Contents

SOP-003: Políticas de Privacidade e Segurança de Dados em Saúde

Standard Operating Procedure para Conformidade com LGPD, GDPR e HIPAA em Implementation Guides FHIR

1. INTRODUÇÃO

1.1 Objetivo

Este documento estabelece as diretrizes e procedimentos para garantir a conformidade com as principais regulamentações de proteção de dados em saúde ao desenvolver Implementation Guides FHIR, incluindo LGPD (Brasil), GDPR (União Europeia) e HIPAA (Estados Unidos).

1.2 Escopo

Aplica-se a todos os aspectos de privacidade, segurança e proteção de dados em projetos de interoperabilidade FHIR, incluindo design, implementação, testes e operação.

1.3 Regulamentações Base

- **LGPD**: Lei Geral de Proteção de Dados (Lei nº 13.709/2018)[1]
- **GDPR**: General Data Protection Regulation (EU 2016/679)[2]
- **HIPAA**: Health Insurance Portability and Accountability Act[3]
- **ISO/IEC 27001**: Information Security Management[4]
- **ISO/IEC 27799**: Health informatics security management[5]

2. PRINCÍPIOS FUNDAMENTAIS

2.1 Princípios Comuns às Três Regulamentações

2.1.1 Minimização de Dados Coletar apenas dados necessários para finalidade específica:

```
Profile: MinimalPatientProfile
Parent: Patient
Description: "Perfil com dados mínimos necessários"
* identifier 1..1 MS  // Apenas identificador obrigatório
* name.given 0..1 MS  // Nome opcional
* name.family 1..1 MS
* birthDate 0..1 MS
* gender 0..1
// Elementos sensíveis marcados como proibidos
* maritalStatus 0..0
* photo 0..0
* contact 0..0
```

2.1.2 Finalidade e Transparência Documentar claramente o propósito do processamento:

```
Extension: DataProcessingPurpose
Id: data-processing-purpose
```

```
Title: "Finalidade do Processamento"
Description: "Documenta a finalidade legal do processamento de dados
* value[x] only CodeableConcept
* valueCodeableConcept from DataPurposeVS (required)

ValueSet: DataPurposeVS
* #treatment "Tratamento médico"
* #research "Pesquisa científica"
* #public-health "Saúde pública"
* #billing "Faturamento"
```

```
Profile: SecureObservation
Parent: Observation
* meta.security 1..* MS
* meta.security from SecurityLabelsVS (required)
* text 0..0  // Proibir narrativa para evitar vazamento
* note 0..0  // Proibir anotações livres
```

2.1.3 Segurança por Design (Security by Design)

3. LGPD - LEI GERAL DE PROTEÇÃO DE DADOS (BRASIL)

3.1 Requisitos Específicos LGPD[6]

```
Extension: LGPDLegalBasis
Id: lgpd-legal-basis
Title: "Base Legal LGPD"
Context: Consent, Contract
* extension contains
    basis 1..1 MS and
    article 0..1 MS
* extension[basis].value[x] only code
* extension[basis].valueCode from LGPDLegalBasisVS (required)
* extension[article].value[x] only string

ValueSet: LGPDLegalBasisVS
* #consent "Consentimento do titular (Art. 7°, I)"
* #vital-interest "Proteção da vida (Art. 7°, II)"
* #legal-obligation "Obrigação legal (Art. 7°, II)"
* #public-health "Tutela da saúde (Art. 7°, VIII)"
* #legitimate-interest "Interesse legítimo (Art. 7°, IX)"
* #research "Pesquisa (Art. 7°, IV)"
```

