Opinion Paper

Giuseppe Lippi*, Salome Akhvlediani, Janne Cadamuro, Elisa Danese, Luis García de Guadiana Romualdo, Herve Delacour, Emmanuel J. Favaloro, Julien Favresse, Brandon M. Henry, Snezana Jovicic, Marge Kütt, Laetitia Moreno y Banuls, Tomris Ozben, Avi Peretz, Antonija Perovic, Jecko Thachil, Dogan Yucel and Mario Plebani

EFLM Task Force Preparation of Labs for Emergencies (TF-PLE) recommendations for reinforcing cyber-security and managing cyber-attacks in medical laboratories

https://doi.org/10.1515/cclm-2024-0803
Received July 10, 2024; accepted July 10, 2024;
published online July 17, 2024

Abstract: The healthcare systems are a prime target for cyber-attacks due to the sensitive nature of the information combined with the essential need for continuity of care. Medical laboratories are particularly vulnerable to cyber-attacks for a number of reasons, including the high level of information technology (IT), computerization and digitization. Based on reliable and widespread evidence that medical laboratories may be inadequately prepared for cyber-terrorism, a panel of experts of the Task Force Preparation of Labs for Emergencies (TF-PLE) of the European Federation of Clinical Chemistry and Laboratory Medicine (EFLM) has recognized the need to provide some general guidance that could help medical laboratories to be less vulnerable and better prepared for the dramatic circumstance of a disruptive cyber-attack, issuing a number of consensus recommendations, which are summarized and described in this opinion paper.

Keywords: laboratory medicine; cyber-security; cyber-attack; malware; recommendations

Cyber-attacks and the healthcare

Cyber-attacks can be conventionally defined as deliberate and malicious attempts to penetrate the information systems of individuals or organizations to gain unauthorized access, disrupt operations, and steal, manipulate, or destroy information by full-time, well-trained, well-equipped, and

***Corresponding author: Prof. Giuseppe Lippi**, MD, Section of Clinical Biochemistry, University Hospital of Verona, Piazzale LA Scuro, 37134 Verona, Italy, E-mail: giuseppe.lippi@univr.it. https://orcid.org/0000-0001-9523-9054
Salome Akhvlediani, Department of Clinical Laboratory and Microbiology, Acad. O. Gudushauri National Medical Center, Tbilisi, Georgia
Janne Cadamuro, Department of Laboratory Medicine, University Hospital Salzburg, Paracelsus Medical University, Salzburg, Austria. https://orcid.org/0000-0002-6200-9831
Elisa Danese, Section of Clinical Biochemistry, University of Verona, Verona, Italy. https://orcid.org/0000-0002-2454-0410
Luis García de Guadiana Romualdo, Laboratory Medicine Department, University Hospital Santa Lucía, Cartagena, Spain. https://orcid.org/0000-0003-3028-3198
Herve Delacour, Department of Laboratory Medicine, Begin Military Teaching Hospital, Saint-Mandé, France
Emmanuel J. Favaloro, Haematology, NSW Health Pathology, Sydney Centres for Thrombosis and Haemostasis, ICPMR, Westmead Hospital, Sydney, Australia. https://orcid.org/0000-0002-2103-1661
Julien Favresse, Services of Clinical Biology, Clinic Saint-Luc, Bouge, Belgium
Brandon M. Henry, Clinical Laboratory, Division of Nephrology and Hypertension, Cincinnati Children's Hospital Medical Center, Cincinnati, OH, USA
Snezana Jovicic, Department for Medical Biochemistry, Faculty of Pharmacy, University of Belgrade, Belgrade, Serbia
Marge Kütt, Laboratory of Diagnostics Division, North Estonia Medical Centre Foundation, Talinn, Estonia
Laetitia Moreno y Banuls, Department of Laboratory Medicine, CHU UCL Namur, Yvoir, Belgium
Tomris Ozben, Department of Medical Biochemistry, Faculty of Medicine, Akdeniz University, Antalya, Türkiye
Avi Peretz, The Clinical Microbiology Laboratory, Tzafon Medical Center, Affiliated With Azrieli Faculty of Medicine, Bar Ilan University, Safed, Israel
Antonija Perovic, Medical Biochemistry Laboratory, Health Care Institution Glavić, Dubrovnik, Croatia. https://orcid.org/0000-0002-2633-3669
Jecko Thachil, Immune Thrombocytopenic Purpura (ITP) Clinic, Haematology Department, Manchester University NHS Foundation Trust – Manchester Royal Infirmary, Manchester, UK
Dogan Yucel, Department of Medical Biochemistry, Lokman Hekim University, Ankara, Türkiye
Mario Plebani, Department of Medicine, University of Padova, Padova, Italy. https://orcid.org/0000-0002-0270-1711

even well-funded cyber-terrorists [1]. Healthcare systems are a prime target for cyber-attacks due to the sensitivity of information (personal and medical data) and the need for continuity of care, whose interruption or delay may jeopardize patient health [2].

