

Opinion

Digitalization, Digital Maturity and Information Security of Processes: Standard ISO 15189, ISO 17025, and EUROLAB Guide

Marco Pradella

Italian Society of Clinical Pathology and Laboratory Medicine, National Quality Commission and Informatic Society Group, I-31033 Castelfranco Veneto, TV, Italy; labmedico@labmedico.it

Abstract

Testing and medical laboratories have been undergoing a process of progressive, unstoppable digitalization. The digitalization of laboratories carries risks for information security. There are differences between medical laboratories according to International Organization for Standardization (ISO) 15189 and testing laboratories according to ISO 17025. ISO 15189 refers to information security based on ISO 27001, while ISO 17025 is limited to certain clauses. Medical laboratories can use the guidelines with sources from Clinical & Laboratory Standards Institute (CLSI) documents. The European Federation of National Associations of Measurement, Testing, and Analysis Laboratories (EUROLAB) provides a guide to digitalization security that combines ISO 17025 requirements with ISO 27001 controls. The Italian Society of Clinical Pathology and Laboratory Medicine (SIPMeL) Q18R1 Recommendations regarding requirements for medical laboratory information systems confirm that laboratories should obtain at least ISO/IEC 27001 certification.

Keywords: cybersecurity; ISO standards; ISO 17025; ISO 15189; EUROLAB guideline; SIPMeL Recommendations

1. Introduction: Laboratory Digitalization

Digitization converts physical or analog information into a digital form, while digitalization uses digital data and technologies to improve processes and workflows. This distinction does not exist in all languages.

Technological innovation and digitalization are transforming industries and organizations worldwide. However, digital maturity is variable in highly regulated and conservative environments, in which a high integrity of service provision is primary, and digitalization is a secondary focus of organizations [1]. Digital maturity is defined as the stage of progress in a company's digital transformation [1] and encompasses both technical and managerial aspects in order to account for the increasingly rapid and continuous changes in the business environment, which require a proactively implemented digital transformation process and ongoing adjustments. For years now, testing laboratories and medical laboratories have been undergoing a process of progressive, unstoppable digitalization [2].

Digitalization is part of a broader trend in which laboratory practices are shifting toward more integrated models. Safety and security are no longer limited to incident

Academic Editor: Peter Glavič

Received: 16 June 2026

Revised: 21 July 2026

Accepted: 5 August 2026

Published: 7 August 2026

Copyright: © 2026 by the author.

Licensee MDPI, Basel, Switzerland.

This article is an open access article distributed under the terms and conditions of the [Creative Commons Attribution \(CC BY\)](https://creativecommons.org/licenses/by/4.0/) license.

management alone, but also include exposure prevention and health monitoring. Training, too, is moving from laboratory benches to immersive environments [2,3].

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) TR 23842-1 presents considerations for using virtual reality content in the learning, education and training domain for reducing reality and virtual reality cross-over confusion among users and assisting users to effectively use these emerging technologies [4].

The reliability of measurements is no longer limited to traditional numerical analysis, but also extends to uncertainty in qualitative and classification results [5].

The world of laboratories that buy goods and services is now convinced that digitalization is not limited to individual, more or less isolated pieces of informatic equipment, but has permeated the entire operations of laboratories, both medical and testing facilities [6].

Digital technologies are now integrated into most processes in modern laboratory operations, to the extent that digitalization is essential for competitiveness, customer satisfaction, and regulatory compliance. In medical laboratories, the focus goes beyond patient satisfaction; there is a need for concrete guarantees regarding the protection of patients' interests, starting with their data and information [7].

Examples of digitalization include measuring instruments and embedded software (such as in chromatography equipment), comprehensive laboratory information management (Laboratory Information Management Systems, LIMS), electronic lab notebooks, external cloud-based informatic resources, the Internet of Things, robotics, electronic signatures, artificial intelligence, barcodes for sample tracking, and blockchain [8], even individual productivity tools such as word processors, spreadsheets, and databases.

This gives rise to specific risks to the confidentiality, integrity, and availability of information: service provider outages, skills gaps, human error, obsolescence over time, declining interoperability, and full-scale cyberattacks, which are increasing in both frequency and complexity [9].

Digital forensics laboratories, for example, report difficulties in complying with ISO requirements. Often there is insufficient capacity to meet a growing demand for services in an area of increasing complexity and fragmented delivery [10].

