ÍNDICE

1. INTRODUÇÃO 1

1.1. ENQUADRAMENTO 1

1.2. MOTIVAÇÃO 2

1.3. OBJETIVOS E CONTRIBUIÇÕES 2

1.4. METODOLOGIA DE TRABALHO 3

1.5. ESTRUTURA DA TESE 4

2. ESTADO DA ARTE 7

2.1. STANDARDS DE INTEROPERABILIDADE 7

2.1.1. RECURSO FHIR 8

2.1.2. RELEVÂNCIA DO FHIR PARA O PROJETO 10

2.1.3. COMUNICAÇÃO DE RECURSOS FHIR 11

2.2. SEGURANÇA E PRIVACIDADE DA INFORMAÇÃO 12

2.2.1. SEGURANÇA - FHIR 13

2.2.2. IHE - INTERNET USER AUTHORIZATION PROFILE 13

2.2.3. OPENID HEART 15

2.2.4. *FHIR OAUTH 2.0 SCOPES* 16

2.2.5. REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS 18

3. ANÁLISE DE REQUISITOS 21

3.1. REQUISITOS FUNCIONAIS 21

3.2. REQUISITOS NÃO FUNCIONAIS 22

3.2.1. AUTENTICAÇÃO E AUTORIZAÇÃO 22

3.2.2. PRIVACIDADE DA INFORMAÇÃO 23

3.2.3. SEGURANÇA DAS COMUNICAÇÕES 23

3.2.4. AUDITORIA 23

3.2.5. CONFORMIDADE COM FHIR 23

4. CONCEPTUALIZAÇÃO E DESENHO 25

4.1. ARQUITETURA DO SISTEMA 25

4.2. TECNOLOGIAS E FRAMEWORKS 26

4.2.1. FHIR SERVER 26

4.2.1.1. HAPI FHIR 27

4.2.1.2. SMART ON FHIR 28

4.2.1.3. FHIRBASE 28

4.2.1.4. COMPARAÇÃO E VEREDITO 28

4.2.2. AUTHORIZATION SERVER 30

4.2.3. GATEWAY 32

4.2.3.1. MIDDLEWARE 32
4.2.3.2. REVERSE PROXY 33
4.2.4. RESUMO DAS TECNOLOGIAS SELECIONADAS 34
4.3. WORKFLOW DE AUTORIZAÇÃO 34
4.3.1. AUTHORIZATION CODE GRANT 35
4.3.2. FHIRBOX AUTHORIZATION FLOW 36
5. FHIRBOX (IMPLEMENTAÇÃO) 39
5.1. FHIR SERVER 39
5.1.1. BASE DE DADOS 39
5.1.2. SERVIDOR RESTFUL 40
5.1.2.1. AUTHORIZATION INTERCEPTOR 41
5.1.2.2. INSTALAÇÃO 43
5.2. AUTHORIZATION SERVER 44
5.3. GATEWAY 48
5.3.1. BASE DE DADOS 48
5.3.2. SCAFFOLDING 48
5.3.3. FHIRBOX AUTHORIZATION FLOW 49
5.3.4. ROUTES 50
5.3.5. REVERSE PROXY 52
5.4. DEVOPS 54
6. REFLEXÃO 57
7. CONCLUSÕES E TRABALHO FUTURO 59
8. BIBLIOGRAFIA 61