The number of cyber-attacks on healthcare facilities has seen an almost exponential increase over the past 15 years. According to HIPAA (Health Insurance Portability and Accountability Act), the number of healthcare data breaches involving more than 500 records in the US has increased from 18 in 2009 to 512 in 2019, 663 in 2020, 715 in 2021, 720 in 2022 and 741 in 2023, to already 333 cases in 2024 (as of June 21) [3]. Accordingly, the Office for Civil Rights (OCR) of the US Department of Health and Human Services (HHS) reported a 2.8-fold and 2.4-fold increase in ransomware attacks and hacking-related data breaches between the beginning of 2018 and the end of 2023, respectively [3].

There are many different types of cyber-attacks that can affect the healthcare industry, but the most common malware inoculation is based on ransomware, distributed denial of service (DDoS), Trojans, spyware, rootkits, botnets, and medical device hijacking, among others [4, 5]. In brief, ransomware infects systems and files and makes them virtually inaccessible to users (e.g., by locking or encrypting data) unless a ransom is paid, but also slows down various critical processes or renders them completely unusable. DDoS attacks aim to flood the attacked host or network with a huge amount of traffic until the system is completely inoperable, thus blocking access to the network for receiving or sending emails, accessing patient records and other information, issuing prescriptions, delivering therapies, and organizing the function of the entire facility (i.e., operating rooms, bed availability, etc.); this malware is also occasionally used to spread other cyber threats (e.g., ransomware). Trojans, which are often spread via malicious emails or the downloading of programs, apps, or software patches, once they have infiltrated the system, permit the cyber-terrorists to perform any actions that legitimate users would make, such as using files, changing information, or even modifying the contents of the device. Spyware is used to steal login credentials, patient information, and other sensitive data. Rootkits transmit malicious payloads into the healthcare facility, resulting in prolonged exposure and manipulation of vulnerabilities. Botnets infect the system and then affect the functioning of various types of devices such as cameras and routers, but can also be used to make the system more vulnerable to DDoS attacks. Medical device hijacking is another type of cyber-attack that primarily aims to disrupt the function of a vast array of medical devices, and is also an efficient gateway for subsequent cyber-attacks.

Among the various cyber threats, ransomware represent perhaps the most effective and escalating malware used to attack the healthcare sector [6], due to the critical nature of healthcare facilities (a disruption can have immediate and severe consequences for patient care), the valuable data they contain (e.g., personal information, clinical and laboratory data), the high vulnerability due to myriad of gateways (personal access and medical devices are easy entry points for cyber-terrorists), the often outdated systems and infrastructure, and the lack of efficient cyber-security resources [7]. According to a recent report published in the HIPAA journal, more than half of US healthcare organizations spend less than 10 % of their information technology (IT) budget on cyber-security, with 53 % and 46 % of organizations admitting to lack local expertise and IT staff, respectively. Even more concerning is the fact that nearly two-thirds of healthcare IT professionals reported that their organization is vulnerable to business email compromise/spoofing phishing. This is not surprising, as a recent study showed that in a simulated phishing campaign, 14.2 % of spoofed emails were actually clicked on by healthcare workers [8]. These findings are also reflected in the results of a recent survey of emergency managers representing nearly 60 healthcare facilities in the US [9], showing that American hospitals appear to be inadequately prepared for cyber-terrorism.

Cyber-attacks and the laboratory

Medical laboratories can be especially vulnerable to cyber-attacks for several reasons [5, 10]. First, they have a high degree of IT, computerization and digital technologies [11, 12]. For example, the normal functioning of most laboratory processes and activities depends on the availability of computerized physician order-entry (COPD), bidirectional connection of instruments to the laboratory information system (LIS) to streamline specimen processing and data management, autoverification rules, generation of digital files containing test results, etc. The shutdown of hospital servers and networks will almost completely disrupt the flow of information between the hospital information system (HIS) and the LIS or even within the LIS itself (including instrument connectivity), resulting in interruption of normal operations.