The digitalization of laboratory activities offers significant advantages, including reduced human error, faster communication, improved measurement and test performance, safety, efficiency, information security, and data processing capabilities.

The digitalization processes involved in reporting test and examination results should not be overlooked. Standardization has produced many standards dedicated to these processes, including several examples in the field of health data: Health Level Seven (HL7) ISO 10781:2023 [11], Fast Health Interoperability Resources (FHIR) ISO/PAS 24305:2025 [12], ISO 13606-1:2019 (Electronic health record communication, revision 2026) [13], ISO 27269:2025 (International patient summary) [14].

In the specific field of laboratories, the ISO 18812:2003 [15] standard, which specifies general messages for electronic information exchange between analytical instruments and laboratory information systems, is still valid. It is applicable to the specialties of clinical chemistry/biochemistry, hematology, toxicology, microbiology, virology, and immunology. ISO 18812:2003 covers the specification of messages used by communicating parties and the syntax in which they are communicated. It does not cover the transport mechanisms used for the message interchange. ISO 18812:2003 is applicable only to character-based message information. It is not applicable to the communication of graphical or image information.

The ongoing ISO 24884 [16] project even goes so far as to define the digital instructions provided by manufacturers of diagnostic devices.

Clinical & Laboratory Standards Institute's (CLSI) AUTO16 (Next-Generation In Vitro Diagnostic Instrument Interface [17] defines a connectivity standard based on the Laboratory Analytical Workflow Profile of the Integrating the Healthcare Enterprise organization [18], which originated from the work of the In Vitro Diagnostic Industry Connectivity Consortium. CLSI AUTO16 includes implementation and integration guidance, security considerations, examples, and other supplemental information. The intended users of CLSI AUTO16 are IVD system manufacturers, as well as the personnel and information technology management of medical laboratories.

However, digitization entails risks that are often not yet adequately considered or addressed.

The timing of ISO standards for laboratory accreditation has led to differences between medical laboratories accredited under ISO 15189 [19] and testing laboratories accredited under ISO 17025 [20]. ISO 15189 addresses cybersecurity and references ISO/IEC 27001 [21]. ISO/IEC 17025:2017 also addresses cybersecurity risks, although it does not reference ISO/IEC 27001.

This note is not a practical guidance article or a comparative discussion of standards, but rather a call to laboratories and accreditation bodies to consider the current need for information security and to thoroughly examine the connections between ISO standards and guidelines from other sources.

2. ISO 17025 Standard and European Federation of National Associations of Measurement, Testing, and Analysis Laboratories (EUROLAB) Guide to the Digitalization of Testing Laboratories

EUROLAB (European Federation of National Associations of Measurement, Testing, and Analysis Laboratories) is an organization that represents laboratories and promotes best practices. Following a survey conducted by the German Federal Institute for Materials Research and Testing, other internal surveys, and investigations carried out by laboratories, EUROLAB presented its proposal on digitalization, noting that laboratories—particularly smaller ones—often lack necessary resources (skills, time, and staff), as do many ISO standards inspectors [6,22].

This was noted by the European Commission in 2021 and the Organization for Economic Cooperation and Development (OECD) in 2019 [23].

ISO/IEC 17025:2017 sets out in section 7.11 (Data control and information management) a number of requirements in clauses 7.11.1 through 7.11.6, which pertain to availability, validation and verification, maintenance, protection, and failure of informatics. EUROLAB considers these points to be directed at computer equipment, while digitalized processes are lacking. Therefore, EUROLAB aims to identify the clauses of the ISO/IEC 17025:2017 standard that are also indirectly applicable to data systems, and to formulate recommendations based on the ISO/IEC 27002 standard and other related standards and guidelines.

The EUROLAB guide is divided into seven chapters (Table 1).

Table 1. Chapters of the European Federation of National Associations of Measurement, Testing, and Analysis Laboratories (EUROLAB) guide [22] on the management of digitalized systems in laboratories accredited to ISO/IEC 17025.

-
- 1: Introduction and scope.
 - 2: Normative references.
 - 3: Definitions of terms from other standards and guidelines, plus specific EUROLAB definitions.
 - 4: Risk assessment of digital processes.
-

-
- 5: Risks that may compromise test results or information security, the factors influencing them, and controls to mitigate them.
- 6: Implementation of controls, based on ISO/IEC 27002:2022.
- 7: Links between ISO/IEC 17025:2017, ISO/IEC 27001:2022, and EUROLAB guidelines.
-

Certain sections of the EUROLAB document deserve special attention.

