CLINICAL AND
LABORATORY
STANDARDS
INSTITUTE®

3rd Edition

CLSI AUTO11™

Information Technology Security of *In Vitro* Diagnostic Instruments and Software Systems

CLSI AUTO11 provides a framework for communication of information technology security issues between the *in vitro* diagnostic system vendor and the health care delivery organization.

A standard for global application developed through the Clinical and Laboratory Standards Institute consensus process.

CLSI AUTO11-Ed3
September 2024
Replaces CLSI AUTO11-A2

Information Technology Security of *In Vitro* Diagnostic Instruments and Software Systems

Ed Heierman, PhD
Riccardo Benedetti, Dr.sc.techn.ETH, Dipl.El.Ing.ETH
Richard Y. Wang, DO
David Chou, MD
Thomas J.S. Durant, MD
Philip R. Foulis, MD, MPH
Anthony Gautier, BS
Derek Holzhauser, MAppSc, BSc
Sean Kocur, PhD, C(ASCP), D(ABFT)FT
James McLean, MBA, PMP, CSSLP
Niklaus Rümmele, BSc
Sheri Terrillion, MT(ASCP)^{CM}, CQA(ASQ), MAOL

Abstract

Clinical and Laboratory Standards Institute AUTO11—*Information Technology Security of* In Vitro *Diagnostic Instruments and Software Systems* specifies technical and operational requirements and technical implementation procedures related to security of *in vitro* diagnostic (IVD) systems (devices, analytical instruments, data management systems, etc.) installed at a health care delivery organization (HDO). The intended users for CLSI AUTO11 are medical device and IVD system manufacturers, users (eg, laboratory personnel), and information technology management of HDOs.

Clinical and Laboratory Standards Institute (CLSI). *Information Technology Security of* In Vitro *Diagnostic Instruments and Software Systems*. 3rd ed. CLSI standard AUTO11 (ISBN 978-1-68440-252-6 [Print]; ISBN 978-1-68440-253-3 [Electronic]). Clinical and Laboratory Standards Institute, USA, 2024.

The Clinical and Laboratory Standards Institute consensus process, which is the mechanism for moving a document through two or more levels of review by the health care community, is an ongoing process. Users should expect revised editions of any given document. Because rapid changes in technology may affect the procedures, methods, and protocols in a standard or guideline, users should replace outdated editions with the current editions of CLSI documents. Current editions are listed in the CLSI catalog and posted on our website at www.clsi.org.

If you or your organization is not a member and would like to become one, or to request a copy of the catalog, contact us at:

P: +1.610.688.0100 **F:** +1.610.688.0700 **E:** customerservice@clsi.org **W:** www.clsi.org

CLINICAL AND
LABORATORY
STANDARDS
INSTITUTE®

Suggested Citation

CLSI. *Information Technology Security of* In Vitro *Diagnostic Instruments and Software Systems.* 3rd ed. CLSI standard AUTO11. Clinical and Laboratory Standards Institute; 2024.

Previous Editions:

October 2006, October 2014

CLSI AUTO11-Ed3

ISBN 978-1-68440-252-6 (Print)

ISBN 978-1-68440-253-3 (Electronic)

ISSN 1558-6502 (Print)

ISSN 2162-2914 (Electronic)

