INFORMATION SECURITY AND CYBERSECURITY POLICY

ISSUE 2 | September 29, 2025
Approved by the BoD Decision No.904/29-09-2025

ATHENS MEDICAL GROUP

CONTENTS

1. INTRODUCTION – PURPOSE AND SCOPE

Information security and personal data protection are non-negotiable prerequisites for the provision of high-quality healthcare services. The company "IATRIKO ATHINON E.A.E." (ATHENS MEDICAL CENTER S.A.) and its subsidiaries, which constitute the Iatriko Athinon Group (hereinafter referred to as the "Group"), recognize their responsibility towards patients, employees, and partners, adopts this Information Security and Cybersecurity Policy, which is an official commitment of the Management and a single point of reference for all matters relating to data security and protection.

This Policy:

- Expresses the Group's strategic commitment to protecting the confidentiality, integrity, and availability of information.
- Complies with applicable European and national legislation (NIS2 Directive, Law 5160/2024, Joint Ministerial Decision 1689/2025, GDPR) and international standards (ISO 27001, ISO 22301).
- It replaces the Group's previous Information Security Policy (version 2023) by linking to the individual processes D.O.10 (Medical Data Management) and D.O.11 (Health Technology and Information Systems Management) of the Quality Management System and is the official reference point for all cybersecurity issues.

Scope

The Information Security and Cybersecurity Policy covers:

- All of the Group's Healthcare Units (hospitals, diagnostic centers, clinics).
- Administrative and support services.
- Information systems (electronic patient records, laboratory systems, medical images, ERP, telemedicine).
- Medical equipment connected to IT networks and systems.
- All employees, partners, suppliers, and third-party service providers.
- All forms of information (electronic, printed, verbal).

2. LEGISLATIVE AND REGULATORY FRAMEWORK

The Iatriko Athinon Group operates in a particularly strict regulatory environment, where compliance with information security and cybersecurity rules is not an option but an obligation. This Policy is based on three main pillars: European and national law, international standards, and the Group's internal policies.

2.1 European and National Framework

- Directive (EU) 2022/2555 – NIS2: Sets minimum rules for cybersecurity risk management and incident reporting obligations.
- Law 5160/2024: Transposes the NIS2 Directive into Greek law, setting out clear obligations for essential and important health entities.
- Joint Ministerial Decision 1689/2025: Sets out the minimum technical, organizational, and operational measures that healthcare entities in Greece must implement.
- General Data Protection Regulation (GDPR) & Law 4624/2019: Regulate the processing of personal data and strengthen patients' rights.
- eIDAS Regulation (910/2014): Sets out the requirements for electronic identification and trust services.

2.2 International Standards and Best Practices

- ISO/IEC 27001:2022: Information Security Management System.
- ISO 22301:2019: Business continuity and crisis management.
- ISO/IEC 27701:2019: Privacy protection in the context of ISO 27001.
- NIST Cybersecurity Framework: Internationally recognized guide to risk-based governance.

2.3 Healthcare Industry Standards

- JCI (Joint Commission International): International standard for quality and safety in healthcare.
- HIPAA (USA): Used as a benchmark for health data protection, without legal obligation in Greece.
- Ministry of Health Guidelines: Specifically for electronic patient records and eHealth services.

2.4 Internal Group Framework

This Policy incorporates and guides:

- Internal procedures for the management of medical data, health technology and information systems.
- The previous Information Security Policy (2023), which is replaced and now considered a historical version.

3. ORGANIZATIONAL STRUCTURE AND ROLES

Cybersecurity at the Iatriko Athinon Group is not just a matter for the IT Department; it is a responsibility that starts with management and permeates every level. To ensure effective governance, we implement a clear framework of roles and responsibilities.

3.1 Role of Management

The Board of Directors and Management:

- ✓ Approve and oversee the Information Security and Cybersecurity Policy.
- ✓ Determine the level of risk appetite.
- ✓ They ensure that the necessary resources (financial, human, technological) are available.
- ✓ They systematically monitor progress through reports and performance indicators.

3.2 Critical Roles

- **Chief Information Security Officer (CISO):** Designs and implements the Information Security Management System, coordinates the incident response team, and recommends improvement measures.
- **Data Protection Officer (DPO):** Monitors compliance with the GDPR and acts as a liaison with the Personal Data Protection Authority.
- **Incident Response Team: Activated** immediately in the event of a cybersecurity incident. It consists of the CISO, the DPO, IT executives, a representative of the Management, as well as experts in legal and communication issues.
- **IT & Data Security Department:** Implements technical measures, ensures the availability of critical systems, and monitors infrastructure with security tools.
- **Quality & Clinical Effectiveness Department:** Integrates security indicators into the overall quality system and conducts internal audits.
- **Medical and Nursing Staff:** Applies confidentiality policies on a daily basis and reports suspicious incidents immediately.
- **External Partners and Suppliers:** They are contractually bound to adhere to the same security standards as the Group and are subject to evaluation and control.