The glossary in chapter 3 contains as many as 200 entries, some of which are quite original: for example, “Backward Compatibility,” “Centralized Data Storage,” “Cryptographic Deletion,” “Code Injection Attack,” “Cryptojacking” (Cryptocurrency Hijacking), “Data Deletion,” “Digitization,” “Exhaustive attack” (synonymous with “brute-force attack”), “Functional testing” (synonymous with “black-box testing”), “Hybrid license” (both proprietary and open-source licensing), “Man-in-the-middle attack” (to insert and modify messages between two parties without their knowledge), and “White-box testing” (which takes into account the internal mechanism of a system).

In section 4, EUROLAB links some clauses of ISO 17025 to cyber risks, as in 8.5 and 8.5.2 (risk assessment), and 8.7.1 (e) (review of risks following a nonconformity). It references standards not cited in ISO 17025, such as ISO 31000 (risk management) [24], IEC 31010 (risk assessment) [25], ISO/IEC 27000 (cybersecurity) [26], ISO/IEC TS 27100 (cybersecurity) [27], and ISO/IEC 27001 (information security) [28]. It adds guidance from a Swiss Working Group (Arbeitsgruppe Informationstechnologie, AGIT), the United States Pharmacopeia (USP) on laboratory instruments, the International Society for Pharmaceutical Engineering (ISPE) Good Automated Manufacturing Practice (GAMP) 5 for computerized systems, and the European Union Agency for Cybersecurity (ENISA) for cloud computing.

Section 5 identifies significant risks and recommends controls to mitigate them. Specifically, these include unsuitable systems or modules, improper use and management, cyberattacks and internal attacks, physical failures due to natural wear and tear, service interruptions, disasters, obsolescence or loss of expertise, unexpected behavior due to development errors or inadequate design, and the provision of incorrect data or data to unauthorized third parties.

Section 6 of EUROLAB describes the controls for mitigating cyber risks and complying with ISO/IEC 17025. Specifically, ISO 17025 5.5(c) (documented procedures), 6.4.3 (handling, transport, storage, use, and scheduled maintenance of equipment), 6.4.13 (description, location, calibration, maintenance, and acceptance testing of equipment), 7.5.1 (records and metadata to enable the repeatability of the activity under conditions as similar as possible to the original ones), and 8.4.1 (legible records).

With regard to user requirements, procurement, and design qualification, EUROLAB identifies the following clauses of ISO/IEC 17025: 6.6.1 (externally provided products and services); 6.6.2 (acceptance criteria for the provision and verification of externally provided products and services); 6.6.3 (communicating its requirements and acceptance criteria to external suppliers); 6.4.2 (equipment requirements, including for off-site information systems controlled by external suppliers and used by the laboratory in the cloud); and 7.11.4 (information systems hosted, maintained, or managed by external suppliers).

EUROLAB recognizes several clauses of ISO 17025 that apply to the acceptance testing of information technology systems: 6.4.4 and 6.4.9 (requirements for equipment prior to commissioning or following failures and maintenance); 6.4.10 (interim checks); 6.4.13 (c) (records for equipment verification); 6.4.5 (equipment meeting performance requirements); 6.6.1 and 6.6.2 (external products and services); 7.2.1.5 (verification of methods); 7.11.2 (information management systems validated prior to use); 7.11.6 (calculation and transfer of verified data); and 7.7.1 (c) (functional testing of equipment).

EUROLAB has added several acceptance controls from ISO/IEC 27001:2022, such as 8.29 (information protection); 8.31 (separate development, test, and production environments); and 8.33 (selected and protected test information). Other controls from ISO/IEC 27001:2022 include 8.25 and 8.26 (security requirements during software development or acquisition); and 8.28 and 8.30 (requirements for outsourced development of systems and software).

For maintenance activities, EUROLAB identifies the following clauses in ISO 17025: 6.4.3 (scheduled maintenance), 6.4.13 (g) and (h) (records of damage, breakdowns, and maintenance), and 7.11.3 (d) (maintenance to ensure data integrity). It adds the controls from ISO/IEC 27001:2022 7.13 (equipment with adequate maintenance).