3.1.1 Bases Legais para Tratamento

```
Profile: LGPDSensitiveData
Parent: Basic
* code = #sensitive-health-data
* extension contains
    DataCategory named category 1..1 MS and
    SpecialProtection named protection 0..* MS
* extension[category].valueCode from SensitiveDataCategoryVS
* extension[protection].valueString 1..1

ValueSet: SensitiveDataCategoryVS
* #genetic "Dados genéticos"
* #biometric "Dados biométricos"
* #health "Dados de saúde"
* #sexual "Vida sexual"
* #religious "Convicção religiosa"
* #racial "Origem racial ou étnica"
```

3.1.2 Dados Sensíveis de Saúde

```
CapabilityStatement: LGPDDataSubjectRights
* rest.resource[0].type = #Patient
* rest.resource[0].interaction[0].code = #read  // Acesso
* rest.resource[0].interaction[1].code = #update  // Correção
* rest.resource[0].interaction[2].code = #delete  // Eliminação
* rest.resource[0].operation[0].name = "portability"
* rest.resource[0].operation[0].definition = "OperationDefinition/da
* rest.resource[0].operation[1].name = "anonymize"
* rest.resource[0].operation[1].definition = "OperationDefinition/an
```

3.1.3 Direitos do Titular[7]

```yaml
# Template RIPD para IG FHIR
ripd:
  projeto: "Implementation Guide XYZ"
  controlador: "Organização ABC"
  encarregado_dpo: "nome@organizacao.com"

  dados_tratados:
    - tipo: "Dados de identificação"
      categoria: "Pessoais"
      volume_estimado: "10000 registros/mês"
    - tipo: "Dados clínicos"
      categoria: "Sensíveis"
      volume_estimado: "50000 registros/mês"
```

```yaml
  finalidades:
    - "Continuidade do cuidado"
    - "Gestão hospitalar"

  medidas_seguranca:
    - "Criptografia AES-256"
    - "Controle de acesso baseado em papéis"
    - "Auditoria completa"

  riscos_identificados:
    - risco: "Vazamento de dados"
      probabilidade: "Baixa"
      impacto: "Alto"
      mitigacao: "Criptografia e monitoramento"
```

3.1.4 Relatório de Impacto (RIPD)[8]

3.2 Implementação LGPD em FHIR

```
Profile: LGPDConsent
Parent: Consent
* status = #active
* scope = http://terminology.hl7.org/CodeSystem/consentscope#patient
* category = http://loinc.org#59284-0 "Consent Document"
* patient 1..1 MS
* dateTime 1..1 MS
* policy.uri 1..1 MS  // Link para política de privacidade
* provision.type 1..1
* provision.period 1..1  // Período de validade
* provision.data.meaning 1..1
* provision.data.reference 1..1  // Recursos cobertos
* sourceReference 1..1  // Documento de consentimento
```

3.2.1 Consentimento LGPD

4. GDPR - GENERAL DATA PROTECTION REGULATION (EU)

4.1 Requisitos Específicos GDPR[9]

```
Extension: GDPRLawfulBasis
Id: gdpr-lawful-basis
Title: "Base Legal GDPR"
* value[x] only CodeableConcept
* valueCodeableConcept from GDPRLawfulBasisVS (required)

ValueSet: GDPRLawfulBasisVS
```

```
* #consent "Consent (Article 6(1)(a))"
* #contract "Contract (Article 6(1)(b))"
* #legal-obligation "Legal obligation (Article 6(1)(c))"
* #vital-interests "Vital interests (Article 6(1)(d))"
* #public-task "Public task (Article 6(1)(e))"
* #legitimate-interests "Legitimate interests (Article 6(1)(f))"
* #special-category "Special category - health (Article 9)"
```

4.1.1 Lawful Basis (Base Legal)

```
Profile: GDPRCompliantResource
Abstract: true
* meta.security 1..* MS
* meta.security contains
    confidentiality 1..1 MS and
    dataController 0..1 MS and
    dataProcessor 0..* MS
* meta.tag contains
    pseudonymized 0..1 MS and
    encrypted 0..1 MS

// Aplicar a todos os recursos
Profile: GDPRPatient
Parent: Patient
Mixins: GDPRCompliantResource
```

