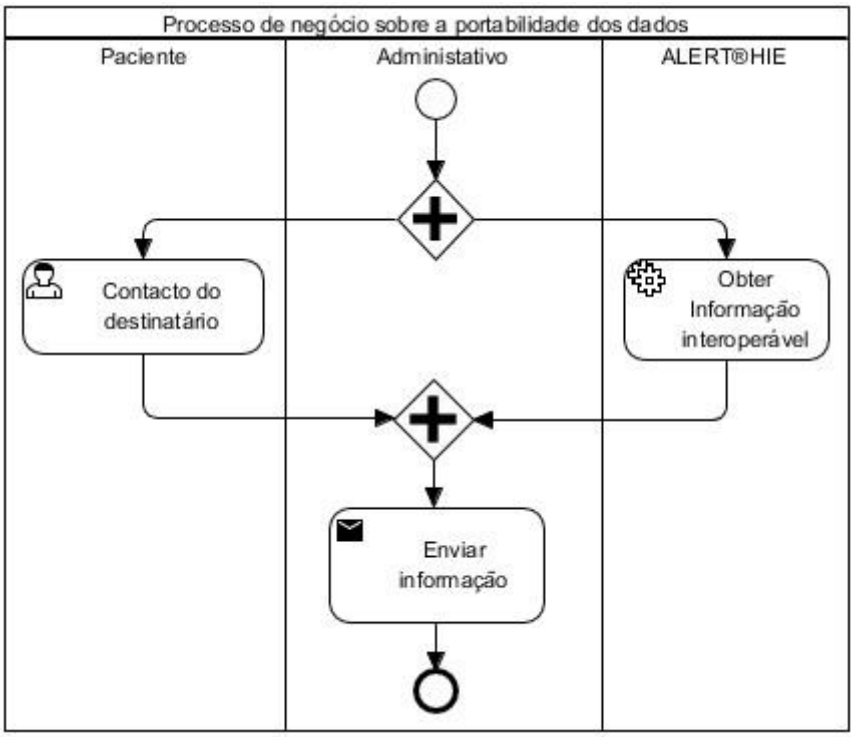


Figura 24 - Processo de negócio sobre a portabilidade dos dados

Quando o paciente retira o seu consentimento de partilha de informação com o ALERT® HIE numa visita a uma instituição de saúde, é necessário eliminar o documento de consentimento para a partilha de informação demográfica existente na instituição e no ALERT® HIE e eliminar o documento de consentimento sobre a decisão individual automatizada sobre correlacionamento de pacientes, como é demonstrado na Figura 25.

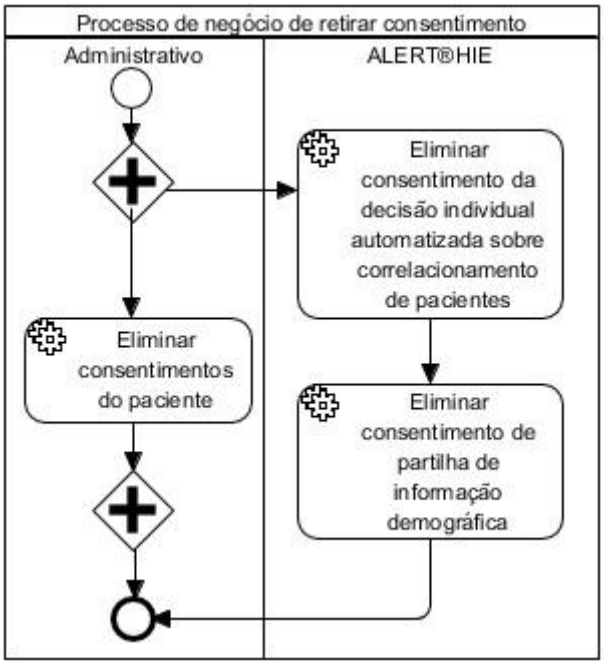


Figura 25 - Processo de negócio de retirar consentimento

4.3 ALERT® HIE

A ALERT contempla uma linha extensa de produtos, mas no âmbito deste documento apenas se focará no produto ALERT® HIE. O ALERT® HIE é um *software middleware* da ALERT que permite a interoperabilidade clínica entre diferentes instituições espalhadas geograficamente, baseando-se em padrões internacionais para a partilha de informação clínica. O ALERT® HIE permite a comunicação com os produtos ALERT® PAPER FREE HOSPITAL (ALERT® PFH), MyALERT® PERSONAL HEALTH RECORD (MyALERT®), ALERT® PRIVATE PRACTICE e ALERT® PRIMARY CARE, como também permite a integração e partilha de informação com produtos comercializados por organizações concorrentes.

Na Figura 26 é apresendo o diagrama de componentes com a possível interação do ALERT® HIE com os outros produtos ALERT® ou produtos de outras organizações.

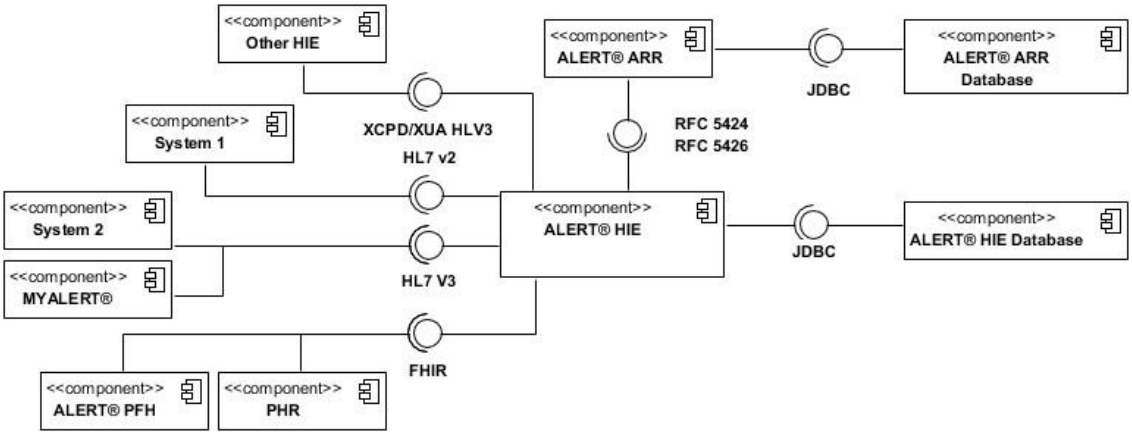


Figura 26 - Diagrama de componentes de contextualização do ALERT® HIE no sistema

4.3.1 Arquitetura ALERT® HIE

O componente ALERT® HIE é, portanto, o núcleo do sistema com vista a interoperabilidade. Na Figura 27 é apresentada uma vista lógica interna do componente ALERT® HIE.

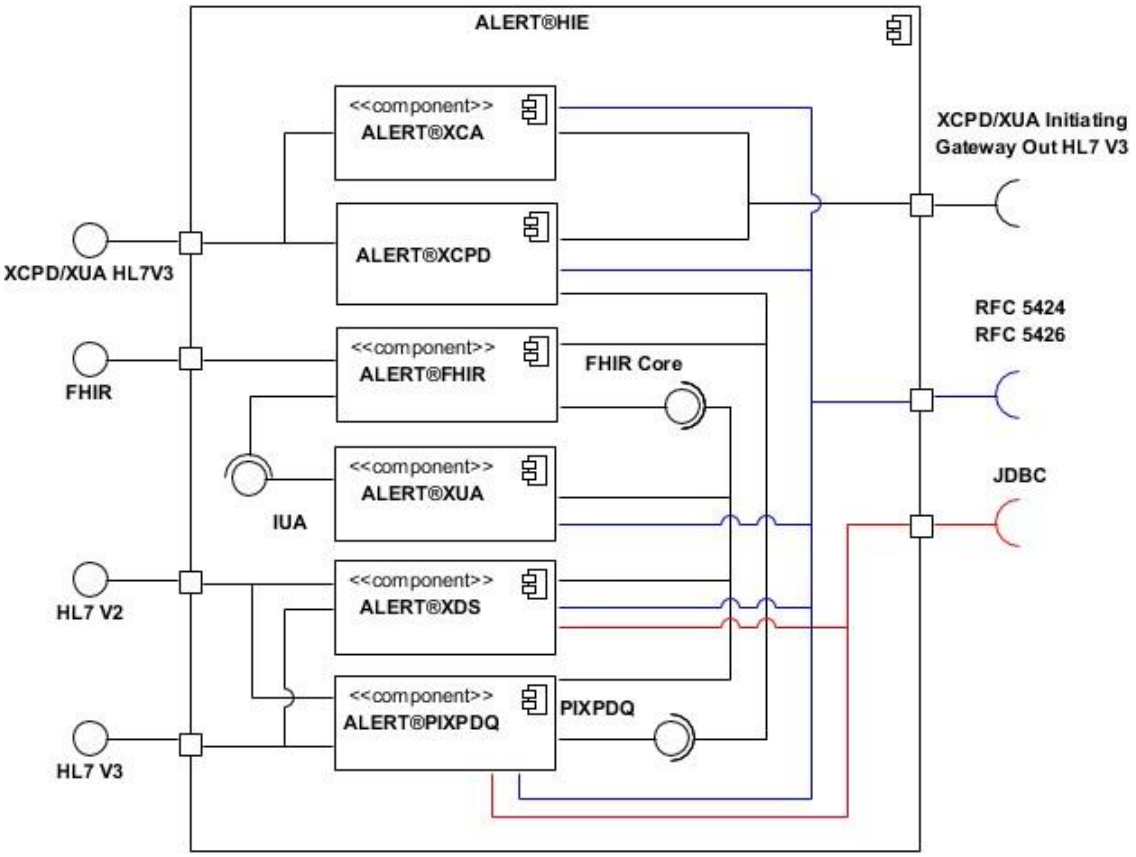


Figura 27 - Diagrama de componentes do ALERT® HIE

Cada um dos componentes internos do ALERT® HIE tem determinada responsabilidade para garantir a interoperabilidade clínica entre instituições:

- **ALERT® PIXPDQ (*Patient Identifier Cross-referencing & Patient Demographics Query*):** serviço que correlaciona as diferentes identificações dos pacientes, quando são criados em diferentes instituições dentro do mesmo domínio;

- **ALERT® XDS-REG (*Cross-Enterprise Document Sharing Registry*):** registo central contendo a lista de todos os documentos publicados no repositório ALERT® HIE;

- **ALERT® XDS-REP (*Cross-Enterprise Document Sharing Repository*):** repositório contendo os documentos clínicos do paciente;

- **ALERT® XCA (*Cross-Community Access*):** permite a pesquisa e obtenção de informação relevante sobre um paciente guardada em diferentes comunidades;

- **ALERT® XCPD (*Cross-Community Patient Discovery*):** permite a correlação do mesmo paciente com diferentes identificações e em diferentes domínios;

- **ALERT® XUA (*Cross-Enterprise User Assertion*):** fornece os meios para verificar a autenticidade de um utilizador, aplicação ou sistema que estejam fora do domínio da organização;

- **ALERT® XDS-AD (*Cross-Enterprise Document Sharing Affinity Domain*):** permite a partilha de informação entre um grupo de organizações que acordaram trabalhar juntos utilizando um conjunto de políticas comum e uma infraestrutura semelhante;

- **ALERT® FHIR (*Fast Healthcare Interoperability Resources*):** permite realizar as operações de transferências de documentos ou correlacionamento de pacientes através de uma interface RESTful;

- **ALERT® ARR (*Audit Record Repository*):** repositório central de logs para auditoria.

Estes componentes permitem que a interoperabilidade clínica aconteça não só entre as instituições que contemplam produtos ALERT® como também com outros produtos de organizações concorrentes, desde que suportem os diversos padrões de partilha utilizados no ALERT® HIE.

4.3.2 Tecnologia

O ALERT®HIE, como em vários projetos de *middleware* da ALERT, são desenvolvidos na linguagem Java com o auxílio da *framework* Spring (Spring, 2019a). O Spring contempla um vasto conjunto de bibliotecas e *frameworks* de modo a facilitar a implementação de projetos consoante as necessidades.

Para persistência de informação pessoal dos pacientes, bem como também a informação registada no EHR de cada paciente, recorre-se a uma base de dados relacional da Oracle (Oracle, 2019b).

O produto é executado num servidor aplicacional web, como por exemplo, o Apache Tomcat (2018) ou WebLogic da Oracle (2019c).

4.3.3 Algoritmo de correlacionamento de pacientes

Apesar da entrada em vigor do RGPD que permite que os cidadãos se oponham a decisões individuais automatizadas, também é possível que estes não se oponham a tal tratamento (cf. subsecção 3.1.9).

Nesse sentido, o ALERT® HIE dispõe dum algoritmo que faz o correlacionamento automático de EHR provenientes de diferentes instituições (i.e. identifica dois ou mais EHR distintos como sendo relativos ao mesmo paciente), comparando a informação demográfica dos dois EHR.

A informação demográfica num EHR inclui os seguintes atributos:

- Nome completo;

- Identificação do paciente:

    - Cartão de segurança social;

    - Bilhete de identidade;
    - Número de segurança social;
- Nome completo da mãe;
- Morada;
- Data de nascimento;
- Género;
- Raça;
- Língua nativa;
- Religião;
- Local de nascimento;
- Grupo étnico;
- Estado civil;
- Nacionalidade;
- Endereço de email;
- Número de telemóvel.

Ao realizar o cálculo de semelhança entre pares de EHR, o algoritmo de correlacionamento pode classificar os EHR com os seguintes estados de correlação:

- V – Válido;
- N - Não válido;
- C – Candidato;
- D – Rejeitado;
- A – Ativo.

Na Figura 28 é apresentado o diagrama de atividades com o fluxo do cálculo da percentagem de correlacionamento efetuado pelo algoritmo de correlacionamento do ALERT® HIE, e que apresenta o significado de cada um dos estados anteriores.

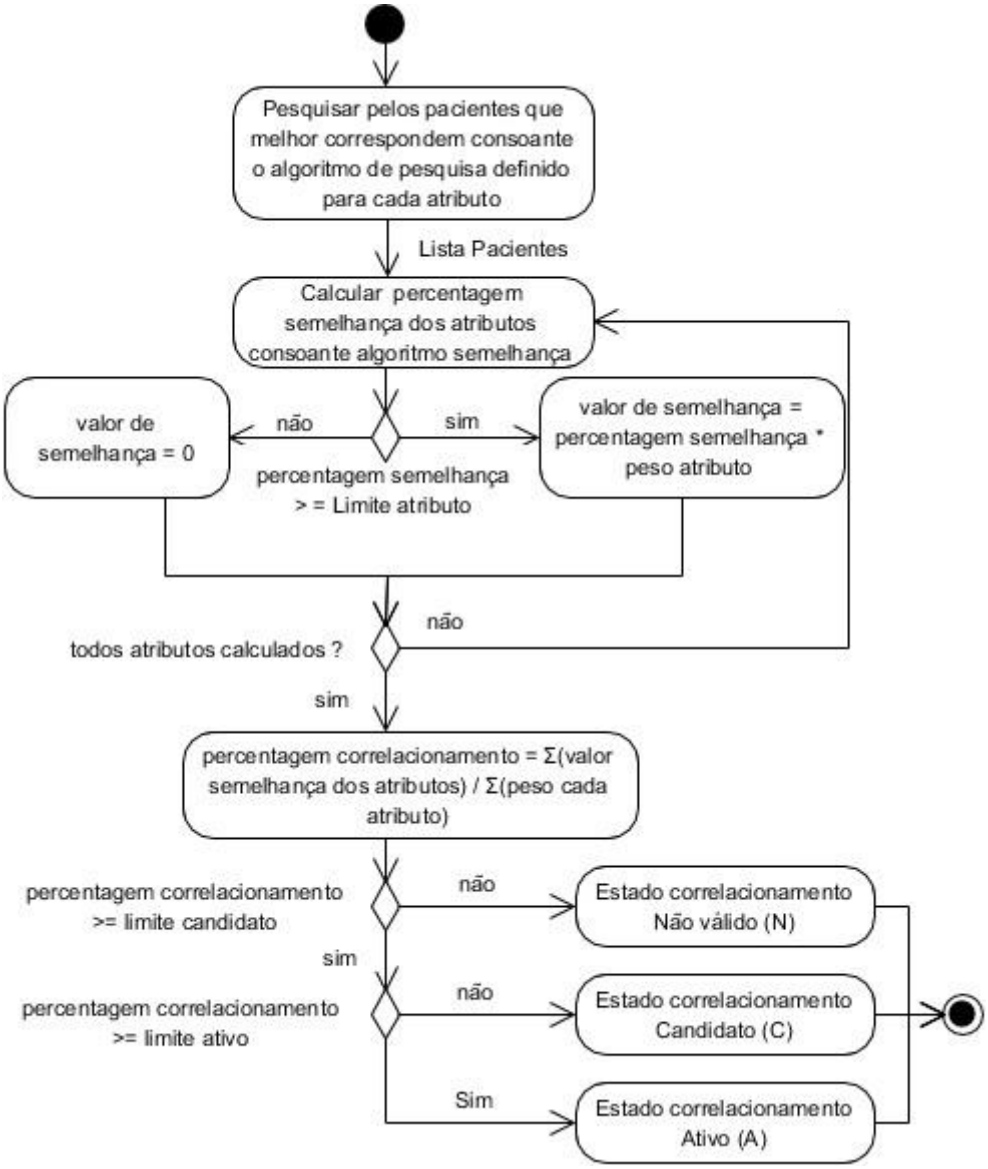


Figura 28 - Diagrama de atividades do algoritmo de correlacionamento

Por omissão, o algoritmo de correlacionamento utiliza apenas os atributos “nome completo”, “data de nascimento” e “género”, mas é possível incluir os outros atributos referidos.

Para cada atributo utilizado é necessário certas configurações:

- Peso relativo – indica o peso que o atributo terá no cálculo final do correlacionamento, sendo este apenas um valor numérico positivo (e.g. o atributo 1 tem um peso de 50, se se considerar que o atributo 2 tem o dobro do peso, o peso deste é 100);

- Limite – é um valor percentual entre 0 e 100, no qual o resultado da comparação terá de ser igual ou superior ao valor definido, de forma a que o atributo seja considerado no cálculo final.

- Algoritmo de pesquisa - o algoritmo de pesquisa a utilizar, de forma a obter as melhores correspondências por atributo;

- Algoritmo de cálculo de semelhança – o algoritmo para calcular a semelhança entre os atributos de informação. Caso o resultado obtido for inferior ao limite definido, o atributo terá como valor 0 a ser considerado no cálculo final.

Existem 5 tipos de algoritmos de pesquisa:

- Oracle Index Text (OIT) – utiliza as capacidades de pesquisa de texto da Oracle, utilizaando um algoritmo de frequência inversa baseado na medida cosseno de Salton[19]. Este algoritmo tem em consideração o quão comum um termo é;

- Lucene - é um motor de pesquisa de texto desenvolvido pela Apache (2019). O desempenho deste, normalmente, é melhor que o algoritmo OIT, mas não tem em consideração o quão comum um termo é;

- Distância de edição – consiste no número de edições necessárias para que a sequência 1 transforme-se na sequência 2. Este é baseado no algoritmo de Levenshtein[20];

- Comparação numérica – compara os atributos de informação de tipo numérico;

- Comparação de datas – compara os atributos de informação do tipo data.

Além disso, os algoritmos de pesquisa permitem algumas variações, tais como:

- Variações difusas - dá uma margem na comparação nos algoritmos. Isto é, permite uma variação mais acentuada. Esta variação é aplicada no algoritmo OIT e Lucene;

- Outras identificações do paciente (POI – *Patient Other Identifier*) – é utilizado nos atributos de identificação de paciente. Cada atributo de identificação está associado um OID que representa o tipo de identificação. Este não pode ser utilizado na comparação de identificações porque influenciará a comparação negativamente. Esta variação pode ser combinada com OIT e Lucene;

- Operadores lógicos e/ou – quando se utiliza o operador "e" todos as palavas contam para atingir o limite de semelhança, enquanto com o operador "ou" basta que uma palavra atinja o limite de semelhança para ser considerado. Os algoritmos OIT e Lucene podem adotar esta variação;

Já os algoritmos disponíveis para o cálculo de semelhança entre atributos são:

- Distância de edição - consiste no número de edições necessárias para que a sequência 1 se transforme na sequência 2. Este é baseado no algoritmo de Levenshtein;

[19]A pontuação de frequência inversa assume que os termos que são usados várias vezes num conjunto de documentos, são termos de ruído obtendo uma pontuação baixa. Já os termos que são apenas usados várias vezes num só documento obtêm uma pontuação alta (Oracle, 2019f).
[20]O algoritmo de Levenshtein consiste no número mínimo de edições de caracteres (i.e. inserção, eliminação, substituição) necessárias para transformar a primeira palavra na segunda (Babar, 2019).

- Igualdade – os atributos de informação terão de ser exatamente iguais senão o atributo não é considerado no cálculo.

Após serem calculados as semelhanças entre os atributos, é calculado o somatório de todos os atributos em que o paciente foi considerado ser o mesmo, tendo em consideração o peso do atributo anteriormente definido.

O valor percentual obtido indica a semelhança entre os pacientes. De forma a apurar se são ou não o mesmo paciente, é necessário definir dois limites:

- Limite candidato – se o valor percentual obtido do somatório dos atributos considerados for maior ou igual a este limite, a informação do paciente usada para inicializar o processo de correlacionamento é candidata a estar associada a outro paciente de outra instituição. Nestes casos, é atribuído ao resultado do correlacionamento a *flag* C (Candidato), sendo necessário, depois, uma decisão humana. Por omissão, o valor deste limite é 60%;

- Limite ativo - se o valor percentual obtido do somatório dos atributos considerados for maior ou igual a este limite, a informação do paciente usada para inicializar o processo de correlacionamento é similar à do paciente de outra instituição. Nestes casos, é atribuído ao resultado do correlacionamento a *flag* A (Ativo). Por omissão, o valor deste limite é 90%.

5 Design

Neste capítulo são (i) selecionadas as alternativas que ajudarão a resolver os problemas identificados e (i) é apresentada a nova arquitetura do produto ALERT® HIE.

5.1 Alternativas concetuais

Nas secções 2.4 e 2.5 foram apresentadas alternativas para ajudarem a resolver os requisitos identificados. No Anexo A, foi utilizado o método multicritério AHP de forma a selecionar as alternativas que melhor se ajustam consoante os critérios de avaliação definidos.

Quanto às alternativas Oracle TDE e VTE, de forma a resolver o requisito da **cifragem** da base de dados, a melhor alternativa a adotar é o Oracle TDE, com base nos resultados apresentados na subsecção A1.2. Porém, como a solução Oracle TDE acarreta custos e autorizações por parte da organização para a sua implementação, foi tomada a decisão de deixar a sua implementação fora do âmbito do projeto.

Quanto ao requisito do **consentimento**, foram apresentadas as alternativas BPPC, APPC e Consent2Share. Os resultados obtidos na subsecção A1.1 indicam que o APPC é a alternativa mais indicada para ajudar a resolver o problema do consentimento do paciente. Além disso, esta solução permitirá resolver o requisito da **oposição à decisão individual automatizada**.

Dito isto, nas secções 5.3 e 5.4 serão apresentadas as decisões arquiteturais tomadas com a adoção da solução APPC e no capítulo 6 será apresentada a sua implementação.

5.2 XACML

Esta secção apresenta os conceitos mais importantes do padrão XACML utilizado pela solução APPC, que influenciarão os artefactos de desenho elaborados de forma a responder aos requisitos identificados na secção 3.2.

Tal como foi descrito na secção 2.4.2, o XACML é um padrão desenvolvido pela organização OASIS que:

- Define uma arquitetura que adota um conjunto de componentes e apresenta a interação entre estes com o objetivo de definir um mecanismo de autorizações;
- Define um modelo de domínio que deverá ser utilizado para formulação das políticas de privacidade, bem como a definição de pedidos de acesso e as respetivas respostas;
- Define ainda um conjunto de regras a utilizar para estabelecer a correlação entre os pedidos e as políticas de privacidade definidas (cf. (OASIS, 2005)).

Nas subsecções seguintes serão explicados cada um dos aspetos referidos.

5.2.1.1 Arquitetura

Dentro da arquitetura do XACML existem cinco componentes:

- Policy Enforcement Point (PEP);
- Policy Decision Point (PDP);
- Policy Information Point (PIP);
- Policy Retrieval Point (PRP);
- Policy Administration Point (PAP).

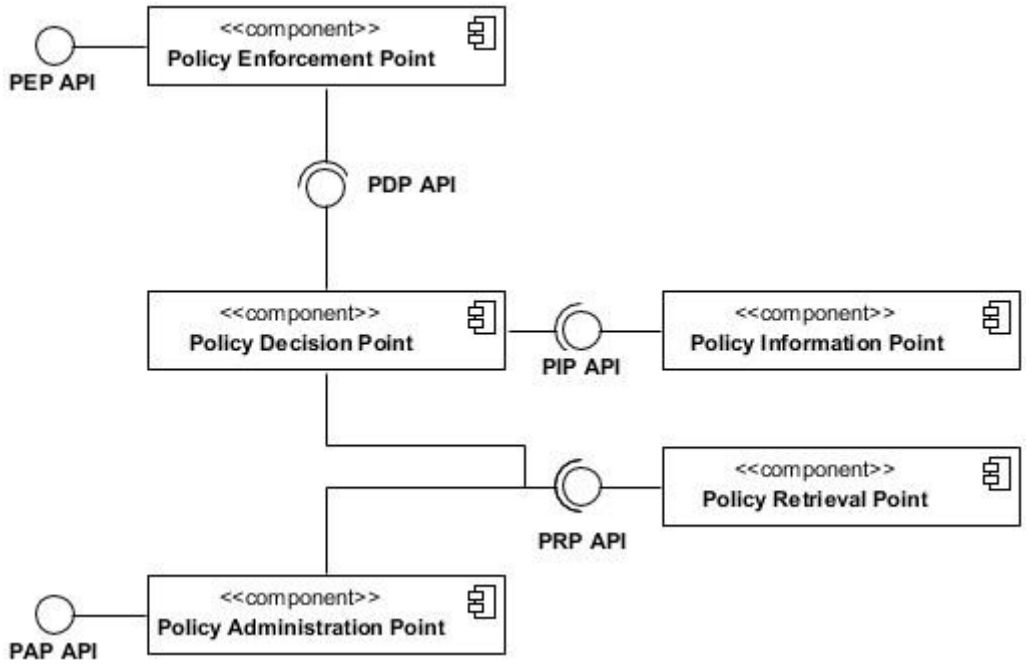


Figura 29 - Arquitetura do padrão XACML [adaptado de (Axiomatics, 2019)]

Na Figura 29 são apresentadas as interações entre cada um dos componentes anteriormente apresentados. O PAP, acedido por aplicações terceiras via a API PAP, é responsável por gerir as

políticas de privacidade que posteriormente serão utilizadas pelo PDP. O PRP é o componente responsável por persistir as políticas de privacidade geridas pelo PAP. O PEP é o componente que tem a responsabilidade de formular os pedidos de acesso e com base na decisão tomada permitir ou negar o acesso ao recurso. O PDP é o componente que toma a decisão com base no pedido recebido e nas políticas de privacidade existentes. O PIP é o componente com o intuito de obter a informação adicional sempre que o PDP necessita quando este não consegue tomar uma decisão.

5.2.1.2 Modelo de domínio das políticas de privacidade

O XACML define o seu próprio modelo de domínio para as políticas de privacidade, conforme é ilustrado na Figura 30. Uma política de privacidade (**Policy**) tem sempre associada um alvo a que se destina (**Target**) como também o algoritmo de combinação de regras (**Rule Combining Algorithm**). A política poderá ter um conjunto de regras (**Rule**), assim como um conjunto de obrigações (**Obligation**).

As políticas de privacidade podem ser agrupadas num conjunto de políticas de privacidade (**PolicySet**) que contêm sempre um algoritmo de combinação de políticas (**Policy Combining Algorithm**) e o alvo a que o conjunto de políticas se destina (**Target**). Um **PolicySet** poderá conter outros **PolicySet**, como também políticas de privacidade e obrigações (**Obligation**) a cumprir dependendo da decisão após a avaliação.

A regra (**Rule**) tem sempre um efeito (**Effect**), poderá ter uma condição (**Condition)** como também um alvo (**Target**).

O alvo (**Target)** é constituído por:

- Sujeito(s) (**Subject)** – representam as características do utilizador que está a fazer o pedido;
- Recurso(s) (**Resources**) - constituem os recursos a que o utilizador está a tentar aceder;
- Ação (**Action**) - representam as possíveis ações que o utilizador faz quando tenta aceder a determinado recurso;
- Meio ambiente (**Environment**) - representa em que condições os pedidos foram feitos.

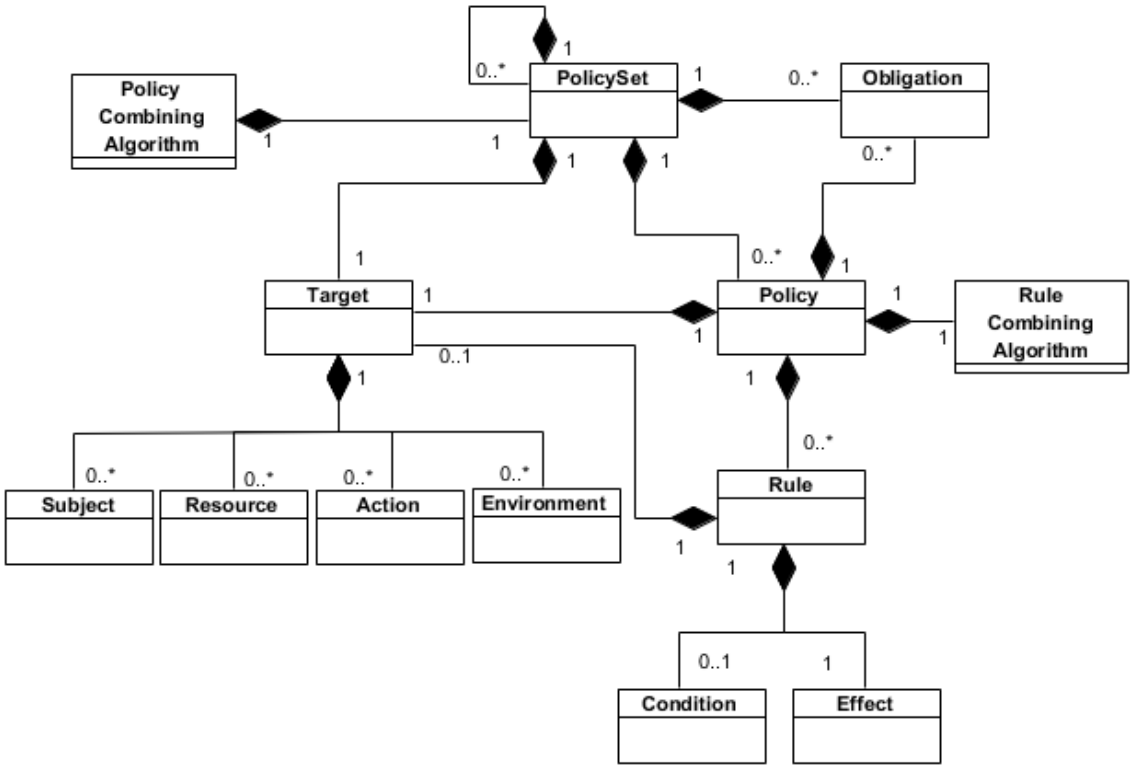


Figura 30 - Modelo de domínio das políticas de privacidade [adaptado de (OASIS, 2005, p. 19)]

5.2.1.3 Modelo de domínio de contexto

O XACML também define o modelo de domínio a utilizar na formulação de pedidos de acesso e as respetivas respostas com os resultados, como é demonstrado na Figura 31. O pedido de acesso (**Request**) é constituído por:

- Uma ou mais características do utilizador que está a fazer o pedido (**Subject**);
- Um ou mais recursos a que está a tentar aceder (**Resource**);
- A ação que está a realizar (**Action**);
- O meio ambiente em que o pedido está a ser executado (**Environment**).

A resposta (**Response**) é constituída por um resultado (**Result**) que contém uma decisão (**Decision**), um estado (**Status**) e zero ou mais obrigações que vão ter que ser aplicadas para que se possa dar autorização consoante a decisão tomada (**Obligation**).

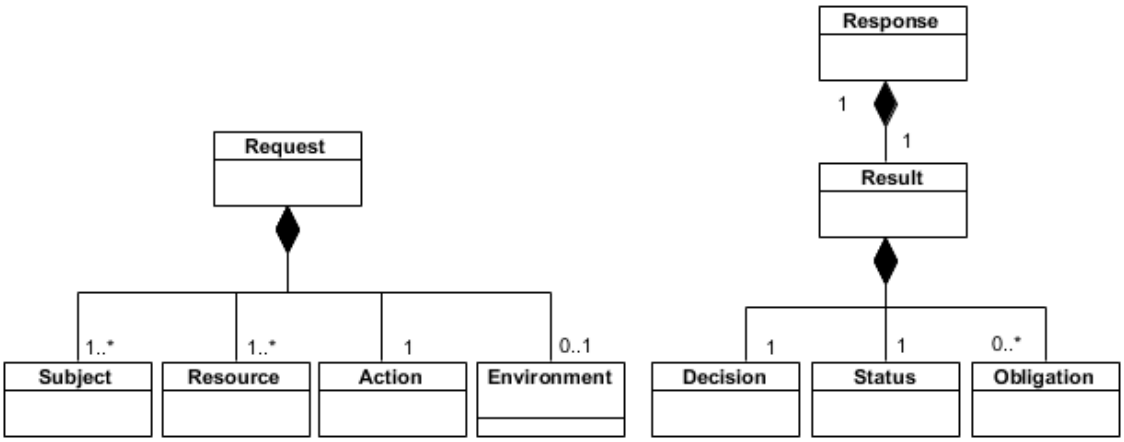


Figura 31 - Modelo de domínio sobre os pedidos e respostas

5.3 Arquitetura ALERT® HIE

Esta secção apresenta a nova arquitetura do ALERT® HIE e os seus novos componentes e excertos de modelo relacional relevantes para dar respostas aos requisitos identificados.

5.3.1 Arquitetura de sistema do ALERT® HIE

Com os problemas e requisitos identificados, é necessário desenhar uma nova arquitetura com novos componentes que permitirão responder aos problemas identificados.

Com a adoção do perfil de integração APPC da IHE, de forma a resolver o problema do consentimento do paciente no ALERT® HIE, foi necessário alterar a arquitetura do sistema que se interliga com o ALERT® HIE, sendo possível visualizar as diferenças na Figura 32 com a arquitetura apresentada na Figura 26.