3.3 Cybersecurity Committee

A special Cybersecurity Committee is established with the participation of representatives from Management, the CISO, the DPO, IT, Quality, and the Legal Department. The Committee meets on a regular basis and:

1. Evaluates the effectiveness of the measures.
2. Approves improvement plans.
3. Submits recommendations to the Board of Directors.

4. SECURITY PRINCIPLES AND STRATEGIC OBJECTIVES

Information security at the Iatriko Athinon Group is not just a technical measure; it is a core value that ensures the trust of our patients and partners. It is based on internationally recognized principles and specific strategic objectives.

4.1 Fundamental Principles

- Confidentiality: Only authorized persons have access to data.
- Integrity: Data remains complete, accurate, and unchanged.
- Availability: Critical health services (e.g., electronic patient records, telemedicine) remain accessible without interruption.
- Accountability: All actions are logged and can be audited.
- Proportionality: Measures are tailored to the severity of the risks and the nature of the data, as required by law.
- Continuous improvement: The policy is reviewed regularly to incorporate new threats, technologies, and best practices.

4.2 Strategic Objectives

1. **Regulatory Compliance:** Ensuring full compliance with the NIS2 Directive, Law 5160/2024, Joint Ministerial Decision 1689/2025, the GDPR, and international ISO standards.
2. **Health Data Protection:** Safeguarding patient confidentiality and privacy, with zero tolerance for breaches.
3. **Cyber resilience:** Ensuring that the Group remains operational even in the event of a cyber attack or crisis, through recovery and business continuity plans.
4. **Security as a Culture:** Raising awareness among all employees through training and continuous information, so that security becomes part of everyday practice.
5. **Risk Management:** Implementing systematic risk assessment and taking measures that reduce the likelihood and impact of security incidents.
6. **Transparency and Trust:** Strengthening the trust of patients and partners through responsible and clear communication on security issues.

5. CYBERSECURITY RISK MANAGEMENT

Information security is not static; it is a constantly evolving process. The Iatriko Athinon Group implements a comprehensive risk management framework in accordance with Directive NIS2, Joint Ministerial Decision 1689/2025, and international standards ISO 27005 and ISO 31000.

5.1 Risk Management Strategy

✓ We recognize that risks can be technical (e.g., malware), operational (e.g., interruption of critical services), regulatory (e.g., GDPR violation), or originate from third-party partners.

✓ We adopt a risk-based approach: each system, data, or partner is assessed in terms of the

likelihood and impact of an incident.

✓ The level of risk appetite is defined by Management and reviewed annually.

5.2 Risk Assessment Process

The process includes:

1. Identification of critical elements (information systems, medical data, technological equipment).
2. Identification of threats and vulnerabilities (e.g., ransomware, phishing, human error, climate crisis, natural disasters).
3. Analysis of operational impacts (Business Impact Analysis): assessment of consequences in the event of an interruption.
4. Probability and severity assessment: categorization of risks into levels (low, medium, high).
5. Preparation of a Contingency Plan: selection of preventive or corrective measures, based on cost/benefit and regulatory requirements.

Risk Categories

✓ Technological: malware attacks, data loss, system failure.

✓ Human: user errors, inadequate training, malicious internal actions.

✓ Physical: fire, earthquake, flood.

✓ Partner-related: inadequate security measures by suppliers or partners.

✓ Regulatory/legal: breach of NIS2 or GDPR obligations.

✓ Risk Mitigation Measures

Appropriate measures are selected for each identified risk, such as:

✓ Technical solutions (firewalls, encryption, access control).

✓ Organizational measures (policies, contracts with partners, procedures).

✓ Staff training and awareness programs.

✓ Disaster Recovery Plans and Business Continuity Plans.

6. INCIDENT RESPONSE AND BUSINESS CONTINUITY

Despite strong preventive measures, no system is completely invulnerable. The Iatriko Athinon Group recognizes that cybersecurity incidents or operational disruptions may occur and has established procedures for their immediate and effective management.

6.1 Incident Response

✓ An Incident Response Team (IRT) has been established, led by the Chief Information Security Officer (CISO) and composed of representatives from the Data Protection Officer (DPO), IT Department, Management, Legal, and Communications.

✓ The Team is immediately activated upon detection of an incident (e.g., cyberattack, data loss).

✓ Priority is given to damage containment, patient protection, and restoration of operations.

✓ Where required, notifications are made to the competent authorities within the prescribed timeframes (24 hours under NIS2, 72 hours under GDPR).

✓ All incidents are recorded and analyzed to extract lessons learned and improve processes.

6.2 Business Continuity

The Group implements a Business Continuity Plan (BCP) and a Disaster Recovery Plan (DRP), which:

✓ Ensure the uninterrupted operation of critical systems (such as electronic patient records).

✓ Define alternative solutions and procedures in the event of a major disruption.
✓ Include Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), establishing clear availability commitments.
✓ Are tested regularly through simulation exercises.

6.3 Communication and Transparency

In the event of an incident affecting patients or associates:

✓ The Group provides immediate, clear, and understandable information.
✓ It provides instructions on any actions that need to be taken by those concerned.
✓ It will strengthen trust through transparent communication and cooperation with the competent authorities.