A recent survey conducted by the Task Force Preparation of Labs for Emergencies (TF-PLE) of the European Federation of Clinical Chemistry and Laboratory Medicine (EFLM) highlighted several critical problems and potential failures in European laboratories [13], such as insufficient familiarity with the strategies used by cyber-criminals to penetrate the systems, lack of adequate information on cyber-security from hospital administrations or IT services, suboptimal use of multi-factor identification for remote

connections, sporadic transfer of HIS or LIS servers to the cloud (where they would be less vulnerable to cyber-attacks), and the widespread lack of incident response plans, both for the laboratory and for the entire healthcare facility.

Given that cyber-attacks can have a significant impact on the normal operation of laboratory services, and at the express request of the majority (over 80 %) of respondents to the recent EFLM TF-PLE survey [13], the TF-PLE has recognized the need to provide some general guidance that can help medical laboratories be less vulnerable and better prepared for the dramatic circumstance of a disruptive cyber-attack.

Strategies for providing indications

The indications were developed with a "consensus approach". In brief, a questionnaire covering the most important aspects of cyber-security and disaster recovery was administered by Google Forms (Google, Mountain View, CA, USA) to all official and corresponding members of the EFLM TF-PLE, with a specific deadline for receipt of responses (i.e., 10 days). All members were asked to indicate the strength of the recommendation with a numerical value, as shown in Table 1, or to indicate the preferred choice among various options (if applicable). The numerical data of all responses were pooled and the mean and standard deviation (SD) of all replies were calculated. The final rating of the recommendations was classified as follows (Table 1): mean value between 4.50 and 5.00, "strongly recommended"; mean value between 3.50 and 4.49, "recommended"; mean value between 2.50 and 3.49, "neutral"; mean value between 1.50 and 2.49, "discouraged"; mean value between 1.00 and 1.49, "strongly discouraged".

Table 1: Strength of recommendations used for surveying the members of the Task Force Preparation of Labs for Emergencies (TF-PLE) of the European Federation of Clinical Chemistry and Laboratory Medicine (EFLM), and final score calculated as the mean of the different responses.

Individual responses	Numerical value
Strongly recommended	5
Recommended	4
Neutral	3
Discouraged	2
Strongly discouraged	1
Mean of the pooled response	**Recommendations**
4.50–5.00	Strongly recommended
3.50–4.49	Recommended
2.50–3.49	Neutral
1.50–2.49	Discouraged
1.00–1.49	Strongly discouraged

Operative recommendations

Responses to the survey were received from 10/10 (100 %) full members and 8/11 (73 %) corresponding members of the EFLM TF-PLE (total: 18/21; 86 %). The summary of the recommendations issued by the panel for preventing and ultimately mitigating the harm caused by cyber-attacks in clinical laboratories is summarized in Table 2. The mean score (±SD) is presented along with the corresponding strength of the recommendation, to provide a more comprehensive representation of the individual propensities for each of the items. Each recommendation that could be categorized as "strongly recommended" or "recommended" was officially endorsed by the panel.

General recommendations on cyber-security

The panel believes that the hospital and laboratory should have valid and regularly updated antivirus software programs and firewalls in place to prevent outside intrusion, but also that consideration should be given to migrating HIS and/or LIS servers to clouds (where access is less vulnerable), that backup of LIS data should be scheduled regularly (preferably every 24 h), and that the use of "shared folders" within the network should be minimized. Clear written guidance on the methods used by cyber-terrorists should be provided to all laboratory staff and regular meetings (e.g. on an annual basis) should be organized for describing the methods used by cyber-terrorists, along with an unforeseen training (e.g. phishing, solicitation to download fake applications) to simulate a cyber-attack. A generic ID should no longer be used and each laboratory employee must use personal (unique) credentials to access the LIS/HIS.