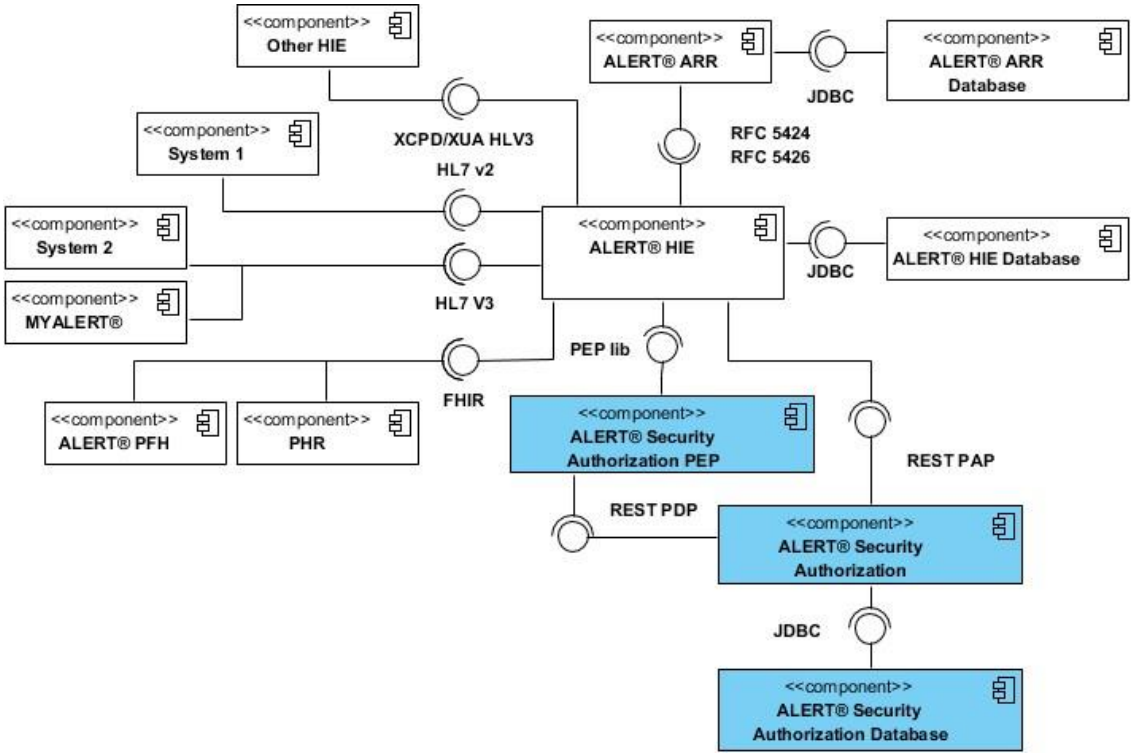


Figura 32 - Diagrama de contextualização do ALERT® HIE (granularidade de sistema)

Existem três novos componentes, face à arquitetura apresentada na Figura 26:

- ALERT® Security Authorization – responsável por conter toda a lógica de negócio do padrão XACML, representando os componentes PAP e PDP do padrão XACML;
- ALERT® Security Authorization PEP – responsável por formular os pedidos de acesso para o ALERT® Security Authorization, corresponde ao componente PEP do XACML;
- ALERT® Security Authorization Database – responsável por persistir as políticas de privacidade, representando o componente PRP do padrão XACML.

Já no componente ALERT® HIE foi desenvolvido um novo componente responsável por conter a lógica do perfil APPC, denominado ALERT® APPC. Este consome as interfaces providenciadas pelo ALERT® Security Authorization e ALERT® Security Authorization PEP, conforme é possível visualizar pelo diagrama de componentes apresentado na Figura 33.

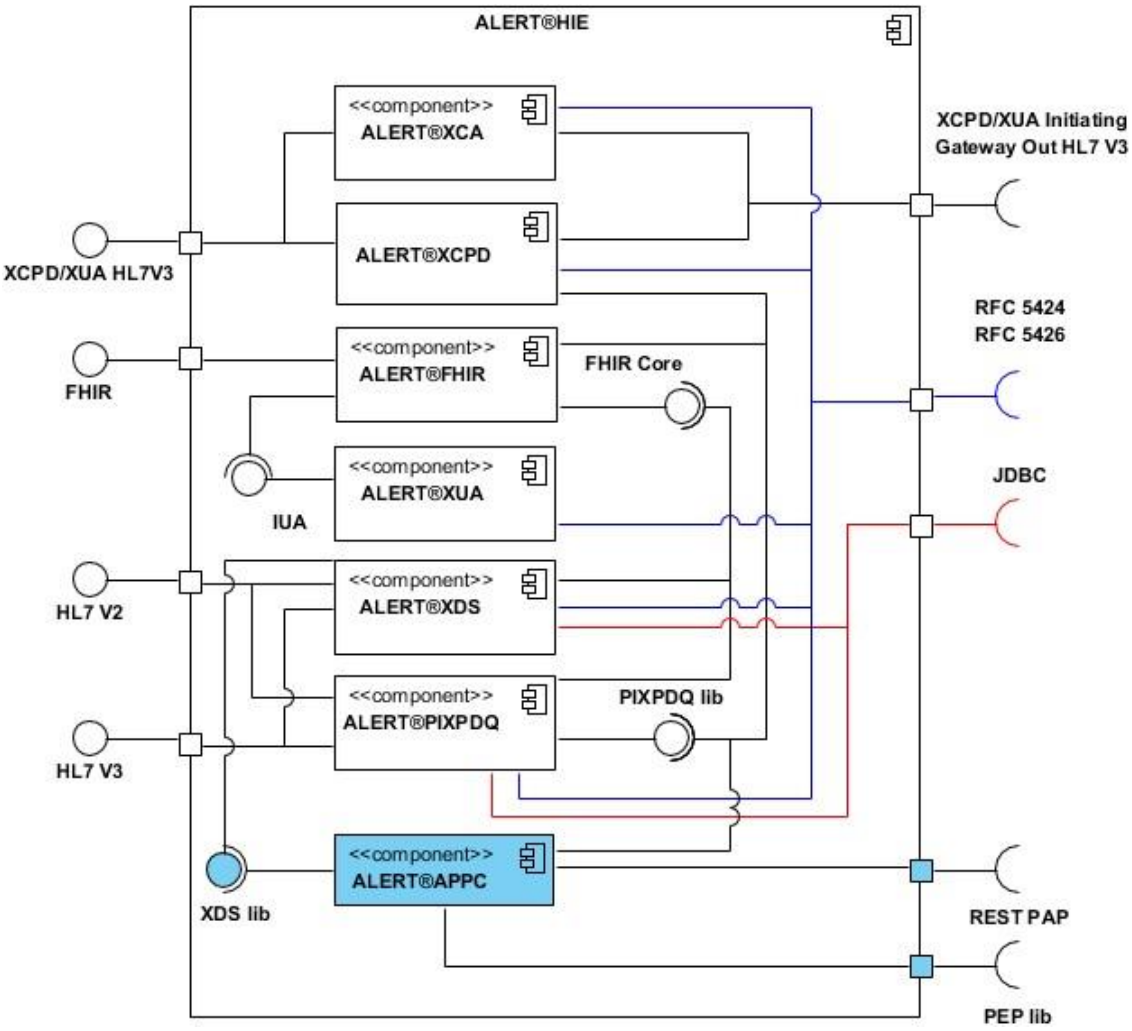


Figura 33 - Diagrama de componentes do ALERT® HIE

5.3.2 Arquitetura do ALERT® APPC

Como referido na subsecção 2.4.2.2, o perfil de integração APPC pressupõe a utilização de outros perfis de integração da IHE para o seu funcionamento. O XDS é um perfil de integração da IHE que permite a partilha de documentos associados ao paciente. Dito isto, o APPC utiliza este perfil para partilhar os seus documentos de consentimento, sendo necessário que tenham a extensão "xml" e nos seus metadados o formato do APPC correspondente ao UUID [21] "urn:ihe:iti:appc:2016:consent" (IHE ITI Technical Committee, 2018b, p. 67; Integrating the HealthCare Enterprise, 2019).

Conforme foi apresentado nos conceitos de negócio na secção 4.1, o ALERT® HIE processa transações. Estas passam por vários estados durante o seu fluxo de vida, como é apresentado na Figura 34.

[21] Um *Universally Unique Identifier* (UUID) é um identificador que permite identificar pacientes, documentos, entre outros (Integrating the HealthCare Enterprise, 2017).

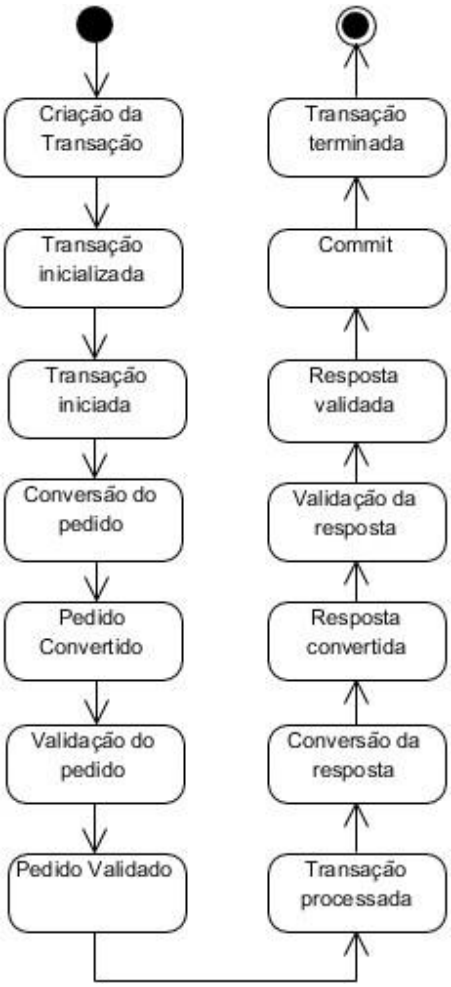


Figura 34 - Diagrama de estados do fluxo de vida de uma transação

Devido a este fluxo existente em todas as transações, é possível utilizar o padrão comportamental observador [22] e adicionar comportamentos adicionais. Na Figura 35 é apresentado um diagrama com todas as classes que estão envolvidas para espoletar a notificação aos observadores. Já na Figura 36 é apresentado um diagrama com a lógica de notificação aos observadores já existente no ALERT® HIE.

[22] O padrão observador permite criar um relacionamento entre a classe "Sujeito" e a classe "Observador", em que a classe "Sujeito" é responsável por notificar os seus observadores quando a sua informação ou estado se alteram, de forma a aplicar lógica de negócio adicional (Taibi, 2007, p. 11).

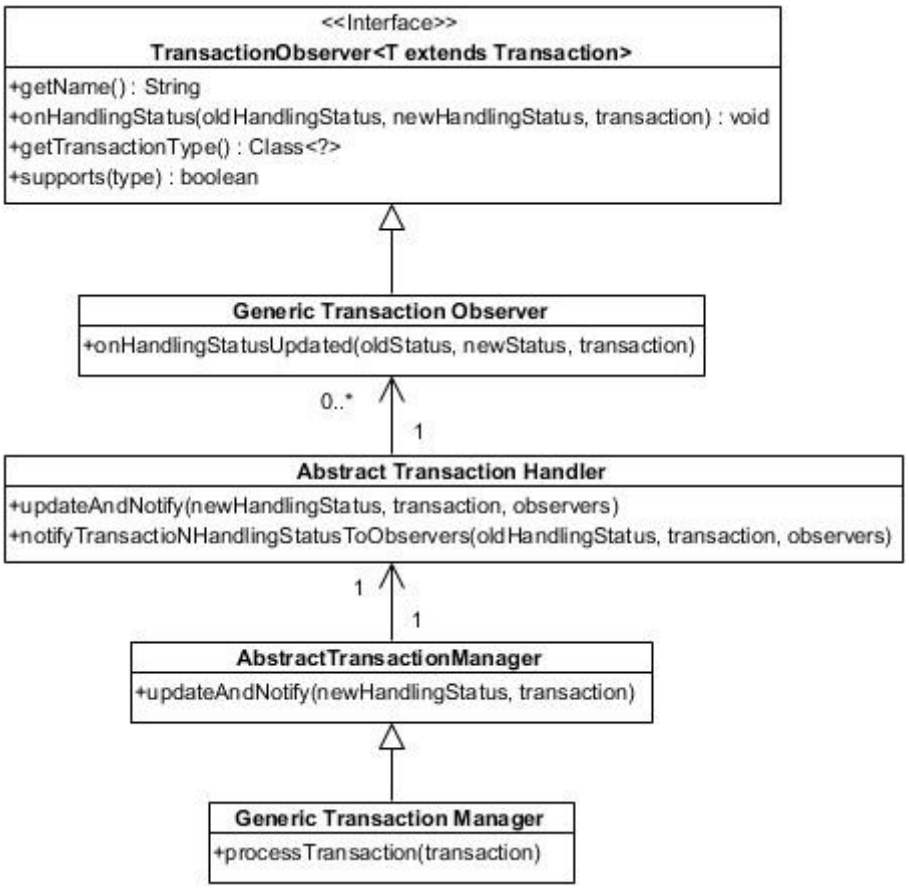


Figura 35 - Diagrama de classes da gestão do fluxo de vida da transação

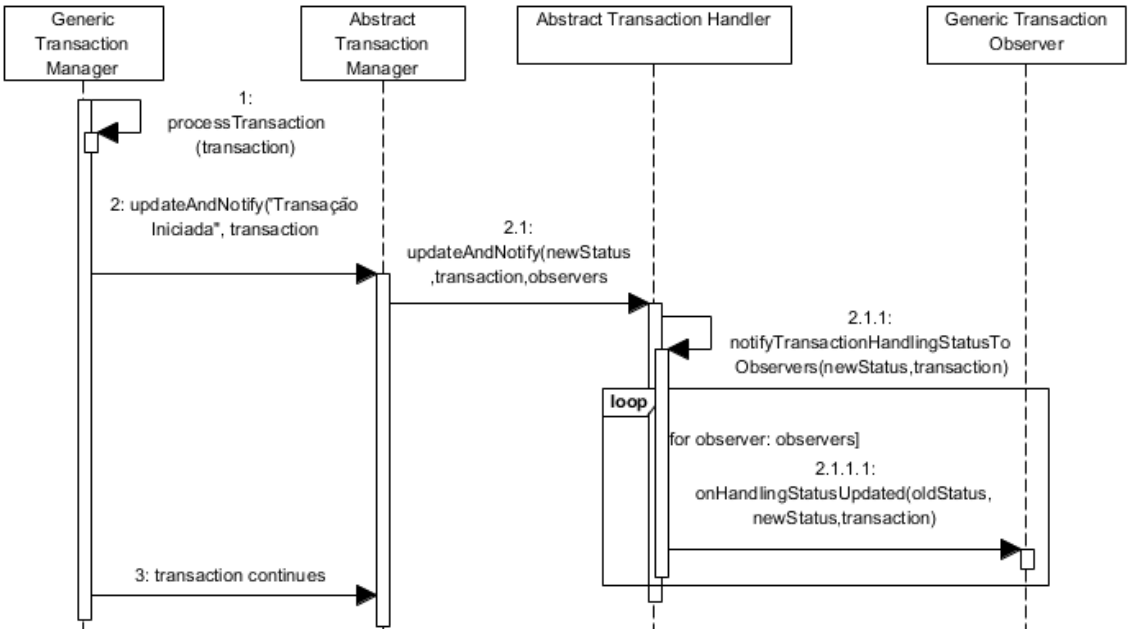


Figura 36 - Diagrama de sequência do padrão observador no ALERT® HIE

Na Figura 37 é ilustrada a estrutura de *packages* do componente ALERT® APPC, em que no *package* "com.alert.hie.appc.observer" estará a implementação dos observadores necessários para implementar o perfil APPC. Já no *package* "com.alert.hie.appc.observer.db" estarão as classes necessárias para acesso aos conteúdos da base de dados do ALERT® HIE que os observadores podem necessitar.

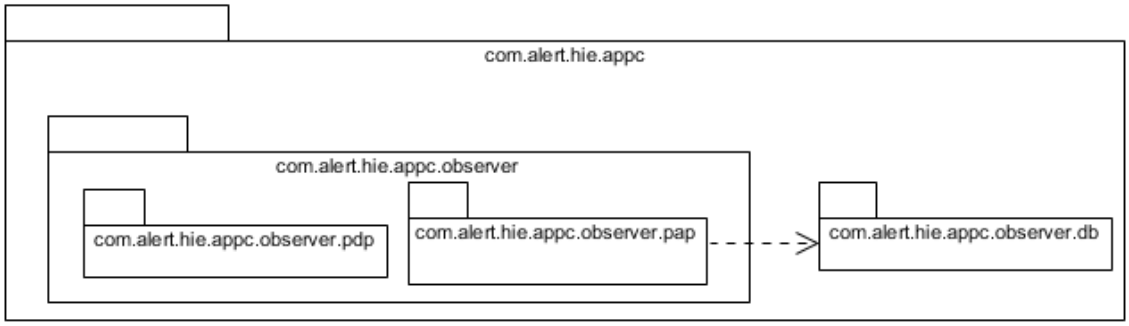


Figura 37 - Diagrama de packages do componente ALERT® APPC

5.3.2.1 Criação das políticas de consentimento

O documento de consentimento do paciente pode ser representado por mais que um documento. Contudo, deverá existir um documento raiz em que terá de ser do tipo "PolicySet" do XACML e que terá de referenciar os outros documentos, conforme é especificado no perfil APPC (IHE ITI Technical Committee, 2018b, p. 31). A Figura 38 demonstra um exemplo de hierarquia de políticas de consentimento que é possível definir com o perfil APPC.

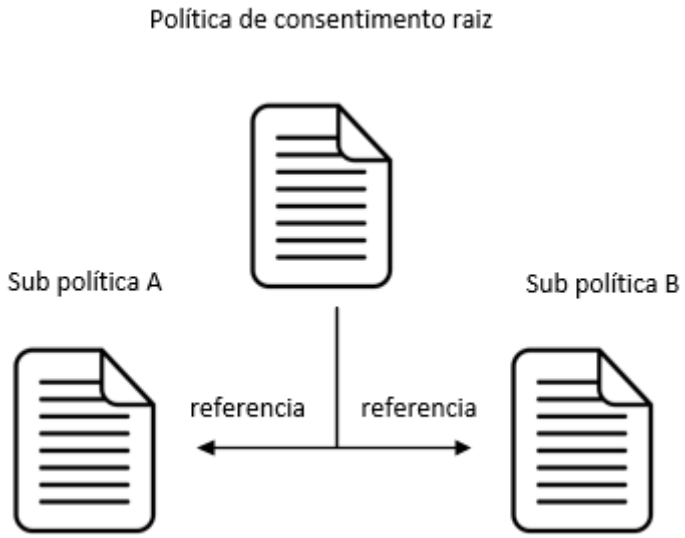


Figura 38 - Exemplo de hierarquia de políticas com o perfil APPC

De forma a armazenar as políticas de consentimento do paciente, é necessário intercetar a transação de partilha documentos do perfil de integração XDS. O observador irá verificar todas as transações de partilha de documentos e verificar quais dos documentos partilhados são do tipo APPC através do atributo *format code* existente em cada documento (IHE ITI Technical Committee, 2018c, pp. 73–74), com o código dos documentos APPC apresentado anteriormente. Os documentos que forem deste tipo passarão por uma verificação que consiste

em averiguar se são o documento de consentimento raiz do paciente segundo a especificação do perfil APPC (IHE ITI Technical Committee, 2018b, p. 31) para posteriormente ser facilmente identificado quando for necessário avaliar as políticas do consentimento. Após todos os documentos de consentimento estarem criados no ALERT® Security Authorization Framework é necessário auditar a persistência do consentimento do paciente. Na Figura 39 é demonstrado o processo de criação e persistência das políticas de consentimento.

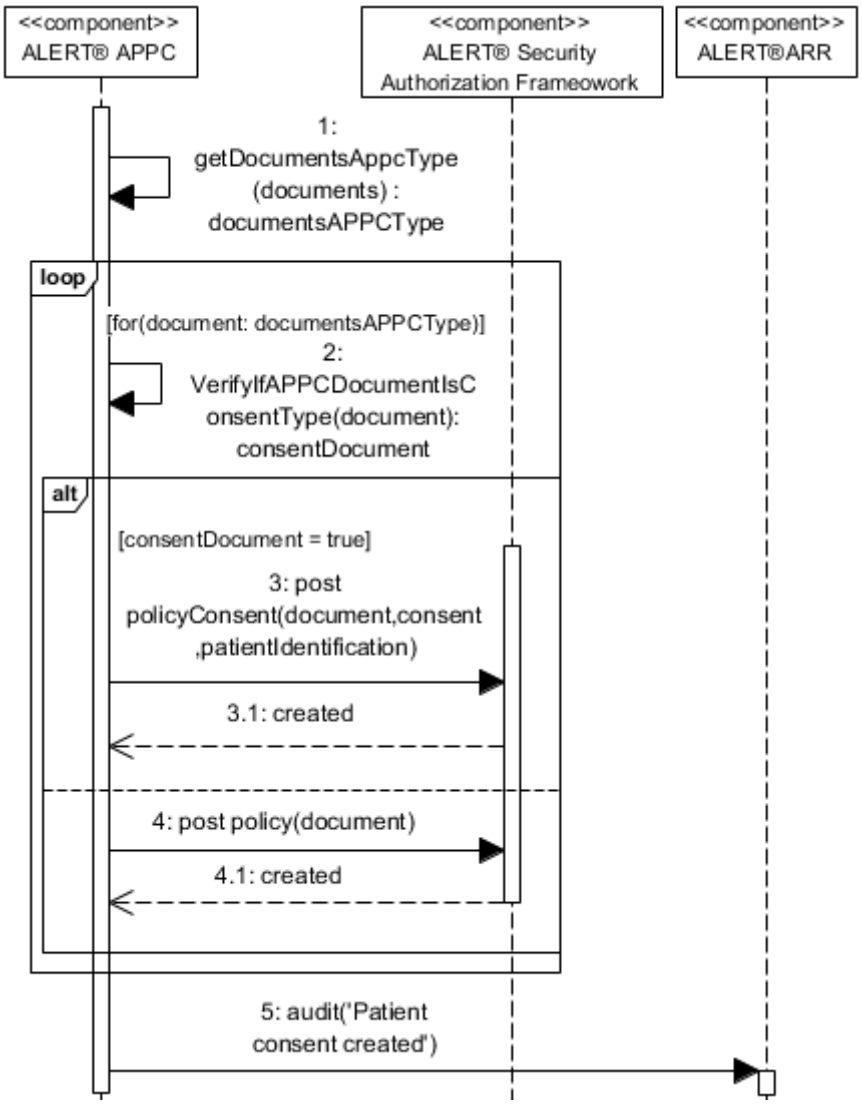


Figura 39 - Diagrama de sequência entre componentes para criação de políticas de consentimento

5.3.2.2 Oposição à decisão individual automatizada

Quanto ao requisito funcional de oposição à decisão individual automatizada, ao partilhar as políticas de consentimento relacionadas com o paciente, deverá existir uma política sobre o consentimento à decisão individual automatizada do algoritmo de correlacionamento de informação de pacientes. Ao partilhar as políticas de consentimento, o observador que interceta a transação de partilha de informação irá verificar se existe alguma política deste tipo. Caso exista, irá atualizar a decisão do paciente sobre o correlacionamento na base de dados do

ALERT® HIE e posteriormente armazenar a política de privacidade no ALERT® Security Authorization Framework. Caso o paciente decida mudar de ideias, bastará atualizar esta política com a decisão do paciente e partilhar novamente no ALERT® HIE. A Figura 40 apresenta o fluxo no ALERT® APPC para oposição à decisão individual automatizada.

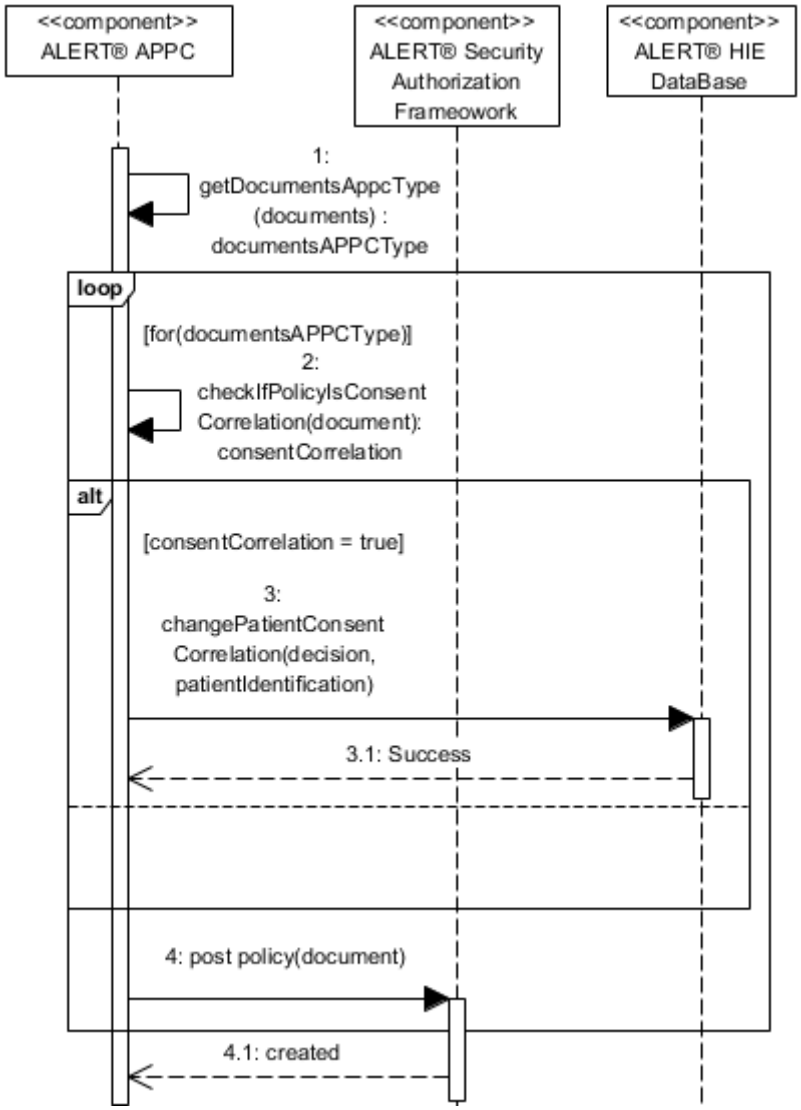


Figura 40 - Diagrama de sequência de oposição à decisão individual automatizada

O consentimento sobre a decisão individual automatizada do paciente é persistido também na base de dados do ALERT®HIE devido à atual implementação do algoritmo ser na própria base de dados. Esta decisão é motivada pela perda de desempenho do algoritmo de correlacionamento, caso este tivesse de comunicar com o ALERT® Security Authorization Framework de forma a saber se cada par de pacientes avaliado consentiu a decisão individual automatizada.

5.3.2.3 Retirar consentimento

Como foi dito na subsecção 3.1.1.1, os pacientes podem retirar o seu consentimento de partilha de informação a qualquer momento. É pressuposto que todos os documentos relacionados com

o perfil APPC estejam dentro de uma única pasta no seu EHR, de forma a que, quando o paciente quiser retirar consentimento, baste eliminar a pasta que contém todos estes documentos.

Para a realização deste requisito funcional é necessário criar um observador para a transação de eliminar documentos partilhados, que irá atuar após o pedido de eliminação dos documentos partilhados ser validado. Como nesta transação só são enviados os identificadores dos documentos, é necessário consultar na base de dados do ALERT®HIE se estes identificadores correspondem aos documentos do tipo APPC. Caso sejam, é retornada a identificação do paciente. Após isso, é feito um pedido REST com a operação *delete* ao componente ALERT® Security Authorization Framework com a identificação do paciente, que terá a responsabilidade de eliminar todas as políticas relacionadas com o paciente. Depois da eliminação dos documentos relacionados com o consentimento do paciente é necessário auditar a eliminação deste consentimento. Na Figura 41 é apresentado o fluxo de retirar consentimento no ALERT®HIE.

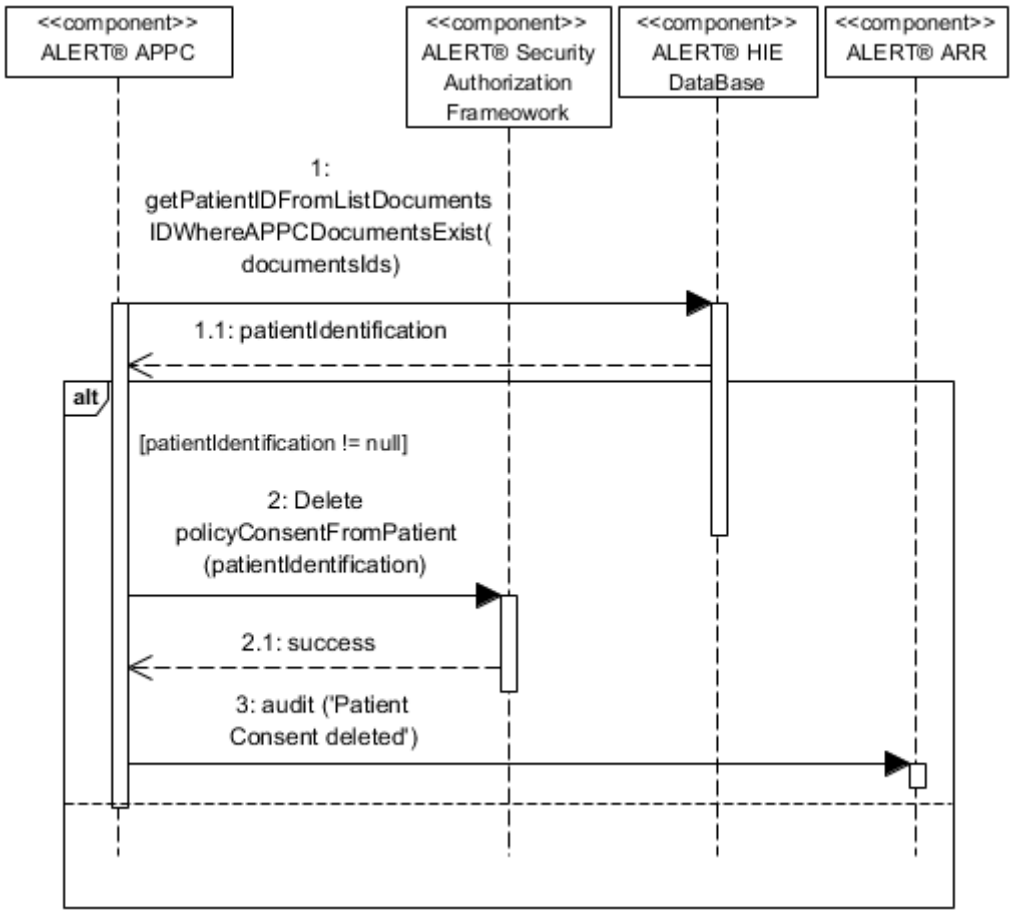


Figura 41 - Diagrama de sequência de retirar consentimento do ALERT®HIE

5.3.2.4 Pedido de Acesso

De modo a realizar o requisito de consultar informação e documentos do paciente, é necessário que as políticas de consentimento estejam previamente criadas e associadas ao paciente. Para verificar o acesso por parte da instituição à informação do paciente é necessário criar um observador que irá enviar a informação necessária para (i) formular o pedido ao ALERT®

Security Authorization PEP sobre o sujeito que está a fazer o pedido, (ii) o recurso que está a tentar aceder e (iii) a ação que pretende realizar como também, se necessário, (iv) o meio ambiente em que está a ser realizado o pedido. Após o ALERT® Security Authorization PEP ter enviado o pedido ao ALERT® Security Authorization Framework e receber o resultado do pedido de acesso, este dará ou não acesso ao recurso. Caso der acesso ao recurso, é necessário auditar este resultado e a transação continuará normalmente. Caso contrário, o resultado será auditado na mesma, mas será levantada uma exceção na transação que parará a transação, não retornando a informação que a instituição estava a tentar aceder. Na Figura 42 é apresentado o fluxo acima descrito.

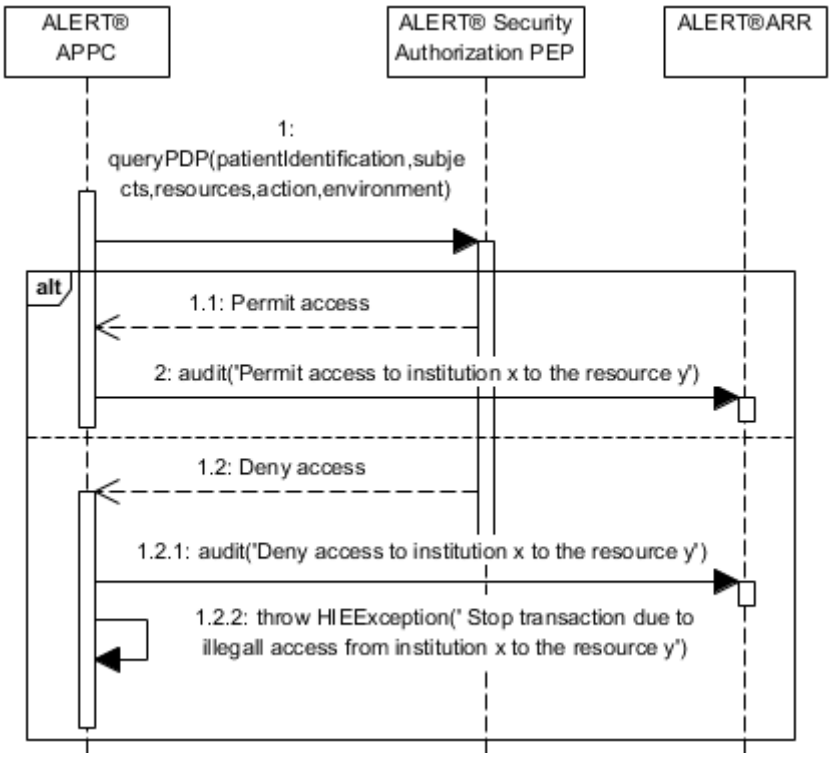


Figura 42 - Diagrama de sequência de verificar acesso a informação do paciente

5.3.3 Modelo relacional

Nesta subsecção serão apresentados os modelos relacionais já implementados na solução e respetivas atualizações necessárias para resolver os problemas identificados.

O ALERT®HIE utiliza uma base de dados do tipo relacional, tal como foi mencionando na subsecção 4.3.2, permitindo assim persistir as informações pessoais e clínicas dos pacientes. De modo a resolver alguns dos requisitos identificados, é necessário haver alguma interação com este componente de forma a obter a informação necessária para concluir os requisitos.

5.3.3.1 Modelo relacional dos pacientes

Na Figura 43 é ilustrado um excerto do modelo relacional do ALERT®HIE, focado nas entidades que fazem parte do algoritmo de correlacionamento de pacientes. Devido aos motivos

mencionados na subsecção 5.3.2.2, foi necessário adicionar uma nova coluna na tabela do paciente (Patient_Record) para guardar a decisão do paciente sobre o consentimento à decisão individual automatizada (i.e. fig_correlation_consent no diagrama da Figura 43).

