sciendo Revista Română de Medicină de Laborator 2023;31(3):157-162 **EDITORIAL**
DOI:10.2478/rrlm-2023-0020

Cybersecurity requirement of ISO 15189 - a simplified protocol for laboratories

Radu Ilinca[1*], Dan Adrian Luțescu[1], Ionuț Adrian Chiriac[1], Smaranda Hristodorescu-Grigore[2], Iulia - Ioana Stănescu - Spînu[3], Ionela Ganea[4], Iuliana Gherlan[5], Rucsandra - Elena Dănciulescu - Miulescu[5]

1. Medical Informatics and Biostatistics, "Carol Davila" University of Medicine and Pharmacy, Faculty of Dentistry, Romania
2. Epidemiology, "Gr. T. Popa" University of Medicine and Pharmacy, Romania
3. Biochemistry, Faculty of Dentistry, "Carol Davila" University of Medicine and Pharmacy, Romania
4. Modern Languages, "Carol Davila" University of Medicine and Pharmacy, Faculty of Medicine, Romania
5. Endocrinology, "Carol Davila" University of Medicine and Pharmacy, Faculty of Dentistry, Romania

Keywords: cybersecurity, ISO 15189:2022, medical laboratory, accreditation, laboratory information system

Received: 21 June 2023; Accepted: 30 June 2023; Published: 5 July 2023

Development and implementation of advanced IT infrastructures in the healthcare environment generate opportunities but also challenges in the field of data security. Worldwide, in the past 3 years, 24% of the total number of identified cybersecurity attacks targeted healthcare organizations [1].

Not only hospitals are at risk for cyber-attacks. Modern medical laboratories tend to implement more and more complex laboratory information systems (LIMS) in order to increase their work efficiency and decrease operational costs. This trend can also be noticed in the requirements of the relevant accreditation standard[2] [3]. While the first version of ISO 15189 [4]contained only an informative, therefore not mandatory Annex of requirements, the 2nd version of the same standard [5] contained detailed requirements for the information systems deployed in a medical laboratory. Those requirements were Information Technology – detailed enough to pose implementation challenges for laboratory professionals who overwhelmingly do not have an advanced IT education. The current version of ISO 15189 [3] has expanded the information systems accreditation requirements with: "*implemented taking cybersecurity into account, to protect the system from unauthorized access and safeguard data against tampering or loss;*" [3]. Coupled with another requirement: "*When the laboratory information system(s) are managed and maintained offsite or through an external provider, the laboratory shall ensure that the provider or operator of the system complies with all applicable requirements of this document*." [3] No matter the choice of LIMS or service provider, the laboratory has the responsibility of the LIMS adequacy to the requirements. The current approach of the standard is to expand the requirements beyond the "*computerized systems*" to "*information systems*" which essentially can mean any record, either electronic or printed, either locally stored or cloud-stored offsite. This plethora of situations, together with the fact that nowadays there is virtually no laboratory that does not use an INTERNET connection (at least for reporting the proficiency testing rounds results) [6] poses relevant data security risks for the laboratory, in short cybersecurity.

Given the fact that cybersecurity can be implemented in multiple ways depending on the field of activity, the complexity of the systems, data sensitivity, etc. Currently, there is no cybersecurity standard developed for medical laboratories. Therefore the baseline reference is the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 - Cybersecurity Act [7] which establishes a cybersecurity certification framework for products and services. This document clarifies that cybersecurity certification is on a voluntary basis (voluntary field) and not a regulated field which means that, in the absence of specific legislation – which is the case of medical laboratories in many countries, it remains at the discretion of the laboratory. Implementing a certified cybersecurity system is by default the choice of preference, yet for small to medium-sized laboratories (up to 20 computerized systems – incl. analyzers, and communication equipment), such an implementation might not

* Correspondence to: Radu Ilinca, Medical Informatics and Biostatistics, "Carol Davila" University of Medicine and Pharmacy, Faculty of Dentistry, Bucharest, Romania. E-mail: radu.ilinca@umfcd.ro

be straightforward from the time (it is a process of up to a year) or financial point of view. Another limitation of this approach is that few companies on the market offer cybersecurity certification services and most of the time these services are not available for medical laboratories but for large corporations, Governmental agencies, etc. Also, for large laboratories, part of hospitals or corporate medical organizations which include a laboratory, usually there is a specialized IT Department which can develop and implement a protocol to ensure compliance with local cybersecurity-related concerns.