The environmental conditions that affect the information system are specified in clauses 6.3.1 through 6.3.4 (environmental conditions) and 7.11.3(c) (information management system in an environment that complies with the supplier's or laboratory's specifications) of ISO/IEC 17025:2017. EUROLAB adds controls 7.5 (physical protection) and 7.8 (secure placement of equipment) from ISO/IEC 27001:2022.

Change control is clearly addressed in ISO/IEC 17025:2017 through clauses 6.4.13 (records of equipment changes), 7.11.2 (authorized, documented, and validated changes to information management systems), 8.3.2 (c) (changes to and revision of documents), and 7.5.2 (changes to technical records). ISO/IEC 27001:2022 includes controls 8.19 (software installation) and 8.32 (changes to the information processing system).

Access control is addressed in several clauses of ISO/IEC 17025:2017: 4.2.1 (confidential information and data), 7.11.3 (a) and (b) (information protected against unauthorized access, tampering, and loss), and 8.4.2 (access to records consistent with confidentiality). In addition to these, there are numerous controls in ISO/IEC 27001:2022: 7.4 (preventing unauthorized physical access to premises), 8.1 (information accessible via protected devices), 8.2 (restricted access rights), 8.3 (access control), 8.4 (managed access to source code), 8.5 (authentication technologies), 8.7 (protections against malicious software), 8.11 (data masking), 8.16 (access with anomalous behavior), 8.18 (utility programs capable of overriding system and application controls), 8.22 (separate systems, software, and users on different networks), and 8.23 (access to external websites).

The EUROLAB document contains additional chapters, which are only mentioned here: technical documentation, general inventory and records, redundancy of facilities, legible records, indexing, archiving and disposal, backup, digital signatures and documents, staff competence, incident reporting, and internal audits.

3. ISO 15189 Standard and Medical Laboratory Informatics

ISO 15189:2022 includes a section (7.6.3, Management of information systems) that lists specific requirements for information technology in the medical laboratory [19].

Systems used for the collection, processing, recording, reporting, archiving, or retrieval of data and test information are validated by the supplier and verified by the laboratory prior to their implementation. Any changes to the system, including the configuration of laboratory software or modifications to commercial software, must be authorized, documented, and validated prior to use. Validation and verification include the proper functioning of interfaces between the laboratory information system and other systems, such as laboratory equipment, hospital patient management systems, and primary care systems. This last requirement is not always given due consideration.

Following its participation in the revision process for ISO 15189, the Italian Society of Clinical Pathology and Laboratory Medicine (SIPMeL) produced a series of recommendation documents that provide guidance on how to implement the standard's requirements within the national context, including those related to cybersecurity (Table 2) [28,29]. The

Q18R1 Recommendations were developed through collaboration between the Quality and Accreditation Commission and the Information Technology Study Group.

Table 2. Excerpt from the Italian Society of Clinical Pathology and Laboratory Medicine (SIPMeL) Q18R1 Recommendations regarding requirements for medical laboratory information systems [28,29].

-
1. Information security for the entire process from request to results, including intermediary systems (middleware).
 2. Information security certification of the laboratory in accordance with ISO 27001.
 3. Continuity of the laboratory's information system, including during maintenance or modifications.
 4. Information security of the laboratory in accordance with CLSI AUTO11 guidelines.
 5. Continuity of the information system in accordance with CLSI AUTO11.
 6. Off-site information management, including cloud-based solutions, in accordance with ISO 15189 requirements.
-

Clause 6.4 (Equipment) of ISO 15189 covers laboratory information systems. Section 7.6 (Control of data and information management) of ISO 15189 requires access to the necessary data and information, regardless of the physical location of the systems—for example, in the organization's data center or even in the cloud.

ISO 15189 references two other ISO documents, thereby incorporating their requirements: ISO 22367:2020 (updated 2026) Annex A.13 regarding risks associated with information systems [30], and ISO/IEC 27001:2022 Annex A (Information security controls) regarding security controls [21].

The requirements of ISO 22367 apply to all aspects of laboratory testing, including the transfer of test results to the electronic health record. ISO 22367 Annex A, section A.13, provides a step-by-step review of laboratory information systems, including the integrity of intermediary systems (middleware) and the risks of intrusion into systems connected to the Internet.