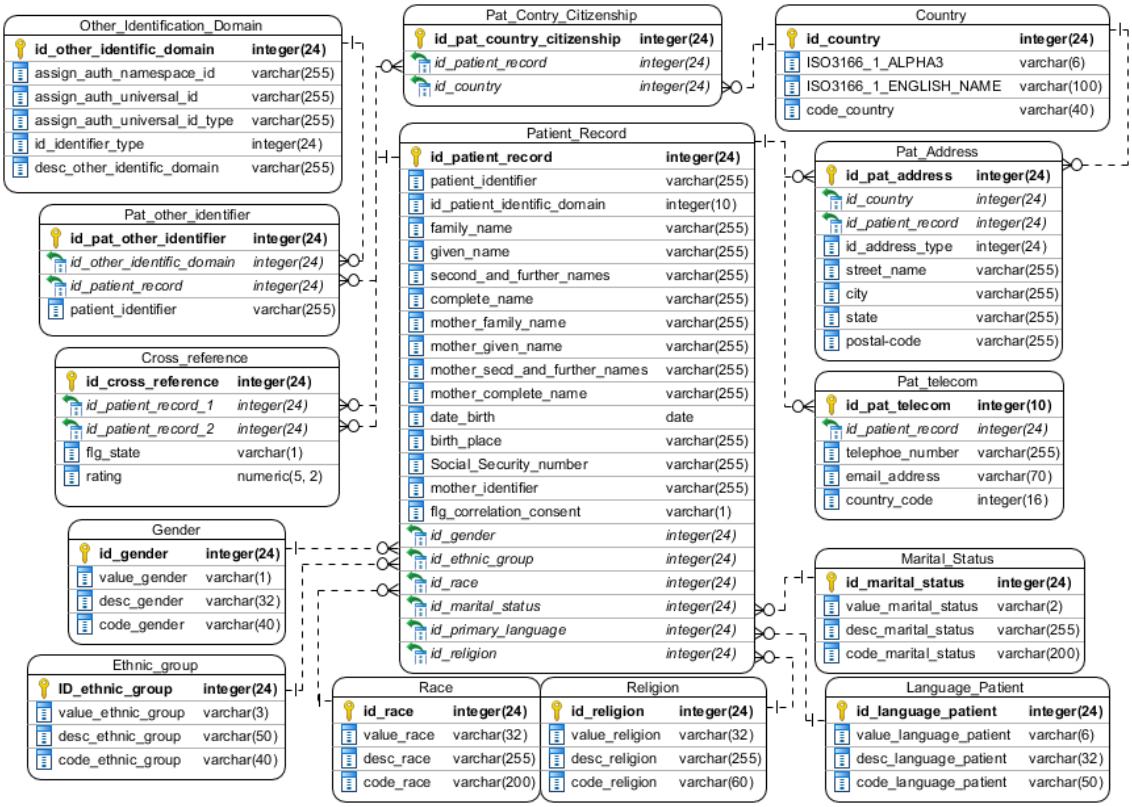


Figura 43 - Modelo relacional dos pacientes no ALERT® HIE

5.3.3.2 Modelo relacional dos documentos

Como o perfil de integração APPC utiliza o perfil XDS para a partilha dos documentos de consentimento do paciente, estes documentos são persistidos no ALERT®HIE como todos os outros tipos de documentos.

A remoção do consentimento pressupõe a utilização da transação de eliminar documentos do perfil XDS. Contudo, como foi mencionado na subsecção 5.3.2.3, nesta transação só são enviados os identificadores dos documentos que devem ser eliminados. Visto que o consentimento também é persistido no ALERT® Security Authorization Framework, é necessário obter a identificação do paciente de forma a retirar as políticas de consentimento deste último componente. Na Figura 44 é apresentado o modelo relacional simplificado sobre a persistência dos meta dados dos documentos. Os identificadores dos documentos representam a coluna "entry_uuid" da entidade "XDS_Object", que por sua vez está relacionada com a entidade "Metadata_object" que conhece a identificação do paciente (entidade "Identifier") e a entidade "Document". Esta última conhece o *format_code* utilizado através de uma chave estrangeira à entidade "Code". Assim é possível verificar que o documento é do tipo APPC através do código de formato que deve existir na entidade "Code" e retornar o paciente a quem o documento pertence.

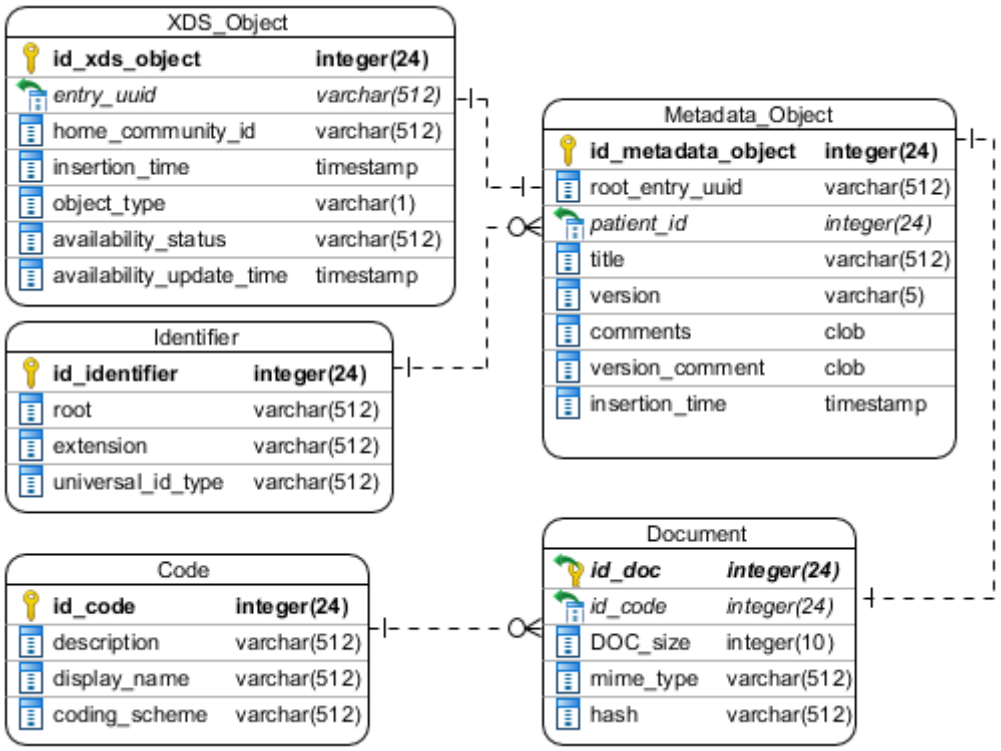


Figura 44 - Modelo relacional dos metadados dos documentos do paciente

5.4 Arquitetura ALERT® Security Authorization

O ALERT® Security Authorization é a implementação do padrão XACML da ALERT. A Figura 45 apresenta a vista lógica da arquitetura deste, e nas subsecções seguintes serão apresentadas as especificações mais detalhadas dos seus componentes.

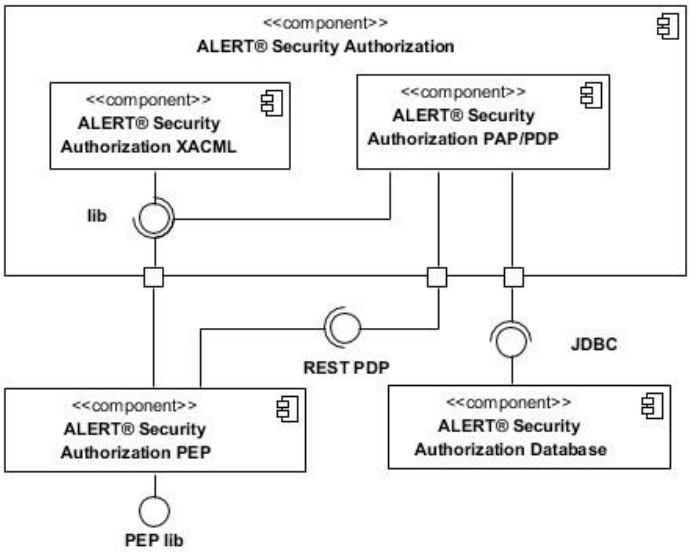


Figura 45 - Diagrama de componentes do ALERT® Security Authorization

5.4.1 Arquitetura ALERT® Security Authorization XACML

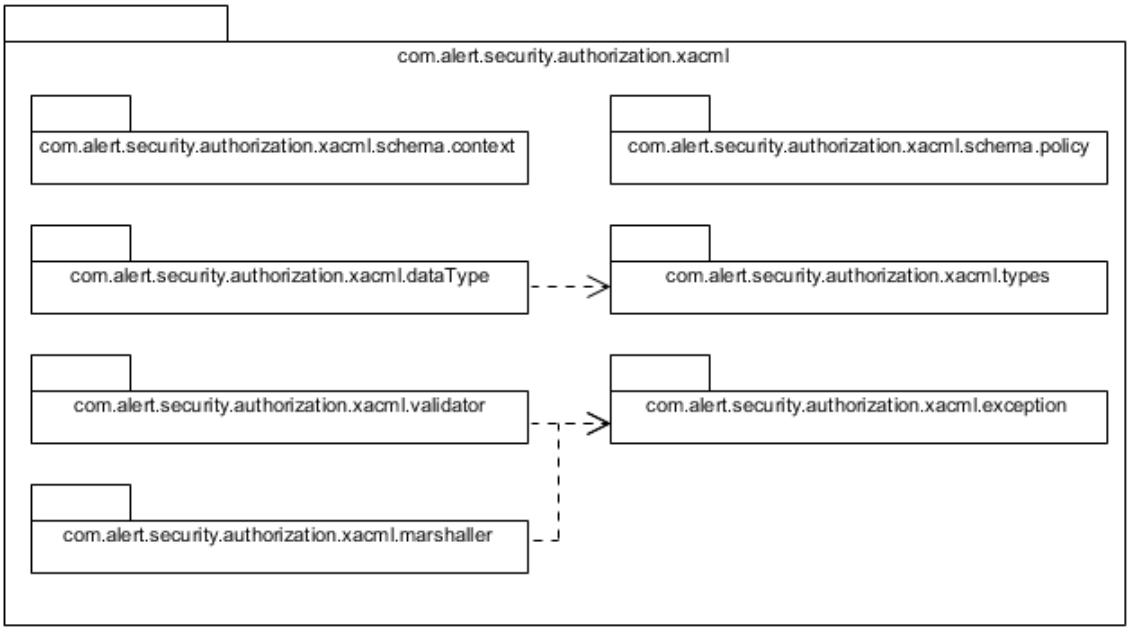


Figura 46 - Diagrama de packages do componente ALERT® Security Authorization XACML

Na Figura 46 é apresentado o diagrama de *packages* do componente ALERT® Security Authorization XACML. Este componente deve conter todo o tipo de lógica do XACML que possa ser reaproveitada em mais que um componente, por exemplo:

- Modelo de domínio para as políticas de privacidade;
- Modelo de domínio para formulação de pedidos/respostas;
- Exceções personalizadas;
- Tipos de dados que a solução suporta;
- Validador de ações das políticas e pedidos.

5.4.2 Arquitetura ALERT® Security Authorization Framework

O componente ALERT® Security Authorization Framework contém a lógica dos componentes PAP e PDP do padrão XACML apresentado na subsecção 5.2.1.1.

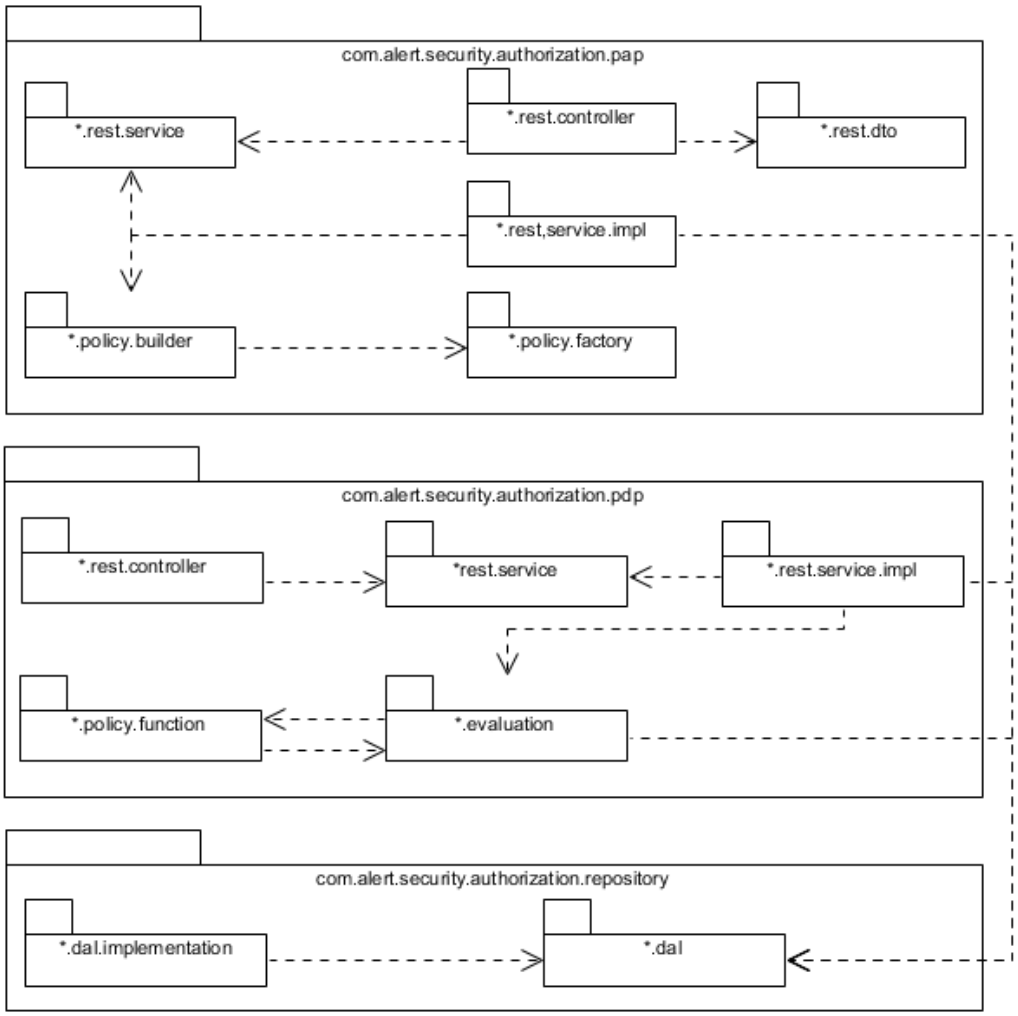


Figura 47 - Diagrama de packages do componente ALERT® Security Authorization Frameowrk

De modo a separar a lógica de negócio que os componentes PAP e PDP necessitam, definiu-se que toda a lógica referente ao PAP fica dentro do package "com.alert.security.authorization.pap". A lógica referente ao PDP fica dentro do "com.alert.security.authorization.pdp" e a lógica de acesso e manipulação das políticas na base de dados fica dentro do package "com.alert.security.authorization.repository", como é demonstrado no diagrama de *packages* da Figura 47.

Foi implementada uma lógica semelhante em cada um dos *packages* que expõe serviços REST, sendo que cada um desses *packages* contém um *package* "rest.services", que por sua vez contém interfaces com métodos que os controladores utilizam para obter a lógica que necessitam consoante o pedido REST que recebem.

5.4.2.1 PAP

A função do componente PAP é permitir gerir as políticas. Na Figura 48 é apresentado um diagrama de sequência que demonstra o fluxo de criação de uma política de privacidade.

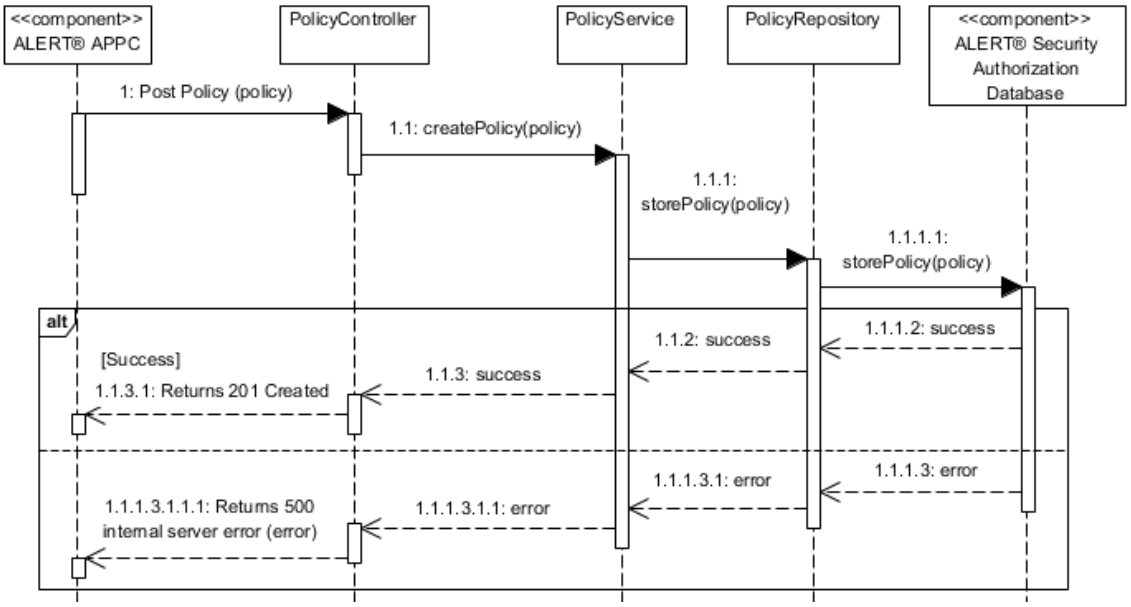


Figura 48 - Diagrama de sequência de criação de uma política no componente ALERT® Security Authorization Framework

Os processos de criação, edição e eliminação de política são semelhantes, diferindo apenas nos métodos invocados. Contudo, como esta solução irá armazenar as políticas de consentimento dos pacientes do ALERT® HIE, foi tomada a decisão de criar um recurso REST que permite eliminar todas as políticas relacionadas com o consentimento de um paciente, correspondendo a um dos requisitos funcionais definidos na Figura 16: o requisito de retirar consentimento. Quando um paciente retirar o seu consentimento, é feito um pedido REST ao ALERT® Security Authorization Framework com o intuito de eliminar todas as políticas de consentimento relacionadas com o paciente. Após receber a identificação do paciente, é necessário primeiramente obter a "PolicySet" raiz correspondente ao paciente, sendo depois necessário obter a lista de políticas referenciadas e eliminar primeiramente estas e por último a política de consentimento raiz. Na Figura 49 é ilustrado o processo de eliminação das políticas de consentimento do paciente no ALERT® Security Authorization Framework.

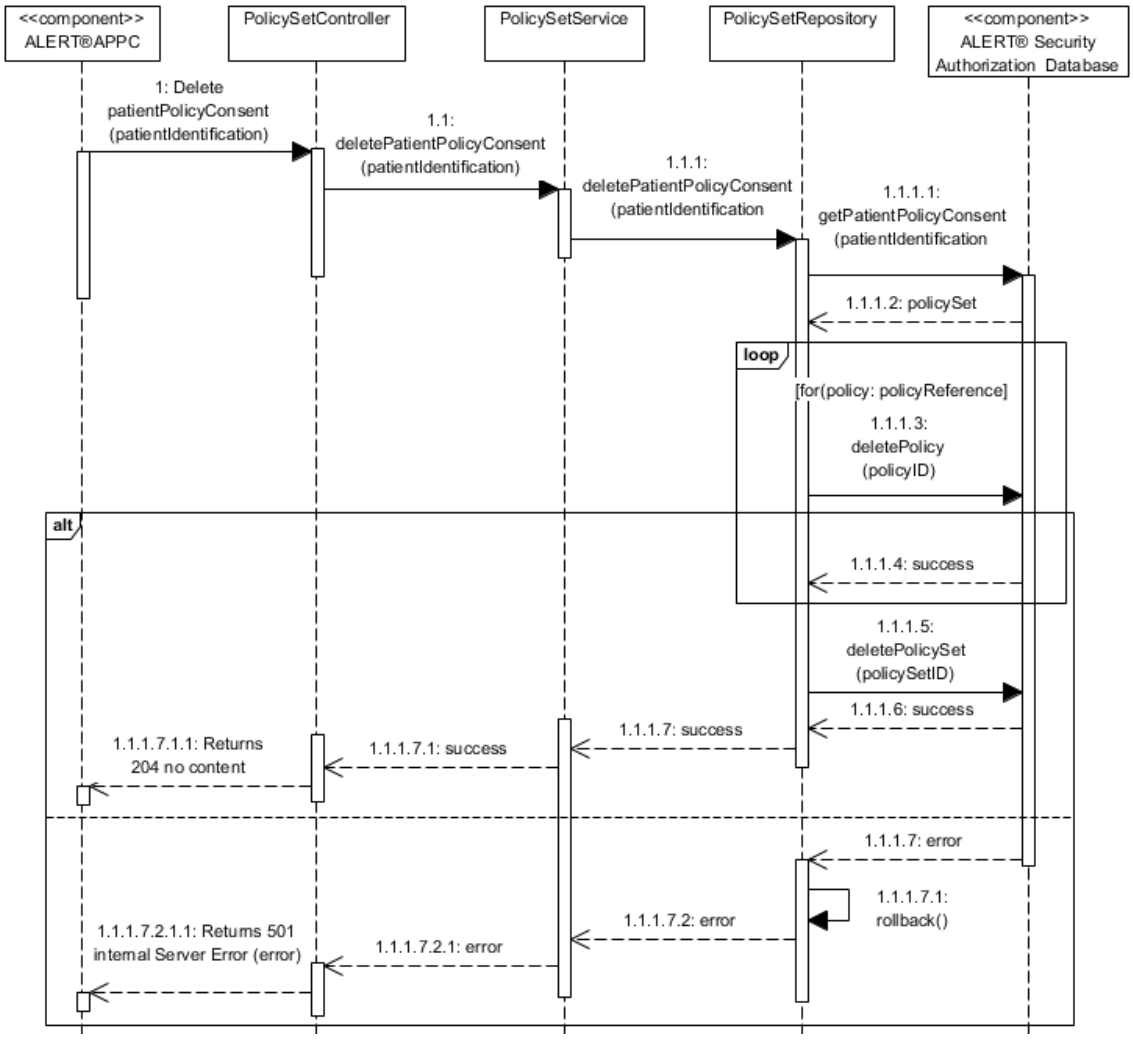


Figura 49 - Diagrama de sequência de eliminar política de consentimento de um paciente

5.4.2.2 PDP

Quando um pedido de decisão chega ao controlador do PDP do componente ALERT® Security Authorization Framework, este contém o pedido formulado com o modelo apresentado na subsecção 5.2.1.3 e a identificação do paciente. Primeiramente obtém-se a política de consentimento raiz associada ao paciente, após o que é invocado o avaliador de conjunto de políticas que irá invocar os avaliadores necessários para avaliar a política de consentimento contra o pedido formulado, e retornar uma resposta com a decisão. Caso a política de consentimento associado a este paciente não exista, a decisão será indeterminada pois não é possível avaliar o pedido recebido com a política de consentimento. Na Figura 50 é ilustrado o diagrama de sequência de obtenção de uma decisão para conforme o que está definido na política de consentimento do paciente e o pedido formulado.

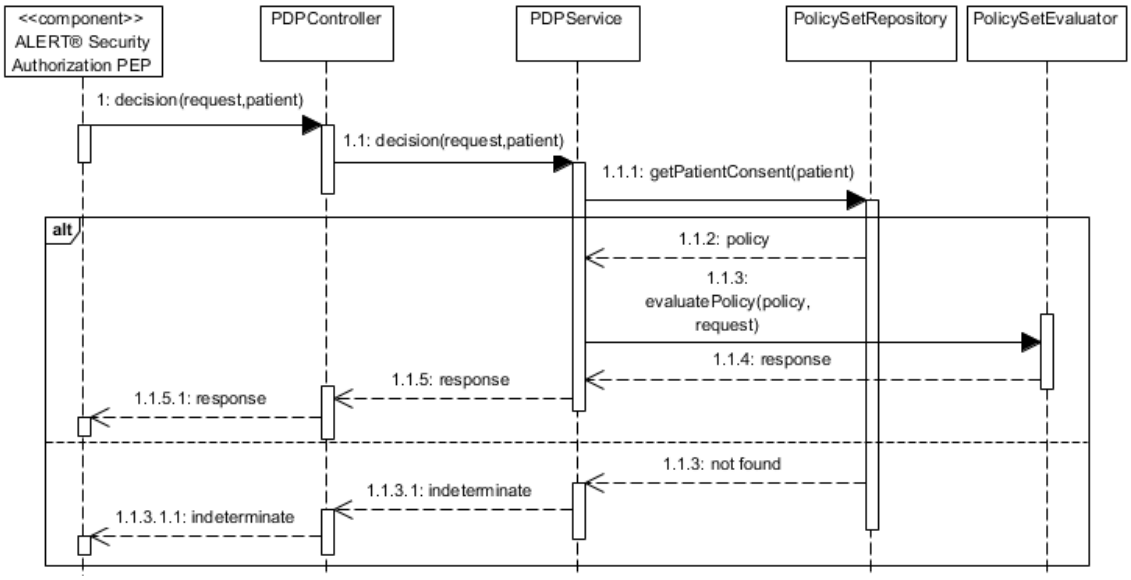


Figura 50 - Diagrama de sequência do pedido de acesso ao ALERT® Security Authorization Framework

5.4.3 Arquitetura ALERT® Security Authorization PEP

O componente ALERT®Security Authorization PEP, como o nome indica, é o componente responsável por transformar o pedido ao(s) recurso(s) que o utilizador pretende aceder com determinada ação para o modelo de negócio do XACML, como foi explicado na subsecção 5.2.1.1. Este componente depende do componente Security Authorization XACML e utiliza a API REST disponibilizada pela Security Authorization Framework, como é apresentado na Figura 45.

O perfil de integração do APPC já define diversos tipos de sujeitos, recursos e ações, como foi referido na subsecção 5.4.2. Este componente também tem as suas *factorys* e *builders* de forma a construir o objeto da maneira correta, como definido no perfil APPC, como é apresentado na Figura 51. Na Figura 52 é apresentado o diagrama de sequência de formulação do pedido no componente ALERT® Security Authorization PEP, que posteriormente é enviado ao componente ALERT® Security Authorization Framework para este decidir se dá acesso ou não com base na definição da política e no pedido formulado.

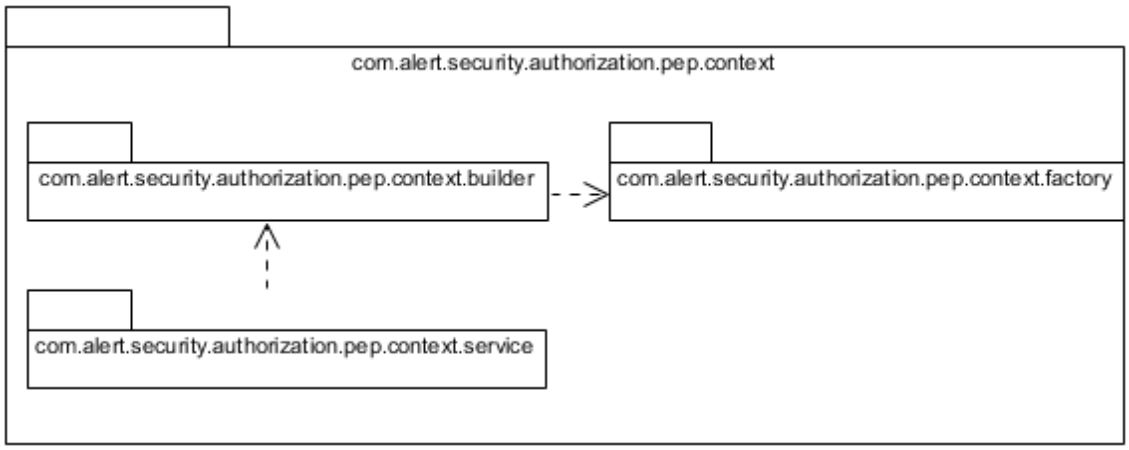


Figura 51 - Diagrama de *packages* do componente ALERT® Security Authorization PEP

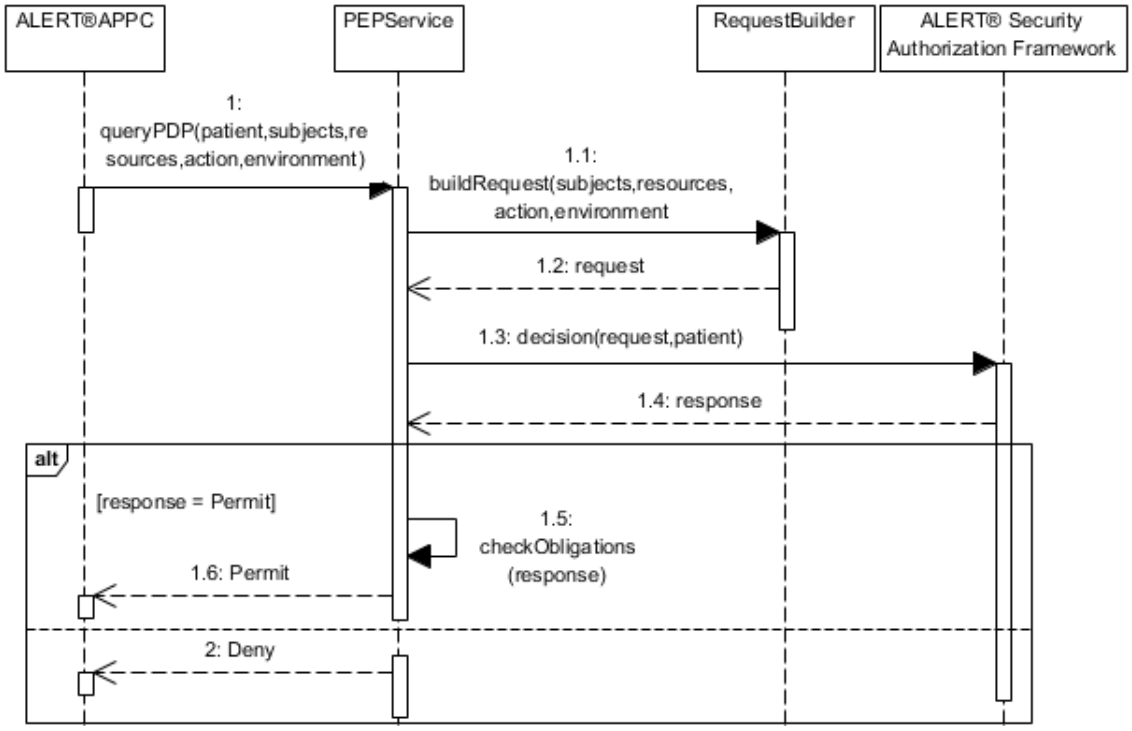


Figura 52 - Diagrama de sequência de formulação do pedido de acesso no ALERT® Security Authorization PEP

6 Implementação

Este capítulo descreve os detalhes mais importantes da lógica de negócio adicionada nos novos componentes, assim como outros aspetos relevantes incluídos no sentido de implementar os requisitos funcionais identificados, tendo em consideração a arquitetura desenhada no capítulo 5.

6.1 ALERT® Security Authorization Framework

O ALERT®Security Authorization Framework tem duas grandes responsabilidades: (i) permitir a gestão das políticas de consentimento do paciente e (ii) decidir com base num pedido XACML se garante o acesso ou não.

O perfil APPC já define um conjunto de sujeitos, recursos e ações que a implementação XACML deve suportar (IHE ITI Technical Committee, 2018b, pp. 34–63). Na Figura 53 é apresentado um exemplo de um sujeito que deve ser suportado, em que este se refere ao identificador da instituição, através do atributo "AttributeId" do elemento "SubjectAttributeDesignator" e o tipo de dados que este sujeito deve conter através do atributo "DataType".

```
<xacml:Subject>
    <xacml:SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
        <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
            urn:oid:1.3.6.1.4.1.33233.2.2.5.4.9
        </xacml:AttributeValue>
        <xacml:SubjectAttributeDesignator
            AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
            DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
    </xacml:SubjectMatch>
</xacml:Subject>
```

Figura 53 - Exemplo de sujeito do tipo organizationID de uma política no XACML

Ao definir os tipos de atributos que devem ser suportados pelo APPC, foi tomada a decisão de instanciar estes conceitos automaticamente através do conceito de bean[23]. Os beans permitem a definição de diversas propriedades, tais como:

- Classe;
- Nome;
- Tipo;
- Argumentos do construtor;
- Propriedades;
- Modo de inicialização;
- Método de inicialização;
- Método de destruição.

Assim, é possível através de um único ficheiro XML suportar todos os conteúdos que o APPC impõe. Desta forma, quando o perfil for atualizado e adicionados/atualizados os conteúdos deste tipo, apenas será necessário atualizar o ficheiro com as novas definições. Esta implementação também não restringe o uso do perfil XACML para uma utilização personalizada caso a ALERT pretenda, apenas tendo que adicionar neste ficheiro os conteúdos personalizados. Na Figura 54 é ilustrado um exemplo com todos os beans necessários e as suas relações para definição do sujeito com identificador da organização.

```
<bean id="appcSubjectMatchUserOrganizationID"
  class="com.alert.security.authorization.xacml.schema.policy.SubjectMatchType">
    <property name="subjectAttributeDesignator" ref="appcSubjectUserOrganizationID"/>
    <property name="attributeValue" ref="appcAttributeValueTypeAnyURI"/>
</bean>

<bean id="appcSubjectUserOrganizationID"
  class="com.alert.security.authorization.xacml.schema.policy.SubjectAttributeDesignatorType">
    <property name="attributeId" value="urn:oasis:names:tc:xspa:1.0:subject:organization-id"/>
    <property name="dataType" ref="anyURIDataType"/>
</bean

<bean id="appcAttributeValueTypeAnyURI"
  class="com.alert.security.authorization.xacml.schema.policy.AttributeValueType">
    <property name="dataType" ref="anyURIDataType"/>
</bean>

<bean id="anyURIDataType" class="java.lang.String">
    <constructor-arg value="http://www.w3.org/2001/XMLSchema#anyURI"/>
</bean>
```

Figura 54 - Definição do bean do sujeito com identificador da organização

[23] No Spring os objetos que formam o esqueleto da aplicação são chamados beans. Um bean é um objeto instanciado, montado e gerido pelo Spring IoC container (Spring, 2019b).

6.1.1 Criação de políticas

De forma a ter um mecanismo de criação de políticas que respeite os conteúdos impostos pelo APPC, criou-se um conjunto de classes que permitem, com base no pedido recebido gerar a política ou conjunto de políticas com a sintaxe do XACML. Esta funcionalidade será útil para a aplicação/componente responsável por partilhar os documentos de consentimento com o ALERT®HIE, pois primeiramente poderá enviar um pedido com a informação de como a política deverá ser constituída e é retornado o respetivo XACML formulado, que será partilhado posteriormente. Na Figura 55 é apresentado o diagrama de classes e suas dependências que permitem gerar o XACML de forma correta.

