Information Security

ISO/IEC 27001: protecting data in the healthcare sector

ICMED Magazine ISSN 3103-1943

Editore ICMED S.r.l.

July 2026

Free promotional guide

www.icmed.net

CONTENTS

CHAPTER 1

Why security — in healthcare

Inherently sensitive data

Healthcare organisations manage data that the GDPR classifies as "special categories" (Art. 9): medical records, laboratory results, diagnostic images, genetic data, therapy information. Protecting this information is not only a regulatory obligation: it is a duty towards the patient and a prerequisite for operational continuity.

The threats are real

91% of cyber attacks start with a phishing email. The healthcare sector is the most targeted by ransomware in Europe. A data breach can shut down operating theatres, prevent access to medical records, compromise the cold chain for cellular products. Information security is patient safety.

The regulatory landscape

- GDPR (EU Regulation 2016/679): personal data protection — maximum penalty: 4% of global turnover
- NIS2 Directive: extends cybersecurity obligations to healthcare, with governance and incident management requirements
- Legislative Decree 231/2001: administrative liability of entities — cybercrime is among the predicate offences
- Italian Privacy Code (Legislative Decree 196/2003, amended by Legislative Decree 101/2018): national rules complementing the GDPR

A cyber attack on a healthcare facility is not an IT problem: it is a clinical emergency. Information security is an integral part of patient safety.

CHAPTER 2

ISO/IEC 27001 — the framework

ISO/IEC 27001 is the international standard for Information Security Management Systems (ISMS). It is not an IT standard: it is an organisational standard covering people, processes and technology to protect the confidentiality, integrity and availability of information.

Standard structure

The standard follows the PDCA (Plan-Do-Check-Act) cycle and requires: context analysis, risk assessment, treatment plan definition, control implementation, indicator monitoring, internal audits and management review. The result is a living management system, not a static document.

93 security controls

Annex A of ISO/IEC 27001:2022 defines 93 controls organised into 4 categories: organisational (37), people-related (8), physical (14) and technological (34). Not all are applicable: the organisation must justify exclusions in the Statement of Applicability (SoA).

Cloud extensions

ISO/IEC 27017 adds 7 controls specific to cloud service security. ISO/IEC 27018 adds 25 controls for the protection of personal data (PII) in the cloud. Together with 27001, they form a comprehensive framework for organisations operating in cloud environments.

CHAPTER 3

Information — classification

4 classification levels

Every piece of information managed by the organisation must be classified according to its sensitivity level. Classification determines the applicable protection measures and behaviours required of staff.

- Public: information intended for dissemination (website, brochures, press releases). No access restrictions
- Internal: information for internal use not intended for external parties (circulars, operating procedures, management reports). Access limited to authorised personnel
- Confidential: information whose unauthorised disclosure could cause harm to the organisation or its stakeholders (contractual data, strategic plans, employee personal data). Restricted and tracked access
- Secret: information whose unauthorised disclosure could cause severe and irreparable harm (system credentials, cryptographic keys, special category health data). Strictly controlled access with strong authentication

Practical application

Classification is not a theoretical exercise: every document, email, shared file and database must have an assigned classification level. Staff must know the required behaviours for each level: how to store, share and dispose of information.

CHAPTER 4

From theory — to practice

Incident management

In the event of a security incident, staff must follow precise rules that may seem counterintuitive but are essential for proper event management:

- DO NOT attempt to resolve the problem alone — non-expert intervention can worsen the situation or destroy forensic evidence
- Notify the CISO (Chief Information Security Officer) within 1 hour of detecting the incident
- DO NOT shut down the computer — volatile memory evidence is crucial for forensic analysis
- Document everything: what happened, when, what you were doing, who was involved

GDPR and roles

In the ICMED context: clients (healthcare facilities) are Data Controllers; ICMED is the Data Processor. The IAAPP platform does not contain patient-identifiable data. In the event of a data breach, notification to the Supervisory Authority must occur within 72 hours.

Clean desk and remote working

The clean desk policy requires desks to be free of confidential documents at the end of the working day, screens to be locked when leaving the workstation, and confidential paper documents to be stored in locked cabinets. For remote working: mandatory VPN, protected Wi-Fi connection, separation between personal and corporate devices.

CHAPTER 5

ICMED: numbers and — implementation

ICMED has implemented an ISMS certified to ISO/IEC 27001:2024 with ISO 27017 and ISO 27018 extensions. The figures reflect a rigorous and comprehensive implementation.

Implemented controls

- 125 total controls: 93 ISO 27001 + 7 ISO 27017 (cloud) + 25 ISO 27018 (PII)
- 89 controls fully implemented, 24 partially implemented (with completion roadmap), 12 not applicable (justified in the SoA)
- 27 information security procedures (SOP-SI-001 through SOP-SI-027) covering every aspect of the ISMS

IAAPP: security in numbers

- 186 defined roles with 162 permissions across 9 controllers — principle of least privilege
- Multi-factor authentication (MFA/TOTP) mandatory for all users
- Rate limiting and 30-minute session timeout
- Audit log: 301 logins and 21 PII data accesses tracked in just 7 days of monitoring
- Automated daily backup at 02:00, GPG-encrypted, disaster recovery tested

ICMED does not merely sell security consulting: it practises it. The IAAPP platform is the operational proof of implementation.

CHAPTER 6

The ICMED — offering

ICMED supports healthcare organisations in implementing an ISMS compliant with ISO/IEC 27001, with an approach that integrates information security into the overall quality management system.

- Consulting for ISO/IEC 27001 ISMS implementation, with 27017/27018 cloud extensions where applicable
- Gap analysis and information risk assessment using ISO 27005 methodology
- Development of customised procedural documentation (SOP-SI) tailored to the organisation's reality
- Awareness training for all staff — ECM-accredited courses for healthcare personnel
- IAAPP: ISO 27001 certified platform, sovereign hosting in Italy, no patient-identifiable data
- Integration with existing quality systems (JACIE, ISO 9001, ISO 15189) for an integrated management system
- Support for CSQA certification and annual surveillance audits

LEARN MORE

Want to explore this topic further?

ICMED offers accredited ECM training programmes, specialised consulting and the IAAPP platform for complete quality management system oversight.

ECM Training

AGENAS-accredited courses (Provider ID 7158)

Consulting

Accreditations, quality systems, regulatory compliance

IAAPP

AI-powered quality management platform — ISO/IEC 27001

Magazine

Quarterly scientific publication (ISSN 3103-1943)

info@icmed.net

www.icmed.net

www.iaapp.net

Editore ICMED S.r.l.

ICMED Magazine — ISSN 3103-1943

ISO 9001 — Quality Management System

ISO/IEC 27001:2024 — Information Security

UNI/PdR 125:2022 — Gender Equality

ECM Provider AGENAS — ID 7158

Consulting · Training
Technology · Research

ICMED S.r.l. — Via Fratelli Casiraghi 34, 20099 Sesto San Giovanni (MI)
P.IVA 10054340962 — REA MI-2501287