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.

Clinical and Laboratory Standards Institute

Setting the standard for quality in medical laboratory testing around the world.

The Clinical and Laboratory Standards Institute (CLSI) is a not-for-profit membership organization that brings together the varied perspectives and expertise of the worldwide laboratory community for the advancement of a common cause: to foster excellence in laboratory medicine by developing and implementing medical laboratory standards and guidelines that help laboratories fulfill their responsibilities with efficiency, effectiveness, and global applicability.

Consensus Process

Consensus—the substantial agreement by materially affected, competent, and interested parties—is core to the development of all CLSI documents. It does not always connote unanimous agreement but does mean that the participants in the development of a consensus document have considered and resolved all relevant objections and accept the resulting agreement.

Commenting on Documents

CLSI documents undergo periodic evaluation and modification to keep pace with advances in technologies, procedures, methods, and protocols affecting the laboratory or health care.

CLSI's consensus process depends on experts who volunteer to serve as contributing authors and/or as participants in the reviewing and commenting process. At the end of each comment period, the committee that developed the document is obligated to review all comments, respond in writing to all substantive comments, and revise the draft document as appropriate.

Comments on published CLSI documents are equally essential and may be submitted by anyone, at any time, on any document. All comments are managed according to the consensus process by a committee of experts.

Appeal Process

When it is believed that an objection has not been adequately considered and responded to, the process for appeal, documented in the CLSI *Standards Development Policies and Processes,* is followed.

All comments and responses submitted on draft and published documents are retained on file at CLSI and are available upon request.

Get Involved—Volunteer!

Do you use CLSI documents in your workplace? Do you see room for improvement? Would you like to get involved in the revision process? Or maybe you see a need to develop a new document for an emerging technology? CLSI wants to hear from you. We are always looking for volunteers. By donating your time and talents to improve the standards that affect your own work, you will play an active role in improving public health across the globe.

For additional information on committee participation or to submit comments, contact CLSI.

Clinical and Laboratory Standards Institute
P: +1.610.688.0100
F: +1.610.688.0700
www.clsi.org
standard@clsi.org

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.

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

Committee Membership

Consensus Council

The Consensus Council sets priorities for CLSI standards development and votes on Final Draft documents to confirm that process requirements have been met. Consensus Council members are listed on the CLSI website: https://clsi.org/standards-development/consensus-council/

Document Development Committee on Information Technology Security of *In Vitro* Diagnostic Instruments and Software Systems

Ed Heierman, PhD
Chairholder
Abbott
USA

Riccardo Benedetti, Dr.sc.techn.ETH, Dipl.El.Ing.ETH
Vice-Chairholder
Roche Diagnostics International Ltd
Switzerland

Richard Y. Wang, DO
Committee Secretary
Centers for Disease Control and Prevention
USA

Thomas J.S. Durant, MD
Yale University School of Medicine
USA

Philip R. Foulis, MD, MPH
James A. Haley Veterans' Hospital
USA

Anthony Gautier, BS
Beckman Coulter
USA

Derek Holzhauser, MAppSc, BSc
RCPA Quality Assurance Programs Pty Limited
Australia

James McLean, MBA, PMP, CSSLP
Siemens Healthineers
USA

Enrique Terrazas, MD, MS
Quest Diagnostics
USA

Sheri Terrillion, MT(ASCP)^{CM}, CQA(ASQ), MAOL
Sentara Healthcare
USA

Expert Panel on Automation and Informatics

Expert panel volunteers support the development of CLSI documents by providing technical expertise in specialty areas. Expert panel members are listed by area of expertise on the CLSI website: https://clsi.org/standards-development/expert-panels/

Acknowledgment

CLSI, the Consensus Council, and the Document Development Committee on Information Technology Security of *In Vitro* Diagnostic Instruments and Software Systems gratefully acknowledge the following volunteers for their important contributions to the revision of CLSI AUTO11:

David Chou, MD
University of Washington Dept of Lab Medicine and Pathology
USA

Sean Kocur, PhD, C(ASCP), D(ABFT)FT
Quest Diagnostics
USA

Niklaus Rümmele, BSc
Roche Diagnostics International Ltd.
Switzerland

Contents

Contents (Continued)

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.