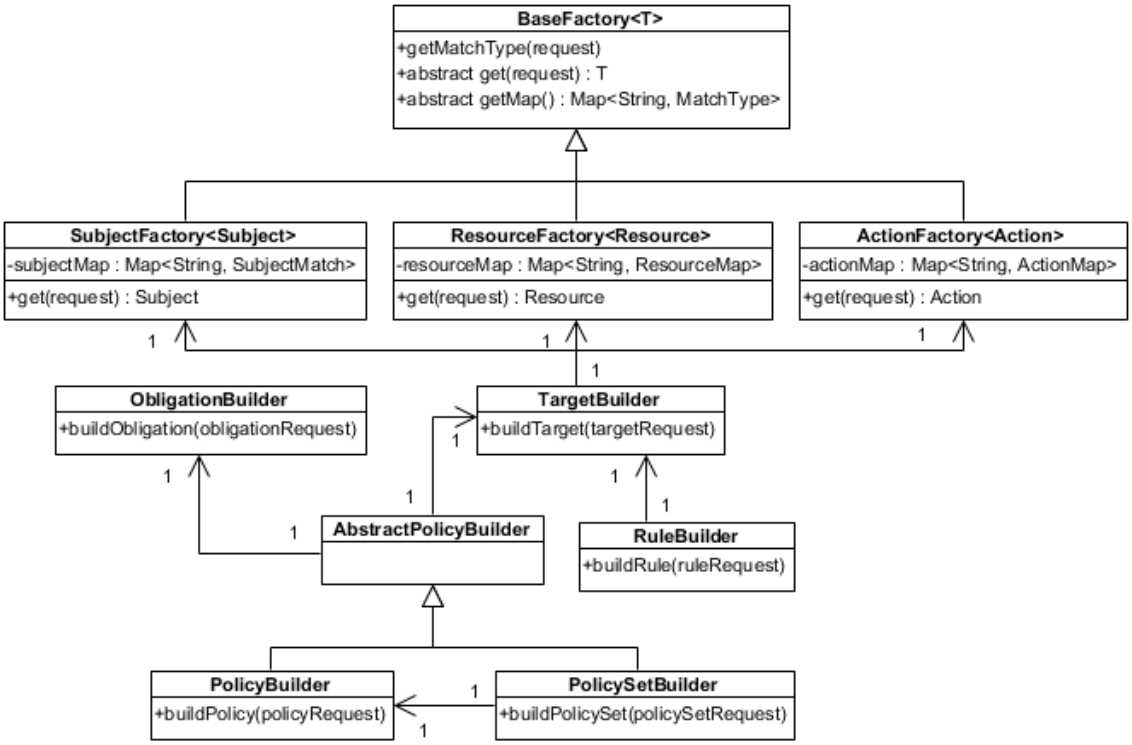


Figura 55 - Diagrama de classe dos construtores e fábricas das políticas e conjunto de políticas

Os sujeitos, recursos e ações que a implementação suporta são instanciados em diferentes mapas em que a chave é o próprio identificador do atributo que deverá ser único. Estes mapas ficam dentro das classes SubjectFactory, ResourceFactory e ActionFactory, que extendem a classe BaseFactory. Esta é responsável por utilizar os tipos de sujeitos, recursos e ações carregados. No Extrato Código 1 é apresentado como os sujeitos, rescursos e ações são registados nos respetivos mapas.

```
<bean id="SubjectFactory" class="com.alert.security.authorization.pap.policy.factory.SubjectFactory">
  <property name="subjectMatchMap" ref="subjectFactoryMap"/>
</bean>
<bean id="ResourceFactory" class="com.alert.security.authorization.pap.policy.factory.ResourceFactory">
  <property name="resourceMatchMap" ref="resourceFactoryMap"/>
 </bean>
<bean id="ActionFactory" class="com.alert.security.authorization.pap.policy.factory.ActionFactory">
  <property name="actionMatchMap" ref="actionFactoryMap"/>
</bean>

<util:map id="subjectFactoryMap" map-class="java.util.HashMap"
 value-type="com.alert.security.authorization.xacml.schema.policy.SubjectMatchType">
  <entry key="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
         value-ref="appcSubjectMatchUserOrganizationID"/>
  ...
</util:map>
<util:map id="resourceFactoryMap" map-class="java.util.HashMap"
 value-type="com.alert.security.authorization.xacml.schema.policy.ResourceMatchType">
  ...
</util:map>
<util:map id="actionFactoryMap" map-class="java.util.HashMap"
 value-type="com.alert.security.authorization.xacml.schema.policy.ActionMatchType">
  ...
</util:map>
```

Extrato Código 1 - Instanciação das fábricas através do Spring

Para criar o objeto pretendido apenas é necessário invocar o método get, existente em cada uma das fábricas, passando como argumento o respetivo pedido com a informação do tipo de conteúdo e respetivo valor que se pretende construir. Este método posteriormente deverá invocar o método getMatchType da superclasse, que é responsável por procurar pelo mapa de conteúdos suportados, carregado pelo Spring. Caso seja encontrado o objeto correspondente, é verificado se o tipo de dados do pedido é o mesmo do conteúdo, e em caso afirmativo é retornado o conteúdo com o seu valor inserido. Caso não seja encontrado o conteúdo ou o tipo de dados diferir é lançada uma exceção, que irá parar a criação do objeto.

```
protected MatchType getMatchType(RequestToXACMLTargetBuilder request) throws InvalidDataTypeException,
         IllegalArgumentException {
  Map<String, ? extends MatchType> map = getMap();
  if(map.containsKey(request.getAttributeId())) {
    MatchType matchType = map.get(request.getAttributeId()).clone();
    if(validateAttributeValueType(matchType.getAttributeDesignator(), request.getValue())) {
      matchType.setMatchId(request.getMatchID());
      matchType.getAttributeValue().addContent(request.getValue().parse());
      return matchType;
    }else {
      throw new InvalidDataTypeException("The data type used in the request "+
        request.getValue().getDataTypeURI()+" isn't the same as in the"+
        " attributeDesignatorType object "+matchType.getAttributeDesignator().getDataType());
    }
  }else {
    throw new IllegalArgumentException("The requested MatchType \""+request.getAttributeId()+
        \" couldn't be found in the Map<String,MatchType> loaded by the Spring.");
  }
}
```

Extrato Código 2 - Exemplo de método de como obter o respetivo objeto

Foi disponibilizado um método REST na interface do PAP do ALERT® Security Authorization Framework que permite enviar no corpo da mensagem um JSON com as especificações do tipo de política ou conjunto de políticas que se pretende criar. No Extrato Código 3 é demonstrado um exemplo de um JSON para criação de uma política, em que está definida uma descrição breve do propósito desta política, o algoritmo de combinação de regras que deverá ser utilizado

e o alvo a que esta política se refere. Depois é definido o conjunto de regras desta política (que neste caso é apenas uma e que está a negar o acesso quando um pedido corresponde com o alvo da política).

```
{
  "description" : "Deny access to patient information to this institution",
  "institutionID": 1,
  "ruleCombiningAlgId" : "urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides",
  "targetRequest": {
    "subjects":[
      {
        "matchID":"urn:oasis:names:tc:xacml:1.0:function:anyURI-equal",
        "attributeID":"urn:oasis:names:tc:xspa:1.0:subject:organization-id",
        "value":{
          "dataType": "http://www.w3.org/2001/XMLSchema#anyURI",
          "value1": "urn:oid:1.3.6.1.4.1.33233.3.1.1.1"
        }
      }
    ],
    "resources":[
      {
        "matchID":"urn:oasis:names:tc:xacml:1.0:function:anyURI-equal",
        "attributeID":"urn:ihe:iti:ser:2016:patient-id",
        "value":{
          "dataType": "urn:hl7-org:v3#II",
          "value1": "114559",
          "value2": "1.3.6.1.4.1.33233.3.1.1.1"

        }
      }
    ],
    actions":[
      {
        "matchID":"urn:oasis:names:tc:xacml:1.0:function:anyURI-equal",
        "attributeID":"urn:oasis:names:tc:xacml:1.0:action:action-id",
        "value":{
          "dataType": "http://www.w3.org/2001/XMLSchema#anyURI",
          "value1": "urn:ihe:iti:2007:RetrieveDocumentSetResponse"
        }
      }

    ],
    "environments":[]
  },
  "ruleRequests": [
    {
      "description": "Do not allow access to patient information in this institution ",
      "effect": "DENY"
    }
  ]
}
```

Extrato Código 3 - JSON de criação de políticas

6.1.2 Avaliação de Políticas

O XACML define, na documentação do seu padrão, como o mecanismo de avaliação de políticas deve ser implementado (OASIS, 2005, pp. 77–88). Na Figura 56 é apresentada a implementação do mecanismo com todas as classes e suas dependências para avaliação das políticas de consentimento.

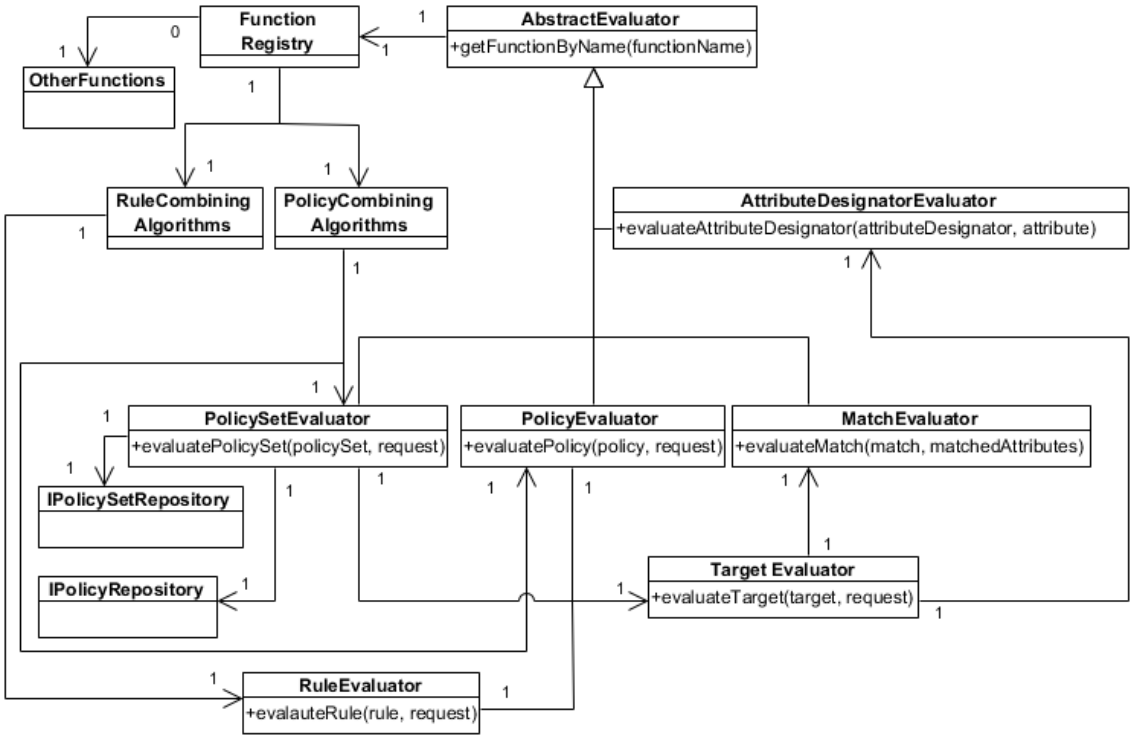


Figura 56 - Diagrama de classes de avaliação de políticas de privacidade

Para garantir o acesso a um determinado pedido, recebido do componente ALERT® Security Authorization PEP, foi necessário reformular o mecanismo de avaliação do pedido com a respetiva política. Como é percetível no diagrama de sequência que demonstra a validação do pedido de acesso ao consentimento do paciente na Figura 58, o PolicySetService invoca o método evaluatePolicySet da classe PolicySetEvaluator que irá começar o processo de análise da política.

O ponto de entrada da avaliação difere dependendo de se a avaliação vai ser feita para uma política ou para um conjunto de políticas, porém o processo é semelhante. Ao invocar o método evaluatePolicySet da classe PolicySetEvaluator é passado como argumento o conjunto de políticas avaliar e o pedido recebido. Primeiramente é necessário avaliar se o alvo da política corresponde com o pedido. Na Figura 57 é apresentada a implementação simplificada da avaliação do alvo de uma política com o pedido, já na Tabela 13 são apresentados todos os possíveis resultados da avaliação de um alvo que a implementação deverá respeitar.

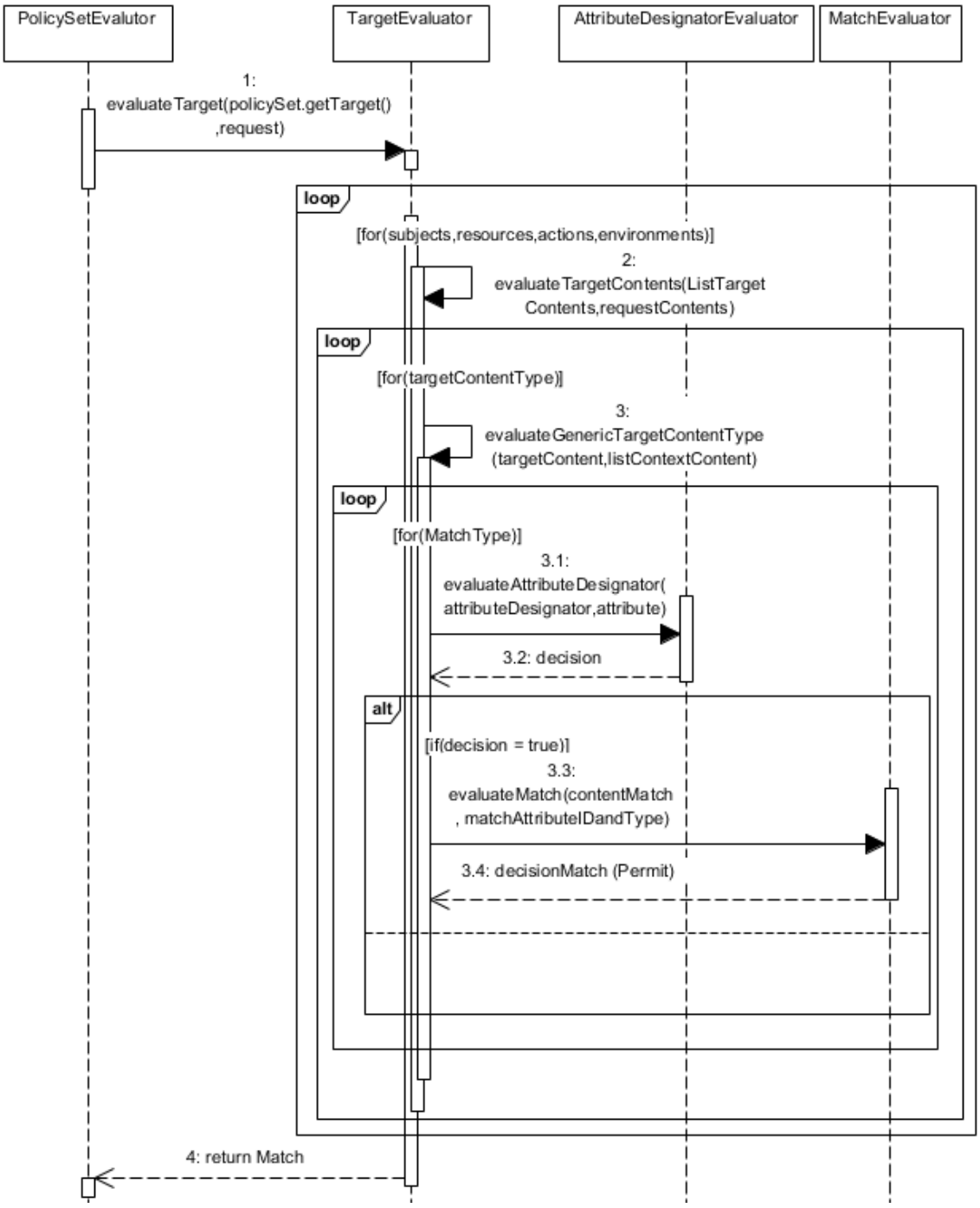


Figura 57 - Diagrama de sequência de avaliação do elemento alvo

Tabela 13 - Possíveis resultados de um alvo(OASIS, 2005, p. 83)

Subjects value	Resources value	Actions value	Environments value	Target value
"Match"	"Match"	"Match"	"Match"	"Match"
"No match"	"Match" or "No match"	"Match" or "No match"	"Match" or "No match"	"No match"
"Match" or "No match"	"No match"	"Match" or "No match"	"Match" or "No match"	"No match"
"Match" or "No match"	"Match" or "No match"	"No match"	"Match" or "No match"	"No match"
"Match" or "No match"	"Match" or "No match"	"Match" or "No match"	"No match"	"No match"
"Indeterminate"	Don't care	Don't care	Don't care	"Indeterminate"
Don't care	"Indeterminate"	Don't care	Don't care	"Indeterminate"
Don't care	Don't care	"Indeterminate"	Don't care	"Indeterminate"
Don't care	Don't care	Don't care	"Indeterminate"	"Indeterminate"

Se os alvos corresponderem é necessário obter todas as subpolíticas, como também todos os subconjuntos de políticas do conjunto de políticas em questão e invocar o método de combinação de políticas referenciado. Na Figura 58 é apresentado o fluxo da implementação da avaliação de um conjunto de políticas.

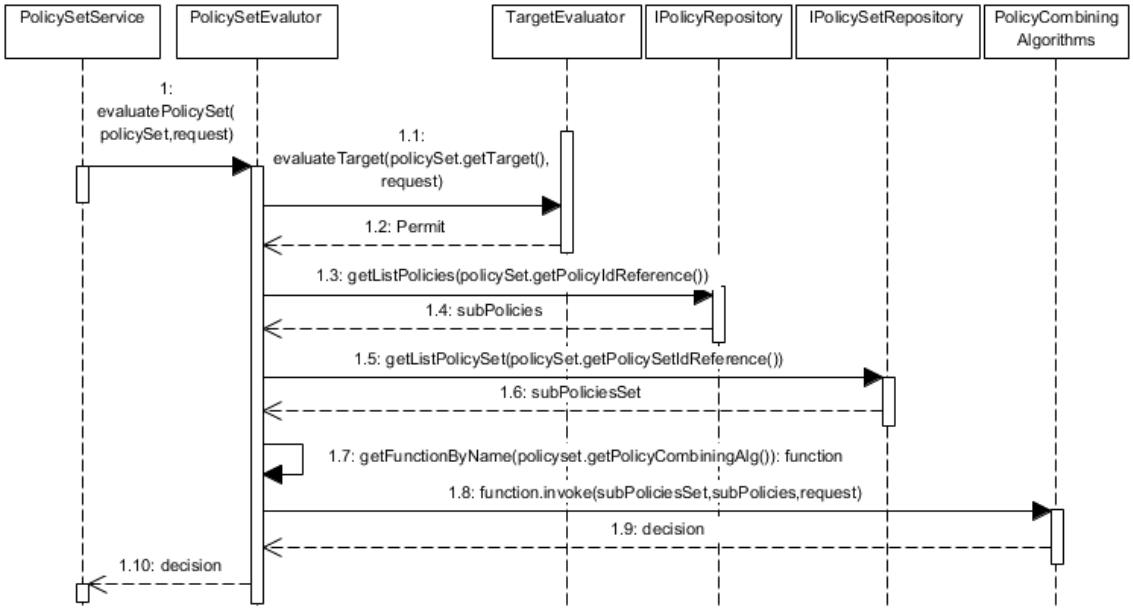


Figura 58 - Diagrama de sequência de avaliação de um conjunto de políticas com o pedido

As implementações XACML devem implementar certos algoritmos de combinação, quer para as regras como para as políticas. Os algoritmos de combinação de regras são utilizados pelas

políticas, já os de combinação de políticas são utilizados pelos conjuntos de políticas. A implementação XACML deverá suportar os seguintes algoritmos (OASIS, 2005, pp. 132–139):

- *Deny overrides* – avalia todas as subpolíticas até encontrar uma que negue o acesso, caso não encontre nenhuma é dado o acesso*;*

- *Ordered deny overrides* – a lógica é exatamente igual ao do d*eny overrides*, mas a avaliação das subpolíticas deve ser pela ordem definida no conjunto de politicas*;*

- *Permit overrides* – avalia todas as subpolíticas até encontrar uma que permita o acesso, caso não encontre nenhuma é retornado negado o acesso*;*

- *Ordered permit overrides* – a lógica é igual ao do *permit overrides*, mas a avaliação das subpolíticas deve ser pela ordem definida no conjunto de políticas*;*

- First applicable – a avaliação das subpolíticas deverá ser na ordem existente no conjunto de políticas, sendo o resultado retornado consoante a primeira política em que o alvo corresponda;

- Only one applicable – apenas deverá existir um alvo nas subpolíticas que corresponda com o do pedido, caso contrário o resultado retornado deverá ser indeterminado.

O XACML, para além de definir os métodos que devem ser implementados, também ilustra um pseudo código da sua implementação. No Extrato Código 4 é apresentado o pseudo código da implementação do método de combinação de políticas *deny overrides* e na Figura 59 é apresentado o fluxo de implementação do mesmo algoritmo no ALERT® Security Authorization Framework.

```
Decision denyOverridesPolicyCombiningAlgorithm(Policy policy[])
{
 Boolean atLeastOnePermit = false;
 for( i=0 ; i < lengthOf(policy) ; i++ )
 {
   Decision decision = evaluate(policy[i]);
   if (decision == Deny){
     return Deny;
   }
   if (decision == Permit){
     atLeastOnePermit = true;
     continue;
   }
   if (decision == NotApplicable){
     continue;
   }
   if (decision == Indeterminate){
     return Deny;
   }
 }
 if (atLeastOnePermit)
 {
   return Permit;
 }
 return NotApplicable;
```

Extrato Código 4 - Pseudo código da implementação do método deny overides das políticas(OASIS, 2005, p. 133)

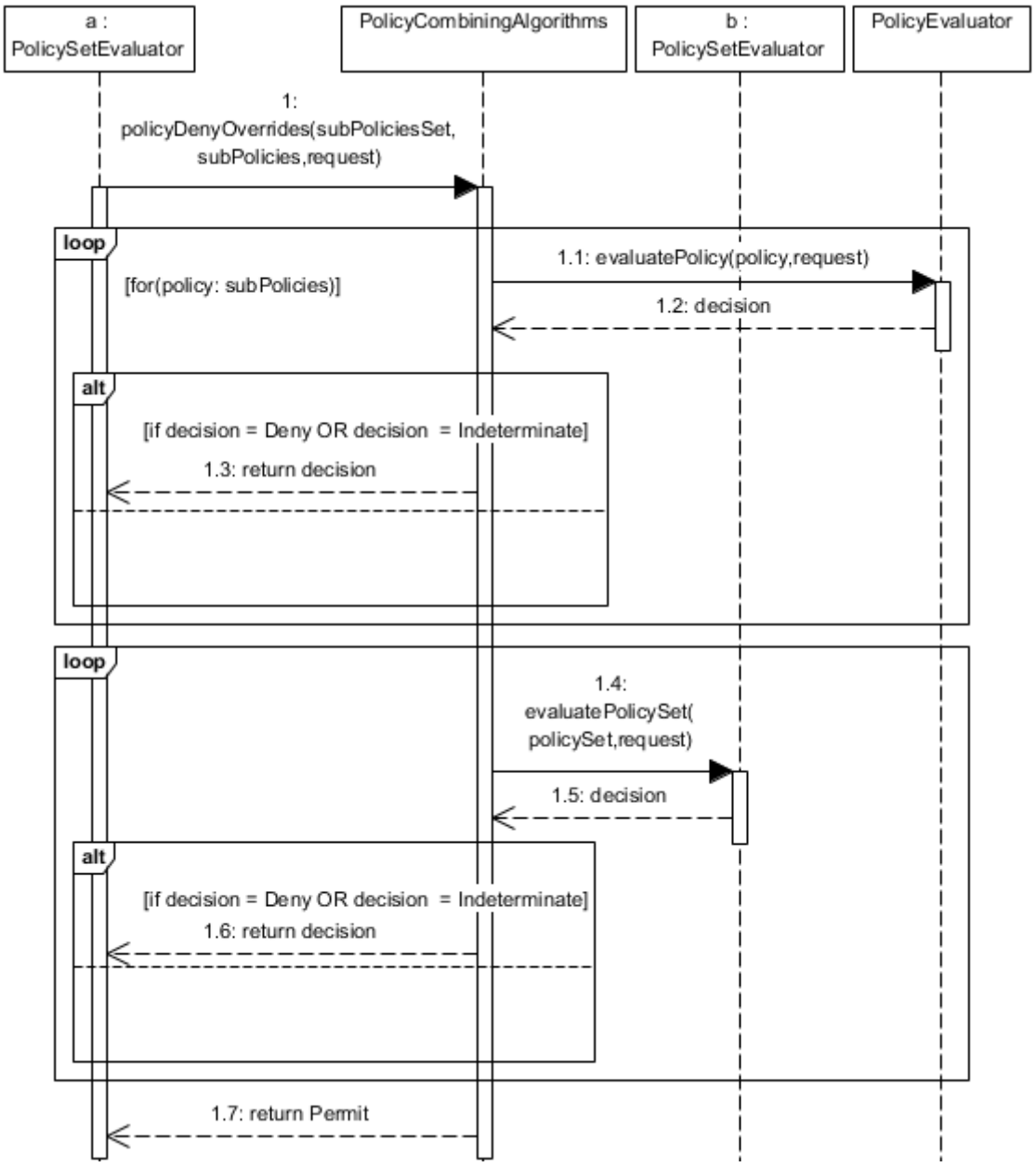


Figura 59 - Diagrama de sequência do algoritmo de combinações de políticas *deny overrides*

De forma a obter o resultado final da avaliação de um conjunto de políticas, pode ser necessário avaliar todos os subconjuntos de políticas e subpolíticas que este referencia, dependendo do tipo de algoritmo de combinação utilizado.

Para avaliar os subconjuntos de políticas bastará invocar novamente o método evaluatePolicySet da classe PolicySetEvaluator passando como argumento o subconjunto de políticas e o pedido inicial feito, conforme é apresentado na Figura 58.

Em relação à avaliação das subpolíticas apenas é necessário invocar o método evaluatePolicy da classe PolicyEvaluator, passando como argumento a política e o pedido inicial, como é percetível através da Figura 60. Caso o alvo da política corresponda com o pedido é necessário avaliar as regras da política de forma a obter o respetivo resultado. O processo de avaliação das

regras é semelhante ao apresentado na Figura 59 para as políticas, do qual apenas difere nos métodos de combinação que terão a sua lógica de combinação para as regras, no facto de ser invocado exclusivamente o método evaluateRule da classe RuleEvaluator. O método de avaliação de regras apenas avalia se o alvo da regra corresponde ao do pedido, e se for o caso retorna o efeito da regra, que será permitir ou negar acesso.

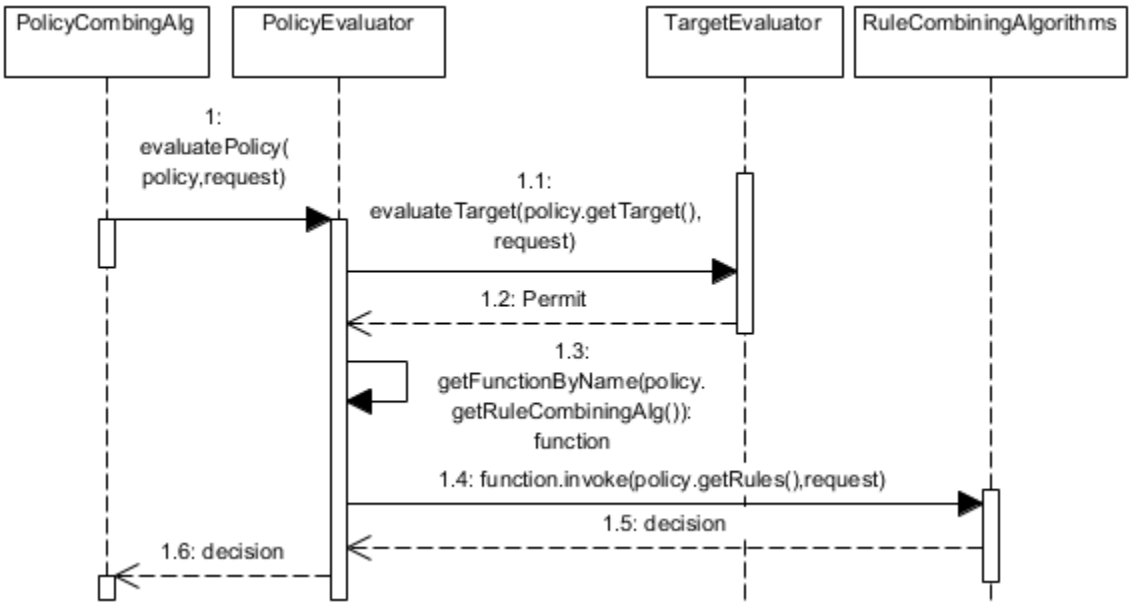


Figura 60 - Diagrama de sequência da avaliação de uma política

6.1.3 Serviços REST

Com o intuito de permitir a fácil utilização do padrão XACML, implementado no componente ALERT® Security Authorization Framework, por qualquer outro componente, foi tomada a decisão de criar duas interfaces REST, uma responsável por receber os pedidos relacionados com a administração de políticas (PAP) e outra responsável por receber o pedido de acesso e tomar uma decisão (PDP). No Anexo B são apresentados as diversas interfaces de comunicação disponibilizadas, de forma a ser possível a comunicação com o componente ALERT® Security Authorization Framework.

6.2 ALERT® Security Authorization PEP

A definição dos conteúdos suportados feita no componente ALERT® Security Authorization Framework e explicada na secção 6.1 teve de ser efetuada também no ALERT® Security Authorization PEP, ainda que, com as devidas modificações do tipo de objetos criados, pois este apenas tem que se preocupar com a formulação de pedidos. A Figura 61 ilustra um exemplo do objeto utilizado num pedido XACML, sendo que a definição de beans é semelhante à apresentada na Figura 54 modificando apenas as classes que são instanciadas e que formam este objeto.

```
<Subject>
  <Attribute AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
    DataType="http://www.w3.org/2001/XMLSchema#anyURI">
      <AttributeValue>urn:oid:1.3.6.1.4.1.33233.2.2.5.4.9</AttributeValue>
  </Attribute>
</Subject>
```

Figura 61 - Exemplo de sujeito do tipo organizationID de um pedido no XACML

A lógica de criação de pedidos neste componente é semelhante à da criação de políticas apresentada na subsecção 6.1.1, mas de forma mais simplificada devido à formulação de pedidos XACML ser menos complexa do que a criação de políticas ou conjuntos de políticas. Na Figura 62 é apresentado o diagrama de classes com os construtores e fábricas necessárias para formular os respetivos pedidos.

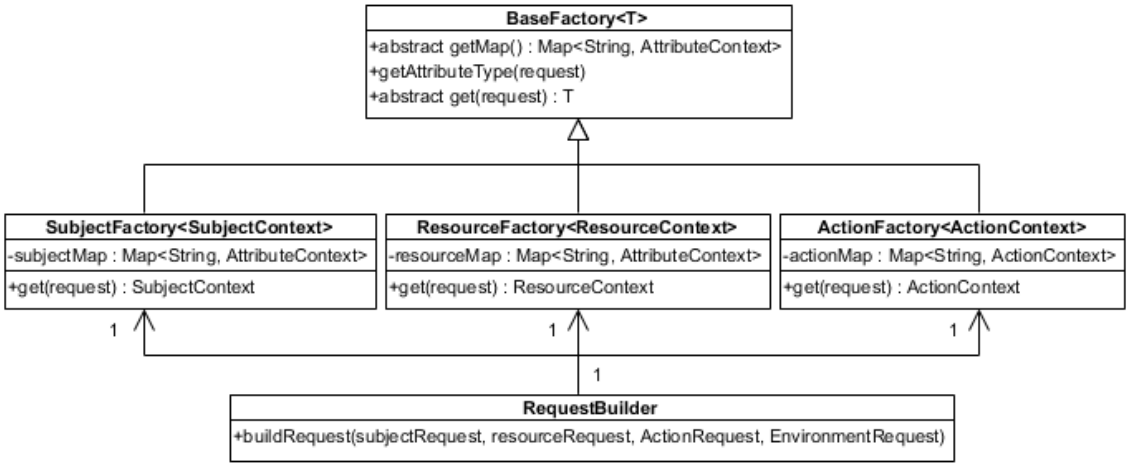


Figura 62 - Diagrama de classe do construtor e fábricas necessárias para criar pedidos XACML

6.3 ALERT®HIE

Nesta secção serão apresentadas todas as implementações realizadas que influenciam diretamente o produto ALERT® HIE e permitem resolver os problemas identificados e explicados durante a secção 3.1 e os requisitos funcionais na secção 3.2.2.

6.3.1 ALERT® APPC

O ALERT® APPC é o novo componente do ALERT®HIE que terá a lógica de negócio relacionada com o perfil de integração APPC, que tem como objetivo resolver primeiramente o problema do consentimento para o processamento e partilha de informação do paciente pelo ALERT®HIE, como também ajudar a resolver o problema da oposição à decisão individual automatizada.

6.3.1.1 Estrutura do consentimento

O consentimento do paciente pode ser subdividido em vários documentos, como foi mencionado na subsecção 5.3.2.1, mas é necessário haver uma política raiz segundo o perfil de

integração APPC (IHE ITI Technical Committee, 2018b, p. 31). Assim, de forma a respeitar o RGPD, o consentimento do paciente deverá ser divido em pelo menos três documentos:

- Política de consentimento raiz do paciente;
- Política de consentimento que dá acesso à partilha e processamento da informação do paciente;
- Política de consentimento sobre a decisão individual automatizada do algoritmo de correlacionamento de informação de pacientes.

Estes três documentos são fundamentais para garantir o tratamento lícito da informação do paciente. No entanto, a escolha da solução APPC deveu-se a esta permitir que o paciente decida com quem a sua informação pode ser partilhada, deste modo podem ser adicionados mais documentos de consentimento consoante as escolhas do paciente.

```
<?xml version="1.0" encoding="UTF-8"?>
<xacml:PolicySet
  xsi:schemaLocation="https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-policy-schema-os.xsd"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:hl7="urn:hl7-org:v3"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  Version="1.0"
  PolicySetId="urn:uuid:727db105-1100-4511-8f17-4b44596d69e1"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-algorithm:deny-overrides">
    <xacml:Description>Patient Consent</xacml:Description>
    <xacml:Target>
      <xacml:Resources>
          <xacml:Resource>
              <xacml:ResourceMatch MatchId="urn:hl7-org:v3:function:II-equal">
                  <xacml:AttributeValue DataType="urn:hl7-org:v3#II">
                      <hl7:InstanceIdentifier extension="111558" root="1.3.6.1.4.1.33233.3.1.1.1"/>
                  </xacml:AttributeValue>
                  <xacml:ResourceAttributeDesignator AttributeId="urn:ihe:iti:ser:2016:patient-id"
                    DataType="urn:hl7-org:v3#II"/>
              </xacml:ResourceMatch>
          </xacml:Resource>
      </xacml:Resources>
    </xacml:Target>
    <xacml:PolicyIdReference>urn:uuid:c4f16df4-557b-4670-9a17-659a5063b1e6</xacml:PolicyIdReference>
    <xacml:PolicyIdReference>urn:uuid:7397b16f-3cf7-46e9-9d5f-f282516cb8f2</xacml:PolicyIdReference>
    <xacml:PolicyIdReference>urn:uuid:03fd9c9a-1e26-4a8d-97e8-d23049eaefe9</xacml:PolicyIdReference>
</xacml:PolicySet>
```

Figura 63 – Política de consentimento raiz do paciente

Na Figura 63 é apresentada a política raiz de consentimento de um paciente. Esta deverá ser do tipo conjunto de políticas, em que o alvo desta tem de ter obrigatoriamente um recurso do tipo "urn:ihe:iti:ser:2016:patient-id" de forma a identificar a que paciente este conjunto de políticas de consentimento está associado. Este conjunto de políticas referencia outras políticas que ajudarão, consoante o pedido recebido, a tomar a decisão de permitir/negar o acesso. A referência a outras políticas é feita pelos seus identificadores de políticas ou de conjunto de políticas.

A IHE disponibiliza um validador, cujo nome é Gazelle (IHE International, 2018), que permite testar as implementações de quem implementa os perfis de integração que elabora. Na Figura 64 é apresentado o teste de validação ao documento de consentimento raiz do paciente.

