Point-of-Care Testing Edited by: P.B. Luppa

Wibke Johannis, Andreas Bietenbeck, Gebhart Malchau and Thomas Streichert*

Point-of-care testing (POCT) and IT security concepts

https://doi.org/10.1515/labmed-2019-0199
Received December 5, 2019; accepted January 15, 2020

Abstract: Point-of-care testing (POCT) has been an essential service in hospitals for many years with a main focus on reliability, classical laboratory quality criteria and easy handling. Hospital information technology (IT) security regulations, however, have not yet been adapted to the specificities of POCT. Following the POCT Symposium in Munich, the "1st Round Table POCT-IT-Security Meeting" held in October 2019 in Cologne addressed these issues and managed to establish first consensus results in the essential fields of user, data and update management, as well as network connections and user-friendliness. First practical steps include optimizing the user management by connection to a directory service and definition of access control (including emergency authorization). Patient data economy on analyzers in combination with data and data transmission encryption as well as technically secure communication protocols are relevant steps in the fields of data management and network connections. An update management needs to be contractually defined for remote services and generally includes testing in a protocol-based scenario. Providing an organizational structure for POCT-IT security is a necessary prerequisite, as are continuous training and awareness for this topic with a strong focus on usability.

Keywords: B3S; BSIG; DIN EN ISO 15189; IT; KRITIS; POCT; POCT Symposium Munich; 1st Round Table POCT-IT-Security Meeting; Protection of (Information) Infrastructures; security.

Introduction

Point-of-care testing (POCT) devices are developing rapidly. During the last few years, new analytical applications were realized and the devices are used either as a complement of the medical laboratory or as a sole diagnostic approach [1], especially in hospitals without an inhouse central laboratory.

In the past, central medical laboratories considered quality criteria and reliability as the basis for purchasing decisions of POCT devices.

As a result, the demands for POCT-information technology (IT) solutions focused on simple operation of the analyzers, documentation of patient results as well as results of quality controls (QCs).

Due to the lack of a general definition, we will use "POCT-IT" as an umbrella term for all aspects of POCT-IT solutions: the analyzer firmware, the operation system (OS, often embedded OSs), the applications, which usually bring a user interface and middleware solutions for data transmission to, for example, laboratory information systems (LISs), clinical information systems and clinical archives.

POCT-IT solutions have been present in hospitals for decades. A novelty is the high integration in the hospital IT network with POCT devices usually being connected to a clinical or hospital information system (HIS) to obtain patient data, e.g. a patient identifier, case number(s), sex, date of birth or further information such as the patient name and the treatment unit. Access to this information ensures the correct application of age- and sex-specific reference intervals [2] on the one hand and linking of the results to the corresponding patient on the other hand, enabling data transfer to an LIS.

The legal and normative requirements of Richtlinie der Bundesärztekammer (RiLiBÄK; Guidelines of the German Federal Medical Council) [3] and Deutsches Institut für Normung Europäische Norm International Organization for Standardization (DIN EN ISO) 15189 and 22870 [4, 5] demand that POCT-IT solutions ensure the prompt availability and integrity of data, while at the same time hamper any unauthorized access [3]. The DIN EN ISO 15189

***Correspondence: Thomas Streichert,** Institute for Clinical Chemistry, Faculty of Medicine, University of Cologne, Cologne, Germany, E-Mail: thomas.streichert@uk-koeln.de
Wibke Johannis and Gebhart Malchau: Institute for Clinical Chemistry, Faculty of Medicine, University of Cologne, Cologne, Germany
Andreas Bietenbeck: Institute of Clinical Chemistry and Pathobiochemistry, Faculty of Medicine, Technical University of Munich, Munich, Germany. https://orcid.org/0000-0002-1228-0770

requires laboratories to establish an information management system with a comprehensive user administration to control authorization and responsibilities of the entire staff using the system [5]. Furthermore, the system(s) used for the collection, processing, recording, reporting, storage or retrieval of examination data and information shall be primarily validated by the supplier and then verified by the laboratory with regard to proper functioning. These system(s) should be protected from unauthorized access and safeguarded against tampering or loss and have to be in compliance with national or international requirements regarding data protection [5].

With the increasing integration of POCT devices into the IT networks of hospitals, the number of necessary online connections has also increased. Numerous middleware solutions have been established in order to transfer measurement and control sample results to presentation systems and archiving systems in the HIS.

Extensive remote maintenance from the clinic as well as from external suppliers (e.g. the device manufacturer) is now standard. This process must be controlled and documented; this also includes the proper day-to-day functioning of the system and the documentation of system failures with the consecutive corrective actions [5].