The current version of the accreditation standard ISO 15189:2022 [3] promotes a risk-based approach when implementing all the technical requirements starting from pre-analytical to post-analytical. This offers the opportunity for a medical laboratory to customize its own cybersecurity strategy to limit its exposure while being aware there is no ultimate full security-proof system. For developing a cybersecurity strategy, it is important to understand the rationale for the attacks. We summarize the main purposes of the cyber attacks and the level where they might occur in the table 1:

As can be seen in table 1, typical information systems architecture in a medical laboratory consists of the following components: i) a LIMS which is a software solution, usually leased, from an IT company which has mainly implemented a 2-way communication with analyzers, process the patient data, generate the medical report and make it available online for patient download; and ii) instruments' software solutions that are implemented at the medical analyzer level and a part of the "system". In the latter case, the laboratory does not need to be concerned about cybersecurity because those information systems are part of the device which bears the CE marking [8]. This marking also confirms an appropriate level of cybersecurity. Therefore, it can be concluded that at this level the security threat is *minimum*. Regarding the LIMS, it is worthwhile pointing out that the same solutions are deployed in different ways in different laboratories according to the working scenarios of each. It is therefore impossible to generalize if one deployment is deemed safe enough. This means that each laboratory has to validate and verify its own deployment (which is also a requirement from ISO 15189:2022). Since essen-

Table 1. Outlook on cybersecurity in a laboratory

General Perspective on Cybersecurity Challenges			
Purpose	**Attack type**	**Objective**	**Probability**
Financial	ransomware	To receive financial funds from the data owner in order to hand back the control of the computer systems / data previously hacked.	Very- high
	theft	This attack assumes stealing data (medical, financial, personal) and commercialization on the illegal markets.	Very- high
Indirect financial	website hacking	To promote various activist group agenda, express dissatisfaction with respect to the medical activity.	Medium
	Data corruption (deletion, alteration)	These attacks are usually carried out by former employees or "vengeful employees".	Medium
Non-financial purposes	Disruption of service	These attacks are carried out just for personal enjoyment of the attacker.	Low
Risks at the level of LIMS components			
Component		**Security assessment**	**Probability**
Proprietary Software deployed in analyzers		Proprietary software running and controlling the analyzers are part of the system, bearing the CE marking, therefore the validation of the device includes the software validation as well.	Very- low
Third-party software deployed		It is very unlikely to encounter such a situation in real world scenario because laboratory users do not have access to the system settings to deploy additional software. Software patches are added automatically from the manufacturer of the service representative.	Very- low
LIMS software solution		Most of the attacks are carried out at this level, especially since virtually all LIMS have an online-component. The risk increases if the LIMS was developed in-house.	High
Communication equipment (routers, hubs, switches, bridges)		An attack at this level is unlikely because it assumes physical access to the equipment. Therefore, the equipment should be placed in an access-controlled environment, outside the reach of laboratory visitors.	Low
Transmission media	Wireless	An attack of this level can happen by means of mobile devices (including smartphones). As the coverage of a wireless network is quite high (tens of meters) the attacker does not have to be next to the equipments.	High
	Wired	An attack at this level is unlikely because it assumes physical access to the cables.	Very- low

tially all the laboratory employees and even outside people (e.g. patients) interact with the LIMS, it can be concluded that at this level the security threat is *very-high;* iii) communication media/types of equipment which act as an interface between the LIMS and the medical analyzers. In most of these cases, the transmission media is by cable, which means that the security threat is *minimum*. If however, the communication between the LIMS and medical analyzers is by wireless communication, then the security risk increases to *medium.* In order to minimize the risk at this particular level, the WiFI communication should be password protected, which has to be strong enough (at least 8 characters some of them being capital letters, numbers and other alphanumeric characters). The name of the WiFI network name is not relevant here because having a human non-intelligible name does not bring any security advantage, yet it might confuse potential maintenance intervention. Therefore, leaving the WiFi network name as it is by default does not add any security risk.

