# PRIVACY RISK TREATMENT PLAN

---

**TREATMENT PLAN SUMMARY**

**Organization:** HealthBook Telemedicine Platform
**Plan Period:** March - May 2025
**Prepared by:** Chief Privacy Officer
**Approved by:** CEO
**Date:** 1 March 2025

---

**RISK 1: UNAUTHORIZED ACCESS TO PATIENT MEDICAL RECORDS**

**Risk ID:** PR-008
**Risk Owner:** Chief Technology Officer

**Current Risk Assessment:**

- Likelihood: 4 (Likely)
- Impact to Patients: 5 (Severe - health data disclosure)
- Impact to Organization: 5 (Severe - GDPR violation, €1M+ fine)
- **Current Risk Score: 20 (CRITICAL)**

**Existing Controls:**

- Basic username/password authentication
- Access logging (not monitored)

**Treatment Option:** REDUCE RISK

---

**Controls to Implement:**

| Control | Responsible | Deadline | Budget |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Multi-factor authentication (MFA) | IT Director | 15-Mar-2025 | €8,000 |
| Role-based access control (RBAC) | IT Director | 30-Mar-2025 | €12,000 |
| Automated access monitoring with alerts | Security Manager | 15-Apr-2025 | €6,000 |
| Quarterly access reviews | CPO | 30-Apr-2025 | €0 |
| Staff training on access controls | HR Manager | 30-Apr-2025 | €3,000 |

**Total Budget:** €29,000
**Timeline:** 60 days

**Success Criteria:**

- 100% medical staff using MFA
- Access restricted based on job role
- Automated alerts for unusual access patterns
- Zero unauthorized access incidents

**Target Residual Risk:**

- Likelihood: 2 (Unlikely)
- Impact: 4 (Major)
- **Target Risk Score: 8 (MEDIUM) - Acceptable**

---

**RISK 2: VIDEO CONSULTATIONS NOT ENCRYPTED**

**Risk ID:** PR-012
**Risk Owner:** Chief Technology Officer

**Current Risk Assessment:**

- Likelihood: 5 (Almost Certain - no encryption currently)
- Impact to Patients: 4 (Major - confidential health discussions exposed)
- Impact to Organization: 5 (Severe - regulatory violation)

- **Current Risk Score: 20 (CRITICAL)**

**Existing Controls:**

- None (video transmitted unencrypted)

**Treatment Option:** REDUCE RISK

---

**Controls to Implement:**

| Control | Responsible | Deadline | Budget |
|---|---|---|---|
| End-to-end encryption for video | IT Director | 31-Mar-2025 | €15,000 |
| Encrypted cloud recording storage | IT Director | 31-Mar-2025 | Included |
| Patient consent for recording | Product Manager | 15-Mar-2025 | €2,000 |
| 30-day auto-deletion of recordings | IT Director | 31-Mar-2025 | €0 |

**Total Budget:** €17,000
**Timeline:** 30 days

**Success Criteria:**

- All video consultations encrypted end-to-end
- Recordings encrypted at rest
- Patient consent obtained before recording
- Recordings automatically deleted after 30 days

**Target Residual Risk:**

- Likelihood: 1 (Rare)
- Impact: 3 (Moderate)
- **Target Risk Score: 3 (LOW) - Acceptable**

---

**RISK 3: NO DATA RETENTION POLICY**

**Risk ID:** PR-015
**Risk Owner:** Chief Privacy Officer

**Current Risk Assessment:**

- Likelihood: 5 (Certain - data kept indefinitely)
- Impact to Patients: 3 (Moderate - unnecessary data retention)
- Impact to Organization: 4 (Major - GDPR storage limitation violation)
- **Current Risk Score: 15 (HIGH)**

**Existing Controls:**

- None (no retention policy exists)

**Treatment Option:** REDUCE RISK

---

**Controls to Implement:**

| Control | Responsible | Deadline | Budget |
|---|---|---|---|
| Data retention policy documented | CPO | 15-Mar-2025 | €0 |
| Retention schedule by data type | CPO + Legal | 30-Mar-2025 | €5,000 |
| Automated deletion workflows | IT Director | 30-Apr-2025 | €10,000 |
| Annual retention review process | CPO | 15-May-2025 | €0 |

**Total Budget:** €15,000
**Timeline:** 75 days

**Retention Schedule:**

- Active patient records: Duration of care + 7 years
- Inactive patient records: 7 years then delete
- Video consultation recordings: 30 days then delete
- Appointment history: 3 years then delete