This deep-seated integration, combined with increased demands for security requirements, has given rise to new aspects of POCT-IT. The sector-specific healthcare standard for hospital health care (B3S) [6] of the German Hospital Association (Deutsche Krankenhaus Gesellschaft [DKG]) summarizes the essential legal requirements arising from §107 [1] Sozialgesetzbuch (SGB) 5 [7] (definition of medical care) and §8a Act on the Federal Office for Information Security (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik [BSIG]) BSIG [8] (requirements for the state of the art) and in particular from DIN EN ISO 27001, 27002 and 27799 standards.

Hospitals are considered as part of a critical infrastructure. They fall under the IT security act if more than 30,000 inpatient cases are treated. The “National Strategy for Critical Infrastructure Protection – Implementation Plan Kritische Infrastrukturen (KRITIS)” divides the health sector into three areas: medical care, pharmaceuticals and vaccines laboratories.

POCT devices could fall into the category “medical care”. If, however, external laboratory service providers offer POCT services, they may instead be categorized as “laboratories”.

According to the B3S, POCT analyzers are often designed as closed system medical devices not meeting the current state-of-the-art standards of information security from an IT point of view. Often, the regulatory requirements for medical devices are inconsistent with the practice of IT (e.g. software or operating system updates or the use of anti-virus programs).

In 2018, the Federal Office for Information Security and the Federal Office for Civil Protection and Disaster Assistance issued current recommendations for the manufacturers of products that are used by critical infrastructure managers. Thus, the POCT device manufacturers are strongly encouraged to regard IT and functional security as an added value and a necessary and relevant part of product quality. For operators of POCT devices, apart from basic quality requirements, the implementation of safety requirements will in future be a selection criterion for a specific POCT manufacturer or device type [9].

This article summarizes the results of “The 1st Round Table POCT-IT-Security Meeting” held in October 2019 in Cologne organized by us with the aim of addressing relevant legal and regulatory POCT-IT topics together with users, suppliers and IT security managers.

Requirements for POCT-IT

Focus safety/security

Increasing digitization in healthcare systems has undoubtedly improved patient care but is also associated with IT risks. The vulnerability of hospitals for cyberattacks, viruses or ransomware in the recent years has led to a shutdown of medical services or to a compromise of health data. Defense mechanisms involving foreclosed information are not suitable for modern healthcare [10], where integration of data and services is mandatory.

The German “National Strategy for Critical Infrastructure Protection” has identified “Health” as one of nine fields with critical infrastructure [11]. “Health care” is one of three subbranches within this field (the others being “Pharmaceuticals and vaccines” and “Laboratories”) and industry-specific security standards (B3S) for health care in hospitals have been created by the German Hospital Society (DKG) as an orientation guide for implementation of the requirements stated in the BSIG, taking the KRITIS protection requirements’ availability, integrity, authenticity and confidentiality into consideration. As mentioned earlier, the framework conditions and sources for establishing the B3S include multiple laws and norms and are in accordance with best practices.

POCT – critical service?

The question whether POCT is a critical service from the perspective of KRITIS is difficult to answer. POCT is defined as medical diagnostic testing near the point (time and place) of patient care. The driving notion behind POCT was to bring clinically important results immediately to the patient and to the treating physician. A broad spectrum of diagnostic tests is meanwhile available with POCT technology (e.g. blood glucose testing, blood gas analysis, rapid coagulation tests). POCT plays an essential role in all hospitals to which B3S can be applied to and falls into the key process steps “diagnostics”, “therapy” and “nursing care” in a hospital setting. POCT blood gas analysis and coagulation tests such as the activated clotting time can directly influence consecutive medical treatment measures, e.g. mechanical patient ventilation and extracorporeal membrane oxygenation (ECMO), and are indeed examples of critical services [12, 13].

We therefore conclude that POCT devices are part of a critical service depending on the use case.

Table 1: User profiles of the University Hospital of Cologne showing the high number of users and a significant difference between active user and total user numbers.

Analyzer	Status/year	2016	2017	2018
Blood gas analyzer	Trained (new)	299	316	438
	User – active	N/A	1330	1653
	User in total	N/A	2393	2754
Glucose measurement	Trained (new)	197	260	311
	User – active	N/A	1630	1806
	User in total	N/A	2842	3142
Hemostasis testing	Trained (new)	113	78	47
	User – active	N/A	192	234
	User in total	N/A	410	466
INR testing	Trained (new)	27	91	43
	User – active	N/A	N/A	108
	User in total	N/A	N/A	129

INR, international normalized ratio; N/A, not available.

POCT analyzers – particularly at risk?