First and foremost, in order to minimize the data security-related risks, the laboratory should carefully ensure when contracting with the LIMS provider there are provisions which ensure that the laboratory has unlimited 24/7 access to its data, with no constraints (e.g. financial). Since in most cases, the data is stored remotely, usually in data centres belonging to the LIMS provider, integrity, availability and access policy to the data should also fall under the responsibility of the provider with adequate provisions in the contract.

An automatic audit trail (system logs) should be available for every interaction. A minimum set of information should be stored within the audit trail: user/device that performed the action, type of action (e.g. data input, data print, etc) and timestamp of the action. This audit trail should be readily available for the laboratory for every medical analysis request in a format that is easily understandable for non-IT experts. To prevent tampering with the medical report, a unique code should automatically be generated and included for each report. Security can be increased by using a coding system that cannot be read or replicated by human readers but by means of electronic devices. Such a simple yet effective system is based on 1-dimensional barcodes or QR codes. A 1-dimensional barcode can be deemed sufficient for average laboratories because it can encode up to 85 alphanumerical characters. Information in the code should contain at least a method to identify the analysis request and other information which helps uniquely identify the laboratory.

It is generally accepted that most of the successful cyber attacks exploit poor usage (most of the time unintentional) of the systems by employees. Therefore, raising awareness and documenting procedures in the quality management system (QMS) is one of the most effective ways to protect laboratory systems.

Raising awareness as a separate topic should always be addressed whenever internal training in the laboratory is delivered or at least once a year, whichever comes first. Key points to be addressed should be as follows: i) password length and complexity (at least 8 characters including small and big caps and numbers; ii) passwords should be programmed to expire every 6 months such that employees are required to change them regularly; iii) even though it might seem unfeasible, in case an employee works on multiple systems, the personal password should be as different as deemed reliable for each system; iv) common habit of password sharing should be discouraged; v) given the fact that a laboratory has a multitude of suppliers with whom the relation is at best loose if not totally remote, e-messages containing spot offers (e.g. an excellent financial deal available for a very limited time slot) should be treated suspiciously. These offers often have grammar or spelling errors, unconnected webpages links and usually are written such that they require immediate action. If that is the case, even though the design and layout of the message are identical to usual offers, employees should report these cases, ignore the offer and inform the truly legitimate sender that a phishing attack might have been launched on their behalf. In any scenario, links and buttons should not be accessed because it can be enough to compromise the system security even though no immediate effect is visible for the user; vi) if the software antivirus or software firewall is signalling alerts, those should not be ignored or disabled. They should be reported immediately to the LIMS supplier to take appropriate action; vii) even if a webpage looks almost identical to a trusted one, there are a few points that can indicate a hoax which can lead to a security breach: pop-up windows or alarming messages or alerts, website addresses that contain one or two inverted letters or spelling mistakes, misspelt names of trusted websites, broken (non-functional) webpages links, requests for personal data, credentials that are irrelevant for visiting the website, etc. The employees should be instructed not to follow up on those websites.

In standard operating procedures, the laboratory can achieve a decent level of cybersecurity by implementing procedures to: i) temporarily disable the user accounts for employees that are absent for long periods of time (e.g. vacation); ii) permanently disable the accounts for employees that are no longer working in the laboratory. The checkout procedure should also include a statement by which the former employee confirms he/she has not transferred any laboratory-related data outside the LIMS; iii) remote work for laboratory professions is be-

coming increasingly popular. If that is the case, the laboratory should ensure that the remote user is connecting to the LIMS via a method involving a Virtual Private Network (VPN). Implementing such a system is beyond the responsibilities of a laboratory, yet it should ask for such a feature from the LIMS supplier; iv) implement an antivirus and firewall (some of them also have a VPN solution which is secure enough for remote working) software solution with automatic updates always on. Also, the operating system should have automatic updates on. This ensures that the laboratory always benefits from the latest security patches as soon as released by the manufacturers, thus reducing the time the LIMS is vulnerable; v) the antivirus solution should always have a scheduled full scan program to check for viruses or malware programs, preferably outside the working hours in order not to interfere with the laboratory routine activity. Most antivirus solutions have an easy-to-use interface to configure such a scanning schedule; vi) as it is customary nowadays, more and more laboratories offer a free "Guest" WiFi network for patients and visitors. If that is the case, no system of which the LIMS is comprised should be connected to that network.