General recommendations on emails

The panel believes that laboratory personnel should change institutional passwords regularly, at least every 3 months, that complex institutional passwords (e.g., with a combination of letters, capital letters, numbers, and symbols) no shorter than 12 characters are advisable, that institutional login information should not be shared with third parties, that remote identification for connecting to institutional services (e.g., via VPN; virtual private network) must be based on multi-factor access (i.e., with at least two factors), suspicious emails or SMS messages (including from your institution, bank or email provider) asking you to enter credentials or click on suspicious links must never be opened, and it is advisable that the actual identity of the

Table 2: Strength of recommendations issued by the Task Force Preparation of Labs for Emergencies (TF-PLE) of the European Federation of Clinical Chemistry and Laboratory Medicine (EFLM) for preventing and mitigating the possible harm caused by a cyber-attack.

Recommendations	Pooled value	Strength of recommendations
Pretend that your hospital and laboratory have installed valid and regularly updated antivirus software programs and firewalls to prevent outside intrusion	4.7±0.7	Strongly recommended
Consider to migrate the HIS and/or LIS servers in clouds, where access is less vulnerable	4.4±0.8	Recommended
Arrange back-up of LIS data periodically	Every 24 h	Recommended
Minimize the use of "shared folders" within the network, since these are the most vulnerable	4.1±0.7	Recommended
Provide clear written indications about the modalities used by cyber-terrorists to all the staff of the laboratory	4.7±0.5	Strongly recommended
Organize regular meetings (e.g., on annual basis) with your laboratory staff about the modalities used by cyber-terrorists	4.2±0.8	Recommended
Organize periodical and unanticipated training (e.g., phishing, request for downloading faked applications) to simulate a cyber-attack	4.4±0.5	Recommended
Dismiss generic IDs, but pretend that each laboratory professional uses personal (unique) credentials for accessing the LIS/HIS	4.8±0.5	Strongly recommended
Periodically change your institutional password, at least every:	3 months	Recommended
Use complex institutional passwords (e.g. using a combination of letters, capital letters, numbers, and symbols), no shorter than 12 characters	4.5±0.7	Strongly recommended
Do not share your institutional login information with anybody	4.9±0.3	Strongly recommended
Remote identification for connecting to institutional services (e.g., by VPN) must be based on multiple-factor access (i.e., using not less than 2 factors)	4.7±0.4	Strongly recommended
Do not open suspect emails or SMS messages (even from your institution, bank or email provider) asking to provide your credentials (especially those institutional) or clicking on suspect links	5.0±0.0	Strongly recommended
Always check the real identity of the email sender, verifying the internal email address extension and not just the name	4.6±0.5	Strongly recommended
Do not access to suspicious websites, especially those not using the prefix "https://", which encompasses encryption for secure communication over a computer network	4.9±0.3	Strongly recommended
Do not use personal IT devices (e.g. smartphones, laptops, tablets, etc.) to perform work tasks and to use them in connection with company IT tools	4.1±0.8	Recommended
Do not download unauthorized software on institutional PCs	4.8±0.5	Strongly recommended
Do not access whatever type of non-medical website during your stay at work	3.6±1.1	Recommended
Remember to always log out when you are finished working on an institutional computer and especially after remote connection	4.8±0.4	Strongly recommended
Define a detailed "incident response plan" for working under a cyber-attack, (when all IT supports may be down), to be shared with medical direction and all hospital wards	4.8±0.4	Strongly recommended
Define a specific "incident response team", including laboratory professionals, for coordinating activities throughout the period of HIS/LIS/network unavailability	4.8±0.5	Strongly recommended
Prioritize critical systems to resume operations (i.e., instrumentation providing urgent/stat tests)	4.9±0.2	Strongly recommended
Prepare a resident folder (e.g., entitled "Emergency Folder") in all hospital PCs, containing detailed instructions and all forms to be used in case the intranet is unavailable	4.6±0.5	Strongly recommended
Prepare an "Emergency Request Form" (in word or PDF), stored on an "Emergency Folder" in local PC in all hospital wards, which can hence be accessed and printed even if the network is down	4.6±0.5	Strongly recommended
The "Emergency Request Form" must contain the following information		
– [First and last name of the patient]	4.8±0.5	Strongly recommended
– [Date of birth of the patient]	4.9±0.2	Strongly recommended
– [Sex of the patient]	4.7±0.5	Strongly recommended
– [Medical number of the patient]	4.3±1.0	Recommended
– [An area to attach a label with medical number of the patient and eventual barcode]	4.8±0.4	Strongly recommended
– [Priority of the request (emergency/urgent/routine)]	4.6±0.6	Strongly recommended
– [Requesting ward]	4.5±0.7	Strongly recommended

