CLINICAL AND LABORATORY STANDARDS INSTITUTE®

October 2014

AUTO11-A2

Information Technology Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard—Second Edition

This document provides a framework for communication of information technology security issues between the *in vitro* diagnostic system vendor and the health care 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 clinical 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 clinical 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 advancements 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 addressed according to the consensus process by a committee of experts.

Appeals Process

If it is believed that an objection has not been adequately addressed, the process for appeals is documented in the CLSI Standards Development Policies and Process document.

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

Clinical and Laboratory Standards Institute
950 West Valley Road, Suite 2500
Wayne, PA 19087 USA
P: 610.688.0100
F: 610.688.0700
www.clsi.org
standard@clsi.org

ISBN 1-56238-979-3 (Print)
ISBN 1-56238-980-7 (Electronic)
ISSN 1558-6502 (Print)
ISSN 2162-2914 (Electronic)

AUTO11-A2
Vol. 34 No. 17
Replaces AUTO11-A
Vol. 26 No. 33

Information Technology Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard—Second Edition

Volume 34 Number 17

Ed Heierman III, PhD
Andrzej J. Knafel, PhD
Ashley A. Frazer-Abel
Wei Bao, CSQE, PMP
Alexis B. Carter, MD, FCAP, FASCP
Diana Del Rio
James Jacobson
Faissal Kaddouri
Babar Khan, MS
Stanley Lu, MS
Chung-Hee Row, MT(ASCP)
Enrique Terrazas, MD
Ginger Wooster, MBA, MT(ASCP)

Abstract

Clinical and Laboratory Standards Institute document AUTO11-A2—*Information Technology Security of* In Vitro *Diagnostic Instruments and Software Systems; Approved Standard—Second Edition* 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 organization (HCO). The intended users for this standard are vendors (IVD system manufacturers), users (eg, laboratory personnel), and information technology management of HCOs.

Clinical and Laboratory Standards Institute (CLSI). *Information Technology Security of* In Vitro *Diagnostic Instruments and Software Systems; Approved Standard—Second Edition*. CLSI document AUTO11-A2 (ISBN 1-56238-979-3 [Print]; ISBN 1-56238-980-7 [Electronic]). Clinical and Laboratory Standards Institute, 950 West Valley Road, Suite 2500, Wayne, Pennsylvania 19087 USA, 2014.

CLINICAL AND LABORATORY STANDARDS INSTITUTE®

Suggested Citation

CLSI. *Information Technology Security of* In Vitro *Diagnostic Instruments and Software Systems; Approved Standard—Second Edition.* CLSI document AUTO11-A2. Wayne, PA: Clinical and Laboratory Standards Institute; 2014.

Proposed Standard
January 2006

Approved Standard
October 2006

Approved Standard—Second Edition
October 2014

ISBN 1-56238-979-3 (Print)
ISBN 1-56238-980-7 (Electronic)
ISSN 1558-6502 (Print)
ISSN 2162-2914 (Electronic)

Committee Membership

Consensus Committee on Automation and Informatics

Richard S. Seaberg, MT(ASCP)
Chairholder
North Shore-Long Island Jewish Health System Laboratories
USA

Ed Heierman III, PhD
Vice-Chairholder
Abbott
USA

Suzanne H. Butch, MA, MT(ASCP), SBB
University of Michigan, Department of Pathology
USA

David Chou, MD
University of Washington Medical Center
USA

Andrew D. Grove, PhD
FDA Center for Devices and Radiological Health
USA

Klaus M. Kjøller, MSc
Radiometer Medical ApS
Denmark

Elizabeth Kenimer Leibach, EdD, MS, MLS, SBB
Centers for Disease Control and Prevention
USA

Ginger Wooster, MBA, MT(ASCP)
Orchard Software Corp.
USA

Jyh-Ching Yaur
Siemens Healthcare Diagnostics, Inc.
USA

Document Development Committee on IT Security of IVD Instruments

Ed Heierman III, PhD
Chairholder
Abbott
USA

Andrzej J. Knafel, PhD
Vice-Chairholder
Roche Diagnostics International Ltd.
Switzerland

Ashley A. Frazer-Abel
Committee Secretary
National Jewish Health
USA

Alexis B. Carter, MD, FCAP, FASCP
Emory University Hospital
USA

James Jacobson
Siemens Healthcare Diagnostics, Inc.
USA

Faissal Kaddouri
Diagnostica Stago
France

Stanley Lu, MS
Diatherix Laboratories, Inc.
USA

Chung-Hee Row, MT(ASCP)
National Institutes of Health Department of Lab Medicine
USA