4. Information Security Standards: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27799

ISO 15189 builds upon and incorporates the requirements of ISO/IEC 27001, the founding standard and cornerstone of the ISO/IEC 27000 family of standards [26], which provides a high-level overview of information security management systems (ISMSs) and is applicable to all types of organizations, regardless of size.

ISO/IEC 27002:2022 [31] defines recommended best practices and guidelines for implementing information security controls. ISO/IEC 27002:2022 is not itself certifiable but serves as a guide and support for information security management systems (ISMSs) and as a foundation for other standards in the ISO 27000 family.

ISO/IEC 27799:2025 [32] provides guidelines for implementing information security in the healthcare sector based on the controls defined by ISO/IEC 27002 for data and information in any form (paper, electronic, voice recordings, medical images). ISO/IEC 27799 has also incorporated ISO/TS 14441:2013 [33].

5. Information Systems Management in ISO 15189: A Practical Guide

Clause 7.6.2 of ISO 15189 stipulates that the laboratory bears ultimate responsibility for the maintenance and modification of information systems, which must be validated by the supplier and verified by the laboratory prior to their implementation; furthermore, any modification must be authorized, documented, and validated before implementation.

Validation and verification include interfaces with other systems, namely laboratory instruments as well as hospital patient management systems and community primary care systems.

According to ISO guidelines, ISO 15189 sets forth principles without specifying detailed requirements [34], but laboratories need practical guidance. To this purpose, Q18R1 includes a reference to the recently revised Clinical & Laboratory Standards Institute (CLSI) AUTO11 [35]. CLSI AUTO11 clearly distinguishes the responsibilities of manufacturers of diagnostic systems (MDMs), users (e.g., laboratory personnel), and the health information management departments of healthcare organizations (HDOs).

Cybersecurity is addressed in ISO 15189, clause 7.6.3, subclauses (b) through (e), which cover documentation, cybersecurity, the environment, data integrity, and system failures.

The management of information systems is strained in emergency situations. ISO 15189 addresses this in section 7.6.4 (Outage plans) and section 7.6.5 (Off-site management). ISO sets forth the principle but does not provide instructions on how to apply it. However, such instructions can be found in the CLSI AUTO11 guide.

It is not easy for laboratories to comply with the ISO requirement regarding system continuity. The alternatives would be fault-tolerant systems, redundancy (multiple systems operating in parallel), or a contingency plan that provides for the use of paper-based materials in extreme cases.

Finally, if we consider medical laboratories as nodes in telemedicine networks, we must broaden our perspective to include recent resources not yet included in the SIPMeL Recommendations: the CLSI AUTO17 guide on semantic interoperability and the three documents in the ISO 6268 series on cybersecurity—one covering an overview and concepts, the second covering the reference model, and the third covering the requirements.

6. Conclusions: Information Technology in Laboratories, from Niche to Backbone

The digital maturity assessment is widely acknowledged as a foundational step in any digital transformation process [36].

The computer-based processing of data is no longer merely an ancillary aspect of measurement or testing activities, but rather a critical component of the entire organizational framework for the purposes of ISO accreditation. All activities that affect the performance of tests or examinations required for a specific area of accreditation are susceptible to accidental changes in data and information, as well as to the use of procedures that lack sufficient detail for digital processes and to personnel with insufficient knowledge. The scientific literature for individual projects does not adequately describe the measures and competencies required for information security.

ISO standards, EUROLAB guidance, CLSI documents, and SIPMeL Recommendations have different normative statuses. Accreditation and certification activities rely on the standard references established by the regulations (EA, ILAC, or IAF) to define requirements. However, these requirements often need application guidelines to provide direction to both laboratories and inspectors. This is precisely the purpose of the EUROLAB and SIPMeL Recommendations. SIPMeL, in particular, considers various CLSI sources to be useful.

In this note, the practical message for laboratories is precisely to gain a deeper understanding of the accreditation requirements by studying the referenced guidelines (SIPMeL, CLSI, and EUROLAB), rather than merely reading the requirements and interpreting them solely based on their own background knowledge, experience, or common sense.

The digitalization of testing and medical laboratories is irreversible. Given the high value of the sensitive data they hold, it is essential to ensure the validation and resilience

of digital data management, information technology systems, and expertise. The SIPMeL Recommendations for medical laboratories are aligned with the EUROLAB guidelines for testing laboratories: laboratories should obtain at least ISO/IEC 27001 certification to ensure compliance with information security requirements.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data are available from references in the bibliography.