4.1.2 Data Protection by Design[10]

```
OperationDefinition: ErasePersonalData
* url = "http://example.org/fhir/OperationDefinition/erase"
* name = "ErasePersonalData"
* title = "GDPR Right to Erasure"
* status = #active
* kind = #operation
* code = #erase
* resource = #Patient
* system = false
* type = false
* instance = true
* parameter[0].name = #confirmation
* parameter[0].use = #in
* parameter[0].min = 1
* parameter[0].max = "1"
* parameter[0].type = #string
* parameter[1].name = #result
```

```
* parameter[1].use = #out
* parameter[1].min = 1
* parameter[1].max = "1"
* parameter[1].type = #OperationOutcome
```

4.1.3 Right to Erasure (Direito ao Esquecimento)[11]

```
OperationDefinition: ExportPersonalData
* url = "http://example.org/fhir/OperationDefinition/export-personal
* name = "ExportPersonalData"
* title = "GDPR Data Portability"
* status = #active
* kind = #operation
* code = #export
* resource = #Patient
* parameter[0].name = #format
* parameter[0].use = #in
* parameter[0].type = #code
* parameter[0].binding.strength = #required
* parameter[0].binding.valueSet = "http://hl7.org/fhir/ValueSet/mime
```

4.1.4 Data Portability[12]

4.2 Privacy by Default[13]

```
Profile: PrivacyByDefaultPatient
Parent: Patient
* name.use = #anonymous  // Default para anônimo
* birthDate.extension contains DataAccuracy named accuracy 0..1
* address.use = #temp  // Endereço temporário por padrão
* telecom 0..0  // Sem contato por padrão
* photo 0..0  // Sem foto por padrão
```

5. HIPAA - HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (USA)

5.1 Requisitos HIPAA[14]

```
Profile: HIPAAProtectedResource
Abstract: true
* meta.security contains
    phi 1..1 MS and
    accessControl 1..* MS
* meta.security[phi] = http://terminology.hl7.org/CodeSystem/v3-Conf
* meta.tag contains
    hipaaCovered 1..1 MS
```

```
CodeSystem: PHIIdentifiers
* #name "Names"
* #geographic "Geographic identifiers"
* #dates "Dates related to individual"
* #phone "Phone numbers"
* #fax "Fax numbers"
* #email "Email addresses"
* #ssn "Social Security numbers"
* #mrn "Medical record numbers"
* #health-plan "Health plan numbers"
* #account "Account numbers"
* #license "License numbers"
* #vehicle "Vehicle identifiers"
* #device "Device identifiers"
* #url "URLs"
* #ip "IP addresses"
* #biometric "Biometric identifiers"
* #photo "Photos"
* #other "Other identifying information"
```

5.1.1 Protected Health Information (PHI)

```
Profile: MinimumNecessaryBundle
Parent: Bundle
* type = #collection
* entry.resource obeys minimum-necessary-rule
* entry.search.mode = #match
* entry.search.score 0..0  // Remover scores desnecessários

Invariant: minimum-necessary-rule
Description: "Only include necessary data elements"
Expression: "resource.meta.tag.where(system='http://hipaa.org/minimu
Severity: #error
```

5.1.2 Minimum Necessary Standard[15]

```
OperationDefinition: DeIdentifySafeHarbor
* url = "http://example.org/fhir/OperationDefinition/deidentify"
* name = "DeIdentify"
* title = "HIPAA Safe Harbor De-identification"
* parameter[0].name = #method
* parameter[0].use = #in
* parameter[0].type = #code
* parameter[0].binding.valueSet = "http://example.org/ValueSet/deide
```

```
ValueSet: DeidentificationMethods
* #safe-harbor "Safe Harbor (Remove 18 identifiers)"
* #expert-determination "Expert Determination"
* #limited-dataset "Limited Data Set"
```

