

Heartsapiens Medikal Teknoloji AŞ Quality and Information Security Policy

1. Purpose

The purpose of this policy is to ensure the highest level of quality in the web and mobile software developed by Heartsapiens Medikal Teknoloji AŞ and the confidentiality, integrity, and availability of patient and/or healthcare professional data. This policy is binding on all our employees, contractors, and business partners.

2. Scope

This policy covers all web and mobile software developed by Heartsapiens Medikal Teknoloji AŞ, the development, testing, deployment, maintenance, and support processes for this software, and all systems, data, and information used in these processes.

3. Principles

Patient and Healthcare Professional Focus: In all our activities, we prioritize patient and healthcare professional safety and the confidentiality of patient and healthcare professional data.

Legal Compliance: We conduct our activities in accordance with all applicable laws, regulations, standards, and industry requirements (e.g., KVKK, HIPAA, GDPR).

Continuous Improvement: We continuously review, evaluate, and improve our quality and information security management system.

Risk Management: We systematically identify, assess, and manage information security risks.

Transparency: We openly share our policies and procedures related to quality and information security with all our stakeholders.

Training and Awareness: We conduct regular training sessions to increase our employees' awareness of quality and information security issues.

Data Confidentiality: We protect patient data against unauthorized access, use, and disclosure.

Data Integrity: We ensure the accuracy and completeness of patient data.

Accessibility: We ensure that authorized users can access patient data in a timely and secure manner.

4. Quality Objectives

Minimize software errors and maximize customer satisfaction.

Align our software development processes with international standards (e.g., ISO 9001, CMMI).

Improve software testing processes to increase the reliability of software.

Effectively manage and resolve customer complaints.

Continuously improve the technical knowledge and skills of our employees.

5. Information Security Objectives

Protect our information assets against unauthorized access, use, disclosure, modification, and destruction.

Detect, analyze, and prevent information security incidents.

Respond quickly and effectively to information security breaches.

Increase information security awareness and ensure that our employees fulfill their responsibilities.

Ensure our business continuity and be prepared for emergencies.

Ensure patient safety by protecting data confidentiality and integrity.

Comply with legal and regulatory requirements.

6. Responsibilities

Board of Directors: Responsible for approving, implementing, and continuously reviewing this policy.

Senior Management: Responsible for the effective implementation of the quality and information security management system and the provision of resources.

Quality Manager: Responsible for developing, implementing, and maintaining the quality management system.

Information Security Manager: Responsible for developing, implementing, and maintaining the information security management system, risk management, incident management, and awareness training.

All Employees: Responsible for complying with this policy, reporting information security breaches, and participating in training.

7. Policy Implementation

This policy is communicated to all employees, contractors, and business partners of Heartsapiens Medikal Teknoloji AŞ.

Procedures, instructions, and guidelines are prepared to ensure the implementation of the policy.

The policy is reviewed and updated at regular intervals (e.g., annually).

Disciplinary action may be taken in case of non-compliance with the policy.

8. Certification and Standardization

Heartsapiens Medikal Teknoloji AŞ aims to certify its quality and information security management system in accordance with international standards (e.g., ISO 9001, ISO 27001, HIPAA, GDPR).

We strive to align our software development processes and products with industry standards (e.g., HL7, DICOM).

9. Communication

Please contact info@heartsapiens.com for any questions or concerns regarding this policy.

10. Approval

This policy was approved by Zeki Çatav on 01/01/2025.