Table 2: (continued)

Recommendations	Pooled value	Strength of recommendations
– [Fax of the ward]	3.2±1.5	Neutral
– [Telephone of the ward]	4.1±0.9	Recommended
– [Name of the requesting physician]	4.4±0.9	Recommended
– [List of all emergency/stat tests]	4.7±0.6	Strongly recommended
– [List of all routine laboratory tests]	3.4±1.2	Neutral
– [Color code for the tube for each test]	3.9±1.0	Recommended
– [Free lines for comments]	3.9±0.7	Recommended
The label on blood tubes collected in the wards should report		
– [First and last name of the patient]	4.7±0.6	Strongly recommended
– [Date of birth of the patient]	4.5±1.0	Strongly recommended
– [Sex of the patient]	4.3±1.0	Recommended
– [Medical number of the patient]	4.3±1.0	Recommended
– [Barcode reporting all patient information (if available)]	4.3±1.0	Recommended
Samples and "Emergency Request Form" must be shipped together, preferably using a single plastic bag	4.5±0.7	Strongly recommended
Prepare a "Samples Receipt Form" to record all samples received in the laboratory, stored on an "Emergency Folder" in PCs located in the lab, which can hence be accessed and printed even if the network is down	4.6±0.6	Strongly recommended
The "Samples Receipt Form" must include		
– [Patient full name]	4.9±0.5	Strongly recommended
– [Patient ID]	4.8±0.5	Strongly recommended
– [Provenience (i.e., ward)]	4.7±0.5	Strongly recommended
– [Time of arrival]	4.6±0.5	Strongly recommended
– [Number of samples]	4.3±1.1	Recommended
– [Types of samples]	4.6±0.6	Strongly recommended
Double-check manual instrument programming (i.e., one operator enters the data, a second operator checks that data are correct)	4.2±0.8	Recommended
Prepare an "Emergency Lab Report", stored on an "Emergency Folder" in PCs located in the lab, which can hence be accessed and printed even if the network is down	4.7±0.4	Strongly recommended
The "Emergency Lab Report" must contain the following information		
– [First and last name of the patient]	4.9±0.5	Strongly recommended
– [Date of birth of the patient]	4.9±0.2	Strongly recommended
– [Sex of the patient]	4.3±1.0	Recommended
– [Medical number of the patient]	4.5±1.1	Strongly recommended
– [Requesting ward]	4.6±0.6	Strongly recommended
– [Fax of the ward]	3.1±1.5	Neutral
– [Telephone of the ward]	3.6±1.2	Recommended
– [Name of the tests (without abbreviation)]	4.3±1.3	Recommended
– [Name of the test (abbreviation)]	4.1±0.9	Recommended
– [Empty field for entering test results]	4.8±0.4	Strongly recommended
– [Measure units for each test]	4.8±0.5	Strongly recommended
– [General reference range for each test]	4.8±0.4	Strongly recommended
– [Age- and sex-specific reference ranges for each test]	4.6±0.6	Strongly recommended
Double-check test results input (i.e., one operator enters the data, a second operator checks that data are correct)	4.2±0.9	Recommended
Using the following means for delivering test results		
– [Always the telephone]	2.8±1.3	Neutral
– [The telephone only for emergency/critical values]	4.8±0.5	Strongly recommended
– [Always the fax machine]	2.7±1.4	Neutral
– [Always the fax machine except for emergency/critical values (in such case use the telephone)]	3.3±1.4	Neutral
– [Transport all lab reports to the wards by hands]	3.3±1.0	Neutral
Do not dismiss fax machines, since they may become the only means for receiving orders and sending test results when the hospital network is down	3.8±1.2	Recommended
When the network is restored, all data obtained during the cyber-attack must be manually entered in the LIS	4.2±1.0	Recommended
All the emergency forms containing patient data used during the cyber-attack must be maintained for at least:	1–3 years	Recommended

HIS, hospital information system; LIS, laboratory information system; PC, personal computer.

email sender should be verified (e.g., checking the internal email address extension and not just the name).