Volume 44, Number 25

Contents

Abstract i
Committee Membership. iii
Foreword. vii
Chapter 1: Introduction 1
1.1 Scope. 2
1.2 Background 2
1.3 Terminology 3
Chapter 2: Delineation of Medical Device Manufacturer and Health Care Delivery Organization Responsibilities 9
Chapter 3: Technical Design Guidelines Related to Regulatory Requirements 13
3.1 Privacy 14
3.2 Preventing Unauthorized Access to Applications. 18
3.3 Preventing Unauthorized Access to the Operating System 27
3.4 Preventing Unauthorized Access From External Devices and Software. 28
3.5 Preventing Unauthorized Data Access 29
3.6 Protection From Malicious Software. 36
3.7 Security Monitoring 39
3.8 Preventing Loss of Data. 41
3.9 Web and Cloud Applications. 43
3.10 *In Vitro* Diagnostic Mobile Applications on Mobile Devices 45
Chapter 4: Process and Operational Requirements. 49
4.1 Cybersecurity Lifecycle Management 50
4.2 Secure Coding Practices 54
4.3 Cybersecurity Risk Management. 54
4.4 Third-Party Components 56
4.5 Medical Device Manufacturer System Verification and Validation 58
4.6 Regulatory Authorities. 58
4.7 Coordinated Vulnerability Disclosure 60
4.8 Security Patching. 61
4.9 Documents for Health Care Delivery Organizations. 64
4.10 Preventive Actions 66
4.11 Key and Certificate Management 69

Contents (Continued)

Chapter 5: Applicability of Requirements to Classes of *In Vitro* Diagnostic Systems 71

5.1 All *In Vitro* Diagnostic Systems...72

5.2 *In Vitro* Diagnostic Systems That Support User Accounts 74

5.3 *In Vitro* Diagnostic Systems That Manage Protected Health Information...........................75

5.4 *In Vitro* Diagnostic Systems That Support Network Connections.......................................75

5.5 *In Vitro* Diagnostic Systems That Support Cloud Applications 75

5.6 *In Vitro* Diagnostic Systems That Support Mobile Applications..75

Chapter 6: Conclusion... 79

References 82

The Quality Management System Approach..88

Foreword

The information technology (IT) security requirements related to various laboratory systems (devices, analytical instruments, data management systems, etc.) are growing, mainly because of:

- New international regulations applicable to health care delivery organizations (HDOs)[1]
- An increase in the degree of integration of the *in vitro* diagnostic (IVD) systems in the IT environment of health care institutions
- Cyberattacks observed in HDOs from a multitude of sources

The real and potential threats for the systems and the organizations are also growing. Examples illustrating how systems could be compromised by malicious software and people include:

- Changing processed/static data (eg, test applications, calibration), resulting in the production of incorrect results
- Unauthorized access to patient EHRs by querying the laboratory information system and EHR system from compromised laboratory systems (eg, laboratory instrument with CLSI LIS02[2] query protocol)
- Unauthorized access or manipulation of patient and sample results from the system
- Damaging the IVD system software or manipulating application configuration data, requiring reinstallation, and resulting in downtime for the user and service costs for the medical device manufacturer (MDM)
- Misusing the IVD system as a means for compromising other systems in the HDO's IT environment
- Misusing the IVD system as a means for entering the MDM's corporate network
- Ransomware malware that prevents or limits users from accessing the system to collect a ransom

Overview of Changes

CLSI AUTO11-Ed3 replaces CLSI AUTO11-A2, published in 2014. Several changes were made in this edition.

Compared with CLSI AUTO11-A2, all the existing requirements have been reviewed. For these, the requirement numbers have been kept as they were. However, some requirements have been moved to new subchapters. Additionally, new requirements have been added, starting with [Req-1001]. The types of changes to the previously existing requirements can be categorized as:

- Adaption to new terminology, such as from "vendor" to "MDM," from "HCO" to "HDO" (eg, Req-0251), and from "antivirus and antispyware" to "antimalware" (ie, Req-0321)
- Clarification by text addition, such as from "system" to "IVD system" (ie, Req-0111, Req-0141, Req-0531), or by being more specific (ie, "risks to an acceptable level as defined by the HDO" in Req-0212, "system by MDMs and HDOs" in Req-0621, "instrument and system" in Req-0162)
- Clarification by rewording (ie, Req-0112, Req-0121, Req-0131, Req-0171, Req-0231, Req-0511)
- Removal of requirement (eg, Req-0742 because of the addition of Req-1061, which provides a broader requirement to follow national regulations and laws)

NOTE: The content of CLSI AUTO11 is supported by the CLSI consensus process and does not necessarily reflect the views of any single individual or organization.