5.1.3 De-identification Safe Harbor[16]

5.2 Security Rule Requirements[17]

```
CapabilityStatement: HIPAAAccessControl
* rest.security.service = http://terminology.hl7.org/CodeSystem/rest
* rest.security.description = "OAuth2 with SMART on FHIR"
* rest.resource.interaction.extension contains
    AccessControl named access 1..1 MS

Extension: AccessControl
* value[x] only CodeableConcept
* valueCodeableConcept from HIPAAAccessLevelVS

ValueSet: HIPAAAccessLevelVS
* #provider "Healthcare Provider"
* #payer "Insurance Payer"
* #patient "Patient Access"
* #emergency "Emergency Access"
* #admin "Administrative"
```

5.2.1 Access Controls

```
Profile: HIAAAAuditEvent
Parent: AuditEvent
* type 1..1 MS
* subtype 1..* MS
* action 1..1 MS
* period 1..1 MS
* outcome 1..1 MS
* outcomeDesc 0..1 MS
* agent 1..* MS
* agent.who 1..1 MS
* agent.requestor 1..1 MS
* source 1..1 MS
* entity 1..* MS
* entity.what 1..1 MS
* entity.role 1..1 MS
```

5.2.2 Audit Logging[18]

6. IMPLEMENTAÇÃO TÉCNICA DE SEGURANÇA

6.1 Criptografia[19]

```
# Configuração TLS mínima
security:
  tls:
    minimum_version: "1.2"
    preferred_version: "1.3"
    cipher_suites:
      - "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
      - "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
    certificate:
      type: "X.509"
      key_size: 2048
```

6.1.1 Em Trânsito

```
Extension: EncryptionMethod
Id: encryption-method
* value[x] only CodeableConcept
* valueCodeableConcept from EncryptionMethodVS

ValueSet: EncryptionMethodVS
* #AES256 "AES 256-bit"
* #AES128 "AES 128-bit"
* #RSA2048 "RSA 2048-bit"
* #RSA4096 "RSA 4096-bit"
```

6.1.2 Em Repouso

6.2 Controle de Acesso (RBAC/ABAC)[20]

```
CodeSystem: SecurityRoles
* #physician "Physician"
* #nurse "Nurse"
* #admin "Administrator"
* #patient "Patient"
* #emergency "Emergency Personnel"

Profile: RBACPractitioner
Parent: Practitioner
* extension contains SecurityRole named role 1..* MS
* extension[role].valueCodeableConcept from SecurityRolesVS
```

6.2.1 Role-Based Access Control

```
Extension: ABACPolicy
* extension contains
    resource 1..1 MS and
    action 1..* MS and
    condition 0..* MS and
    obligation 0..* MS
* extension[resource].value[x] only Reference
* extension[action].value[x] only code
* extension[condition].value[x] only Expression
```

6.2.2 Attribute-Based Access Control

6.3 Anonimização e Pseudonimização[21]

```javascript
// Função de anonimização
function anonymizePatient(patient) {
  return {
    ...patient,
    identifier: generatePseudonym(patient.identifier),
    name: [{use: "anonymous"}],
    birthDate: generalizeDate(patient.birthDate),
    address: generalizeAddress(patient.address),
    telecom: [],
    photo: [],
    contact: []
  };
}

// Generalização de data
function generalizeDate(date) {
  const year = new Date(date).getFullYear();
  return `${year}-01-01`; // Apenas ano
}

// Generalização de endereço
function generalizeAddress(address) {
  return address.map(addr => ({
    ...addr,
    line: [],
    text: undefined,
    postalCode: addr.postalCode?.substring(0, 3) + "00"
  }));
}
```