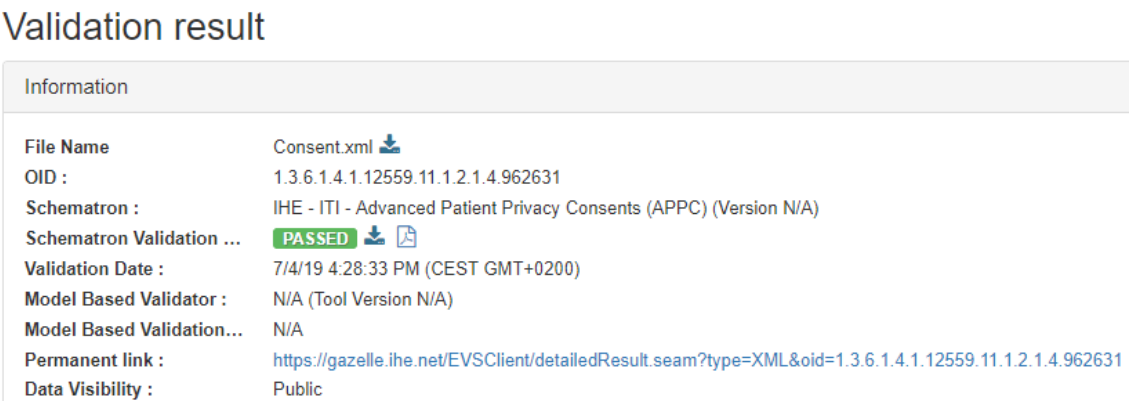


Figura 64 - Validação do documento de consentimento raiz

```
<?xml version="1.0" encoding="UTF-8"?>
<xacml:Policy
 xsi:schemaLocation="https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-policy-schema-os.xsd"
 xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
 xmlns:hl7="urn:hl7-org:v3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 Version="1.0" PolicyId="urn:uuid:c4f16df4-557b-4670-9a17-659a5063b1e6"
 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
    <xacml:Description>Allow access to patient information</xacml:Description>
    <xacml:Target>
        <xacml:Resources>
            <xacml:Resource>
                <xacml:ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <xacml:AttributeValue DataType="urn:hl7-org:v3#II">
                        <hl7:InstanceIdentifier extension="111558" root="1.3.6.1.4.1.33233.3.1.1.1"/>
                    </xacml:AttributeValue>
                    <xacml:ResourceAttributeDesignator
                         AttributeId="urn:ihe:iti:ser:2016:patient-id" DataType="urn:hl7-org:v3#II"/>
                </xacml:ResourceMatch>
            </xacml:Resource>
        </xacml:Resources>
    </xacml:Target>
    <xacml:Rule RuleId="urn:uuid:a54a2778-1504-471a-92d7-2b6cdca1c23a" Effect="Permit">
        <xacml:Description>Allow access to patient information</xacml:Description>
        <xacml:Target/>
    </xacml:Rule>
</xacml:Policy>
```

Figura 65 - Política de consentimento que dá acesso à partilha e processamento da informação do paciente

Na Figura 65 é apresentada a política de consentimento que dá acesso à informação do paciente a qualquer instituição. Para um pedido de acesso corresponder com esta política, apenas é necessário que a identificação do paciente no alvo da política corresponda à identificação do paciente num dos recursos do pedido.

A Figura 66 demonstra a política de consentimento sobre a decisão individual automatizada do algoritmo de correlacionamento de informação de pacientes. O alvo desta política é composto por um recurso que consiste na identificação do paciente e uma ação personalizada sobre a decisão individual automatizada, pois não existe nenhuma ação no perfil do APPC sobre o algoritmo de correlacionamento de informação de pacientes. Esta ação personalizada sobre o algoritmo de correlacionamento de informação de pacientes foi definida num bean dentro do ficheiro XML que é carregado pelo Spring no ALERT® Security Authorization Framework, como

explicado na secção 6.1. Por fim, a política é composta por uma regra que consoante o seu efeito consentirá (Permit) ou não (Deny) à decisão individual automatizada.

```
<?xml version="1.0" encoding="UTF-8"?>
<xacml:Policy
  xsi:schemaLocation="https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-policy-schema-os.xsd"
  xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
  xmlns:hl7="urn:hl7-org:v3"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  Version="1.0" PolicyId="urn:uuid:03fd9c9a-1e26-4a8d-97e8-d23049eaefe9"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
    <xacml:Description>Access to the correlation algorithm</xacml:Description>
    <xacml:Target>
        <xacml:Resources>
            <xacml:Resource>
                <xacml:ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <xacml:AttributeValue DataType="urn:hl7-org:v3#II">
                        <hl7:InstanceIdentifier extension="111558" root="1.3.6.1.4.1.33233.3.1.1.1"/>
                    </xacml:AttributeValue>
                    <xacml:ResourceAttributeDesignator
                        AttributeId="urn:ihe:iti:ser:2016:patient-id"
                        DataType="urn:hl7-org:v3#II"/>
                </xacml:ResourceMatch>
            </xacml:Resource>
        </xacml:Resources>
        <xacml:Actions>
            <xacml:Action>
                <xacml:ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                        urn:alert:hie:pix:correlation-decision
                    </xacml:AttributeValue>
                    <xacml:ActionAttributeDesignator
                         AttributeId="urn:alert:hie:action"
                         DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                </xacml:ActionMatch>
            </xacml:Action>
        </xacml:Actions>
    </xacml:Target>
    <xacml:Rule RuleId="urn:uuid:d8fc30a5-0416-4437-b20e-98d0734601d0" Effect="Permit">
        <xacml:Description>Allow the correlation of patients</xacml:Description>
        <xacml:Target/>
    </xacml:Rule>
</xacml:Policy>
```

Figura 66 - Política de consentimento sobre a decisão individual automatizada do algoritmo de correlacionamento de informação de pacientes

Apresentados os três documentos de consentimento necessários para que o tratamento feito sobre a informação do paciente pelo ALERT®HIE seja lícito, a Figura 67 apresenta uma política de consentimento que permite negar o acesso à informação a uma determinada instituição. O alvo desta política deverá ser constituído pelo(s) sujeito(s) que não deverão ter acesso à informação do paciente, o recurso que deverá ter a identificação do paciente e as ações em questão a que não deverá ser dado acesso. Por último, existe uma regra cujo efeito é negar (Deny) o acesso.

De momento, o tipo de restrição de acesso é exclusivamente feito ao nível da instituição devido ao ALERT®HIE apenas ter conhecimento da instituição que enviou a informação, portanto na formulação do pedido só é possível indicar como sujeito a instituição. Contudo, se futuramente o produto sofrer alterações e se souber qual o profissional de saúde que está a fazer o pedido, a solução já está preparada para analisar autorização de acesso ao nível do profissional. As autorizações também podem ser mais específicas ao nível da informação a que é dado acesso, ainda que de momento é toda a informação do paciente, a solução também está preparada para todos os outros tipos de recursos existentes (e.g. episódio clínico).

```
<?xml version="1.0" encoding="UTF-8"?>
<xacml:Policy xsi:schemaLocation="https://docs.oasis-open.org/xacml/2.0/access_control-xacml-2.0-policy-schema-os.xsd"
 xmlns:xacml="urn:oasis:names:tc:xacml:2.0:policy:schema:os"
 xmlns:hl7="urn:hl7-org:v3" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 Version="1.0" PolicyId="urn:uuid:7397b16f-3cf7-46e9-9d5f-f282516cb8f2"
 RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:deny-overrides">
    <xacml:Description>Deny access to patient information to this institution</xacml:Description>
    <xacml:Target>
        <xacml:Subjects>
            <xacml:Subject>
                <xacml:SubjectMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                        urn:oid:1.3.6.1.4.1.33233.3.1.1.1
                    </xacml:AttributeValue>
                    <xacml:SubjectAttributeDesignator
                        AttributeId="urn:oasis:names:tc:xspa:1.0:subject:organization-id"
                        DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                </xacml:SubjectMatch>
            </xacml:Subject>
        </xacml:Subjects>
        <xacml:Resources>
            <xacml:Resource>
                <xacml:ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <xacml:AttributeValue DataType="urn:hl7-org:v3#II">
                        <hl7:InstanceIdentifier extension="114559" root="1.3.6.1.4.1.33233.3.1.1.1"/>
                    </xacml:AttributeValue>
                    <xacml:ResourceAttributeDesignator
                        AttributeId="urn:ihe:iti:ser:2016:patient-id"
                        DataType="urn:hl7-org:v3#II"/>
                </xacml:ResourceMatch>
            </xacml:Resource>
        </xacml:Resources>
        <xacml:Actions>
            <xacml:Action>
                <xacml:ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
                    <xacml:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
                        urn:ihe:iti:2007:RegistryStoredQueryResponse
                    </xacml:AttributeValue>
                    <xacml:ActionAttributeDesignator
                        AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id"
                        DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
                </xacml:ActionMatch>
            </xacml:Action>
        </xacml:Actions>
    </xacml:Target>
    <xacml:Rule RuleId="urn:uuid:19687642-16f2-4d06-9a7e-39c2e414a8e6" Effect="Deny">
        <xacml:Description>Doesn't allow this institution to access patient information</xacml:Description>
        <xacml:Target/>
    </xacml:Rule>
</xacml:Policy>
```

Figura 67 - Política de consentimento que nega o acesso à partilha e processamento a uma instituição

6.3.1.2 Criação das políticas de consentimento

A criação do consentimento do paciente no ALERT®HIE é possível através da transação de partilhar documentos do perfil de integração XDS, como foi explicado na subsecção 5.3.2.1. Para isso criou-se um observador que irá intercetar a transação de partilha de documentos, como foi explicado na subsecção 5.3.2. Como é possível visualizar através do diagrama de classes da Figura 68, o observador PatientConsentObserver irá intercetar a transação quando esta estiver no estado “Pedido validado”. Devido a este observador verificar todos os documentos partilhados e confirmar se são do tipo APPC, decidiu-se que este também será responsável por verificar as políticas que referenciam o consentimento sobre a decisão individual automatizada do paciente, por questões de desempenho.

O observador contempla um mecanismo que guarda as política de consentimento que foram criadas com sucesso no ALERT® Security Authorizaiton Framework, de forma a que se posteriormente acontecer algum erro durante a persistência das políticas no ALERT® HIE, a

transação passará pelo estado Roll back e o observador apagará do componente ALERT® Security Authorization Framework todas as políticas criadas com sucesso anteriormente.

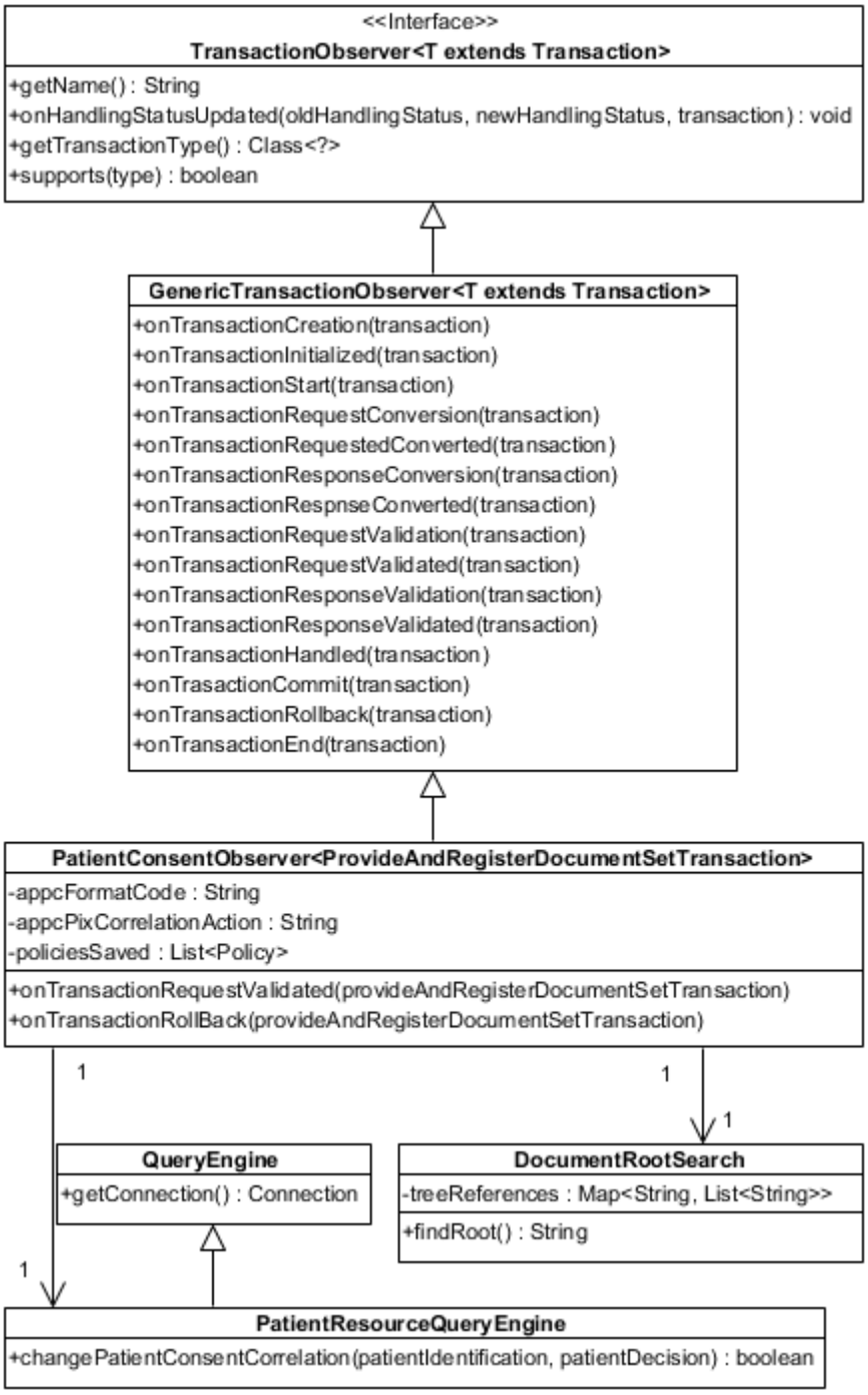


Figura 68 - Diagrama de classes do observador da partilha de consentimento do paciente

De modo a averiguar se uma política de consentimento partilhada é sobre o consentimento da decisão individual automatizada é necessário verificar todas as políticas e se a ação corresponde à ação personalizada, ilustrada na Figura 66. Após verificar que determinada política refere este tipo de consentimento, é invocado um procedimento de base de dados que irá atualizar a decisão do paciente sobre o correlacionamento automático de informação

de pacientes. No Extrato Código 5 é apresentado o excerto de código implementado que verifica se a política está relacionada com o consentimento à decisão individual automatizada e se for o caso é atualizada a decisão na base de dados do ALERT® HIE.

```
private void verifyPolicyConsentCorrelation(PolicyType policy, Id patientID) throws HIEException {
  List<ActionType> actions = policy.getTarget().getActions().getAction();
  for(ActionType action: actions) {
    List<ActionMatchType> actionMatchType = action.getActionMatch();
    boolean validAction = actionMatchType.stream().
        anyMatch(a -> a.getAttributeValue().getContent().get(0).equals(appcPixCorrelationAction));
    if(validAction) {
      String correlationDecision = getDecisionFromBD(policy.getRules().get(0).getEffect());
      String message = "There was an error on updating the patient decision about the correlation"
                       +" algorithm. Rollbacking the transaction";
      try {
        boolean result =PatientResourceQueryEngine.getInstance().changePatientConsentCorrelation(
                        patientID.getRoot(), patientID.getExtension(), correlationDecision);
        if(!result) {
          LOGGER.error(message);
          throw new HIEException(message);
        }
      } catch (SQLException e) {
        LOGGER.error(message,e);
        throw new HIEException(message,e);
      }
    }
  }
}
```

Extrato Código 5 - Verificação se política é sobre o consentimento da decisão individual automatizada

Ao partilhar os documentos de consentimento é necessário analisar qual dos conjuntos de políticas é a raiz do consentimento, de modo a informar o ALERT® Security Authorization Framework por qual conjunto de políticas a avaliação da decisão deverá começar. Para isso é necessário verificar em todos os conjuntos de políticas qual destes é a raiz do consentimento.

O Extrato Código 6 demonstra a implementação da verificação do conjunto de política de consentimento, esta recebe por parâmetro uma lista de políticas e conjunto de políticas, como também a identificação do paciente da atual transação. Primeiramente são filtrados todos os documentos do tipo conjunto de políticas, posteriormente é verificado qual documento é a raiz de consentimento, após isso é necessário verificar que o documento de consentimento segue as especificações obrigatórias definidas na documentação do perfil APPC (IHE ITI Technical Committee, 2018b, p. 31), que implica a existência de um recurso com a identificação do paciente que terá de ser igual à identificação do paciente na transação.

```
private void processListOfAppcConsentDocuments(List<AbstractPolicyType> listPolicies, Id patientID)
  throws HIEException{
  List<PolicySetType> listPoliciesSet = listPolicies.stream().filter(x ->  x instanceof PolicySetType)
                                                            .map(x -> (PolicySetType)x)
                                                            .collect(Collectors.toList());
  DocumentRootSearch drs = new DocumentRootSearch(listPoliciesSet);
  String documentRootId = drs.findRoot();
  if(documentRootId != null) {
    PolicySetType documentRoot = listPoliciesSet.stream().filter(x->x.getID().equals(documentRootId))
                                                         .findFirst().get();
    if(checkIfAPPCDocumentIsConsentType(documentRoot, patientID)) {
      List<AbstractPolicyType> listPolicy = listPolicies.stream()
                                            .filter(x -> (!x.getID().equals(documentRootId)))
                                            .collect(Collectors.toList());
      saveListOfAppcConsentDocument(documentRoot, listPolicy, patientID);
    }else {
      throw new HIEException("The appc Document"+documentRootId+
                " doesn't follow the specifications in the standard for beeing a root Document");
    }
  }else{
    throw new HIEException("The appc hierarchy tree is malformed, please correct it.");
  }
}

public String findRoot() {
  Set<String> nodes = treeReferences.keySet();
  for(String node : nodes) {
    if(numberDocuments == findRoot(node)) {
      return node;
    }
  }
  return null;
}

private int findRoot(String node) {
  int numberNodes = 1;
  Set<String> leafNodes = treeReferences.containsKey(node)? treeReferences.get(node) : new HashSet<String>();
  for(String leafNode : leafNodes) {
    if(auxMap.containsKey(leafNode)) {
      numberNodes+=auxMap.get(leafNode);
    }else {
      numberNodes+=findRoot(leafNode);
    }
  }
  this.auxMap.put(node, numberNodes);
  return numberNodes;
}
private boolean checkIfAPPCDocumentIsConsentType(PolicySetType policy, Id patientID) {
  List<ResourceType> resources = policy.getTarget().getResources().getResource();
  for(ResourceType resource: resources) {
    List<ResourceMatchType> resourcesMatchType = resource.getResourceMatch();
    for(ResourceMatchType resourceMatchType : resourcesMatchType) {
      AttributeDesignatorType attributeDesignator = resourceMatchType.getAttributeDesignator();
      if(attributeDesignator.getAttributeId().equals(ResourceTypeConstants.appcResourcePatientID)) {
        HL7InstanceIdentifierType instance =  getHL7InstanceIdentifier(resourceMatchType);
        if(instance.getRoot().equals(patientID.getRoot())){
          if(instance.getExtension().equals(patientID.getExtension())) {
            return true;
          }
        }
      }
    }
  }
    return false;
}
```

Extrato Código 6 - Verificação se o conjunto de política é raiz dos documentos de consentimento

Com a lógica do observador implementada, apenas é necessário registar o observador na transação. Como o ALERT®HIE utiliza Spring, as suas transações e outras propriedades são carregadas através do conceito bean apresentado anteriormente. Portanto para adicionar um

novo observador a uma transação, apenas é necessário criar o bean correspondente ao observador e fazer a respetiva referência à lista de observadores associada a essa transação, como é demonstrado no Extrato Código 7.

```
<!-- Provide and Register Document Set -->
<bean class="com.alert.hie.xds.repository.transaction.handler.ProvideAndRegisterDocumentSetTransactionHandler">
        ...
        <property name="observers">
          <util:list>
            ...
            <ref bean="patientConsentObserver"/>
          </util:list>
        </property>
</bean>

<bean id="patientConsentObserver" class="com.alert.hie.appc.observer.PatientConsentObserver">
  <constructor-arg type="java.lang.String" name="appcFormatCode" ref="APPCFormatCode"/>
  <constructor-arg type="java.lang.String" name="appcPixCorrelationAction" ref="APPCPixCorrelationAction"/>
</bean>

<bean id="APPCPixCorrelationAction" class="java.lang.String">
        <constructor-arg value="urn:alert:hie:pix:correlation-decision"/>
</bean>

<bean id="APPCFormatCode" class="java.lang.String">
        <constructor-arg value="urn:ihe:iti:appc:2016:consent"/>
</bean>
```

Extrato Código 7 - Registo de um observador numa transação

6.3.1.3 Retirar consentimento

O paciente, ao dar o seu consentimento para o processamento de dados, também o pode retirar a qualquer momento, como foi mencionado na subsecção 3.1.1.1. Como não é possível eliminar a informação pessoal e clínica do paciente, como mencionado na subsecção 3.1.4, só é possível retirar o consentimento do paciente que permitirá negar o acesso às informação do paciente devido ao mecanismo de avaliação de políticas não encontrar a política para fazer avaliação.

Para retirar o consentimento é necessário recorrer à transação de eliminar documentos do perfil de integração do XDS, e para esse efeito criou-se o observador DeletePatientConsentObserver. Esta transação traz como informação a lista com as identificações dos documentos e pastas que são para ser eliminados[24]. Ao intercetar a transação no estado "Pedido validado" é invocado um procedimento na base de dados do ALERT®HIE que verificará se algum dos documentos eliminados é do tipo APPC, caso o resultado seja positivo é retornada a identificação do paciente. Como mencionado na subsecção 5.3.2.3 está pressuposto que todos os documentos relacionados com o consentimento do paciente (documentos do tipos APPC) estejam dentro de uma única pasta. No Extrato Código 8 é demonstrado como é obtido a identificação do paciente com base na lista com as identificações dos documentos.

[24] Apesar do nome da transação aparentar que elimina os documentos, esta apenas marca os documentos como desativados, tal como foi explicado na subsecção 3.1.4.

```
function get_patient_from_entryuuids(i_list_entry_uuids      IN T_VARCHAR_TBL ,
                                     i_document_format_code  IN varchar2,
                                     i_document_type         IN varchar2,
                                     o_patient_root          OUT varchar2,
                                     o_patient_extension     OUT varchar2,
                                     o_error_message         IN OUT varchar2)
  RETURN BOOLEAN IS

  Begin
    Select distinct i.root,i.extension into o_patient_root, o_patient_extension

      FROM XDS_Object x, metadata_object m, Document d, Code c, Identifier i
      Where x.object_type = i_document_type and
      x.entry_uuid in (select column_value FROM TABLE(i_list_entry_uuids))
      and x.entry_uuid = m.root_entry_uuid and d.id_doc = m.id_metadata_object
      and c.description = i_document_format_code and d.id_code_format = c.id_code
      and i.id_identifier = m.patient_id;

     return true;

  EXCEPTION
    WHEN OTHERS THEN
      o_error_message := 'Error getting patient from the list of entryUUIDS';
      return false;
END;
```

Extrato Código 8 - Função de base de dados de obter a identificação do paciente com base na lista de documentos que estão prestes a ser eliminados

O observador, ao receber o resultado do procedimento da base de dados, verifica se é retornada alguma identificação de um paciente, e caso se verifique isso significa que estamos perante um retirar consentimento do paciente, sendo necessário fazer um pedido REST ao ALERT® Security Authorization Framework, exemplificado no Extrato Código 13, de forma a eliminar todos os documentos relacionados ao consentimento do paciente, enviando por parâmetro a sua identificação. Na Figura 69 é apresentado o diagrama de classes com o observador em questão e o fluxo apresentado segue com o descrito no diagrama de sequência apresentado na Figura 41.

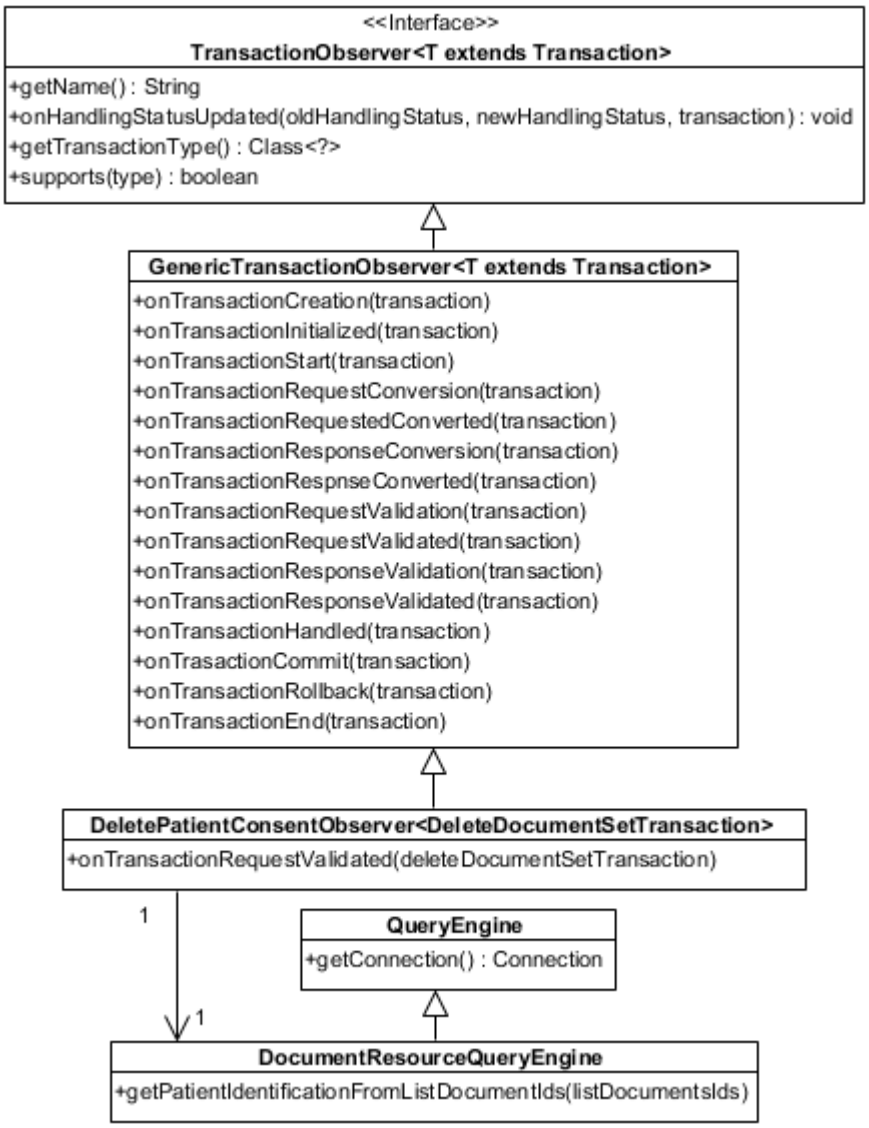


Figura 69 - Diagrama de classes do observador para retirar o consentimento do paciente

6.3.1.4 Consultar Informação

As transações que retornam a informação do paciente terão que ser intercetadas, de modo a verificar se o paciente consentiu ou não à partilha de informação com a instituição que está a realizar o pedido. Dito isto, criou-se um observador genérico de forma a intercetar qualquer tipo de transação e verificar o acesso consoante o consentimento do paciente.

O observador "GenericPepObserver" pode ser utilizado em qualquer uma das transações devido a utilizar a interface "*Transaction*" que é implementada por todas as transações existente no produto, sendo apenas necessário fornecer o tipo de ação que a transação em questão realiza. Uma transação ao chegar ao estado de "Pedido validado", que tenha este observador, irá enviar ao ALERT® Security Authorization PEP os sujeitos, recursos e a ação da transação que posteriormente formulará o pedido para ser enviado ao ALERT® Security Authorization Framework que tomará a decisão e retornará a mesma, conforme é ilustrado na

Figura 52. Na Figura 70 é apresentado o diagrama de classes com as principais associações relacionadas com o observador.

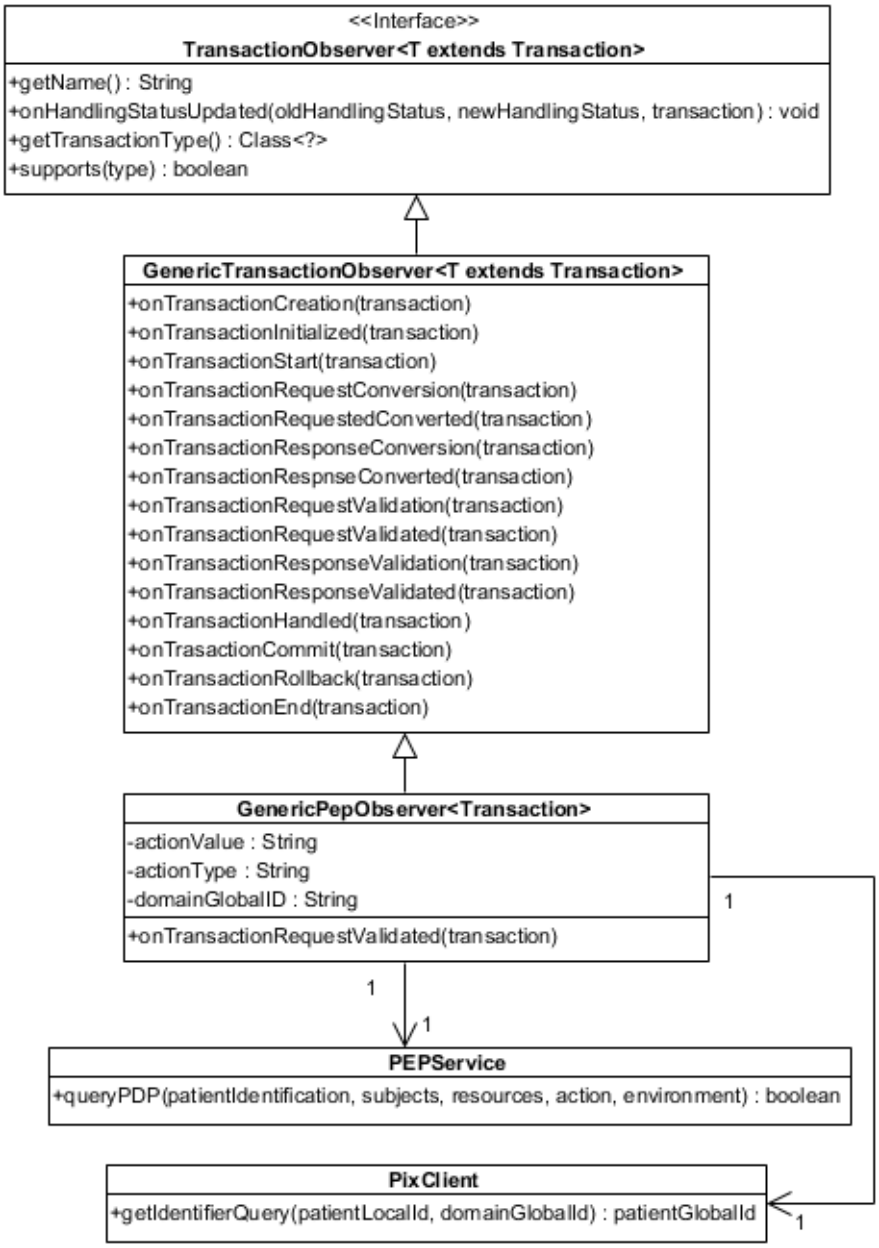


Figura 70 - Diagrama de classes do observador para consultar o acesso à informação do paciente

Como a obtenção da informação e documentos relacionados com o paciente é feita através da identificação global do paciente, sendo esta normalmente associada um PHR (e.g. MyALERT®), é necessário em todas as transações que utilizem este observador obter a identificação global do paciente caso seja enviada a identificação do paciente na instituição, para que seja encontrada o documento de consentimento relacionado com o paciente no ALERT® Security Authorization Framework. Para isso são utilizados os serviços do componente PIXPDQ, que permitem obter a identificação global do paciente através da identificação do paciente na instituição que fez o pedido.

6.3.2 ALERT® HIE Database

Devido à implementação do algoritmo de correlacionamento de informação de pacientes se encontrar na base de dados do ALERT®HIE, tomou-se a decisão de a oposição à decisão individual automatizada ficar dentro da base de dados por questões de desempenho.

O algoritmo de correlacionamento de informação de pacientes tem diversos estados possíveis, conforme foi apresentado na subsecção 4.3.3. O estado que viola o artigo 22º do RGPD é o (A)tivo, pois permite o acesso aos documentos do(s) paciente(s). Este estado é atingido quando o resultado do correlacionamento dos pacientes é superior ou igual ao limite ativo definido, tal como foi explicado na subsecção 4.3.3, violando assim o artigo 22º do RGPD.

Para evitar que o algoritmo de correlacionamento de informação de pacientes correlacione automaticamente os pacientes, foi necessário identificar o(s) ponto(s) em que o algoritmo registava a sua decisão. Existem duas situações em que o algoritmo regista a sua decisão: (i) quando é criado um novo registo do resultado do correlacionamento; (ii) quando é atualizado um registo já existente.

```
procedure verify_pat_consent_correlation(i_id_patient_record IN patient_record.id_patient_record%TYPE,
                                         i_id_patient_record_2 IN patient_record.id_patient_record%TYPE,
                                         io_flg_state IN OUT cross_reference.flg_state%TYPE) is

    l_pat_correlation_decision patient_record.FLG_CORRELATION_CONSENT%TYPE;
    l_pat2_correlation_decision patient_record.FLG_CORRELATION_CONSENT%TYPE;

  begin

    if io_flg_state = pk_pix_constant.g_cross_activ then

        l_pat_correlation_decision := pk_cross_reference_n.get_pat_correlation_consent(
                                                      i_id_patient_record => i_id_patient_record);

        if l_pat_correlation_decision = pk_pix_constant.g_flg_valid_true then
          l_pat2_correlation_decision := pk_cross_reference_n.get_pat_correlation_consent(
                                        i_id_patient_record => i_id_patient_record_2);

          if l_pat2_correlation_decision = pk_pix_constant.g_flg_valid_false then
            io_flg_state := pk_pix_constant.g_cross_candidate;
          end if;
        else
          io_flg_state := pk_pix_constant.g_cross_candidate;
        end if;

     end if;

  end verify_pat_consent_correlation;
```

Extrato Código 9 - Procedimento que consoante a decisão do paciente atualiza o estado do correlacionamento

Portanto, antes de ser feito o registo/atualização do estado do correlacionamento é invocado o procedimento apresentado no Extrato Código 9 que irá verificar, no caso em que o estado decidido pelo algoritmo for do tipo (A)tivo, se ambos os pacientes que estão a ser correlacionados aceitaram a decisão individual automatizada a decisão mantém-se, caso contrário é retornado o estado (C)andidato.

7 Experimentação e avaliação

Uma das funcionalidades mais importante no ALERT® HIE é a correlação de pacientes entre instituições de saúde. Apesar do algoritmo de correlação de pacientes já estar implementado, foi necessário realizar uma reengenharia ao algoritmo, apresentada na subsecção 6.3.2, devido ao facto de este tomar decisões automaticamente e o paciente poder opor-se a essa automatização ao abrigo do RGPD.

Nas próximas secções serão apresentados os objetivos da experimentação, a definição da hipótese, a abordagem preconizada, a preparação da experimentação, a execução, os resultados obtidos e avaliação da experimentação.

7.1 Objetivos

Como foi explicado na subsecção 4.3.3, o algoritmo de correlacionamento tem várias configurações possíveis.