There are certain features of POCT, which make it more vulnerable to safety issues than other IT-based critical services in hospitals. (1) POCT instruments are usually transportable and often even handheld so it is quite demanding to control them over their operational lifecycle (the use on different wards, maintenance and service, repair and replacement). (2) POCT instruments are commonly found in very high numbers in hospitals. (3) POCT instruments are typically operated by a very large number of personnel staff with completely different functions and roles. Table 1 displays the user numbers at the University Hospital of Cologne; a similar profile with an according discrepancy between active and total users has been reported to the authors for a further German University Hospital. The high number of users for the different analyzer types clearly shows the need for a sufficient user management combined with continuous training.

What are the specific technical needs for POCT-IT?

Five areas of interest were consensually identified during “The 1st Round Table POCT-IT-Security Meeting”: (1) user management, (2) data management, (3) update management, (4) network connections and (5) user-friendliness.

1. User management

The POCT devices require access control, which should consist of a user ID in combination with a passcode (this could be a personal identification number [PIN] with a minimum of four digits or a password). The log-in and log-off procedures are a time-consuming and sometimes bothersome step in the clinical routine, which should not lead to a delay in medical service.

The connection of the POCT devices to a central user management system could assist in identifying inactive users. Possible technical solutions are, for example, a connection to a directory service (Active Directory) and/or to a middleware. For the technical and organizational implementation, user-friendliness must be considered.

It is important to establish a technical and organizational emergency management, i.e. an “emergency authorization” must guarantee access to the device for patients in life-threatening situations even without entering a user ID and PIN. In these cases, patient safety prevails over IT security. This way, testing is available but the “emergency authorization” would prevent the user from seeing any other patient data from previous measurements. It might be necessary to combine technical solutions with organizational procedures to achieve clinical feasibility. “Locked-away” (e.g. deposited on the device in a closed envelope) emergency cards with passwords could be one tool.

Biometric access control methods are currently not recommended for a variety of reasons.

Radio-frequency identification (RFID)-based procedures are suitable for access control in combination with a passcode. Alternatively, scanning the user ID (for example, as a barcode for scanning) in combination with a RFID keycard (functioning as a password) could offer a fast login-process.

A further possibility would be to enter the user ID (for example, as a barcode for scanning) in combination with a passcode that can be scanned as another barcode.

As POCT devices are not always under the direct control of medical staff, log-off procedures need to be established. There should be an auto log-off after a fixed time or after each measurement, a manual log-off and an automatic log-off when the POCT device is placed in its docking station. Serial measurements on devices with sample management modules (like blood gas analyzers) pose a problem in this context and can currently only be solved organizationally by, for example, a spatial access regulation.

The POCT user management should map different user roles and authorizations (examples below) to the middleware and to the devices. Two roles are the minimum requirements: (1) a trained operator with insight into patient measurements, calibration data and QC and (2) medical technicians (in-house and external) with access to calibration data and QC, higher-level settings and log files. The latter can potentially contain patient data which needs to be considered: contracts for maintenance services covering all aspects of medical data safety as well as agreements on secrecy are a necessary prerequisite in this setting and should be part of an organizational and legally compliant solution.

Middleware helps to manage access rules for different user roles. The connection to a directory service (e.g. Active Directory) for the middleware and device operators is a worthwhile investment because it maps permissions related to the device (analyzer) type and the site of installation (wards, emergency departments, intensive care units [ICUs]).

There is a clear need for a user role management with recertification assisted by eLearning and a notification system (connection to an e-mail server) combined with a rule-based blocking of users after prolonged non-use. A further connection of human resource management software (in addition to directory services such as Active Directory) could improve user management. The point in time of user data transmission to the devices needs to be synchronized, e.g. event triggered (when a new user is created) or scheduled (following a fixed time plan).

2. Data management

The General Data Protection Regulation (GDPR, German: Datenschutz-Grundverordnung [DSGVO]) made addressing requirements for data privacy necessary. This is not only a technical question but it is also linked to organizational changes like contracts for maintenance of POCT devices covering confidentiality agreements. Data economy however should also be considered: Is it necessary to store all the data from a Health Level 7 (HL7) message on the device? How long should the data be stored on the POCT device? From the GDPR perspective, it is evident that patient data needs a higher level of protection than quality control or calibration data. Depending on the application scenario, it may be useful to map an access-controlled separation of QC, calibration data and patient results. An automated removal of “unnecessary patient data” could help to implement the principles of data austerity. One example could be the deletion of patient data on the POCT device following the transmission to the corresponding middleware or LIS (via secure communication and standardized protocols: Point-of-Care Connectivity Standard [POCT1a], HL7-Fast Healthcare Interoperability Resources [FHIR], American Society for Testing and Materials Communication Standard [ASTM]). Another conceivable alternative could be an automated process, which removes data after a defined period of time (not violating any legally mandated storage period).