Acknowledgments: I would like to thank the members of the SIPMeL Informatics Study Group and the SIPMeL National Quality and Accreditation Commission for their diligent oversight of the development of the SIPMeL Q18R1 Recommendations, approved by the National Council on 27 February 2024.

Conflicts of Interest: The author declares no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
CLSI	Clinical & Laboratory Standards Institute
EUROLAB	European association representing laboratories and other conformity assessment bodies
HL7	Health Level Seven International
FHIR	Fast Health Interoperability Resources
AGIT	Arbeitsgruppe Informationstechnologie
USP	United States Pharmacopeia
ISPE	International Society for Pharmaceutical Engineering
GAMP	Good Automated Manufacturing Practice
ENISA	European Union Agency for Cybersecurity
LIMS	Laboratory Information Management Systems
SIPMeL	Italian Society of Clinical Pathology and Laboratory Medicine
MDMs	Manufacturers of diagnostic systems
HDOs	Healthcare organizations

References

1. Ladu, L.; Koch, C.; Asna Ashari, P.; Blind, K.; Castka, P. Technology adoption and digital maturity in the conformity assessment industry: Empirical evidence from an international study. *Technol. Soc.* **2024**, *77*, 102564. <https://doi.org/10.1016/j.tech-soc.2024.102564>.
2. Hodaifa, G. From Safety and Quality Assurance to Digital Transformation: Emerging Directions in Laboratory Science and Practice. *Laboratories* **2026**, *3*, 7. <https://doi.org/10.3390/laboratories3020007>.
3. Cuautle-Gutierrez, L.; Cordero-Guridi, J.d.J. Development of an Immersive Virtual Reality (IVR) Laboratory for the Execution of Multidisciplinary Experiences in Students of a Private Mexican University. *Laboratories* **2026**, *3*, 3. <https://doi.org/10.3390/laboratories3010003>.
4. ISO/IEC TR 23842-1:2020; Information Technology for Learning, Education and Training—Human Factor Guidelines for Virtual Reality Content. Part 1: Considerations When Using VR Content. International Organization for Standardization: Geneva, Switzerland, 2020.
5. Pradella, M. Measurement Uncertainty: New Definition, Viewpoints, and Laboratories. *Laboratories* **2026**, *3*, 4.
6. Salingros, E. Presentation of the new EUROLAB guidance document on the management of digitalised processes in laboratories accredited to ISO/IEC 17025:2017. *Accred. Qual. Assur.* **2026**, *31*, 191–197. <https://doi.org/10.1007/s00769-026-01704-x>.