É de ter em conta que o mercado em que o algoritmo vai atuar é um fator crítico. Por exemplo, o atributo “nome completo” num domínio de aplicação pode ser um fator que permite distinguir facilmente registos, enquanto noutros domínios de aplicação este atributo pode não ter esse impacto por existirem muitos registos com o mesmo “nome completo”. Logo, é necessário ter em consideração as variâncias que possam existir de domínio para domínio.

Pretende-se avaliar o desempenho de diferentes configurações, de forma a avaliar qual a melhor configuração para atingir certos valores de precisão e cobertura de correlacionamento de registos de pacientes.

Assim, o objetivo da experimentação passa por avaliar a eficácia do algoritmo de correlacionamento de pacientes do ALERT®HIE. Para tal, será calculada a precisão e cobertura do mesmo em diferentes configurações.

7.2 Abordagem

No sentido de avaliar o algoritmo de correlação de informação de pacientes ir-se-á realizar uma experiência de modo a calcular a precisão (P) e cobertura (C) do mesmo. O algoritmo, ao propôr possíveis candidatos, irá retornar resultados dentro de um conjunto em que poderão existir dois tipos de resultado:

- Verdadeiros positivos (TP): são os resultados dentro do conjunto que são, de facto, o mesmo paciente que iniciou a correlação;

- Falsos positivos (FP): são os resultados dentro do conjunto que não são o mesmo paciente que iniciou a correlação.

Para além do conjunto de resultados, existe também o total da amostra, em que se podem considerar outros dois tipos de resultados:

- Falsos negativos (FN): é um conjunto da amostra que não foi considerado no conjunto de resultados e que, de facto, representam o mesmo paciente que iniciou o correlacionamento;

- Verdadeiros negativos (TN): é o conjunto da amostra que não foi considerado dentro do conjunto de resultados e que, de facto, não representam o mesmo paciente que iniciou o correlacionamento

A seguinte equação demonstra como a precisão é calculada:

$$P = \frac{TP}{TP + FP}$$

Já a cobertura é calculada através:

$$C = \frac{TP}{TP + FN}$$

A Figura 71 representa estes tipos de possíveis condições e fórmulas de cálculo para a precisão e cobertura de uma forma sucinta (Powers, 2011).

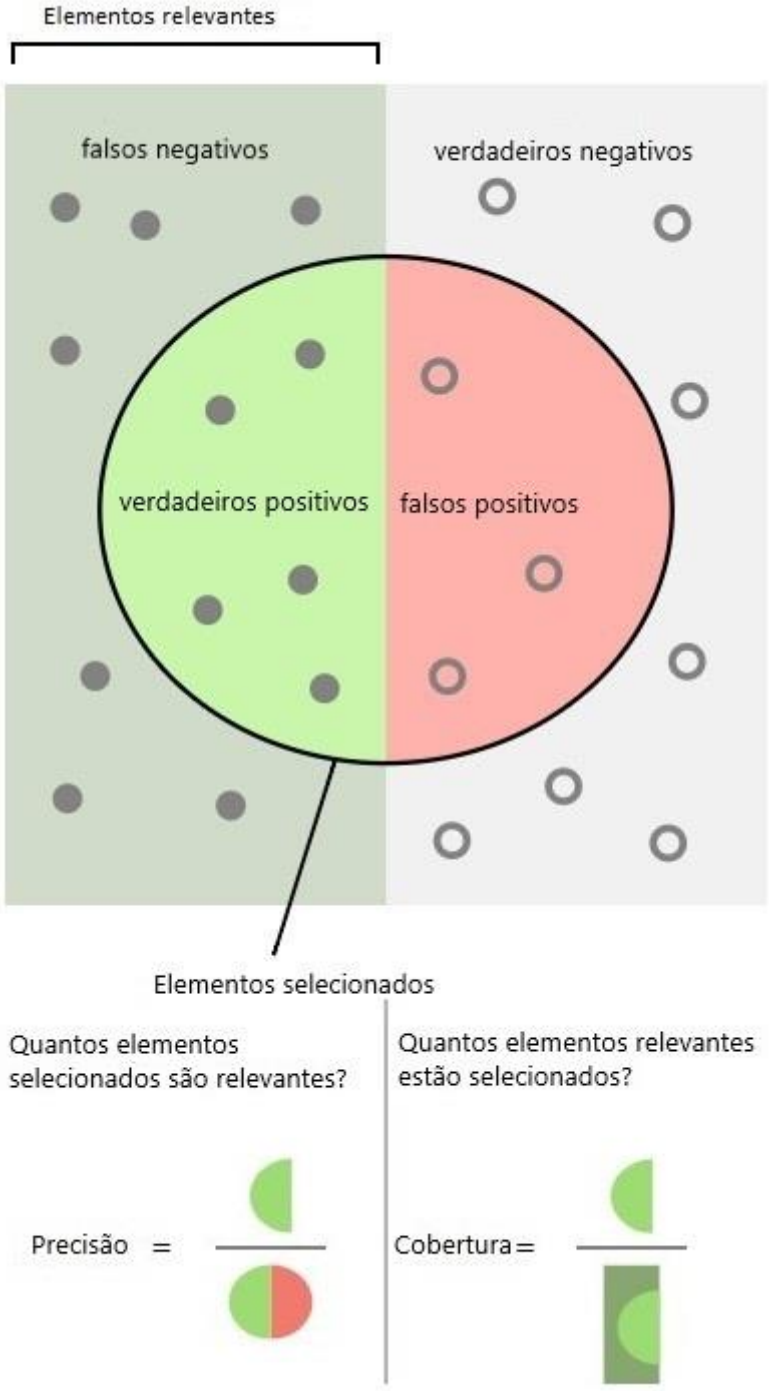


Figura 71 - Precisão e cobertura de uma amostra [adaptado de (Michalis, 2015)]

Os objetivos a atingir após a realização da experimentação são:

- Cobertura deverá ser pelo menos 90%;
- Precisão deverá ser superior a 95%;

A precisão será priorizada em relação à cobertura, pois o algoritmo de correlação de informação de pacientes pode dar acesso à informação pessoal dos pacientes caso a correlação esteja incorreta, afetando a privacidade dos dados pessoais do paciente.

7.3 Preparação

Conforme foi mencionado na secção 7.1 e explicado na subsecção 4.3.3, o algoritmo de correlacionamento de informação de pacientes permite diversas configurações. É do interesse da organização que uma das experiências a realizar seja com a configuração instalada por omissão, de forma a apurar a precisão e cobertura desta configuração. Também se irão realizar experiências com outras configurações devido às razões mencionadas na secção 7.1.

7.3.1 Ambiente de execução

O ambiente de execução da experimentação será no ambiente de desenvolvimento da ALERT, pois os fatores de desempenho e quantidade de memória utilizada não têm influência sobre os objetivos determinados. Contudo, para não haver interferências enquanto os outros colaboradores estejam a trabalhar sobre o ambiente, decidiu-se criar três novas instituições fictícias (A, B e C) no ALERT®HIE de forma a simular um ambiente real, mas em que não houvesse interferência externas. Cada uma das instituições terá a sua amostra com informação de pacientes que depois se correlacionará com a informação dos pacientes das outras instituições criadas.

No sentido de obter informação de pacientes para realização da experimentação, decidiu-se criar um algoritmo que gera pacientes de forma aleatória, de modo a não haver interferência humana sobre a amostra. Todos os pacientes gerados serão criados na instituição A, posteriormente 90% serão repartidos para a instituição B e os outros 10% para a instituição C. Os pacientes da instituição C não sofrerão qualquer transformação, portanto espera-se que o algoritmo correlacione com precisão de 100% os pacientes da instituição A com os da C.

Já os pacientes da instituição B passarão por um algoritmo que aleatoriamente efetuará uma ou mais transformações nos seus atributos de informação. O objetivo da amostra da instituição B é verificar a precisão e cobertura do algoritmo, consoante a configuração utilizada, quando os dados inseridos não são exatamente iguais nas duas instituições. As transformações podem representar um possível erro humano durante a criação dos pacientes na instituição que acontece em situações reais, ou transformações de forma a serem outros pacientes com atributos de informação semelhantes.

Devido a alguns dos pacientes poderem sofrer grandes alterações aleatoriamente nos seus atributos de informação, é possível que estes venham a correlacionar com outros pacientes que existam na instituição A ou C. Na Figura 72 é apresentado sistematicamente o ambiente em que a experiência se irá realizar.

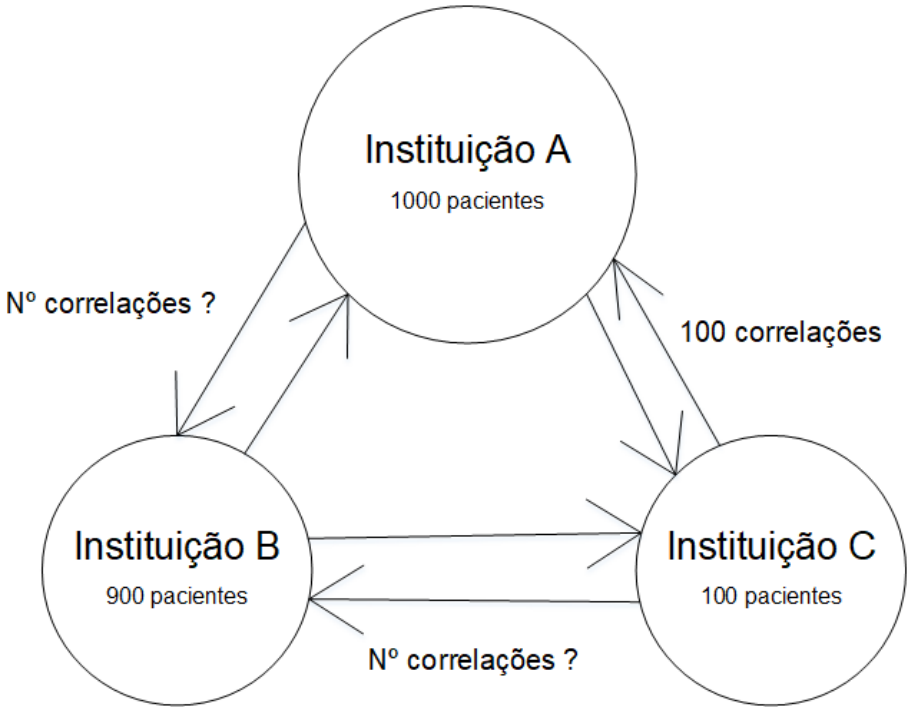


Figura 72 - Ambiente da experimentação

7.3.2 Estrutura dos dados de paciente

O algoritmo de geração de informação de pacientes teve em conta todos os atributos de informação suportados pelo algoritmo de correlacionamento de pacientes, apresentados na subsecção 4.3.3. O modelo relacional que permite visualizar as relações entre os atributos é ilustrado na Figura 43.

As transformações realizadas sobre os pacientes que serão criados na instituição B tiveram em conta todos os atributos de informação. As transformações podem ser de dois tipos: (i) transformação por erros de inserção humana; (ii) transformação noutro paciente com alguns atributos de informação semelhantes.

Quanto ao primeiro tipo de transformação, é gerado um número aleatório de 0 a 100 é realizado um número de transformações de acordo com a Tabela 14. Em relação aos erros de inserção humana, apenas eram feitas pequenas alterações nos atributos de informação, como por exemplo:

- Em campos de texto livre é retirada a acentuação ou uma das palavras ou letras de uma palavra;
- Nos campos numéricos um dos algarismos sofre uma substituição por outro;
- Na data de nascimento é modificado o dia;
- Nos campos de seleção é inserido um novo valor dos possíveis.

Tabela 14 - Tabela com número de possíveis transformações para erros humanos

Número gerado	Número de transformações
<= 70	1
<= 80	2
<= 90	3
<= 95	4
<= 100	5

Em relação ao segundo tipo de transformação o número de campos a serem transformados varia entre 3 e 10, sendo que os atributos de informação selecionados receberão um novo valor.

7.3.3 Configurações

Como mencionado na secção 7.1, pretende-se testar diversas configurações, de forma a averiguar a precisão e cobertura do algoritmo de correlacionamento de informação dos pacientes. A subsecção 4.3.3 apresentou os tipos de configurações que o algoritmo de correlacionamento de informação de pacientes permite.

No Anexo C são apresentados todos os detalhes das cinco configurações que serão utilizadas durante a execução da experimentação que será abordada na secção 7.4.

7.4 Execução e resultados

Nas seguintes subsecções serão apresentados os resultados de precisão e cobertura obtidos, após a execução do algoritmo de correlacionamento nos pacientes gerados em cada umas das configurações apresentadas no Anexo C. Posteriormente serão apresentados os detalhes dos questionários realizados de forma a aferir se os pacientes da instituição A que foram transformados continuam a ser os mesmos e os resultados atingidos. Por fim, os valores de precisão e cobertura serão novamente recalculados consoante os resultados obtidos nos questionários.

7.4.1 Primeira fase de resultados

A primeira fase de resultados consiste no cálculo da precisão e cobertura do algoritmo de correlacionamento, com base na decisão tomada pelo do algoritmo de geração de pacientes ao realizar as transformação nos pacientes. A Tabela 15 apresenta os resultados obtidos para a primeira fase da experimentação.

Tabela 15 - Resultados da primeira fase da experimentação

	Total	Verdadeiros positivos (TP)	Falsos positivos (FP)	Falsos Negativos (FN)	Precisão	Cobertura
Configuração 1	431	354	77	127	82,13%	73,60%

	Total	Verdadeiros positivos (TP)	Falsos positivos (FP)	Falsos Negativos (FN)	Precisão	Cobertura
Configuração 2	480	427	59	54	88,96%	88,77%
Configuração 3	451	410	41	71	90,91%	85,24%
Configuração 4	449	419	30	62	93,32%	87,11%
Configuração 5	437	424	13	57	97,03%	88,15%

7.4.2 Questionário

Os resultados obtidos na Tabela 15, foram calculados de acordo com a decisão da transformação realizada pelo algoritmo de geração de pacientes sobre os pacientes. Contudo, de forma a obter a precisão e cobertura do algoritmo de correlacionamento, em cada uma das configurações, sem a influência da decisão tomada pelo algoritmo de geração de pacientes, decidiu-se realizar um questionário de modo a obter o *gold standard*[25].

Porém, devido ao tamanho da amostra ser demasiado grande para o questionário, considerou-se apenas os pacientes que causam diretamente um maior impacto nos resultados da precisão e cobertura obtidos anteriormente, neste caso todos os pacientes que foram considerados como falsos positivos ou negativos em qualquer uma das configurações. Dito isto, no total foram considerados 227 pacientes, sendo que estes foram divididos por 8 questionários com aproximadamente 30 pacientes cada um.

Os questionários foram entregues aos inquiridos num ficheiro excel, em que este comparavam os pares de pacientes e respondiam "Sim/Não", com o intuito de verificar se são ou não o mesmo paciente. No final obteve-se um total 60 respostas, aproximadamente 7 respostas por cada questionário.

De forma a analisar os resultados obtidos, as respostas foram agrupadas por questionário, onde se substituiu as respostas "Sim e Não" pelos valores 1 e -1 respetivamente, com a finalidade de se obter a média destas. Com isto, é possível aferir que os resultados superiores a 0 indicam que os inquiridos decidiram que o par de pacientes é o mesmo, e abaixo de 0 indica que estes não são o mesmo. Caso a média seja igual a 0, significa que não houve consenso entre os inquiridos.

No total houve 8 ocorrências em que a média das respostas foi igual a 0, sendo que nestes casos o algoritmo de correlacionamento deverá registar o par de pacientes como Candidatos. Nas Figuras 73, 74, 75, 76, 77, 78, 79 e 80 são apresentados os gráficos de distribuição das respostas por cada questionário.

[25] O termo *gold standard* refere-se à melhor precisão de resultados acessíveis sob condições razoáveis. (Cardoso et al., 2014).

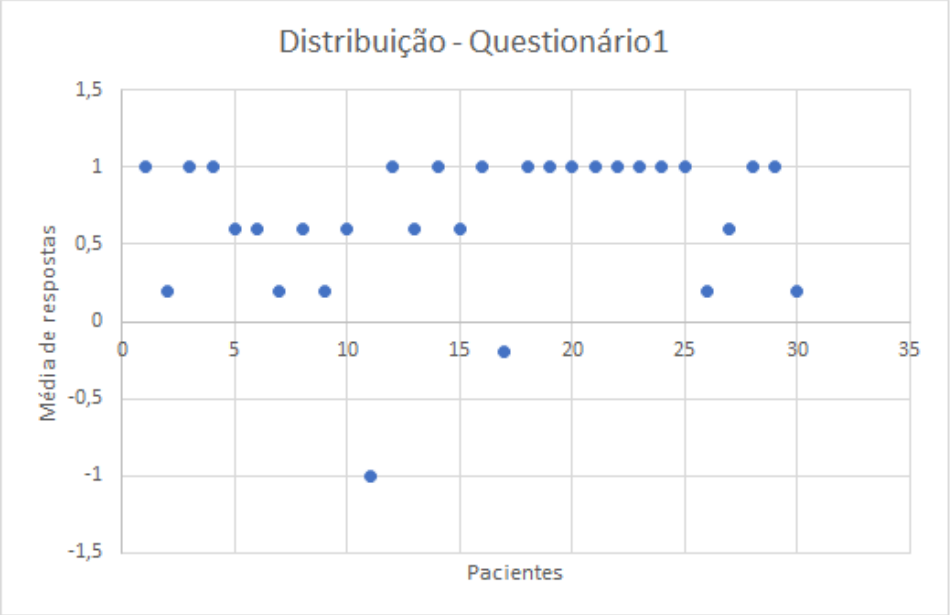


Figura 73 - Distribuição dos resultados no questionário 1

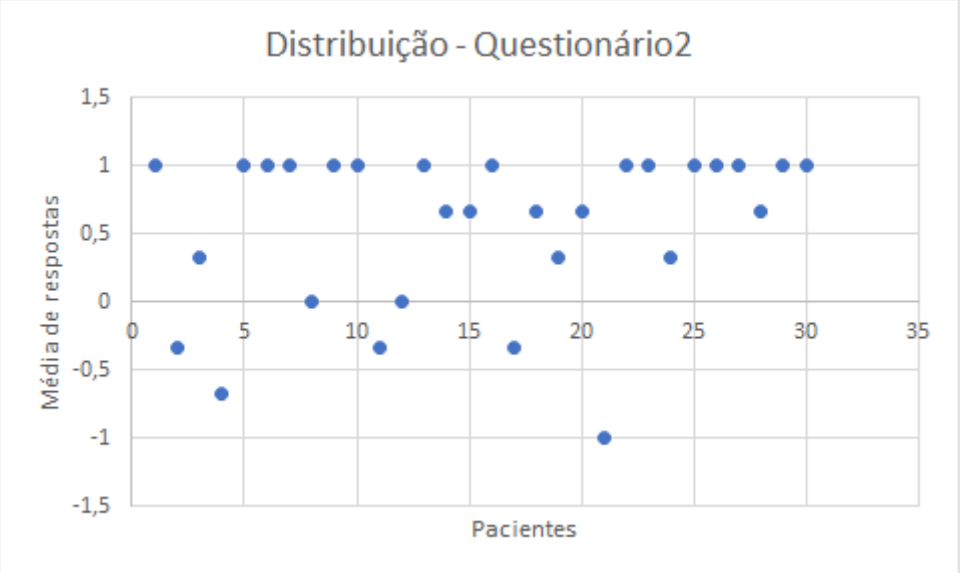


Figura 74 - Distribuição dos resultados no questionário 2

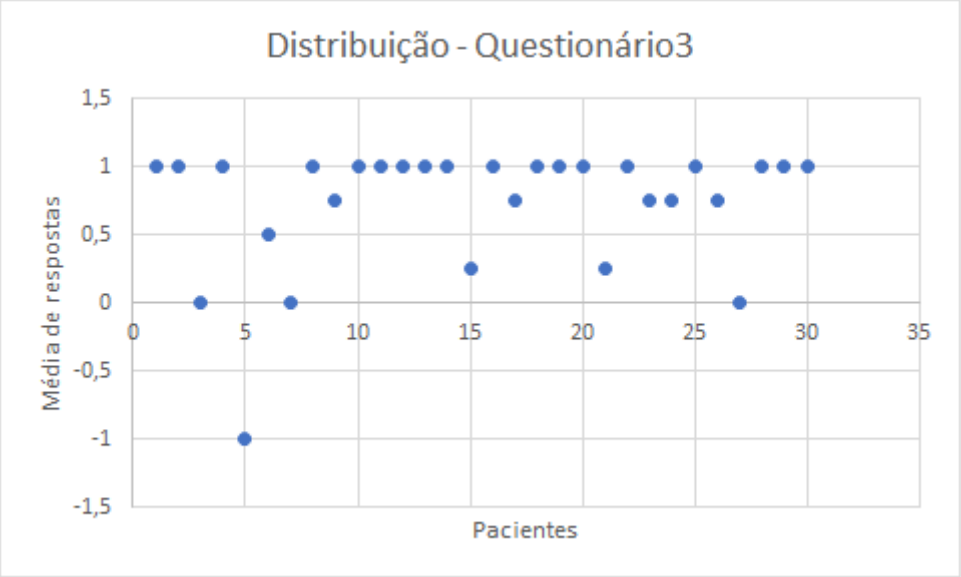


Figura 75 - Distribuição dos resultados no questionário 3

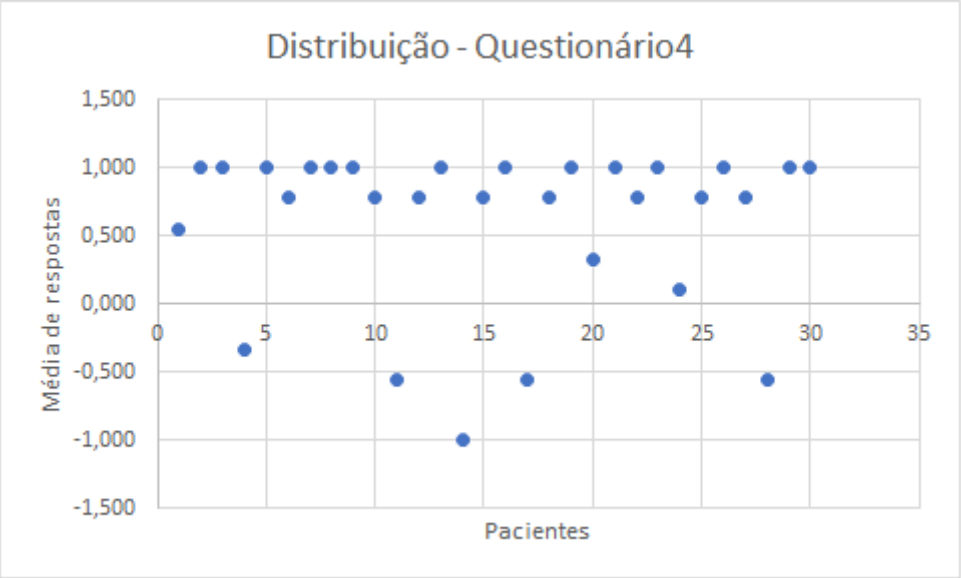


Figura 76 - Distribuição dos resultados no questionário 4

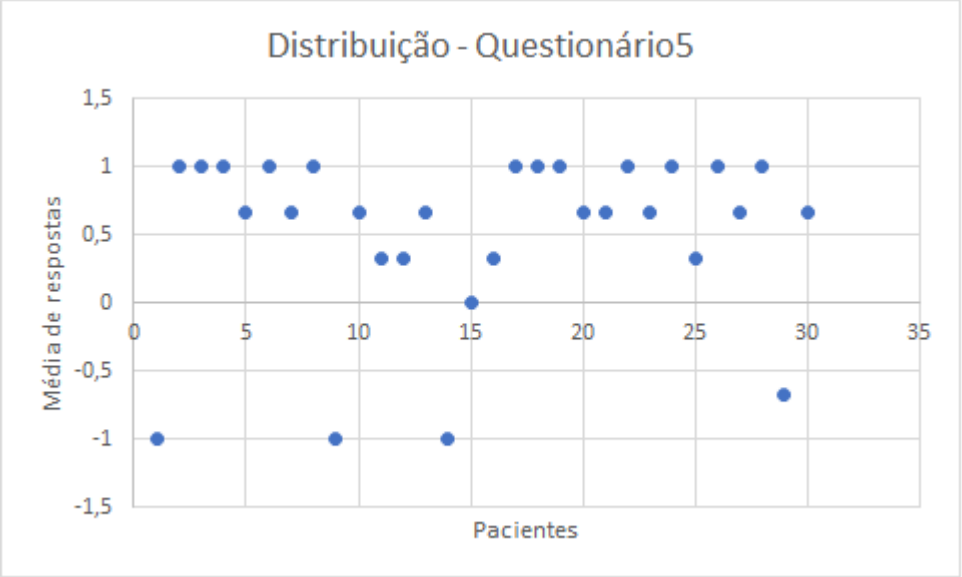


Figura 77 - Distribuição dos resultados no questionário 5

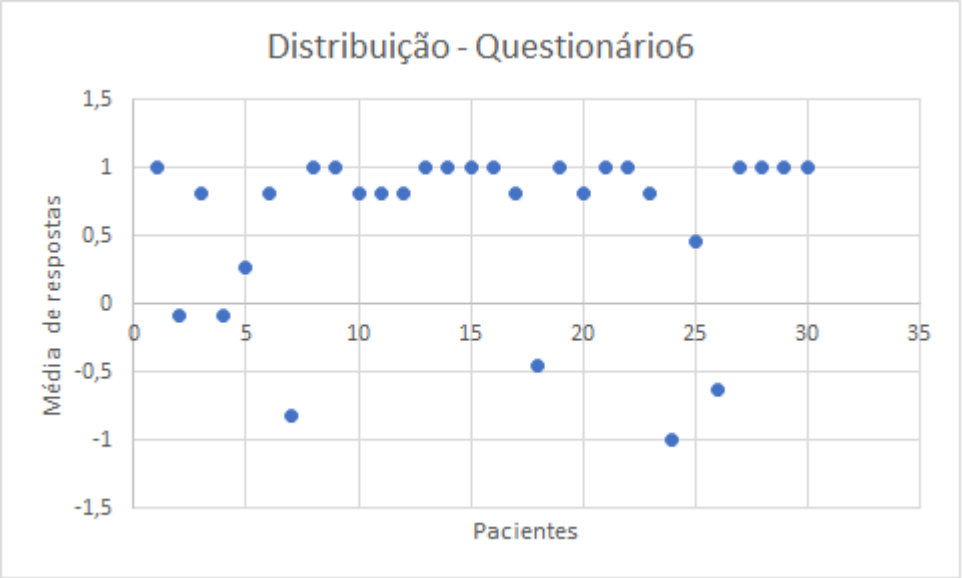


Figura 78 - Distribuição dos resultados no questionário 6

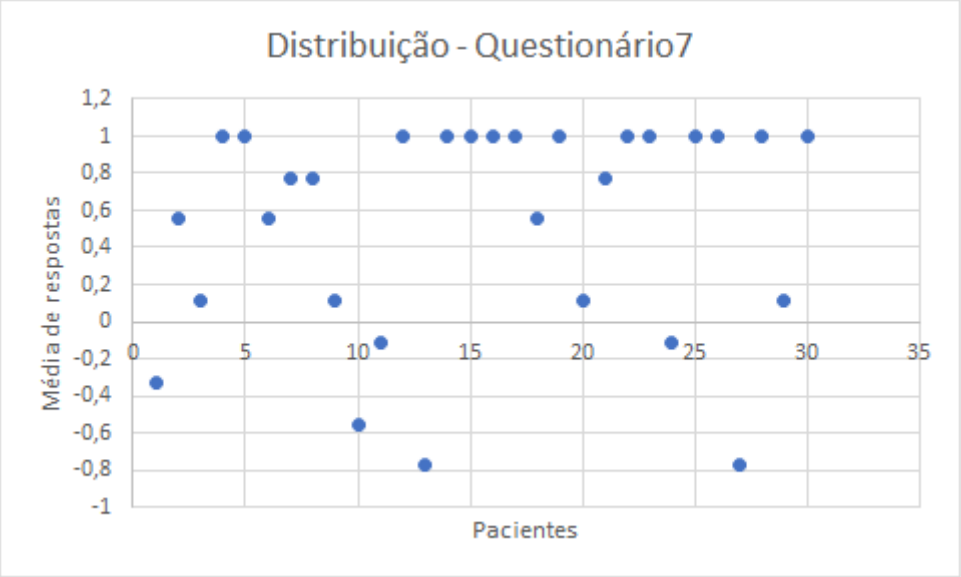


Figura 79 - Distribuição dos resultados no questionário 7

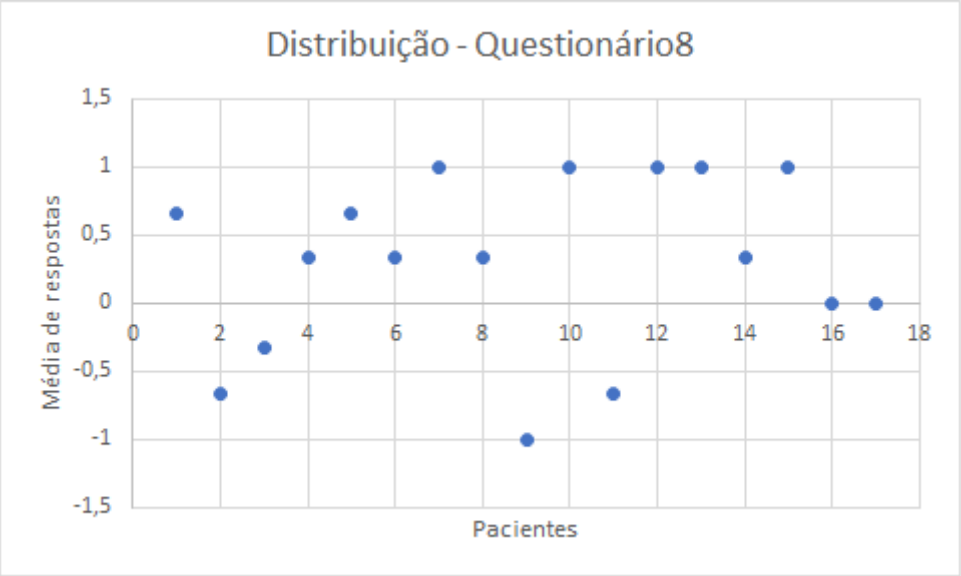


Figura 80 - Distribuição dos resultados no questionário 8

7.4.3 Resultado final

Após a obtenção dos resultados dos questionários, atualizou-se a decisão de cada par de pacientes e calculou-se novamente os valores de precisão e cobertura para cada configuração, sendo que estes valores são apresentados na Tabela 16.

Tabela 16 - Resultados da segunda fase da experimentação

	Total	Verdadeiros positivos (TP)	Falsos positivos (FP)	Falsos Negativos (FN)	Precisão	Cobertura
Configuração 1	431	397	34	141	92,11%	73,79%
Configuração 2	480	471	9	67	98,13%	87,55%
Configuração 3	451	446	5	92	98,89%	82,90%
Configuração 4	449	446	3	92	99,33%	82,90%
Configuração 5	437	435	2	103	99,54%	80,86%

7.5 Avaliação

Ao analisar os resultados obtidos nas Tabelas 15 e 16, é possível verificar que a utilização de mais atributos de informação permite obter uma maior precisão do algoritmo. Quanto à cobertura, na Tabela 15 os valores obtidos também sobem progressivamente quantos mais atributos de informação existirem. No entanto, após a obtenção dos resultados dos questionários e recalculados os valores de cobertura, este padrão já não se verifica, como é percetível na Tabela 16. Este comportamento da cobertura poderá estar relacionado com o facto de estarem a serem considerados muitos atributos de informação, sendo que a inserção de erros do primeiro tipo nos atributos de informação possa comprometer os resultados de se considerar todos os pacientes, resultando num maior número de falsos negativos.

Quanto aos objetivos definidos, todas as configurações, exceto a primeira, atingiram o valor de precisão definido de 95%. Porém, nenhuma das configurações atingiu o objetivo da cobertura pretendido. No entanto, a configuração 2 fica próxima do valor de cobertura esperado, com cerca de 87.55%.

Como foi mencionado na subsecção 7.4.2, os inquiridos dos questionários não conseguiram decidir entre os 227 pacientes se 8 eram ou não o mesmo. Na Tabela 17 são demonstrados os resultados de correlacionamento obtidos para estes pacientes, ao longo das configurações utilizadas. À medida que são utilizados um maior número de atributos de informação é percetível que os pares de pacientes deixam de ser classificados como ativos, mas sim como candidatos, o que permitirá posteriormente que a decisão seja feita por um humano. Esta é a melhor classificação para estes pacientes, devido ao facto de não se decidir se são ou não o mesmo paciente e os documentos clínicos não serem partilhados até que um ser humano decida que são o mesmo paciente.

Tabela 17 – Resultados dos correlacionamentos em que não houve consenso entre os inquiridos

Configuração	Nº de pares pacientes correlacionados como ativos	Nº de pares de pacientes correlacionados como candidatos
Configuração 1	6	2
Configuração 2	4	4
Configuração 3	2	6
Configuração 4	3	5
Configuração 5	1	7

Concluindo, se o principal objetivo do algoritmo é correlacionar com quase 100% de precisão a melhor configuração a utilizar é a 5, pois utiliza todos os atributos de informação. No entanto, esta precisão pode comprometer a cobertura de todos os pacientes. Se o objetivo do algoritmo é tentar cobrir o maior número de pacientes e a sua correlação seja com uma eficácia acima de 95% a melhor configuração é a 2.

8 Conclusão

Este capítulo descreve as conclusões retiradas, de acordo com o trabalho realizado e os problemas e objetivos identificados anteriormente.

Por fim, é realizada uma apreciação global acerca do projeto e aprendizagem obtida a nível pessoal e profissional.

8.1 Visão geral

O principal objetivo desta adaptação era identificar e resolver os requisitos necessários para que o produto ALERT®HIE cumprisse com as exigências do RGPD. De modo alcançar este objetivo, foram analisados os conceitos teóricos necessários para a contextualização do negócio e do problema em questão, nomeadamente os conceitos EHR, interoperabilidade clínica e privacidade dos dados. Em seguida, analisou-se o RGPD, que por consequência permitiu aferir os requisitos necessários para o seu cumprimento. Identificados os requisitos necessários, estudou-se o produto em foco neste projeto, de forma a verificar o estado atual de cumprimento e reconhecer os problemas inerentes.

Com os problemas identificados, procedeu-se a um estudo de possíveis soluções que auxiliassem na resolução dos mesmos, sendo procuradas soluções para resolver o problema do consentimento e cifragem da base de dados. A solução escolhida para resolver o problema do consentimento e oposição à decisão individual automatizada foi o perfil de integração APPC, pois este permite ao paciente uma escolha mais fina sobre quem pode aceder à sua informação pessoal e clínica. Já a solução escolhida para cifragem foi o Oracle TDE, visto que permite cifrar a informação sensível das ameaças externas sem comprometer a lógica de negócio existente na base de dados.

Apesar de se ter escolhido uma solução com o intuito de resolver o problema da cifragem, a sua implementação na solução ficou fora do âmbito do trabalho realizado, devido esta ser uma solução que acarreta custos e necessita de autorizações por parte da organização para a sua implementação.