Ginger Wooster, MBA, MT(ASCP)
Orchard Software
USA

Staff

Clinical and Laboratory Standards Institute
Wayne, Pennsylvania, USA

Luann Ochs, MS
Senior Vice President – Operations

David E. Sterry, MT(ASCP)
Staff Liaison

Megan L. Tertel, MA
Editorial Manager

Joanne P. Christopher, MA
Editor

Patrice E. Polgar
Editor

Acknowledgment

CLSI and the Consensus Committee on Automation and Informatics gratefully acknowledge the following individuals for their help in preparing this document:

Wei Bao, CSQE, PMP
BD Diagnostic Systems
USA

Anthony L. Camisa, MS
Beckman Coulter
USA

Diana Del Rio
Beckman Coulter
USA

Babar Khan, MS
ContraFect Corporation
USA

Enrique Terrazas, MD
University of California San Francisco
USA

Contents

Foreword

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

- New international regulations applicable to health care organizations (HCOs)[1]
- An increase in the degree of integration of the *in vitro* diagnostic (IVD) systems in the IT environment of health care institutions
- Cyber-attacks observed in HCOs 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/people include:

- Changing processed/static data (eg, test applications, calibration), resulting in the production of incorrect results
- Unauthorized access to patient electronic health records (EHRs) by querying the LIS/EHR from compromised laboratory systems (eg, laboratory instrument with CLSI document LIS02[2] query protocol)
- Unauthorized access or manipulation of patient/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 vendor
- Misusing the IVD system as a means for compromising other systems in the HCO's IT environment
- Misusing the IVD system as a means for entering the vendor's corporate network

This document replaces the first edition of the approved standard, AUTO11-A, which was published in 2006. This document was revised to align with standards and best practices that have emerged since publication of its first edition. This standard was also updated to provide guidance on cloud applications and mobile devices, and reorganized to improve its clarity.

Note that the trade names Bluetooth®, Windows ®, and Linux® are included in Chapters 4.3.1, 4.4, and 4.8 of this document. It is Clinical and Laboratory Standards Institute's policy to avoid using a trade name unless the product identified is the only one available or it serves solely as an illustrative example of the procedure, practice, or material described. In this case, the document development committee and consensus committee believe the trade names are important descriptive adjuncts to the document. In such cases, it is acceptable to use the product's trade name, as long as the words, "or the equivalent" are added to the references. It should be understood that information on these products in this standard also apply to any equivalent products. Please include in your comments any information that relates to this aspect of AUTO11.

Key Words

Authentication, authorization, cloud, encryption, IVD IT security, mobile, user account management, wireless

Information Technology Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard—Second Edition

1 Scope

This standard 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 organization (HCO). This standard also provides guidance to meet and use existing technical standards for medical device IT security and recommendations for identifying the parties responsible for implementing these requirements.

The intended users for this standard are vendors (IVD system manufacturers), users (eg, laboratory personnel), and IT management of HCOs.

This standard is not intended for use as the final written policy for the HCO. For example, local organizations will 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 IEEE. In addition, this standard may not apply to certain devices used in health care (see Chapter 4.8).

The suggested best practices contained in this document 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 this standard may not be necessary or desired for IVD systems during clinical trials. The HCO and vendor should clearly state in the corresponding contract how the standard would be applied during clinical trials. In addition, some requirements, procedures, and guidelines specified by this standard may not be practical technically or financially for legacy IVD systems or HCO IT departments to implement. In these situations, the vendor and HCO will need to use their best judgment to decide what to implement. It will be important for the vendor and HCO to clearly document any deviations from the standard.

2 Terminology

2.1 A Note on Terminology

CLSI, as a global leader in standardization, is firmly committed to achieving global harmonization wherever possible. Harmonization is a process of recognizing, understanding, and explaining differences while taking steps to achieve worldwide uniformity. CLSI recognizes that medical conventions in the global metrological community have evolved differently in the United States, Europe, and elsewhere; that these differences are reflected in CLSI, ISO, and European Committee for Standardization (CEN) documents; and that legally required use of terms, regional usage, and different consensus timelines are all important considerations in the harmonization process. In light of this, CLSI's consensus process for development and revision of standards and guidelines focuses on harmonization of terms to facilitate the global application of standards and guidelines.

Please note that the term *hospital information system (HIS)* has been replaced in CLSI documents with the term *electronic health record (EHR)*. This change reflects the current prevailing terminology throughout the laboratory and health care environments.