KEY WORDS

authentication

authorization

cloud

encryption

IVD IT security

mobile

user account management

wireless

Use of Bluetooth®, Windows®, Linux®, CVE®, OWASP®, and Cyber Kill Chain® in CLSI AUTO11 is not an endorsement on the part of CLSI. With each use of the trade name, "or the equivalent" is added to indicate that CLSI AUTO11 also applies to any equivalent products.

Chapter 1

Introduction

Information Technology Security of *In Vitro* Diagnostic Instruments and Software Systems

1 Introduction

1.1 Scope

CLSI AUTO11 specifies technical and operational requirements and technical implementation procedures related to information technology (IT) security of *in vitro* diagnostic (IVD) systems (devices, analytical instruments, data management systems, etc.) installed at a health care delivery organization (HDO). CLSI AUTO11 also provides guidance on meeting and using existing technical standards for medical device IT security and recommendations on identifying the parties responsible for implementing these requirements.

CLSI AUTO11 is primarily meant to be used by manufacturers (ie, medical device manufacturers [MDMs], IVD system manufacturers) and HDOs. Regulatory agencies may also find useful information in CLSI AUTO11.

CLSI AUTO11 is not intended for use as the final written policy for the HDO. For example, local organizations need to include in their own documentation the technical and process aspects of medical device security addressed by other standards organizations, such as the International Organization for Standardization (ISO) and Institute of Electrical and Electronics Engineers (IEEE). In addition, CLSI AUTO11 may not apply to certain devices used in health care (see Subchapter 3.10).

The suggested best practices contained in CLSI AUTO11 are based on the state of technology at the time of publication. These best practices are distinguished from the requirements through their inclusion in a text box.

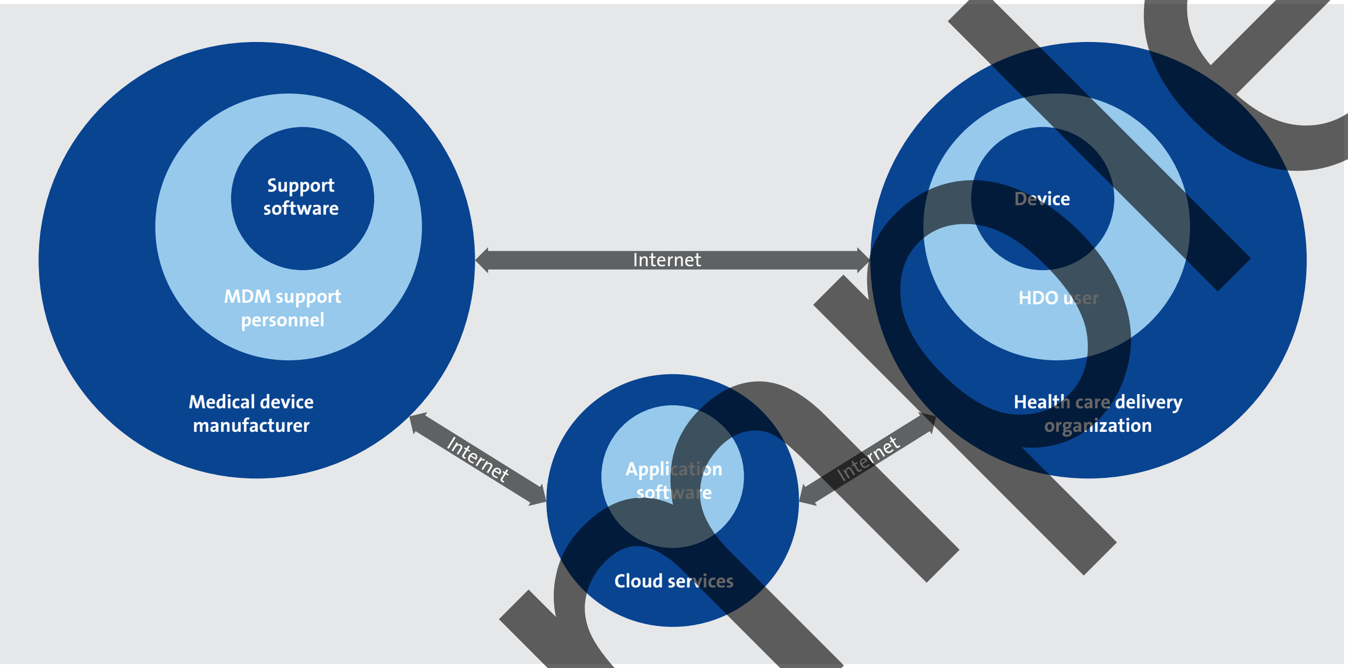
Some requirements, procedures, and guidelines specified by CLSI AUTO11 may not be necessary or desired for IVD systems during clinical trials. The HDO and manufacturer should clearly state in the corresponding contract how CLSI AUTO11 would be applied during clinical trials. In addition, some requirements, procedures, and guidelines specified by CLSI AUTO11 may not be practical, technically or financially, for legacy IVD systems or HDO IT departments to implement. In these situations, the manufacturer and HDO should use their best judgment to decide what to implement. It is important for the manufacturer and HDO to clearly document any deviations from CLSI AUTO11.