Segundo o artigo 29º da portaria portuguesa que subscreve o RGPD, aprovada no dia 14 de junho de 2019 pela Assembleia da República e publicado no Diário da República no dia 08 de agosto de 2019, o consentimento para uso e partilha de informação de saúde não é necessário, visto esta reger-se pelo princípio da necessidade de conhecer a informação (Assembleia da República, 2019a, pp. 16–17, 2019b). Apesar do consentimento já não ser necessário no mercado português, o consentimento pode ser necessário em outros mercados europeus e extra-europeus. Para além disto, a solução adotada permitirá dar uma escolha ao paciente sobre quem pode aceder à sua informação e auxiliou na implementação do problema da oposição à decisão individual automatizada existente. Para além disto, o mecanismo de acesso implementado poderá ser utilizado para outros fins não relacionados com o consentimento do paciente, o que enriquece a solução.

8.2 Objetivos atingidos

Na Tabela 18 é apresentado o estado de cumprimento dos requisitos definidos anteriormente na Tabela 1.

O consentimento do paciente foi implementado com sucesso, permitindo assim aos pacientes darem o seu consentimento de partilha e escolher com que instituições a sua informação pode ser partilhada.

Quanto à oposição à decisão individual automatizada, os pacientes neste momento podem não ficar sujeitos à decisão tomada pelo algoritmo de correlacionamento de informação. Para isso, a instituição apenas terá de partilhar uma política de consentimento que não consinta à decisão, como demonstrado na subsecção 6.3.1.1.

A notificação aos destinatários não se implementou, no entanto, o ALERT®HIE já cumpre parte deste requisito ao conseguir saber com quem a informação do paciente foi partilhada. Além disso, a não implementação deste requisito não põe em causa a licitude do tratamento, nem a privacidade dos dados pessoais.

O implementação do APPC, ao reutilizar as transações já imlementadas do perfil de integração XDS, que por sua vez já tem os seus próprios eventos de auditoria, fez com que não fosse necessário implementar novos eventos de auditoria. Portanto, a implementação do APPC faz com que o ALERT® HIE cumpra com os eventos de auditoria.

No que diz respeito à cifragem, foi proposta uma solução que permite a cifragem dos conteúdos da base de dados que não compromete a lógica de negócio existente nesta. No entanto a sua implementação ficou fora do âmbito do trabalho realizado, como mencionado na secção 8.1.

Tabela 18 - Objetivos atingidos

Requisitos	Cumprimento pelo ALERT® HIE
Consentimento	✓
Acesso aos dados pessoais	✓
Retificar dados pessoais	✓
Apagamento dos dados pessoais	Não se aplica
Limitação do tratamento	✓

Requisitos	Cumprimento pelo ALERT® HIE
Notificação aos destinatários dos dados pessoais	✓/×
Portabilidade dos dados	✓
Oposição ao tratamento	Não se aplica
Oposição às decisões individuais automatizadas	✓
Auditoria de eventos	✓
Cifragem	✓/×
Mecanismos de autenticação e autorização	✓
Disponibilidade	✓
Resiliência	✓

A experimentação realizada foi sobre o algoritmo de correlacionamento de informação de pacientes do ALERT® HIE, sendo avaliadas a precisão e a cobertura do algoritmo em diferentes configurações testadas. Depois da execução da experimentação foi possível analisar que quantos mais atributos de informação forem utilizados na configuração, maior será a precisão do algoritmo, mas a cobertura do mesmo poderá ser comprometida devido à possível existência de erros humanos na inserção dos dados dos pacientes. Portanto, pode-se concluir que o algoritmo de correlacionamento de informação de pacientes atinge valores de precisão muito significativos, sendo recomendável que os pacientes não se oponham à decisão individual automatizada.

8.3 Limitações e trabalho futuro

No que diz respeito às limitações da solução XACML implementada no ALERT® Security Authorization Framework, esta solução não considera as obrigações existentes nas políticas e conjuntos de políticas que devem ser aplicadas no retorno antes de ser dado o acesso. Esta funcionalidade é interessante para que ocorram certos eventos antes de ser dado acesso, como por exemplo a auditoria de acesso quando estamos perante um caso de *break the glass*[26].

A estrutura do consentimento considerada serve para os requisitos necessários para o cumprimento do RGPD. Porém, a solução está preparada para evoluir o tipo de consentimento utilizado consoante a evolução do produto ALERT®HIE.

Quanto à experimentação realizada, nenhuma das configurações testadas usou o atributo de informação morada, devido a este não estar totalmente implementado no algoritmo de correlacionamento. No entanto, como este atributo de informação pode ser bastante instável, os possíveis resultados obtidos da experimentação não deveriam ser muito diferentes dos resultados obtidos. O algoritmo de geração de pacientes também apenas considerou que os pacientes tinham uma nacionalidade, o que é uma possível melhoria para uma experimentação futura, devido à possibilidade de os pacientes terem mais que uma nacionalidade.

Após a obtenção de feedback dos inquiridos quanto ao questionário realizado, os seres humanos têm opiniões diferentes sobre os atributos de informação que caracterizam melhor os pacientes. Portanto, teria sido interessante realizar um questionário de forma a conhecer

[26] O *break the glass* consiste num profissional de saúde que não tem acesso a determinada informação, ganhar acesso em ocasiões especiais que deverão implicar o registado do motivo (Petritsch, 2014, p. 9).

quais os atributos de informação que são considerados mais relevantes para a identificação de um paciente e criar uma configuração com os respetivos atributos. Além disso, a experimentação poderia ser melhorada ao elaborar questionários que englobassem todos os pacientes que sofreram transformações, como também o número de respostas por questionário ter sido maior de forma a ter uma maior relevância estatística.

8.4 Apreciação final

Considero que desenvolvi conhecimentos sobre a importância da privacidade dos dados no mundo digital e conceitos de negócio sobre a partilha de informação na área da saúde. Além disso, as capacidades de pesquisa e aprendizagem individual foram sem dúvida melhoradas, como também as competências de integração numa equipa no contexto empresarial.

Quanto ao tema, de início foi difícil aprender os novos conceitos relacionados com a privacidade e proteção de dados, necessários para o cumprimento de um novo regulamento que entrou em vigor há apenas 1 um ano. Para além disso, o domínio de negócio em que o produto ALERT®HIE está inserido já contém muitos conceitos para partilha de informação de saúde, sendo necessário conhecer os processos de negócio já existentes e identificar os problemas existentes no produto.

Os principais requisitos propostos foram atingidos, de modo a que neste momento o ALERT® HIE tem uma solução para o consentimento do paciente que permite dar escolhas ao paciente e que auxilia também no problema da oposição à decisão individual automatizada. Além disso, a solução de consentimento desenvolvida pode ser evoluída de forma a dar escolha mais granulares, consoante a evolução do produto ALERT® HIE.

Referências

ALERT Life Sciences Computing, 2018a. ALERT® HEALTH INFORMATION EXCHANGE também comercializado como HEALTH BOX® | ALERT® ONLINE - PT [WWW Document]. URL http://www.alert-online.com/pt/hie (accessed 10.15.18).

ALERT Life Sciences Computing, 2018b. Missão e valores | ALERT® ONLINE - PT [WWW Document]. URL http://www.alert-online.com/pt/mission-values (accessed 11.27.18).

ALERT Life Sciences Computing, 2018c. Os nossos clientes | ALERT® ONLINE - PT [WWW Document]. URL http://www.alert-online.com/pt/customers (accessed 11.27.18).

Apache, 2019. Apache Lucene - Welcome to Apache Lucene [WWW Document]. URL http://lucene.apache.org/ (accessed 2.22.19).

Apache, 2018. Apache Tomcat® - Welcome! [WWW Document]. URL http://tomcat.apache.org/ (accessed 1.7.19).

Assembleia da República, 2019a. Texto de substituição da proposta de lei Nº 120/XIII/3.ª.

Assembleia da República, 2019b. Lei nº 58/2019. Diário da República Eletrónico 38.

Atil, G., 2016. Reading Data From Oracle Data Files (without Connecting Database) – Gokhan Atil's Blog [WWW Document]. URL https://gokhanatil.com/2016/06/reading-data-from-oracle-data-files-without-connecting-database.html (accessed 2.15.19).

Axiomatics, 2019. 100% Pure XACML [WWW Document]. URL https://www.axiomatics.com/100-pure-xacml/ (accessed 4.23.19).

Babar, N., 2019. The Levenshtein Algorithm [WWW Document]. URL https://www.cuelogic.com/blog/the-levenshtein-algorithm (accessed 2.23.19).

Bamberger, K.A., Mulligan, D.K., 2011. New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry.

Beebe, C., 2018. Introduction to Health Level Seven (HL7) International Organization Process Orientation.

Benson, T., 2012. Principles of Health Interoperability HL7 and SNOMED.

Benson, T., Grieve, G., 2016. Principles of Health Interoperability: SNOMED CT, HL7 and FHIR, 3rd ed.

Cardoso, J.R., Pereira, L.M., Iversen, M.D., Ramos, A.L., 2014. What is gold standard and what is ground truth? Dental Press J. Orthod. 19, 27–30. https://doi.org/10.1590/2176-9451.19.5.027-030.ebo

Carrol, Á., Corbridge, R., 2016. National Electronic Health Record Strategic Business Case.

Clark, J., van Oorschot, P.C., 2013. SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements, in: 2013 IEEE Symposium on Security and Privacy. IEEE, pp. 511–525. https://doi.org/10.1109/SP.2013.41

Dey, N., Ashour, A.S., Fong, S.J., Borra, S., 2018. U-Healthcare monitoring systems. Volume 1, Design and applications. Academic Press.

Digital Imaging and Communication in Medicine, 2018. DICOM Standard [WWW Document]. URL

https://www.dicomstandard.org/ (accessed 11.15.18).

Docker, 2018. What is a Container | Docker [WWW Document]. URL https://www.docker.com/resources/what-container (accessed 1.30.19).

Docker, 2017. About images, containers, and storage drivers | Docker Documentation [WWW Document]. URL https://docs.docker.com/v17.09/engine/userguide/storagedriver/imagesandcontainers/ (accessed 1.30.19).

eHGI, 2012. DISCUSSION PAPER ON SEMANTIC AND TECHNICAL INTEROPERABILITY Proposed by the eHealth Governance Initiative.

FEI Systems, 2018a. Consent2Share [WWW Document]. URL http://www.feisystems.com/what-we-do/health-it-application-development/consent2share/ (accessed 12.27.18).

FEI Systems, 2018b. Consent2Share [WWW Document]. URL https://github.com/bhits/consent2share

FEI Systems, 2018c. Consent2Share Technical Components BluePrint.

FEI Systems, 2017a. Consent2Share V3.4.0 Provider User Guide.

FEI Systems, 2017b. Consent2Share User Interface [WWW Document]. URL https://github.com/bhits/c2s-ui (accessed 12.27.18).

Hall, T., 2019. ORACLE-BASE - Transparent Data Encryption (TDE) in Oracle 10g Database Release 2 [WWW Document]. URL https://oracle-base.com/articles/10g/transparent-data-encryption-10gr2 (accessed 2.15.19).

Health Level Seven International, 2019. Introduction to OIDs [WWW Document]. URL http://www.hl7.org/Oid/information.cfm (accessed 1.30.19).

Health Level Seven International, 2018a. Health Level Seven International - Homepage [WWW Document]. URL https://www.hl7.org/ (accessed 10.15.18).

Health Level Seven International, 2018b. About Health Level Seven International [WWW Document]. URL http://www.hl7.org/about/ (accessed 11.13.18).

Health Level Seven International, 2018c. HL7 Standards Product Brief - HL7 Version 2 Product Suite | HL7 International [WWW Document]. URL http://www.hl7.org/implement/standards/product_brief.cfm?product_id=185 (accessed 12.5.18).

Health Level Seven International, 2018d. HL7 Standards Product Brief - HL7 Version 3 Product Suite | HL7 International [WWW Document]. URL https://www.hl7.org/implement/standards/product_brief.cfm?product_id=186 (accessed 12.6.18).

Health Level Seven International, 2018e. HL7 Standards Product Brief - CDA® Release 2 | HL7 International [WWW Document]. URL http://www.hl7.org/implement/standards/product_brief.cfm?product_id=7 (accessed 12.6.18).

Health Level Seven International, 2018f. HL7 Standards Product Brief - HL7 Fast Healthcare Interoperability Resources Specification (FHIR®), DSTU Release 1 | HL7 International [WWW Document]. URL http://www.hl7.org/implement/standards/product_brief.cfm?product_id=343 (accessed 12.6.18).

Heart, T., Ben-Assuli, O., Shabtai, I., 2017. A review of PHR, EMR and EHR integration: A more

personalized healthcare and public health policy. Heal. Policy Technol. 6, 20–25. https://doi.org/10.1016/J.HLPT.2016.08.002

IEEE, 1990. IEEE Standard Glossary of Software Engineering Terminology. IEEE. https://doi.org/10.1109/IEEESTD.1990.101064

IHE International, 2018. Gazelle | INTEROPERABILITY; CONFORMANCE TESTING FOR E-HEALTH INFORMATION SYSTEMS [WWW Document]. URL https://gazelle.ihe.net/ (accessed 7.4.19).

IHE ITI Technical Committee, 2018a. IHE IT Infrastructure (ITI) Technical Framework.

IHE ITI Technical Committee, 2018b. IHE IT Infrastructure Technical Framework Supplement Advanced Patient Privacy Consents (APPC).

IHE ITI Technical Committee, 2018c. IHE IT Infrastructure 5 Technical Framework Volume 3 IHE ITI TF-3 Cross-Transaction Specifications and Content Specifications.

InfoWatch Analytics Center, 2017. Global Data Leakage Report.

Integrating the Healthcare Enterprise, 2019. Profiles - IHE International [WWW Document]. URL https://www.ihe.net/resources/profiles/ (accessed 9.22.19).

Integrating the Healthcare Enterprise, 2018a. IHE Process - IHE International [WWW Document]. URL https://www.ihe.net/about_ihe/ihe_process/ (accessed 11.16.18).

Integrating the Healthcare Enterprise, 2018b. IHE Domains - IHE International [WWW Document]. URL https://www.ihe.net/ihe_domains/ (accessed 11.16.18).

Integrating the Healthcare Enterprise, 2018c. Profiles - IHE Wiki [WWW Document]. URL https://wiki.ihe.net/index.php/Profiles#IHE_IT_Infrastructure_Profiles (accessed 10.15.18).

Integrating the Healthcare Enterprise, 2018d. Audit Trail and Node Authentication - IHE Wiki [WWW Document]. URL https://wiki.ihe.net/index.php/Audit_Trail_and_Node_Authentication (accessed 12.13.18).

Integrating the Healthcare Enterprise, 2017. Basic Patient Privacy Consents - IHE Wiki [WWW Document]. URL https://wiki.ihe.net/index.php/Basic_Patient_Privacy_Consents (accessed 12.18.18).

Integrating the HealthCare Enterprise, 2019. IHE Format Codes - IHE Wiki [WWW Document]. URL https://wiki.ihe.net/index.php/IHE_Format_Codes (accessed 6.17.19).

Integrating the HealthCare Enterprise, 2017. Creating Unique IDs - OID and UUID - IHE Wiki [WWW Document]. URL https://wiki.ihe.net/index.php/Creating_Unique_IDs_-_OID_and_UUID (accessed 7.5.19).

Johnston, D., Pan, E., Walker, J., 2004. The value of CPOE in ambulatory settings.

Kasunic, M., Anderson, W., 2004. Measuring Systems Interoperability: Challenges and Opportunities.

Lopes, S., 2016. Privacidade dos dados em ambientes de interoperabilidade - a área da saúde. Évora.

Michalis, M., 2015. Precision and Recall in Social Listening [WWW Document]. URL https://www.digital-mr.com/blog/view/precision-and-recall-in-social-listening (accessed 2.4.19).

Michigan State University, 2018. Health care providers – not hackers – leak more of your data | MSUToday | Michigan State University [WWW Document]. 2018-11-16. URL https://msutoday.msu.edu/news/2018/health-care-providers-not-hackers-leak-more-of-your-

data/ (accessed 11.21.18).

Michigan State University, 2017. Hospitals put your data at risk, study finds [WWW Document]. 2017-04-06. URL https://msutoday.msu.edu/news/2017/hospitals-put-your-data-at-risk-study-finds/ (accessed 11.21.18).

Mogull, R., Lane, A., 2019. Understanding and Selecting a Database Encryption or Tokenization Solution.

OASIS, 2005. eXtensible Access Control Markup Language (XACML) Version 2.0.

OASIS, 2003. A Brief Introduction to XACML [WWW Document]. URL https://www.oasis-open.org/committees/download.php/2713/Brief_Introduction_to_XACML.html (accessed 12.26.18).

Object Management Group, 2011. Business Process Model And Notation (BPMN) Version 2.0.

Oracle, 2019a. Database - Oracle [WWW Document]. URL https://www.oracle.com/database/ (accessed 1.21.19).

Oracle, 2019b. Introduction to the Oracle Database [WWW Document]. URL https://docs.oracle.com/cd/B19306_01/server.102/b14220/intro.htm (accessed 7.2.19).

Oracle, 2019c. Oracle WebLogic Server Technical Information [WWW Document]. URL https://www.oracle.com/middleware/technologies/weblogic.html (accessed 1.7.19).

Oracle, 2019d. Introduction to Oracle Real Application Clusters [WWW Document]. URL https://docs.oracle.com/cd/B28359_01/rac.111/b28254/admcon.htm#RACAD7148 (accessed 2.14.19).

Oracle, 2019e. Transparent Data Encryption Frequently Asked Questions [WWW Document]. URL https://www.oracle.com/technetwork/database/security/tde-faq-093689.html#A13016 (accessed 2.14.19).

Oracle, 2019f. The Oracle Text Scoring Algorithm [WWW Document]. URL https://docs.oracle.com/cd/B28359_01/text.111/b28304/ascore.htm#CCREF2307 (accessed 2.23.19).

Oracle, 2016a. Securing Stored Data Using Transparent Data Encryption [WWW Document]. URL https://docs.oracle.com/cd/E11882_01/network.112/e40393/asotrans.htm#ASOAG600 (accessed 2.11.19).

Oracle, 2016b. Introduction to Oracle Advanced Security [WWW Document]. URL https://docs.oracle.com/cd/E11882_01/network.112/e40393/asointro.htm#ASOAG9479 (accessed 4.22.19).

Oracle, 2016c. Glossary [WWW Document]. URL https://docs.oracle.com/cd/E11882_01/network.112/e40393/asogls.htm#i996793 (accessed 4.22.19).

Oracle, 2015a. Physical Storage Structures [WWW Document]. URL https://docs.oracle.com/cd/E11882_01/server.112/e40540/physical.htm#CNCPT003 (accessed 2.15.19).

Oracle, 2015b. Logical Storage Structures [WWW Document]. URL https://docs.oracle.com/cd/E11882_01/server.112/e40540/logical.htm#CNCPT89139 (accessed 2.13.19).

Parlamento Europeu e Conselho, 2016. REGULAMENTO (UE) 2016/ 679 DO PARLAMENTO EUROPEU E

DO CONSELHO - Regulamento Geral sobre a Proteção de Dados.

Parlamento Europeu e Conselho, 1995. Diretiva 95/46/CE Do Parlamento Europeu e do Conselho. Luxemburgo.

Petritsch, H., 2014. Break-glass : handling exceptional situations in access control, Illustrada. ed.

Powers, D.M.W., 2011. Evaluation: from Precision, Recall and F-measure to ROC, Informedness, Markedness and Correlation. J. Mach. Learn. Technol. 2, 37–63.

Reddy, C.K., Aggarwal, C.C., 2015. Healthcare data analytics, ilustrada. ed. Chapman and Hall/CRC.

Saaty, T.L., 2008. Decision making with the analytic hierarchy process. Int. J. Serv. Sci. 1, 83. https://doi.org/10.1504/IJSSCI.2008.017590

Smirnoff, P., 2017. Understanding Hardware Security Modules (HSMs) [WWW Document]. URL https://www.cryptomathic.com/news-events/blog/understanding-hardware-security-modules-hsms (accessed 2.12.19).

SNOMED International, 2018a. SNOMED - Home | SNOMED International [WWW Document]. URL https://www.snomed.org/ (accessed 11.5.18).

SNOMED International, 2018b. SNOMED - Our organization [WWW Document]. URL http://www.snomed.org/our-organization/our-organization (accessed 11.15.18).

Spring, 2019a. Spring Framework Overview [WWW Document]. URL https://docs.spring.io/spring/docs/current/spring-framework-reference/overview.html (accessed 6.18.19).

Spring, 2019b. Core Technologies [WWW Document]. URL https://docs.spring.io/spring/docs/current/spring-framework-reference/core.html#beans-definition (accessed 6.19.19).

Stelzer, D., Fischer, D., Nirsberger, I., 2006. A Framework for Assessing Inter-organizational Integration of Business Information Systems, International Journal of Interoperability in Business Information Systems. Issue.

Taibi, T., 2007. Design patterns formalization techniques, ilustrada. ed. IGI Pub.

Thales eSecurity, 2018. Vormetric Transparent Encryption.

Warwick Manufacturing Group, 2007. Product Excellence using Six Sigma: Quality Function Deployment. Coventry.

World Health Organization, 2018. WHO | International Classification of Diseases, 11th Revision (ICD-11) [WWW Document]. WHO. URL http://www.who.int/classifications/icd/en/ (accessed 11.15.18).

Anexo A. Criação de alternativas

A criação de alternativas consiste na apresentação de várias alternativas de design. Foram identificadas alternativas que apresentam capacidades para resolver o consentimento do paciente, na secção 2.4, nomeadamente:

- BPPC;
- APPC;
- Consent2Share.

Além disso, as soluções contém funcionalidades que podem auxiliar na resolução des outros problemas identificadas, sendo que os aspetos relevantes foram identificados na secção 2.4.

No entanto, as alternativas acima mencionadas não auxiliam na cifragem da base de dados, pelo que foi necessário identificar outras abordagens que permitissem cifrar o conteúdo da base de dados, sendo estas:

- Oracle TDE;
- VTE.

As alternativas apresentadas vão de encontro ao objetivo identificado na secção 3.1.11, como foi justificado na secção 2.5.

A1. Análise e avaliação

A fase de análise e avaliação, consiste na avaliação das diferentes alternativas apresentadas na secção Anexo A. Nesse sentido, irá ser utilizado o método de análise hierárquica (AHP), de modo a auxiliar as comparações entre as alternativas. No final do processo serão apresentadas as alternativas que melhor se ajustam para resolver os problemas identificados.

A1.1 Avaliação das alternativas do consentimento

Para a avaliação das alternativas do consentimento foram definidos os seguintes critérios:

- Compreensão e decisão das políticas de privacidade do consentimento;
- Integração no produto;
- Integração com o sistema de auditoria de eventos;
- Conformidade com padrões de interoperabilidade.

O significado de cada um destes critérios foi explicado na secção 2.4, aquando da avaliação de cada uma das soluções perante os critérios apresentados.

A utilização do método AHP permitirá obter a melhor alternativa para resolver o problema do consentimento, consoante os critérios definidos e os pesos aplicados a cada um desses critérios. Ao aplicar este método de decisão, primeiramente deve ser construída a árvore hierárquica de decisão. No topo da árvore é definido o problema que é necessário solucionar, depois o problema é divido em critérios e por fim são apresentadas as possíveis alternativas que podem ajudar a resolver o problema em questão. Na Figura 81 é apresentado a árvore hierárquica de decisão para o problema do consentimento existente no ALERT® HIE.

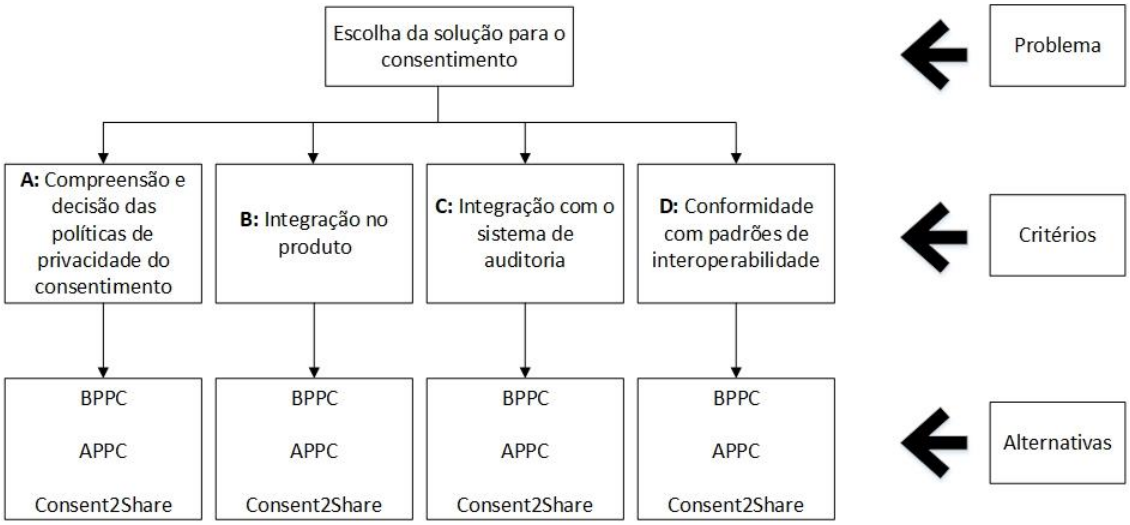


Figura 81 - Árvore hierárquica de decisão para o problema do consentimento

Após a construção da árvore hierárquica de decisão, a segunda fase consiste na comparação entre critérios com base na escala fundamental de Saaty (2008, p. 86), apresentada naFigura 82.

Intensity of Importance	*Definition*	*Explanation*
1	Equal Importance	Two activities contribute equally to the objective
2	Weak or slight	
3	Moderate importance	Experience and judgement slightly favour one activity over another
4	Moderate plus	
5	Strong importance	Experience and judgement strongly favour one activity over another
6	Strong plus	
7	Very strong or demonstrated importance	An activity is favoured very strongly over another; its dominance demonstrated in practice
8	Very, very strong	
9	Extreme importance	The evidence favouring one activity over another is of the highest possible order of affirmation
Reciprocals of above	If activity *i* has one of the above non-zero numbers assigned to it when compared with activity *j*, then *j* has the reciprocal value when compared with *i*	A reasonable assumption
1.1–1.9	If the activities are very close	May be difficult to assign the best value but when compared with other contrasting activities the size of the small numbers would not be too noticeable, yet they can still indicate the relative importance of the activities.

Figura 82 - Escala fundamental de Saaty (2008, p. 86)

A Tabela 19 compara a importância dos critérios entre si.

Tabela 19 - Comparação de critérios do consentimento

	A	**B**	**C**	**D**
A	1	$^1/_3$	$^1/_2$	$^1/_2$
B	3	1	2	2
C	2	$^1/_2$	1	2
D	2	$^1/_2$	$^1/_2$	1

Após a comparação entre critérios estar realizada, o próximo passo é a normalização da matriz, como é demonstrado nas Tabelas 20 e 21.

Tabela 20 – Primeiro passo de normalização da matriz de comparação de critérios do consentimento

	A	**B**	**C**	**D**
A	1	$^1/_3$	$^1/_2$	$^1/_2$
B	3	1	2	2
C	2	$^1/_2$	1	2

	A	B	C	D
D	2	$^1/_2$	$^1/_2$	1
Somatório	8	$^7/_3$	4	$^{11}/_2$

Tabela 21 - Segundo passo de normalização da matriz de comparação de critérios do consentimento

	A	B	C	D
A	$^1/_8$	$^1/_7$	$^1/_8$	$^1/_{11}$
B	$^3/_8$	$^3/_7$	$^1/_2$	$^1/_3$
C	$^1/_4$	$^2/_9$	$^1/_4$	$^1/_3$
D	$^1/_4$	$^2/_9$	$^1/_8$	$^1/_5$

Em seguida é calculado o vetor de prioridades, apresentado na Tabela 22, que irá ser utilizado para verificar a consistência da comparação feita nos critérios de avaliação das alternativas.

Tabela 22 – Cálculo do vetor de prioridades da matriz de comparação de critérios do consentimento

	A	B	C	D	Prioridade
A	$^1/_8$	$^1/_7$	$^1/_8$	$^1/_{11}$	0,12
B	$^3/_8$	$^3/_7$	$^1/_2$	$^1/_3$	0,42
C	$^1/_4$	$^2/_9$	$^1/_4$	$^1/_3$	0,27
D	$^1/_4$	$^2/_9$	$^1/_8$	$^1/_5$	0,19

Pode-se concluir, através da análise do vetor de prioridades na Tabela 22, que o critério de integração no produto é o mais prioritário com 42%. De seguida o integração com sistema de auditoria com 27%, depois o de conformidade com padrões de interoperabilidade com 19% e por fim o de compreensão e decisão das políticas de privacidade do consentimento com 12%.

O próximo passo é avaliar a consistência das prioridades definidas na Tabela 19. Para isso será necessário calcular a razão de consistência (RC), de modo a averiguar se os julgamentos feitos sobre os critérios foram consistentes. A fórmula para calcular o RC é $RC = IC/IR$, em que o IC representa o índice de consistência e IR o índice aleatório. O IC é calculado através da fórmula:

$$IC = \frac{\lambda_{max} - n}{n - 1}$$

Em que n representa o números de critérios definidos, que neste caso é 4. O λ_{max} pode ser calculado através da fórmula $Ax = \lambda_{max} x$ em que A representa a matriz original, ou seja os valores apresentados na Tabela 19, e x é o vetor de prioridades calculado na Tabela 22:

1. $$\begin{bmatrix} 1 & 0.33 & 0.5 & 0.5 \\ 3 & 1 & 2 & 2 \\ 2 & 0.5 & 1 & 2 \\ 2 & 0.5 & 0.5 & 1 \end{bmatrix} \times \begin{bmatrix} 0.12 \\ 0.42 \\ 0.27 \\ 0.19 \end{bmatrix} \cong \lambda_{max} \begin{bmatrix} 0.12 \\ 0.42 \\ 0.27 \\ 0.19 \end{bmatrix}$$

2. $\begin{bmatrix}0.49\\1.70\\1.11\\0.78\end{bmatrix} \cong \lambda_{max} \begin{bmatrix}0.12\\0.42\\0.27\\0.19\end{bmatrix}$

3. $\lambda_{max} = 4.071$

Tendo o valor λ_{max} é possível determinar o IC:

$$IC = \frac{4.071 - 4}{4 - 1} = 0.024$$

Agora é necessário obter o valor de IR para se conseguir calcular o RC. Para isso será utilizado o valor aleatório correspondente a um dos valores apresentados na Tabela 23, definidos pelo o Laboratório Nacional de *Oak Ridge*. Como o número de critérios é 4 o valor correspondente é 0,90.

Tabela 23 - Valores de IR definidos pelo Laboratório Nacional Oak Ridge (Nicola, 2018, p. 23)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	16
0,00	0,00	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48	1,56	1,57	1,59

Neste momento já temos todos os dados necessários para calcular o RC:

$$RC = \frac{0{,}024}{0{,}9} = 0{,}026$$

Para garantir que os valores são consistentes, é necessário que o RC seja inferior a 0,1. Como 0,026<0,1 é possível garantir que os valores são consistentes.

A próxima fase do AHP consiste em calcular o vetor de prioridades para cada um dos critérios definidos, tendo em consideração as alternativas selecionadas, aplicando os cálculos do mesmo modo. As Tabelas 24, 25, 26 e 27 representam os cálculos efetuados sobre as alternativas apresentadas para o critério de compreensão e decisão sobre as políticas de privacidade do paciente.

Tabela 24 - Comparação de alternativas para o critério **A** do consentimento

Compreensão e decisão	BPPC	**APPC**	**Consent2Share**
BPPC	1	3	6
APPC	$^1/_3$	1	4
Consent2Share	$^1/_6$	$^1/_4$	1

Tabela 25 - Primeiro passo de normalização da matriz de comparação de alternativas para o critério **A** do consentimento

Compreensão e decisão	**BPPC**	**APPC**	**Consent2Share**
BPPC	1	3	6
APPC	$^1/_3$	1	4
Consent2Share	$^1/_6$	$^1/_4$	1

Compreensão e decisão	BPPC	APPC	Consent2Share
Somatório	$^{3}/_{2}$	$^{17}/_{4}$	11

Tabela 26 - Segundo passo de normalização da matriz de comparação de alternativas para o critério **A** do consentimento

Compreensão e decisão	BPPC	APPC	Consent2Share
BPPC	$^{2}/_{3}$	$^{5}/_{7}$	$^{1}/_{2}$
APPC	$^{2}/_{9}$	$^{1}/_{4}$	$^{1}/_{3}$
Consent2Share	$^{1}/_{9}$	$^{1}/_{17}$	$^{1}/_{11}$

Tabela 27 - Cálculo do vetor de prioridades da matriz de comparação de alternativas para o critério **A** do consentimento

Compreensão e decisão	BPPC	APPC	Consent2Share	Prioridade
BPPC	$^{2}/_{3}$	$^{5}/_{7}$	$^{1}/_{2}$	0.64
APPC	$^{2}/_{9}$	$^{1}/_{4}$	$^{1}/_{3}$	0.27
Consent2Share	$^{1}/_{9}$	$^{1}/_{17}$	$^{1}/_{11}$	0.09

Para o critério de compreensão e decisão das políticas de privacidade do consentimento, foi obtido o seguinte vetor de prioridades: $\begin{bmatrix}0{,}64\\0{,}27\\0{,}09\end{bmatrix}$.

Avaliando agora o RC da comparação de alternativas para este critério:

1. $\begin{bmatrix}1 & 2 & 6\\0{,}33 & 1 & 4\\0{,}166 & 0{,}25 & 1\end{bmatrix} \times \begin{bmatrix}0{,}64\\0{,}27\\0{,}09\end{bmatrix} \cong \lambda_{max}\begin{bmatrix}0{,}64\\0{,}27\\0{,}09\end{bmatrix}$

2. $\begin{bmatrix}1{,}98\\0{,}83\\0{,}26\end{bmatrix} \cong \lambda_{max}\begin{bmatrix}0{,}64\\0{,}27\\0{,}09\end{bmatrix}$

3. $\lambda_{max} = 3{,}054$

Tendo o valor de λ_{max} é possível determinar o IC:

$$IC = \frac{3{,}054 - 3}{3 - 1} = 0{,}027$$

Como o número de soluções é 3 o $IR = 0.58$, segundo a Tabela 23, portanto o valor de RC é:

$$RC = \frac{0{,}027}{0{,}58} = 0{,}047$$

Como 0,047<0,1 é possível concluir que os valores são consistentes para o critério de compreensão e decisão sobre as políticas de privacidade do consentimento.

Nas Tabelas 28, 29, 30 e 31 são apresentados os cálculos efetuados para o critério de integração no produto.

Tabela 28 - Comparação de alternativas para o critério **B** do consentimento

Integração no produto	**BPPC**	**APPC**	**Consent2Share**
BPPC	1	$^1/_3$	3
APPC	3	1	5
Consent2Share	$^1/_3$	$^1/_5$	1

Tabela 29 - Primeiro passo de normalização da matriz de comparação de alternativas para o critério **B** do consentimento

Integração no produto	**BPPC**	**APPC**	**Consent2Share**
BPPC	1	$^1/_3$	3
APPC	3	1	5
Consent2Share	$^1/_3$	$^1/_5$	1
Somatório	$^{13}/_3$	$^3/_2$	9

Tabela 30 - Segundo passo de normalização da matriz de comparação de alternativas para o critério **B** do consentimento

Integração no produto	**BPPC**	**APPC**	**Consent2Share**
BPPC	$^1/_4$	$^2/_9$	$^1/_3$
APPC	$^2/_3$	$^2/_3$	$^5/_9$
Consent2Share	$^1/_{13}$	$^1/_8$	$^1/_9$

Tabela 31 - Cálculo do vetor de prioridades da matriz de comparação de alternativas para o critério **B** do consentimento

Integração no produto	**BPPC**	**APPC**	**Consent2Share**	**Prioridade**
BPPC	$^1/_4$	$^2/_9$	$^1/_3$	0,26
APPC	$^2/_3$	$^2/_3$	$^5/_9$	0,63
Consent2Share	$^1/_{13}$	$^1/_8$	$^1/_9$	0,11

Para o critério de integração no produto, foi obtido o seguinte vetor de prioridades: $\begin{bmatrix}0{,}26\\0{,}63\\0{,}11\end{bmatrix}$.