General recommendations on website navigation

The panel is of the opinion that suspicious websites (especially those that do not use the prefix "https://") should not be accessed with institutional computers, that personal IT devices (e.g., smartphones, laptops, tablets, etc.) must not be used to perform work tasks or used in connection with hospital IT tools, that unauthorized software should not be downloaded to the institutional computers, that access to

any kind of non-medical websites should be avoided while at work, and that logging off after finishing work on an institutional computer (especially after remote connection) must always be done.

General recommendations for early response to a cyber-attack

The panel believes that a detailed "incident response plan" for working in the event of a cyber-attack (when all IT support fails) should be prepared and shared with the medical direction and all hospital departments, together with the establishment of an "incident response team" including laboratory experts. Critical operations (i.e., devices performing urgent/stat tests) must be prioritized when reactivating systems. The panel also believes that a resident folder (e.g., entitled "Emergency Folder" and containing detailed instructions and all forms to be used in case the intranet is unavailable) must be stored in all hospital computers. An "Emergency Request Form" (in Word or PDF) must be prepared and stored in the "Emergency Folder" on the local PC of all hospital departments (so that it can be retrieved and printed even if the network is down), containing the following information: first and last name of the patient, date of birth of the patient, sex of the patient, patient's medical number, a field for attaching a label with the patient's medical number and any barcode, priority of the request (emergency/urgent/routine), requesting ward, telephone of the ward, name of the requesting physician, list of all emergency/stat tests, color code for the tube for each test and blank lines for comments.

General recommendations for sample collection and registration

The panel is of the opinion that the label of blood samples collected in the wards during the unavailability of IT systems should include at least the patient's first and last name, date of birth, sex, medical number, and barcode (if available). The samples and the "Emergency Request Form" must be sent together, preferably in a single plastic bag. A "Samples Receipt Form" should be prepared in advance to record all specimens received in the laboratory, which should be stored in the "Emergency Folder" on the computers in the laboratory (so that it can be accessed and printed even if the network is down), and must include the patient's full name, patient ID, origin (i.e., ward), time of arrival, number and type of specimens.

General recommendations for instrument programming and test results reporting

The panel believes that manual programming of instruments with dual control (i.e., one operator enters the data, a second operator checks the accuracy) is advisable and that an "Emergency Lab Report", stored in the "Emergency Folder" on the computers in the laboratory (which can thus be accessed and printed even if the network fails), must be prepared in advance and should include the patient's first and last name, date of birth, sex, medical number, requesting ward, the telephone of the ward (and eventually the fax number), name of the test (with its standard abbreviation), the blank field for entering test results, units of measurement for each test, general reference range (but preferably also age- and sex-specific reference ranges) for each test. An example of "Emergency Lab Report" developed using Microsoft Excel (and therefore can be edited and saved multiple times with patient's name, times and dates) is shown in Figure 1. This format would also allow the development of several queries in Excel to update the reference ranges according to the date of birth and sex of the patient (when available). The entry of test results should be double-checked (i.e. one staff member enters the data, and a second operator checks the accuracy). The advantage of this form is that it can also be used in the event of other system failures that are not directly related to cyber-attacks.

General recommendations for delivering test results

The panel considers that the preferred means of transmitting test results during a cyber-attack (and not in routine circumstances) is the telephone for emergency/critical values, while there is much uncertainty about the use of different options (e.g., telephones, fax machines, paper sheet conveyed by hands) for delivering other test results. Nonetheless, the panel agrees on the general advice that fax machines should not be dismissed, as they may become the only means of receiving orders and transmitting reports with test results if the hospital network fails. The panel also suggests that once the network is restored, all data generated during the cyber-attack must be manually entered into the LIS and that all emergency forms containing patient data used during the cyber-attack must be retained for at least 1–3 years.

Conclusions

Cyber-crime continues to evolve and cyber-terrorism against healthcare organizations is increasing dramatically due to the growing IT dependency of modern healthcare, of