1.2 Background

As automation becomes more prevalent in the medical laboratory, standards for IVD instruments and software have become necessary. Over recent decades, with passage of bills such as the Health Information Technology for Economic and Clinical Health Act, health care information has become increasingly digitized across medical specialties. Subsequently, there has been widespread adoption of health IT systems, such as EHR and LIS. In the medical laboratory, software solutions have similarly become more prevalent and coupled with modern IVD devices. Increasingly, IVD devices are implemented with network connectivity within local area networks (LANs) and are often reliant on communication with IVD manufacturer support by way of the public network (ie, the Internet). As a result of increasing network connectivity, cybersecurity is becoming a pertinent topic of discussion with the purchase, implementation, and maintenance of IVD devices. Any software development shall consider data privacy issues, including how the data will be secured, how access will be controlled, and how data integrity will be maintained. CLSI AUTO11 seeks to provide clarity on the state of modern cybersecurity as it pertains to IVD systems and to offer guidance on decisions that may be encountered by a manufacturer or HDO when designing or implementing these systems, respectively.

2 Delineation of Medical Device Manufacturer and Health Care Delivery Organization Responsibilities

MDM responsibility, as shown in Figure 1, for the expected life of a device is defined by the US Food and Drug Administration (FDA) as "the time that a device is expected to remain functional after it is placed into use. Certain implanted devices have specified end-of-life (EOL) dates. Other devices are not labeled as to their respective EOL but are expected to remain operational through activities such as maintenance, repairs, or upgrades, for an estimated period of time."[9]



Abbreviations: HDO, health care delivery organization; MDM, medical device manufacturer.

Figure 1. MDM and HDO Security Architecture Design

Medical devices may be operated in complex networked environments, which increasingly require Internet connections between the MDM and the HDO and may include the use of cloud services. As shown in Figure 1, the overall security architecture should consider design, environmental, and operational controls. This requires cooperation and a shared responsibility between the MDM and the HDO.

During the expected life of the medical device, the MDM is expected to provide any security patches or software replacement necessary for the proper secure operation of the device. It is strongly recommended that the MDM and HDO establish a software license and support agreement that defines the level of software support and security the MDM will provide (including maintenance and upgrades). These agreements should include the management of HDO sensitive information and data collected by the MDM. The HDO shall be notified when the software support for the device or a third-party software component of the device is no longer available. The HDO shall be notified well in advance of any MDM plans to phase out a model or version of its device, so that the HDO has time to budget and conduct MDM evaluations and selections for a replacement.

CLINICAL AND
LABORATORY
STANDARDS
INSTITUTE®

PRINT ISBN 978-1-68440-252-6

ELECTRONIC ISBN 978-1-68440-253-3

CLSI AUTO11-Ed3