Avaliando agora o RC da comparação de alternativas para este critério:

1. $\begin{bmatrix} 1 & 0.33 & 3 \\ 3 & 1 & 5 \\ 0.33 & 0.2 & 1 \end{bmatrix} \times \begin{bmatrix} 0.26 \\ 0.63 \\ 0.11 \end{bmatrix} \cong \lambda_{max} \begin{bmatrix} 0.26 \\ 0.63 \\ 0.11 \end{bmatrix}$

2. $\begin{bmatrix} 0.79 \\ 1.95 \\ 0.32 \end{bmatrix} \cong \lambda_{max} \begin{bmatrix} 0.26 \\ 0.63 \\ 0.11 \end{bmatrix}$

3. $\lambda_{max} = 3.039$

Tendo o valor de λ_{max} é possível determinar o IC:

$$IC = \frac{3.039 - 3}{3 - 1} = 0.019$$

Como o número de soluções é 3 o $IR = 0.58$, segundo a Tabela 23, portanto o valor de RC é:

$$RC = \frac{0.019}{0.58} = 0.033$$

Como 0.033<0.1 é possível concluir que os valores são consistentes para o critério de integração no produto.

Nas Tabelas 32, 33, 34 e 35 é demonstrado o processo para o cálculo do vetor de pesos para o critério de integração com o sistema de auditoria de eventos.

Tabela 32 - Comparação de alternativas para o critério **C** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**
BPPC	1	1	5
APPC	1	1	5
Consent2Share	$^1/_5$	$^1/_5$	1

Tabela 33 - Primeiro passo de normalização da matriz de comparação de alternativas para o critério **C** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**
BPPC	1	1	5
APPC	1	1	5
Consent2Share	$^1/_5$	$^1/_5$	1
Somatório	$^{11}/_5$	$^{11}/_5$	11

Tabela 34 - Segundo passo de normalização da matriz de comparação de alternativas para o critério **C** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**
BPPC	$^4/_9$	$^4/_9$	$^4/_9$
APPC	$^4/_9$	$^4/_9$	$^4/_9$
Consent2Share	$^1/_{11}$	$^1/_{11}$	$^1/_{11}$

Tabela 35 - Cálculo do vetor de prioridades da matriz de comparação de alternativas para o critério **C** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**	**Prioridade**
BPPC	$^3/_7$	$^3/_7$	$^3/_7$	0.45
APPC	$^3/_7$	$^3/_7$	$^3/_7$	0.45
Consent2Share	$^1/_7$	$^1/_7$	$^1/_7$	0.09

Para o critério de integração com sistema de auditoria, foi obtido o seguinte vetor de prioridades: $\begin{bmatrix}0.45\\0.45\\0.09\end{bmatrix}$.

Avaliando agora o RC da comparação de alternativas para este critério:

1. $\begin{bmatrix}1 & 1 & 5\\1 & 1 & 5\\0.2 & 0.2 & 1\end{bmatrix} \times \begin{bmatrix}0.45\\0.45\\0.09\end{bmatrix} \cong \lambda_{max} \begin{bmatrix}0.45\\0.45\\0.09\end{bmatrix}$
2. $\begin{bmatrix}1.36\\1.36\\0.27\end{bmatrix} \cong \lambda_{max} \begin{bmatrix}0.45\\0.45\\0.09\end{bmatrix}$
3. $\lambda_{max} = 3.00$

Tendo o valor de λ_{max} é possível determinar o IC:

$$IC = \frac{3.00 - 3}{3 - 1} = 0.000$$

Como o número de soluções é 3 o $IR = 0.58$, segundo a Tabela 23, portanto o valor de RC é:

$$RC = \frac{0.000}{0.58} = 0.0$$

Como 0.0<0.1 é possível concluir que os valores são consistentes para o critério de integração com o sistema de auditoria.

Por último, nas Tabelas 36, 37, 38 e 39 será demonstrado o processo para o cálculo do vetor de prioridade para o critério de conformidade com padrões de interoperabilidade.

Tabela 36 - Comparação de alternativas para o critério **D** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**
BPPC	1	1	3
APPC	1	1	3
Consent2Share	$^1/_3$	$^1/_3$	1

Tabela 37 - Primeiro passo de normalização da matriz de comparação de alternativas para o critério **D** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**
BPPC	1	1	3
APPC	1	1	3
Consent2Share	$^1/_3$	$^1/_3$	1
Somatório	$^7/_3$	$^7/_3$	7

Tabela 38 - Segundo passo de normalização da matriz de comparação de alternativas para o critério **D** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**
BPPC	$^3/_7$	$^3/_7$	$^3/_7$
APPC	$^3/_7$	$^3/_7$	$^3/_7$
Consent2Share	$^1/_7$	$^1/_7$	$^1/_7$

Tabela 39 - Cálculo do vetor de prioridades da matriz de comparação de alternativas para o critério **D** do consentimento

Integração com sistema de auditoria	**BPPC**	**APPC**	**Consent2Share**	**Prioridade**
BPPC	$^3/_7$	$^3/_7$	$^3/_7$	0.43
APPC	$^3/_7$	$^3/_7$	$^3/_7$	0.43
Consent2Share	$^1/_7$	$^1/_7$	$^1/_7$	0.14

Para o critério de integração no produto, foi obtido o seguinte vetor de prioridades: $\begin{bmatrix}0.43\\0.43\\0.14\end{bmatrix}$.

Avaliando agora o RC da comparação de alternativas para este critério:

1. $\begin{bmatrix}1 & 1 & 3\\1 & 1 & 3\\0.33 & 0.33 & 1\end{bmatrix} \times \begin{bmatrix}0.43\\0.43\\0.14\end{bmatrix} \cong \lambda_{max} \begin{bmatrix}0.43\\0.43\\0.14\end{bmatrix}$
2. $\begin{bmatrix}1.29\\1.29\\0.43\end{bmatrix} \cong \lambda_{max} \begin{bmatrix}0.30\\0.54\\0.16\end{bmatrix}$
3. $\lambda_{max} = 3.00$

Tendo o valor de λ_{max} é possível determinar o IC:

$$IC = \frac{3.00 - 3}{3 - 1} = 0.00$$

Como o número de soluções é 3 o $IR = 0.58$, segundo a Tabela 23, portanto o valor de RC é:

$$RC = \frac{0.00}{0.58} = 0.0$$

Como 0.0<0.1 é possível concluir que os valores são consistentes para o critério de conformidade com padrões de interoperabilidade.

O último passo é identificar a alternativa mais adequada para resolver o problema do consentimento do ALERT® HIE, baseando-se no peso de cada critério e os vetores de prioridades obtidos para alternativas em cada um dos critérios, como é representado na Figura 83.

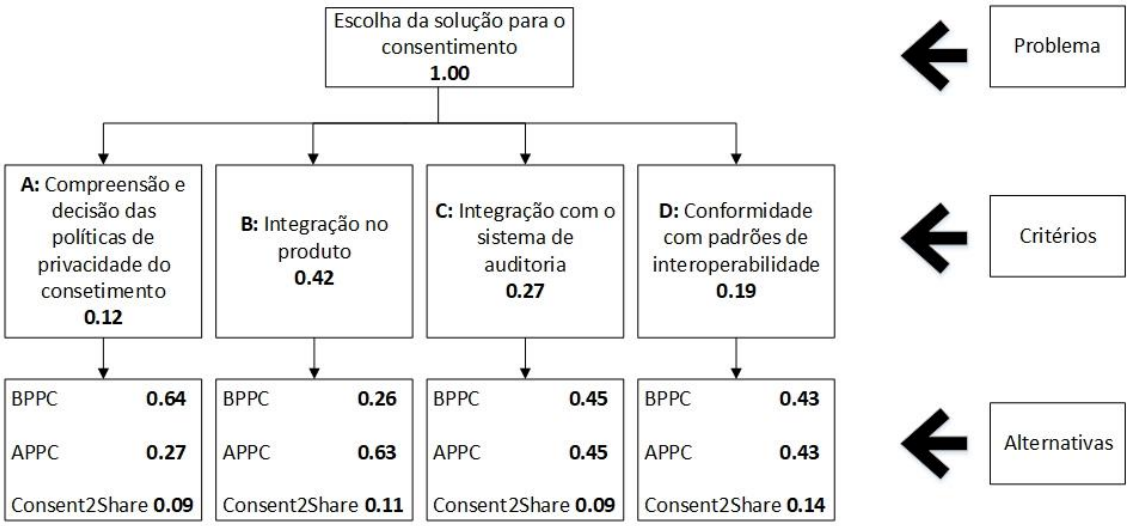


Figura 83 - Árvore hierárquica com as prioridades calculadas para o problema do consentimento

De seguida, irá obter-se a prioridade composta para as alternativas:

$$\begin{bmatrix} 0.64 & 026 & 0.45 & 0.43 \\ 0.27 & 0.63 & 0.45 & 0.43 \\ 0.09 & 0.11 & 0.09 & 0.14 \end{bmatrix} \times \begin{bmatrix} 0.12 \\ 0.42 \\ 0.27 \\ 0.19 \end{bmatrix} = \begin{bmatrix} 0.39 \\ \mathbf{0.50} \\ 0.11 \end{bmatrix}$$

Ao observar resultado obtido através da multiplicação das prioridades calculadas para cada critério e o peso de cada um é possível concluir que a solução APPC é a que mais se adequa como solução a adotar, para resolver o problema de consentimento, obtendo um valor de 50%. Já o BPPC obteve um valor de 39% e o Consent2Share 11%.

A1.2 Avaliação das alternativas da cifragem

Para a avaliação das alternativas da cifragem foram definidos os seguintes critérios:

- Facilidade de integração com as outras opções Oracle – é importante que a solução adotada seja compatível e fácil de integrar com opções de base de dados que podem ser utilizadas no produto, e.g. Oracle RAC;

- Compatibilidade com diferentes tipos de base de dados – Apesar de o atual produto apenas utilizar base de dados do tipo Oracle, pode ser interessante que a solução adotada seja compatível com outros tipos de base de dados;

- Compatibilidade com diferentes SO – Como os ambientes de instalação do produto nos clientes pode variar, é importante que a solução adotada seja compatível com diversos tipos de SO;

- Preço – é importante tentar minimizar os custos da solução adotada, de forma a não agravar os custos finais para o cliente.

Apesar de se ter definido quatro critérios, não vai ser possível utilizar o critério preço, pois não foi possível aferir o preço da alternativa VTE, apresentada na subsecção 2.5.3, deste modo não é possível fazer a comparação entre preços.

A utilização do método AHP permitirá obter a melhor alternativa para resolver o problema da cifragem, consoante os critérios definidos e os pesos aplicados a cada um desses critérios. Na Figura 84 é apresentado a árvore hierárquica de decisão para o problema do consentimento existente no ALERT® HIE.

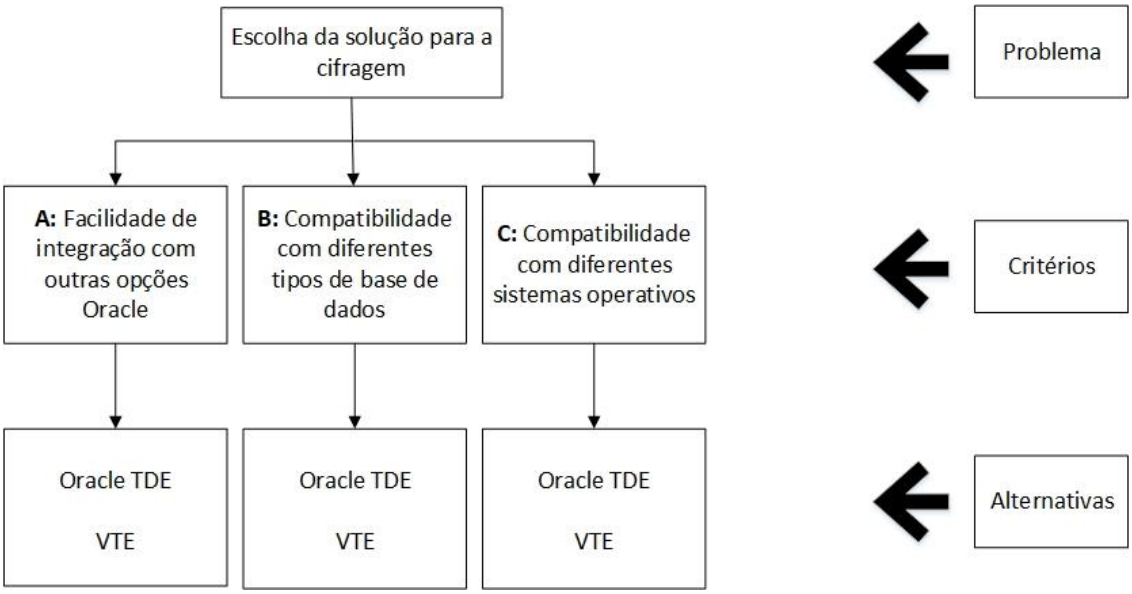


Figura 84 - Árvore hierárquica de decisão para o problema da cifragem

Após a construção da árvore hierárquica de decisão, a segunda fase consiste na comparação entre critérios com base na escala fundamental de Saaty apresentada na Figura 82

Como o cálculo do AHP já foi demonstrado durante a subsecção A1.1, apenas serão apresentadas as tabelas de comparação de critérios e soluções, como também a tabela com o vetor de prioridades após o cálculo das normalizações.

A Tabela 40 compara a importância dos critérios entre si.

Tabela 40 - Comparação de critérios da cifragem

	A	**B**	**C**
A	1	7	3
B	$^1/_7$	1	$^1/_5$
C	$^1/_3$	5	1

Tabela 41 - Cálculo do vetor de prioridades da matriz de comparação de critérios de cifragem

	A	**B**	**C**	**Prioridade**
A	$^2/_3$	$^1/_2$	$^5/_7$	0.643
B	$^2/_6$	$^1/_{13}$	$^5/_{105}$	0.074
C	$^2/_9$	$^2/_5$	$^1/_4$	0.283

Pode-se concluir, através da análise do vetor de prioridades na Tabela 41, que o critério de facilidade de integração com outras opções Oracle é o mais prioritário com 64%, de seguida a compatibilidade com diferentes SO com 28% e por fim a compatibilidade com diferentes base de dados 7%.

O próximo passo é avaliar a consistência das prioridades definidas na Tabela 23, sendo necessário calcular o RC.

1. $\begin{bmatrix} 1 & 7 & 3 \\ 0.14 & 1 & 0.2 \\ 0.33 & 5 & 1 \end{bmatrix} \times \begin{bmatrix} 0.643 \\ 0.074 \\ 0.283 \end{bmatrix} \cong \lambda_{max} \begin{bmatrix} 0.643 \\ 0.074 \\ 0.283 \end{bmatrix}$

2. $\begin{bmatrix} 2.01 \\ 0.22 \\ 0.87 \end{bmatrix} \cong \lambda_{max} \begin{bmatrix} 0.643 \\ 0.074 \\ 0.283 \end{bmatrix}$

3. $\lambda_{max} = 3.066$

Tendo o valor de λ_{max} é possível determinar o IC:

$$IC = \frac{3.066 - 3}{3 - 1} = 0.033$$

Como o número de soluções é 3 o $IR = 0.58$, segundo a Tabela 23, portanto o valor de RC é:

$$RC = \frac{0.033}{0.58} = 0.056$$

Como 0.056<0.1 é possível concluir que os valores são consistentes para os critérios definidos para escolha da cifragem.

A próxima fase do AHP consiste em calcular o vetor de prioridades para cada um dos critérios definidos, tendo em consideração as alternativas selecionadas, aplicando os cálculos do mesmo modo.

Tabela 42 - Comparação de alternativas para o critério **A** da cifragem

Critério A	**TDE**	**VTE**
TDE	1	2
VTE	$^1/_2$	1

Tabela 43 - Cálculo do vetor de prioridades da matriz de comparação de alternativas para o critério **A** da cifragem

Critério A	**TDE**	**VTE**	**Prioridades**
TDE	$^2/_3$	$^2/_3$	0.67
VTE	$^1/_3$	$^1/_3$	0.33

Para o critério de facilidade de integração com outras opções Oracle, foi obtido o seguinte vetor de prioridades: $\begin{bmatrix} 0.67 \\ 0.33 \end{bmatrix}$.

Tabela 44 - Comparação de alternativas para o critério **B** da cifragem

Critério B	**TDE**	**VTE**
TDE	1	$^1/_8$

VTE	8	1

Tabela 45 - Cálculo do vetor de prioridades da matriz de comparação de alternativas para o critério **B** da cifragem

Critério B	**TDE**	**VTE**	**Prioridades**
TDE	$^1/_9$	$^1/_9$	0.11
VTE	$^8/_9$	$^8/_9$	0.89

Para o critério compatibilidade com diferentes tipos de bases de dados, foi obtido o seguinte vetor de prioridades: $\begin{bmatrix}0.11\\0.89\end{bmatrix}$.

Tabela 46 - Comparação das alternativas para o critério **C** da cifragem

Critério C	**TDE**	**VTE**
TDE	1	1
VTE	1	1

Tabela 47 - Cálculo do vetor de prioridades da matriz de comparação de alternativas para o critério **C** da cifragem

Critério C	**TDE**	**VTE**	**Prioridades**
TDE	$^1/_2$	$^1/_2$	0.50
VTE	$^1/_2$	$^1/_2$	0.50

Para o critério compatibilidade com diferentes tipos de SO, foi obtido o seguinte vetor de prioridades: $\begin{bmatrix}0.50\\0.50\end{bmatrix}$.

O último passo é identificar a alternativa mais adequada para resolver o problema da cifragem do ALERT® HIE, baseando-se no peso de cada critério e os vetores de prioridades obtidos para alternativas em cada um dos critérios, como é representado na Figura 85.

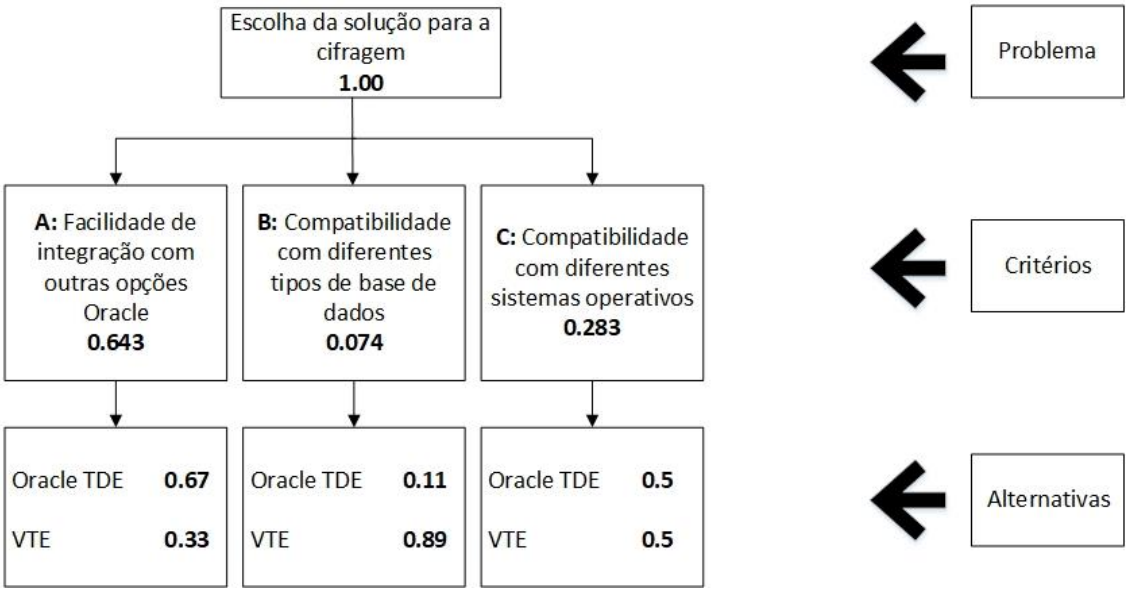


Figura 85 - Árvore hierárquica com as prioridades calculadas para o problema da cifragem

De seguida, irá obter-se a prioridade composta para as alternativas:

$$\begin{bmatrix} 0.67 & 0.11 & 0.5 \\ 0.33 & 0.89 & 0.5 \end{bmatrix} \times \begin{bmatrix} 0.643 \\ 0.074 \\ 0.283 \end{bmatrix} = \begin{bmatrix} \mathbf{0.58} \\ 0.42 \end{bmatrix}$$

Ao observar resultado obtido através da multiplicação das prioridades calculadas para cada critério e o peso de cada um é possível concluir que a solução Oracle TDE é a que mais se adequa como solução a adotar, para resolver o problema da cifragem, obtendo um valor de 58%. Já o VTE obteve um valor de 42%.

É de ter em conta que os peso do critério de compatibilidade com diferentes tipos de base de dados teve um peso inferior que os outros dois critérios, devido ao facto de o produto apenas utilizar base de dados do tipo Oracle. Se este critério tivesse um maior peso na escolha da alternativa, com certeza que o VTE seria a melhor solução adotar, devido à sua compatibilidade com diferentes tipos de base de dados.

A2. Implementação

A última fase do processo de análise valor é a fase de implementação no produto. Neste caso em concreto passa pela adoção das alternativas selecionadas, através do método AHP, para resolver o problema do consentimento do paciente e cifragem existente no ALERT® HIE.

Com base nos resultados obtidos através do método AHP realizado na subsecção A1.1 e A1.2, a alternativa APPC é a mais indicada para ajudar a resolver as funcionalidades identificadas na secção 3.3.2 sobre o consentimento. Em relação à cifragem, a melhor alternativa a adotar é o Oracle TDE. Porém, como a solução Oracle TDE acarreta custos e autorizações por parte da organização para a sua implementação, foi tomada a decisão de deixar a sua implementação fora do âmbito do projeto.

As decisões arquiteturais tomadas com adoção da solução APPC são apresentadas na secção 5.3 e a sua implementação no capítulo 6.

Anexo B. Serviços Rest

Neste anexo é apresentado a implementação das interfaces de comunicação REST, para a implementação do padrão XACML.

Nos Extratos de Código 10 e 11 são apresentados os serviços REST que permitem a criação e eliminação de políticas respetivamente.

```
@RequestMapping(method=RequestMethod.POST,
 produces=MediaType.TEXT_XML_VALUE,consumes=MediaType.TEXT_XML_VALUE)
public ResponseEntity<String> createPolicy(
        @RequestBody PolicyType consentPolicy){
  logger.debug("Entry on rest method createPolicy!");
  String policy = this.policyService.createPolicy(consentPolicy);
  if(policy != null) {
    return ResponseEntityBuilder.buildCreatedResponse(policy);
  }else {
    return ResponseEntityBuilder.buildKoResponse();
  }
}
```

Extrato Código 10 - Serviço REST de criação de política

```
@RequestMapping(method=RequestMethod.DELETE,value="/{policyID}",
        produces=MediaType.APPLICATION_JSON_VALUE )
public ResponseEntity<String> deletePolicy(
        @PathVariable(value="policyID") String policyID){
  try{
    if(policyService.deletePolicy(policyID)) {
      return ResponseEntityBuilder.buildNoContentResponse("");
    }else {
      return new ResponseEntity<String>(HttpStatus.NOT_FOUND);
    }
  }catch(JDBCException e) {
    logger.error(e);
    return ResponseEntityBuilder.buildKoResponse("An error has occurred internally,"+
                        " please try again later.");
  }
}
```

Extrato Código 11 - Serviço REST de eliminação de política

O Extrato Código 12 apresenta o serviços REST que permite a criação de conjuntos de políticas, sendo que estas poderão representar o documento de consentimento raiz do paciente. Já no Extrato Código 13 são apresentados dois serviços REST que permitem eliminar os conjuntos de políticas por duas maneiras:

- Identificação do conjunto de política – que permite eliminar o conjunto de políticas e as suas respetivas referências.

- Identificação do paciente – permite eliminar o conjunto de políticas raiz que está associado ao documento de consentimento raiz do paciente e as suas respetivas referências.

```
@RequestMapping(method=RequestMethod.POST, value="/{patientIdentification:.+}",
        produces=MediaType.TEXT_XML_VALUE, consumes=MediaType.TEXT_XML_VALUE)
public ResponseEntity<String> createPolicySet(
        @PathVariable(value="patientIdentification") String patientIdentification,
        @RequestParam(required = false, defaultValue = "false") boolean consent,
        @RequestParam(required=false,defaultValue="0") String institutionID,
        @RequestBody PolicySetType policyRequestDTO){
  logger.debug("Received Request to create PolicySet.");
  String policySet = this.policySetService.createPolicySet (policyRequestDTO,
                              institutionID,consent,patientIdentification);
  if(policySet != null) {
    return ResponseEntityBuilder.buildCreatedResponse(policySet);
  }else {
    return ResponseEntityBuilder.buildKoResponse();
  }
}
```

Extrato Código 12 - Serviço REST de criação de conjunto de políticas

```
@RequestMapping(method=RequestMethod.DELETE, value="/{policySetID}",
        produces=MediaType.APPLICATION_JSON_VALUE)
public ResponseEntity<String> deletePolicy(
        @PathVariable(value="policySetID") String policySetID){
  logger.debug("Received Request to DELETE PolicySet with this id "+policySetID);
  try {
    if(policySetService.deletePolicySet(policySetID)) {
      return ResponseEntityBuilder.buildNoContentResponse("");
    }else {
      return new ResponseEntity<String>(HttpStatus.NOT_FOUND);
    }
  } catch (JDBCException e) {
    logger.error(e);
    return ResponseEntityBuilder.buildKoResponse("An error has occurred internally,"
                +" please try again later.");
  }
}

@RequestMapping(method=RequestMethod.DELETE, value="/patient/{patientIDentification:.+}",
        produces=MediaType.APPLICATION_JSON_VALUE)
public ResponseEntity<String> deletePatientPolicyConsent(
        @PathVariable(value="patientIDentification") String patientIDentification){
  logger.debug("Received Request to DELETE PolicySet with this id "+patientIDentification);
  try {
    if(policySetService.deletePatientPolicyConsent(patientIDentification)) {
      return ResponseEntityBuilder.buildNoContentResponse("");
    }else {
      return new ResponseEntity<String>(HttpStatus.NOT_FOUND);
    }
  } catch (JDBCException e) {
    logger.error(e);
    return ResponseEntityBuilder.buildKoResponse(e.getMessage());
  }
}
```

Extrato Código 13 - Serviços REST de eliminação de conjuntos de políticas por identificação do conjunto de política ou identificação do paciente

No Extrato Código 14 é apresentado o serviço REST que questiona com base no pedido recebido e a identificação do paciente se deve ser dado acesso ou não. Este pedido está relacionado com o componente PDP do XACML.

```
@RequestMapping(method=RequestMethod.POST, value="/{patientID:.+}",
        produces=MediaType.TEXT_XML_VALUE, consumes=MediaType.TEXT_XML_VALUE)
public ResponseEntity<String> decide(
        @PathVariable(value="patientID") String patientID,
        @RequestBody RequestContext request){
  try {
    String content = policyDecisionPointService.decisionConsent(request, patientID);
    return ResponseEntityBuilder.buildOkResponse(content);
  } catch (StringMarshallException e) {
    return ResponseEntityBuilder.buildKoResponse("It was impossible to evaluate the request,"+
                " please try again later.");
  }
}
```

Extrato Código 14 - Serviço REST de pedido de acesso

Anexo C. Configurações

Neste anexo são apresentadas as diversas configurações que foram utilizadas durante a realização da experimentação.

Tabela 48 - Primeira configuração do algoritmo de correlacionamento

Parâmetros	Modo Pesquisa	Modo cálculo de semelhança	Peso	Limite
Data de Nascimento	Comparação de datas	Igualdade	300	70
Género	Comparação numérica	Igualdade	100	70
Nome completo	Variações difusas do OIT com operador lógico “OU”	Distância de edição	500	70

Na Tabela 48 é apresentada a primeira configuração a utilizar durante a realização da experimentação, esta configuração é a configuração utilizada por omissão quando o produto é instalado no cliente. Ao analisar a tabela é possível aferir que o atributo de informação data de nascimento terá um peso três vezes maior que o atributo género, já em relação ao atributo nome completo este terá um peso cinco vezes maior. É de ter em contra que este último atributo utilizará um modo de pesquisa que terá em consideração o quão comum é o conjunto de nomes que formam o nome completo, como também utilizará para o cálculo da semelhança o algoritmo de distância de edição.

Tabela 49 - Segunda configuração do algoritmo de correlacionamento

Parâmetros	Modo Pesquisa	Modo cálculo de semelhança	Peso	Limite
Data de Nascimento	Comparação de datas	Igualdade	300	70
Género	Comparação numérica	Igualdade	100	70
Nome completo	Variações difusas do OIT com operador lógico “OU”	Distância de edição	500	80
NIF	POI OIT	Distância de edição	700	80
Endereço de email	Variações difusas do OIT com operador lógico “E”	Distância de edição	150	70
Número telemóvel	Variações difusas do OIT com operador lógico “E”	Distância de edição	250	70

Na Tabela 49 é apresentado a segunda configuração a utilizar durante a realização da experimentação. Esta configuração, para além de utilizar os atributos de informação da configuração apresentada na Tabela 48, utiliza também os atributos de informação NIF, endereço de email e número telemóvel do paciente. Sendo o atributo de informação NIF um identificador pessoal único dos pacientes, definiu-se um peso de 700 para este identificador. Quanto aos atributos endereço de email e número de telemóvel, os pesos definidos são de 150 e 250 respetivamente, pois são atributos de informação que podem mudar muito facilmente, principalmente o endereço de email devido a ser gratuita a criação de endereços de email. Todos os atributos adicionados utilizarão o algoritmo de distância de edição para o algoritmo de cálculo de semelhança, mas o NIF terá um limite de 80 devido a ser um identificador único.

Tabela 50 - Terceira configuração do algoritmo de correlacionamento

Parâmetros	Modo Pesquisa	Modo cálculo de semelhança	Peso	Limite
Data de Nascimento	Comparação de datas	Igualdade	300	70
Género	Comparação numérica	Igualdade	100	70
Nome completo	Variações difusas do OIT com	Distância de edição	500	80

	operador lógico “OU”			
NIF	POI OIT	Distância de edição	700	80
Endereço de email	Variações difusas do OIT com operador lógico “E”	Distância de edição	150	70
Número telemóvel	Variações difusas do OIT com operador lógico “E”	Distância de edição	250	70
Língua Nativa	Comparação numérica	Igualdade	100	70
Nacionalidade	Comparação numérica	Distância de edição	150	70

Na Tabela 50 é apresentada a terceira configuração a utilizar na realização da experimentação. Esta configuração utiliza todos os atributos de informação da configuração apresentada na Tabela 49, como também a língua nativa e a nacionalidade do paciente. Quanto aos atributos de informação língua nativa e nacionalidade, foi utilizado o algoritmo de pesquisa de comparação numérica, pois é guardado na tabela do paciente “patient_record” o identificador da língua nativa correspondente à tabela “language_patient”. Já a identificação da nacionalidade do paciente é guardada na tabela “pat_country_citizenship” devido ao paciente poder ter mais uma nacionalidade, como é possível verificar no modelo relacional apresentado na Figura 43.

Os algoritmos de cálculo de semelhança utilizados foram o de igualdade para o atributo língua nativa e distância de edição para a nacionalidade, pois neste último a comparação pode ser baseada numa lista de nacionalidades. Definiu-se que para o atributo língua nativa que o peso seria de 100 devido à probabilidade de vários pacientes terem a mesma língua nativa, já nacionalidade o peso definido foi de 150 por causa do paciente poder adquirir outras nacionalidades ou ter mais que uma nacionalidade e indicar diferentes nacionalidades em visitas a instituições diferentes. Portanto estes dois atributos de informação não permitem identificar inequivocamente o paciente.

Tabela 51 - Quarta configuração do algoritmo de correlacionamento

Parâmetros	**Modo Pesquisa**	**Modo cálculo de semelhança**	**Peso**	**Limite**
Data de nascimento	Comparação de datas	Igualdade	300	70
Género	Comparação numérica	Igualdade	100	70
Nome completo	Variações difusas do	Distância de edição	500	80

Parâmetros	Modo Pesquisa	Modo cálculo de semelhança	Peso	Limite
	OIT com operador lógico “OU”			
NIF	POI OIT	Distância de edição	700	80
Endereço de email	Variações difusas do OIT com operador lógico “E”	Distância de edição	150	70
Número telemóvel	Variações difusas do OIT com operador lógico “E”	Distância de edição	250	70
Língua nativa	Comparação numérica	Igualdade	100	70
Nacionalidade	Comparação numérica	Distância de edição	150	70
Local de nascimento	Variações difusas com operador lógico “E”	Distância de edição	100	70
Nome completo da mãe	Variações difusas com operador lógico “OU”	Distância de edição	500	80

A quarta configuração do algoritmo de correlacionamento utiliza todos os atributos de informação da configuração apresentada na Tabela 51, como também o local de nascimento e o nome completo da mãe, conforme é possível aferir através da análise Tabela 51. Quanto ao atributo local de nascimento o algoritmo de correlacionamento de informação de pacientes só considera a cidade que consta no local de nascimento, pelo que, deste modo, apenas se deu um peso de 100 a este atributo. Já o atributo nome completo da mãe ficou com as mesmas características que o atributo nome completo.

Tabela 52 - Quinta configuração do algoritmo de correlacionamento

Parâmetros	Modo Pesquisa	Modo cálculo de semelhança	Peso	Limite
Data de nascimento	Comparação de datas	Igualdade	300	70
Género	Comparação numérica	Igualdade	100	70

Parâmetros	Modo Pesquisa	Modo cálculo de semelhança	Peso	Limite
Nome completo	Variações difusas do OIT com operador lógico “OU”	Distância de edição	500	80
NIF	POI OIT	Distância de edição	700	80
Endereço de email	Variações difusas do OIT com operador lógico “E”	Distância de edição	150	70
Número telemóvel	Variações difusas do OIT com operador lógico “E”	Distância de edição	250	70
Língua nativa	Comparação numérica	Igualdade	100	70
Nacionalidade	Comparação numérica	Distância de edição	150	70
Local de nascimento	Variações difusas com operador lógico “E”	Distância de edição	100	70
Nome completo da mãe	Variações difusas com operador lógico “OU”	Distância de edição	500	80
Estado Civil	Comparação numérica	Igualdade	100	70
Religião	Comparação numérica	Igualdade	100	70
Raça	Comparação numérica	Igualdade	100	70
Etnia	Comparação numérica	Igualdade	100	70

A quinta e última configuração do algoritmo de correlacionamento de informação de pacientes utiliza todos os atributos apresentados na Tabela 51 com a adição dos seguintes atributos de informação, estado civil, religião, raça e etnia, conforme é ilustrado na Tabela 52. Como estes quatro atributos de informação estão presentes na tabela do paciente “Patient_Record” como identificadores, será utilizado o método de pesquisa de comparação numérica e o cálculo de semelhança será o de igualdade. O peso destes atributos será de 100, pois são atributos que não permitem identificar inequivocamente o paciente, mas todos eles considerados terão um peso significativo no processo de correlação.