6.3.1 Técnicas de Anonimização

```
Profile: PseudonymizedPatient
Parent: Patient
* identifier.system = "http://example.org/pseudonym"
* identifier.value 1..1 MS
* identifier.extension contains
    PseudonymMapping named mapping 0..1 MS
* name.given 0..0
* name.family = "PSEUDONYMIZED"
* birthDate.extension contains
    DatePrecision named precision 0..1 MS

Extension: PseudonymMapping
Id: pseudonym-mapping
* value[x] only Identifier
* valueIdentifier.system = "http://example.org/mapping-key"
```

6.3.2 Pseudonimização Reversível

6.4 Auditoria e Monitoramento[22]

```
Profile: ComprehensiveAuditEvent
Parent: AuditEvent
* type from http://terminology.hl7.org/ValueSet/audit-event-type (re
* subtype 1..* MS
* action 1..1 MS
* period.start 1..1 MS
* period.end 1..1 MS
* outcome 1..1 MS
* agent ^slicing.discriminator.type = #pattern
* agent ^slicing.discriminator.path = "type"
* agent contains
    user 1..1 MS and
    system 0..1 MS
* agent[user].who.identifier 1..1 MS
* agent[user].requestor = true
* agent[system].who.identifier 1..1 MS
* agent[system].requestor = false
* source.observer 1..1 MS
* entity 1..* MS
* entity.what 1..1 MS
* entity.securityLabel 0..* MS
```

6.4.1 Padrão de Auditoria FHIR

```
ValueSet: MandatoryAuditEvents
* #C "Create"
* #R "Read/View"
* #U "Update"
* #D "Delete"
* #E "Execute"
* http://dicom.nema.org/resources/ontology/DCM#110100 "Application A
* http://dicom.nema.org/resources/ontology/DCM#110101 "Audit Log Use
* http://dicom.nema.org/resources/ontology/DCM#110102 "Begin Transfe
* http://dicom.nema.org/resources/ontology/DCM#110103 "DICOM Instanc
* http://dicom.nema.org/resources/ontology/DCM#110104 "DICOM Instanc
* http://dicom.nema.org/resources/ontology/DCM#110105 "DICOM Study D
* http://dicom.nema.org/resources/ontology/DCM#110106 "Export"
* http://dicom.nema.org/resources/ontology/DCM#110107 "Import"
* http://dicom.nema.org/resources/ontology/DCM#110108 "Network Entry
* http://dicom.nema.org/resources/ontology/DCM#110109 "Order Record"
* http://dicom.nema.org/resources/ontology/DCM#110110 "Patient Recor
* http://dicom.nema.org/resources/ontology/DCM#110111 "Procedure Rec
* http://dicom.nema.org/resources/ontology/DCM#110112 "Query"
* http://dicom.nema.org/resources/ontology/DCM#110113 "Security Aler
* http://dicom.nema.org/resources/ontology/DCM#110114 "User Authenti
```

6.4.2 Eventos de Auditoria Obrigatórios

7. CONSENTIMENTO E GESTÃO DE PREFERÊNCIAS

7.1 Modelo Unificado de Consentimento[23]

```
Profile: UnifiedConsent
Parent: Consent
* status 1..1 MS
* scope 1..1 MS
* category 1..* MS
* patient 1..1 MS
* dateTime 1..1 MS
* performer 1..1 MS
* organization 1..* MS
* source[x] 1..1 MS
* policy 1..* MS
* policy.authority 0..1 MS
* policy.uri 1..1 MS
* verification 0..* MS
* provision 1..1 MS
* provision.type 1..1 MS
* provision.period 0..1 MS
* provision.actor 0..* MS
```

```
* provision.action 0..* MS
* provision.securityLabel 0..* MS
* provision.purpose 0..* MS
* provision.class 0..* MS
* provision.code 0..* MS
* provision.dataPeriod 0..1 MS
* provision.data 0..* MS
* provision.provision 0..* MS

// Extensões para regulamentações específicas
* extension contains
    LGPDCompliance named lgpd 0..1 MS and
    GDPRCompliance named gdpr 0..1 MS and
    HIPAACompliance named hipaa 0..1 MS
```