- Marketing consent: Until withdrawn + 30 days

**Success Criteria:**

- Board-approved retention policy
- Automated deletion implemented
- First deletion cycle completed

**Target Residual Risk:**

- Likelihood: 2 (Unlikely)
- Impact: 2 (Minor)
- **Target Risk Score: 4 (LOW) - Acceptable**

---

**RISK 4: THIRD-PARTY PRESCRIPTION SERVICE LACKS PROCESSOR AGREEMENT**

**Risk ID:** PR-020
**Risk Owner:** Chief Operating Officer

**Current Risk Assessment:**

- Likelihood: 5 (Certain - no agreement in place)
- Impact to Patients: 4 (Major - data shared without proper controls)
- Impact to Organization: 4 (Major - GDPR Article 28 violation)
- **Current Risk Score: 16 (CRITICAL)**

**Existing Controls:**

- Basic commercial contract (no privacy terms)

**Treatment Option:** REDUCE RISK

---

**Controls to Implement:**

| Control | Responsible | Deadline | Budget |
|---|---|---|---|
| GDPR-compliant processor agreement | Legal Counsel | 31-Mar-2025 | €8,000 |
| Security assessment of processor | Security Manager | 15-Apr-2025 | €5,000 |
| Audit rights negotiated | Legal Counsel | 31-Mar-2025 | Included |
| Annual compliance reviews | CPO | Ongoing | €0 |

**Total Budget:** €13,000
**Timeline:** 45 days

**Success Criteria:**

- Signed processor agreement in place
- Security assessment completed and acceptable
- Audit rights established
- First annual review scheduled

**Target Residual Risk:**

- Likelihood: 2 (Unlikely)
- Impact: 3 (Moderate)
- **Target Risk Score: 6 (MEDIUM) - Acceptable**

---

**TREATMENT PLAN SUMMARY**

| Risk ID | Risk | Current Score | Target Score | Budget | Deadline |
|---|---|---|---|---|---|
| PR-008 | Unauthorized access | 20 (CRITICAL) | 8 (MEDIUM) | €29,000 | 30-Apr-2025 |
| PR-012 | Video not encrypted | 20 (CRITICAL) | 3 (LOW) | €17,000 | 31-Mar-2025 |

| | | | | | |
|---|---|---|---|---|---|
| PR-015 | No retention policy | 15 (HIGH) | 4 (LOW) | €15,000 | 15-May-2025 |
| PR-020 | No processor agreement | 16 (CRITICAL) | 6 (MEDIUM) | €13,000 | 15-Apr-2025 |
| **TOTALS** | **4 risks** | - | - | **€74,000** | **15-May-2025** |

---

**IMPLEMENTATION SCHEDULE**

**March 2025:**

- Week 1-2: MFA and video encryption implementation
- Week 3-4: RBAC, consent mechanisms, processor agreement negotiation

**April 2025:**

- Week 1-2: Access monitoring, security assessments
- Week 3-4: Retention automation, training delivery, quarterly access reviews

**May 2025:**

- Week 1-2: Final testing, annual review processes established
- Week 3: Post-implementation reviews and documentation

---

**MONITORING AND REPORTING**

**Weekly:** Implementation progress reported to CPO

**Bi-weekly:** Status update to executive team

**Monthly:** Board report on risk treatment progress

**Upon Completion:** Full implementation report with residual risk assessment

---


**RISK OWNER APPROVALS**

| Risk ID | Risk Owner | Approval | Date |
|---|---|---|---|
| PR-008 | CTO | _____ | _____ |
| PR-012 | CTO | _____ | _____ |
| PR-015 | CPO | _____ | _____ |
| PR-020 | COO | _____ | _____ |

---

**EXECUTIVE APPROVAL**

**Chief Privacy Officer:** _____ Date: _____

**Chief Executive Officer:** _____ Date: _____

---

**End of Risk Treatment Plan**

**GROUP ACTIVITIES**

**Scenario:** You are the CPO of a healthcare telemedicine app with 150,000 patients. You're implementing a new AI symptom checker feature.

**Tasks:**

**1. Operational Planning (6.1):**

- Define 3 process criteria for the "AI Symptom Checker Privacy Review" process
- Identify 2 preventive controls and 1 detective control

**2. Risk Assessment (6.2):**

- Identify 3 privacy risks from this new AI feature
- This is a "significant change proposed" - explain why a risk assessment is required

...global validation

**3. Risk Treatment (6.3):**

- For one HIGH risk you identified, create a simple treatment plan showing:
    - Treatment option selected
    - 2 controls to implement
    - How you'll verify effectiveness
    - What documentation you'll retain