Even if the above-mentioned items are rigorously and consistently implemented, there is always a chance of a successful cyber attack. Therefore, coupled with requirement *7.6.4 – Downtime Plans* of the ISO 15189:2022 [3], the downtime plans should include measures taken in case of a cyberattack. An effective strategy should contain at least: a) automatic and frequent enough (depending on the data volumes) backup of data considered to be critical in a secure location, preferably outside the laboratory. Backup solutions could include: backup servers, external drivers, and cloud-based solutions; b) a list of systems and data considered to be critical that require recovery; b) detailed steps are taken to retrieve data from the last backup point; c) what happens with the routine activities during the resolution period; d) how the process is updated to prevent similar incidents in the future. This last point is also supported by the Continual Improvement requirement (8.6.1) of ISO 15189:2022 [3].

This paper explored the challenges induced by the cybersecurity requirement of the new ISO 15189 [3]. This requirement is essential also for concepts of quality assurance, like patient safety[9]. While it might seem distant from the daily laboratory routine activities, this requirement becomes increasingly important given the exponential number of cyber attacks motivated by various factors, the most important one being financial. The cybersecurity apparatus should be dimensioned by employing a risk assessment which is one of the main focuses of the new ISO 15189 [3]. The most convenient way for such an analysis is using a matrix[10]. The paper concluded that for standard, medium-sized laboratories, the main risks come from the LIMS. While achieving a cybersecurity certification is a gold standard, a sufficient level of data protection can be achieved by implementing a simple yet efficient protocol which does not assume advanced IT security expertise. Meeting the requirement is based on two main pillars: raising awareness and procedure development. Thus, a simple and straightforward protocol was developed and detailed. Yet, for larger or multisite laboratories, other accounts have to be considered and the cybersecurity strategy has to be tailored accordingly. However, those cases are usually handled by specialised IT Departments of those companies.

AUTHORS' CONTRIBUTION

Authors declare equal contribution in all regards.

CONFLICT OF INTEREST

None to declare.

PUBLISHER'S NOTE

Editorial Office stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

1. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). Front Digit Health. 2022 Aug 11;4:862221. DOI: 10.3389/fdgth.2022.862221
2. Ilinca R, Chiriac IA, Luțescu DA, Ganea I, Hristodorescu-Grigore S, Dănciulescu-Miulescu RE. Understanding the key differences between ISO 15189:2022 and ISO 15189:2012 for an improved medical laboratory quality of service . Rev Romana Med Lab. 2023;31(2):77-81. DOI: 10.2478/rrlm-2023-0011
3. Iso/iec 15189:2022 [Internet]. ISO. 2020 [cited 2023 16.06.2023]. Available https://www.iso.org/standard/76677.html
4. Iso/iec 15189:2007[Internet]. ISO. 2020 [cited 2023 16.06.2023]. Available https://www.iso.org/obp/ui/#iso:std:iso:15189:ed2:v1:en
5. Iso/iec 15189:2012 [Internet]. ISO. 2020 [cited 2023 16.06.2023]. Available https://www.iso.org/standard/56115.html
6. Taina A. Software validation with respect to requirements specified by SR EN 15189:2013 and SR EN 17025:2005. A practical approach for a medical laboratory information management system (LIMS) and a gas meter in testing laboratory. 2015 9th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania. 2015:720-4. DOI:

10.1109/ATEE.2015.7133899

7. Eur-Lex[Internet].[cited 2023 13.03.2023]. Available https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&qid=1687353646824
8. European Commission [Internet].[cited 2023 13.03.2023]. Available https://single-market-economy.ec.europa.eu/single-market/ce-marking_en
9. Kazamer A, Ilinca R, Nitu A, Iuonuț AM, Bubenek-Turconi SI, Sendlhofer G, et al. A Brief Assessment of Patient Safety Culture in Anesthesia and Intensive Care Departments. Healthcare (Basel). 2023 Feb 2;11(3):429. DOI: 10.3390/healthcare11030429
10. David RE. Approaching Risk Management in Medical Laboratories. Rev Romana Med Lab. 2022;30(2):125-39. DOI: 10.2478/rrlm-2022-0017