7.2 Granularidade de Consentimento[24]

```
ValueSet: ConsentGranularity
* #all "Todos os dados"
* #category "Por categoria"
* #resource "Por tipo de recurso"
* #instance "Por instância específica"
* #element "Por elemento de dado"

Profile: GranularConsent
Parent: Consent
* provision.data ^slicing.discriminator.type = #pattern
* provision.data ^slicing.discriminator.path = "meaning"
* provision.data contains
    included 0..* MS and
    excluded 0..* MS
* provision.data[included].meaning = #authorizes
* provision.data[excluded].meaning = #denies
```

8. GESTÃO DE INCIDENTES E VIOLAÇÕES

8.1 Detecção de Violações[25]

```
Profile: DataBreachIncident
Parent: DetectedIssue
* status = #final
* code from DataBreachTypeVS (required)
* severity 1..1 MS
* patient 0..* MS  // Pacientes afetados
* identified[x] 1..1 MS
* author 1..1 MS
```

```
* implicated 1..* MS  // Recursos comprometidos
* detail 1..1 MS
* mitigation 0..* MS

ValueSet: DataBreachTypeVS
* #unauthorized-access "Acesso não autorizado"
* #data-loss "Perda de dados"
* #data-theft "Roubo de dados"
* #malware "Infecção por malware"
* #phishing "Ataque de phishing"
* #insider-threat "Ameaça interna"
* #physical-breach "Violação física"
```

8.2 Processo de Notificação[26]

```
Task: BreachNotificationTask
* status = #requested
* intent = #order
* priority = #urgent
* code = #breach-notification
* description = "Notificar autoridades e afetados sobre violação de
* for 1..* MS  // Pacientes afetados
* authoredOn 1..1 MS
* requester 1..1 MS
* owner 1..1 MS  // DPO ou responsável
* restriction.period.end 1..1 MS  // Prazo legal (72h GDPR, 2 dias L
* input contains
    breachDetails 1..1 MS and
    affectedCount 1..1 MS and
    riskAssessment 1..1 MS
```

9. TRANSFERÊNCIA INTERNACIONAL DE DADOS

9.1 Mecanismos de Transferência[27]

```
Extension: InternationalTransfer
Id: international-transfer
* extension contains
    destination 1..1 MS and
    mechanism 1..1 MS and
    safeguards 0..* MS
* extension[destination].value[x] only CodeableConcept
* extension[destination].valueCodeableConcept from CountryCodeVS
* extension[mechanism].value[x] only CodeableConcept
* extension[mechanism].valueCodeableConcept from TransferMechanismVS
* extension[safeguards].value[x] only string
```

```
ValueSet: TransferMechanismVS
* #adequacy "Decisão de adequação"
* #scc "Cláusulas contratuais padrão"
* #bcr "Binding Corporate Rules"
* #consent "Consentimento explícito"
* #legitimate-interest "Interesse legítimo"
```

9.2 Adequação e Garantias[28]

```
Profile: CrossBorderDataTransfer
Parent: Contract
* type = #data-transfer-agreement
* subject 1..* MS  // Dados transferidos
* authority 0..* MS  // Autoridade supervisora
* domain 1..* MS  // Jurisdições envolvidas
* term.offer.party 1..* MS  // Exportador de dados
* term.offer.answer 1..1 MS
* term.asset 1..* MS  // Categorias de dados
* term.action 1..* MS  // Obrigações de proteção
* legal 0..* MS  // Base legal
* rule 0..* MS  // Salvaguardas aplicáveis
```

10. PRIVACIDADE DIFERENCIAL E TÉCNICAS AVANÇADAS

10.1 Privacidade Diferencial[29]

```javascript
// Implementação de ruído Laplaciano
function addLaplacianNoise(value, sensitivity, epsilon) {
  const scale = sensitivity / epsilon;
  const u = Math.random() - 0.5;
  const noise = -scale * Math.sign(u) * Math.log(1 - 2 * Math.abs(u))
  return value + noise;
}

// Aplicar a contagens agregadas
function differentiallyPrivateCount(realCount, epsilon = 1.0) {
  const sensitivity = 1; // Sensibilidade para contagem
  return Math.round(addLaplacianNoise(realCount, sensitivity, epsilon
}
```