7. Pradella, M. Le Raccomandazioni SIPMeL per l'accreditamento ISO 15189 di organizzazione e direzione. *Riv. Ital. Med. Lab.* **2025**, *21*, 82–94. <https://doi.org/10.23736/S1825-859X.25.00275-0>.
8. Bartling, S. Blockchain for Science and Knowledge Creation. In *Gesundheit Digital*; Haring, R., Ed.; Springer: Berlin/Heidelberg, Germany, 2019; pp 159–180. https://doi.org/10.1007/978-3-662-57611-3_10.
9. European Union Agency for Cybersecurity. ENISA Threat Landscape 2024. Available online: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (accessed on 15 June 2026).
10. Tully, G.; Cohen, N.; Compton, D.; Davies, G.; Isbell, R.; Watson, T. Quality standards for digital forensics: Learning from experience in England & Wales. *Forensic Sci. Int. Digit. Investig.* **2020**, *32*, 200905. <https://doi.org/10.1016/j.fsidi.2020.200905>.
11. ISO 10781:2023; Health Informatics—HL7 Electronic Health Record-System Functional Model, Release 2.1 (EHR FM). International Organization for Standardization: Geneva, Switzerland, 2023.
12. ISO/PAS 24305:2025; Health Informatics—Guidelines for Implementation of HL7 FHIR Based on ISO 13940:2015, ISO 13606-1:2019 and ISO 13606-3:2019. International Organization for Standardization: Geneva, Switzerland, 2025.
13. ISO/DIS 13606-1:2026; Health Informatics—Electronic Health Record Communication. Part 1: Reference Model. International Organization for Standardization: Geneva, Switzerland, 2026.
14. ISO 27269:2025; Health Informatics—International Patient Summary. International Organization for Standardization: Geneva, Switzerland, 2025.
15. ISO 18812:2003; Health Informatics—Clinical Analyser Interfaces to Laboratory Information Systems—Use Profiles. International Organization for Standardization: Geneva, Switzerland, 2003.
16. ISO/FDIS 24884; Electronic Instructions for Use for In Vitro Diagnostic Medical Devices—Minimum Required Information and Means of Delivery. International Organization for Standardization: Geneva, Switzerland, 2026.
17. AUTO16 Ed2 2023; Next-Generation In Vitro Diagnostic Instrument Interface. CLSI—Clinical and Laboratory Standards Institute: Malvern, PA, USA, 2023.
18. IHE. IHE Pathology and Laboratory Medicine (PaLM) Technical Framework. Volume 1 (PaLM TF-1) Profiles. Available online: https://www.ihe.net/uploadedFiles/Documents/PaLM/IHE_PaLM_TF_Vol1.pdf (accessed on 15 June 2026).
19. ISO 15189:2022; Medical Laboratories—Requirements for Quality and Competence. International Organization for Standardization: Geneva, Switzerland, 2022.
20. ISO/IEC 17025:2017; General Requirements for the Competence of Testing and Calibration Laboratories. International Organization for Standardization: Geneva, Switzerland, 2017.
21. ISO/IEC 27001:2022; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. International Organization for Standardization: Geneva, Switzerland, 2022.
22. EUROLAB. *Guidelines for the Management of Digitalised Systems in Laboratories Accredited to ISO/IEC 17025*; EUROLAB: Brussels, Belgium, 2024.
23. Organisation for Economic Co-Operation and Development (OECD). *OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring—Number 22—Advisory Document of the Working Party on Good Laboratory Practice on GLP Data Integrity*; Organisation for Economic Co-Operation and Development (OECD): Paris, France, 2021.
24. ISO 31000:2018; Risk Management—Guidelines. International Organization for Standardization: Geneva, Switzerland, 2018.
25. IEC 31010:2019; Risk Management—Risk Assessment Techniques. International Electrotechnical Commission: Geneva, Switzerland, 2019.
26. ISO/IEC 27000:2026; Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Overview. International Organization for Standardization: Geneva, Switzerland, 2026.
27. ISO/IEC TS 27100:2020; Information Technology—Cybersecurity—Overview and Concepts. International Organization for Standardization: Geneva, Switzerland, 2020.
28. SIPMeL. Q18R1 Informazioni_Raccomandazioni per Accredimento ISO1 15189 del Laboratorio Medico: Processi Della Gestione Dati e Informazioni. 2024. Available online: <https://www.sipmel.it/it/lineeguida/approvate/121260> (accessed on 15 June 2026).
29. Pradella, M. Le Raccomandazioni SIPMeL per l'accreditamento ISO della gestione dati e informazioni. *Riv. Ital. Med. Lab.* **2024**, *20*, 225–227. <https://doi.org/10.23736/S1825-859X.24.00235-4>.
30. ISO 22367:2026; Medical Laboratories—Application of Risk Management to Medical Laboratories. International Organization for Standardization: Geneva, Switzerland, 2026.
31. ISO/IEC 27002:2022; Information Security, Cybersecurity and Privacy Protection—Information Security Controls. International Organization for Standardization: Geneva, Switzerland, 2022.

32. ISO 27799:2025; Health Informatics—Information Security Controls in Health Based on ISO/IEC 27002. International Organization for Standardization: Geneva, Switzerland, 2025.
33. ISO/TS 14441:2013; Health Informatics—Security and Privacy Requirements of EHR Systems for Use in Conformity Assessment. International Organization for Standardization: Geneva, Switzerland, 2013. (Withdrawn)
34. Pradella, M. New ISO standards for medical biology laboratories, prescriptions and deviations. *Ann. Biol. Clin.* **2022**, *80*, 451–453. <https://doi.org/10.1684/abc.2022.1755>.
35. CLSI. *AUTO11. Information Technology Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard*, 3rd ed.; Clinical and Laboratory Standards Institute: Malvern, PA, USA, 2024.
36. Aydel, O.A. Assessing the Digital Maturity of an Enterprise as the First Step to Digital Transformation. *Bus. Strateg.* **2021**, *9*, 369–370. <https://doi.org/10.17747/2311-7184-2021-12-369-370>.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.