In addition, the B3S demands encryption. The encrypted storage of (patient) data on the device (decryption only by authentication) is therefore required.

3. Update management

For testing of new versions, updates and patches in OSs or LIS installations in large hospitals, a test environment strictly separated from the productive system is often established. The support of a test environment without real data (concrete anonymized data) and a productive system is advisable; an additional evaluation system for POCT-IT would be preferable. Updates via internet or local solutions (prerequisites are secure file transfer solutions that can be tested and then be imported centrally or locally) could allow a controlled roll-out procedure. This should include a support of test scenarios at the site of the user. It is clear that updates for all delivered components are needed, involving firmware, OS, applications and middleware solutions.

If there is a remote service needed for updates, the question is “What’s on the other side of the tunnel?”. This should be defined and documented in a data processing agreement (“Auftragsverarbeitungs-Vertrag”).

4. Network connections

The rapid development of handheld POCT devices led to the need of a fast transmission of the results to the electronic patient archive. As the B3S asks for encryption, this standard should also be applied to the transmission of data. A secure connection via wireless local area network (WLAN)/virtual local area network (VLAN) connectivity with Wi-Fi Protected Access 2 (WPA2)/

Enterprise (certificate based) should be available. The minimum of required services, e.g. ports to ensure functionality of the device, should be defined. In accordance with the standard, the middleware to LIS or HIS communication should offer the possibility of end-to-end encryption.

5. User-friendliness

It needs to be noted that all organizational procedures and technical solutions with regard to data security only make sense if the POCT devices remain user-friendly without an extensive need for training.

To dos

The first step toward POCT-IT security management in accordance with legal requirements is the implementation of a structure for IT security, e.g. an integration to a POCT committee. The risks during the diagnostic processes with POCT devices should be identified and reviewed. General threats, IT-specific threats and vulnerabilities must be monitored with respect to the POCT-IT solutions on different analyzers or middleware(s). Risk-reducing measures for POCT should be implemented beginning with basic steps such as access control, cryptography and secure communication. All these steps must be accompanied by constant training, education and last but not least awareness.

Regarding the POCT devices and the middleware solutions, a security by design is needed.

Finally, a periodic evaluation of the system needs to be performed to achieve the goal of a secure POCT-IT system as a part of the hospital IT security.

Author contributions: All the authors have accepted responsibility for the entire content of this submitted manuscript and approved submission.
Research funding: None declared.
Employment or leadership: None declared.
Honorarium: None declared.
Competing interests: The funding organization(s) played no role in the study design; in the collection, analysis, and interpretation of data; in the writing of the report; or in the decision to submit the report for publication.

References

1. Luppa PB, Bietenbeck A, Beaudoin C, Giannetti A. Clinically relevant analytical techniques, organizational concepts for application and future perspectives of point-of-care testing. Biotechnol Adv 2016;34:139–60.
2. Haeckel R, Wosniok W, Arzideh F, Zierk J, Gurr E, Streichert T. Critical comments to a recent EFLM recommendation for the review of reference intervals. Clin Chem Lab Med 2017;55:341–7.
3. Bundesärztekammer. Richtlinie der Bundesärztekammer zur Qualitätssicherung laboratoriumsmedizinischer Untersuchungen. Deutsches Ärzteblatt 2014;Jg. 111:1583–618.
4. Point-of-care testing (POCT) – Requirements for quality and competence (ISO 22870:2016); German version EN ISO 22870:2016, 2017.
5. Medical laboratories – Requirements for quality and competence (ISO 15189:2012, Corrected version 2014-08-15), 2014.
6. Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus, 2019.
7. Sozialgesetzbuch (SGB) Fünftes Buch (V) – Gesetzliche Krankenversicherung, 1988, last revison 2019.
8. Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG), 2009, last revison 2017.
9. Expertenkreis-CyberMed. Sicherheit von Medizinprodukten. 2019.
10. Krüger-Brand HE. IT-Sicherheit im Krankenhaus – Cyberrisiken als Herausforderung. Dtsch Arztebl 2017;114:A-1910/B-620/C-586.
11. Schutz Kritischer Infrastrukturen durch IT-Sicherheitsgesetz und UP KRITIS (2017).
12. Egi M, Kataoka J, Ito T, Nishida O, Yasuda H, Okamaoto H, et al. Oxygen management in mechanically ventilated patients: a multicenter prospective observational study. J Crit Care 2018;46:1–5.
13. Raman J, Alimohamed M, Dobrilovic N, Lateef O, Aziz S. A comparison of low and standard anti-coagulation regimens in extracorporeal membrane oxygenation. J Heart Lung Transplant 2019;38:433–9.