10.2 K-Anonimato[30]

```
Profile: KAnonymousDataset
Parent: Bundle
* type = #collection
```

```
* entry.resource obeys k-anonymity-rule

Invariant: k-anonymity-rule
Description: "Cada combinação de quasi-identificadores deve aparecer
Expression: "entry.resource.where(
  birthDate = %resource.birthDate and
  address.postalCode = %resource.address.postalCode
).count() >= 5"
Severity: #error
```

10.3 Homomorphic Encryption[31]

```
Extension: HomomorphicEncryption
Id: homomorphic-encryption
* extension contains
    algorithm 1..1 MS and
    publicKey 1..1 MS and
    operations 0..* MS
* extension[algorithm].value[x] only code
* extension[algorithm].valueCode from HomomorphicAlgorithmVS
* extension[publicKey].value[x] only base64Binary
* extension[operations].value[x] only code

ValueSet: HomomorphicAlgorithmVS
* #paillier "Paillier cryptosystem"
* #gentry "Gentry's scheme"
* #bgv "Brakerski-Gentry-Vaikuntanathan"
* #ckks "Cheon-Kim-Kim-Song"
```

11. MONITORAMENTO E MÉTRICAS DE CONFORMIDADE

11.1 KPIs de Privacidade[32]

```
Measure: PrivacyComplianceMetrics
* status = #active
* subjectCodeableConcept = #Location
* date = "2024-01-01"
* publisher = "Organization"
* group contains
    consentRate 1..1 MS and
    breachCount 1..1 MS and
    dataMinimization 1..1 MS and
    encryptionCoverage 1..1 MS
* group[consentRate].code = #consent-rate
* group[consentRate].population.code = #initial-population
* group[breachCount].code = #breach-incidents
```

```
* group[dataMinimization].code = #data-minimization-score
* group[encryptionCoverage].code = #encryption-percentage
```

11.2 Dashboard de Conformidade

```yaml
privacy_dashboard:
  metrics:
    - id: consent_coverage
      name: "Cobertura de Consentimento"
      target: 100%
      current: 98.5%

    - id: encryption_status
      name: "Dados Criptografados"
      target: 100%
      current: 99.9%

    - id: audit_completeness
      name: "Completude de Auditoria"
      target: 100%
      current: 100%

    - id: incident_response_time
      name: "Tempo de Resposta a Incidentes"
      target: "<24h"
      current: "18h"

    - id: data_retention_compliance
      name: "Conformidade de Retenção"
      target: 100%
      current: 97%
```

12. TEMPLATES E CHECKLISTS

12.1 Checklist de Conformidade LGPD/GDPR/HIPAA

```markdown
## Checklist de Conformidade

### LGPD
- [ ] Base legal definida para cada tratamento
- [ ] Consentimento documentado quando aplicável
- [ ] RIPD elaborado para operações de alto risco
- [ ] DPO/Encarregado designado
- [ ] Canal de comunicação com titulares
- [ ] Procedimento para atender direitos dos titulares
- [ ] Notificação de incidentes à ANPD
```

```
### GDPR
- [ ] Lawful basis identificada
- [ ] DPIA conduzida quando necessário
- [ ] Privacy by Design implementado
- [ ] Privacy by Default configurado
- [ ] Registro de atividades de tratamento
- [ ] Acordos com processadores
- [ ] Mecanismos para transferência internacional

### HIPAA
- [ ] PHI identificada e classificada
- [ ] Minimum necessary implementado
- [ ] De-identification aplicada quando apropriado
- [ ] BAA com business associates
- [ ] Security Rule safeguards implementados
- [ ] Breach notification procedures
- [ ] Training documentation
```