					Date	/ /		
First name			Last name		Date of birth	/ /	Sex	
Medical n.			Ward		Fax		Tel	
Test		Value	Meaure unit	Range*				
Clinical Chemistry								
Amylase			U/L	28-100				
Lipase			U/L	13-60				
Alananine Aminostransferase (ALT)			U/L	8-40				
Aspartate Aminostransferase (ALT)			U/L	7-50				
Creatine Kinase (CK)			U/L	30-170				
Lactate Dehydrogenase (LDH)			U/L	100-230				
Calcium			mmol/L	1.9-2.7				
Albumin			g/L	35-52				
Bilirubin (total)			µmol/L	17-20				
Body urea nitrogen (BUN)			mmol/L	0.5-40				
Creatinine			µmol/L	50-115				
Glucose			mmol/L	3.9-5.6				
Sodium			mmol/L	135-145				
Potassium			mmol/L	3.5-5.5				
Chloride			mmol/L	90-105				
Cardiac troponin I			mg/L	<14				
NT-proBNP			pg/mL	<125				
Procalcitonin			ng/mL	<0.5				
B-HCG			U/L	<5				
Hematology								
While Blood Cells (WBC)			$\times 10^9$/L	4-10				
Red Blood Cells (RBC)			$\times 10^{12}$/L	3.5-6.0				
Hemoglobin (Hb)			g/L	120-170				
Hematocrit (Hct)			%	40-50				
Platelets (PLT)			$\times 10^9$/L	150-400				
Coagulation								
Prothrombin time (PT)			INR	0.9-1.1				
Activated partial thromboplastin time (APTT)			Ratio	0.8-1.2				
Fibrinogen			g/L	2.0-4.0 g/L				
D-dimer			mg/L	<0.50				
Other								
* Reference values are indicative; test results must be interpreted according to age and sex								

Figure 1: Example of "Emergency Lab Report" developed using Microsoft Excel.

which laboratory medicine is a paradigmatic example. We sincerely hope that the list of recommendations issued by an expert panel of the EFLM TF-PLE could be useful for all medical laboratories to prevent and ultimately mitigate the possible harm caused by the increasing wave of cyber-attacks in the healthcare sector [14].

Research ethics: Not applicable.
Informed consent: Not applicable.
Author contributions: The authors have accepted responsibility for the entire content of this manuscript and approved its submission.
Competing interests: The authors state no conflict of interest.
Research funding: None declared.
Data availability: Data will be available upon reasonable request to the corresponding author.

References

1. Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: a systematic review of modern threats and trends. Technol Health Care 2017;25:1–10.

2. Cartwright AJ. The elephant in the room: cybersecurity in healthcare. J Clin Monit Comput 2023;37:1123–32.
3. HIPAA Journal. Healthcare data breach statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/ [Accessed 2 Jul 2024].
4. Center of Internet Security. Cyber attacks: in the healthcare sector. https://www.cisecurity.org/insights/blog/cyber-attacks-in-the-healthcare-sector [Accessed 2 Jul 2024].
5. Patel AU, Williams CL, Hart SN, Garcia CA, Durant TJS, Cornish TC, et al. Cybersecurity and information assurance for the clinical laboratory. J Appl Lab Med 2023;8:145–61.
6. van Boven LS, Kusters RWJ, Tin D, van Osch FHM, De Cauwer H, Ketelings L, et al. Hacking acute care: a qualitative study on the health care impacts of ransomware attacks against hospitals. Ann Emerg Med 2024;83:46–56.
7. Murray-Watson R. State of healthcare cybersecurity. HIPAA J. https://www.hipaajournal.com/healthcare-cybersecurity/ [Accessed 2 Jul 2024].
8. Gordon WJ, Wright A, Aiyagari R, Corbo L, Glynn RJ, Kadakia J, et al. Assessment of employee susceptibility to phishing attacks at US health care institutions. JAMA Netw Open 2019;2:e190393.
9. Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A national survey of hospital cyber attack emergency operation preparedness. Disaster Med Public Health Prep 2023;17:e363.
10. Lippi G, Ferrari A. Lessons learnt in medical laboratories during a disruptive cyber-attack. J Lab Precis Med 2024;9:1.
11. Lippi G, Mattiuzzi C, Favaloro EJ. Artificial intelligence in the pre-analytical phase: state-of-the art and future perspectives. J Med Biochem 2024;43:1–10.
12. Çubukçu HC, Topcu Dİ, Yenice S. Machine learning-based clinical decision support using laboratory data. Clin Chem Lab Med 2023;62:793–823.
13. Lippi G, Cadamuro J, Danese E, Favaloro EJ, Favresse J, Henry BM, et al. EFLM task force preparation of labs for emergencies (TF-PLE) survey on cybersecurity. Clin Chem Lab Med 2024. https://doi.org/10.1515/cclm-2024-0727.
14. Devi S. Cyber-attacks on health-care systems. Lancet Oncol 2023;24:e148.