7. TRAINING, AWARENESS, AND SECURITY CULTURE

Cybersecurity does not depend solely on systems and procedures; it is based primarily on human behavior. The Iatriko Athinon Group invests in training and in fostering a culture of security that permeates the entire organization.

7.1 Mandatory Training

✓ All employees, from medical and nursing staff to administrative and technical staff, participate in mandatory information security training programs.
✓ The programs cover topics such as: recognizing suspicious emails (phishing), secure use of passwords, protection of medical data, and confidentiality rules.
✓ Training is repeated on an annual basis and adapted to new threats.

7.2 Awareness and Information

✓ Regular awareness campaigns are organized to reinforce "security in practice".
✓ Internal information material (guides, fact sheets, newsletters) with practical advice is available.
✓ The Group encourages ongoing communication: every employee can and should report suspicious incidents immediately.

7.3 Fostering a Culture of Safety

✓ Safety is seen not as an obstacle, but as the foundation of quality in healthcare.
✓ Staff involvement is crucial: compliance with rules and responsible use of systems strengthen the Group's resilience.
✓ Management promotes and rewards responsible behavior, reinforcing the belief that "security is everyone's responsibility."

8. PARTNERS, SUPPLIERS, AND THIRD PARTIES

Cybersecurity is not just about the internal systems of the Iatriko Athinon Group. In the healthcare sector, partnerships with external entities (e.g., technology suppliers, IT service providers, contractual partners) are critical and can directly affect the security of data and systems.

8.1 Contractual Obligations

✓ All external partners and suppliers sign contracts that include information security clauses.
✓ The contracts incorporate Service Level Agreements (SLAs) and Data Processing Agreements (DPAs) to ensure compliance with the same security standards applied by the Group.

8.2 Assessment and Monitoring

✓ Partners are assessed based on the criticality of their services and the level of risk they may pose (risk tiering).
✓ Regular audits are conducted to verify their compliance with cybersecurity requirements.
✓ In the event of an incident affecting them, they are required to notify the Group immediately and in any case within 24 hours.

8.3 Joint Responsibility

Cooperation with third parties is based on the principle of shared responsibility:

✓ The Group ensures that partners meet high security standards.
✓ Partners are required to implement equivalent protection measures.
✓ Together, they form a single security chain with no weak links.

9. CONTINUOUS IMPROVEMENT AND REVIEW OF POLICY

Cybersecurity is a dynamic field that evolves daily with new threats, technologies, and regulatory requirements. The Iatriko Athinon Group recognizes that the Information Security and Cybersecurity Policy must remain relevant and effective.

9.1 Principle of Continuous Improvement

□ The Policy incorporates the "Plan – Do – Check – Act" principle, with the aim of achieving a continuous cycle of improvement.
□ Every incident, audit, or change in the environment (technological or regulatory) is an opportunity to review the measures.
□ Key performance indicators (KPIs) and key risk indicators (KRIs) are regularly evaluated to achieve measurable improvements.

9.2 Periodic Review

□ The Policy is reviewed at least once a year by the Cybersecurity Committee and reapproved by Management.
□ In addition, it is revised immediately in the event of:
  - changes in legislation (e.g., new regulatory acts or European directives),
  - significant technological developments,
  - serious cybersecurity incidents.

9.3 Everyone's Involvement

□ Improvement is not just a matter for security managers; it is everyone's business.
□ Employees and partners are encouraged to suggest improvements and report gaps or weaknesses.
□ Management is committed to taking into account all feedback and incorporating them where necessary.

10. MANAGEMENT COMMITMENT AND FINAL PROVISIONS

The Management of the Iatriko Athinon Group recognizes that information protection and cybersecurity are an essential part of the Group's mission to provide quality, safe, and reliable healthcare services. The Management assumes full responsibility for the implementation of this Policy and is committed to continuously strengthening security mechanisms in accordance with international practices and regulatory requirements.

10.1 Management Commitment

The Management of the Iatriko Athinon Group recognizes that information protection and cybersecurity are an essential part of the Group's mission to provide quality, safe, and reliable healthcare services. Management:

- bears ultimate responsibility for the implementation of this Policy,
- ensures the availability of the necessary resources (technical, human, and financial),
- approves and supervises the implementation of all cybersecurity measures,
- is committed to continuous improvement and timely adaptation of the Policy to new requirements.

10.2 Binding Effect

- This Policy is binding and mandatory for all members of staff, associates, and suppliers of the Group.
- It constitutes a public commitment to patients, associates, and society that information security is always at the heart of the Group's operations.
- This version supersedes all previous versions of the Information Security Policy.

10.3 Disclosure and Transparency

- This Policy is published on the Group's corporate website, ensuring accessibility to all interested parties.
- Revised versions are communicated in a timely manner and uploaded in the same location.
- The Group is committed to clearly communicating any significant changes.

ANNEX I: DOCUMENT HISTORY

Date of Issue / Revision	Issue Number	Details of Changes	Approval	Date of Issue of Changes
21.09.2023	1	ISSUE	BoD	21.09.2023
29.09.2025	2nd	Replacement and changes related to Directive NIS2, Law 5160/2024, Joint Ministerial Decision 1689/2025	BoD	29.09.2025