12.2 Template de Privacy Notice

```
# Aviso de Privacidade / Privacy Notice

## Controlador de Dados / Data Controller
[Nome da Organização]
[Endereço]
[Contato do DPO]

## Dados Coletados / Data Collected
- Identificação pessoal
- Dados de saúde
- [Outras categorias]

## Finalidade do Tratamento / Purpose of Processing
- Prestação de cuidados de saúde
- Pesquisa médica (com consentimento)
- [Outras finalidades]

## Base Legal / Legal Basis
- LGPD Art. 7°, VIII (tutela da saúde)
- GDPR Art. 9(2)(h) (healthcare)
- HIPAA covered entity obligations

## Compartilhamento / Data Sharing
[Descrever com quem os dados são compartilhados]

## Direitos do Titular / Data Subject Rights
```

```
- Acesso / Access
- Correção / Rectification
- Exclusão / Erasure
- Portabilidade / Portability
- Oposição / Objection

## Retenção / Retention
[Período de retenção e critérios]

## Contato / Contact
[E-mail e telefone para exercício de direitos]
```

13. REFERÊNCIAS

1. Brasil. Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
2. European Union. Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj
3. U.S. Department of Health & Human Services. HIPAA Administrative Simplification. Disponível em: https://www.hhs.gov/hipaa/index.html
4. ISO/IEC 27001:2022. Information security management systems. ISO.
5. ISO 27799:2016. Health informatics — Information security management in health. ISO.
6. ANPD. Guia Orientativo para Definições dos Agentes de Tratamento. Disponível em: https://www.gov.br/anpd/
7. ANPD. Direitos do Titular. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/direitos-do-titular
8. ANPD. Guia de Boas Práticas para Relatório de Impacto. 2023.
9. European Data Protection Board. Guidelines on consent under Regulation 2016/679. 2020.
10. ENISA. Privacy by Design. Disponível em: https://www.enisa.europa.eu/
11. Article 29 Working Party. Guidelines on the right to data portability. 2017.
12. EDPB. Guidelines 01/2022 on data subject rights - Right of access. 2022.
13. ICO. Privacy by design. Disponível em: https://ico.org.uk/
14. HHS. Summary of the HIPAA Privacy Rule. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/
15. HHS. Minimum Necessary Requirement. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/
16. HHS. Methods for De-identification of PHI. Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/
17. HHS. HIPAA Security Rule. Disponível em: https://www.hhs.gov/hipaa/for-professionals/security/
18. HHS. Audit Controls. 45 CFR 164.312(b).
19. NIST. SP 800-175B - Guideline for Using Cryptographic Standards. 2020.
20. NIST. SP 800-162 - Guide to Attribute Based Access Control. 2014.
21. ISO/IEC 20889:2018. Privacy enhancing data de-identification terminology and classification of techniques.
22. HL7. FHIR Security and Privacy Module. Disponível em: http://hl7.org/fhir/security.html
23. HL7. Consent Resource. Disponível em: http://hl7.org/fhir/consent.html
24. Kantara Initiative. Consent Receipt Specification. 2018.

25. ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches. 2013.
26. GDPR Art. 33 & 34. Personal data breach notification.
27. EDPB. Recommendations 01/2020 on measures that supplement transfer tools. 2020.
28. European Commission. Standard Contractual Clauses. 2021.
29. Dwork, C. Differential Privacy. ICALP 2006.
30. Sweeney, L. k-anonymity: a model for protecting privacy. 2002.
31. Gentry, C. Fully homomorphic encryption using ideal lattices. STOC 2009.
32. ISO/IEC 27701:2019. Privacy information management. ISO.

Documento aprovado por: [Comitê de Privacidade e Segurança]
Data de vigência: 2024-2025
Próxima revisão: Janeiro 2026