CLINICAL AND LABORATORY STANDARDS INSTITUTE®

October 2014

AUTO11-A2

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

SAMPLE

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

SAMPLE

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)

SAMPLE

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.

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, and to request a copy of the catalog, contact us at: Telephone: 610.688.0100; Fax: 610.688.0700; E-Mail: customerservice@clsi.org; Website: www.clsi.org.

Copyright ©2014 Clinical and Laboratory Standards Institute. Except as stated below, any reproduction of content from a CLSI copyrighted standard, guideline, companion product, or other material requires express written consent from CLSI. All rights reserved. Interested parties may send permission requests to permissions@clsi.org.

CLSI hereby grants permission to each individual member or purchaser to make a single reproduction of this publication for use in its laboratory procedure manual at a single site. To request permission to use this publication in any other manner, e-mail permissions@clsi.org.

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

SAMPLE

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

Contents

SAMPLE

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

SAMPLE

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.

SAMPLE

©*Clinical and Laboratory Standards Institute. All rights reserved.*

2.2 Definitions

authentication – the process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system; **NOTE:** This process is usually achieved by supplying the user ID and a unique password (what the user knows), security token (what the user has), or biometrics (who the user is).

authorization – the process of granting rights or access to systems, applications, or networks; **NOTE:** Authorization determines who is trusted for a given purpose.

biometrics – the measurement and analysis of unique physical characteristics of an individual (eg, fingerprints, voice pattern, retinal scan) as a means of verifying personal identity.

cloud – a software model in which data, resources, and the software are shared and provided to clients over the Internet, based on demand.

closed system – a system in which the vendor provides all hardware and software to the health care organization. The majority of medical devices are closed systems.

de-identification – the removal of names and other explicit identifiers from personal records; **NOTE 1:** Under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, data are de-identified if either:

- An experienced expert/qualified statistician determines the risk that certain information could be used to identify an individual is "very small," and documents as well as justifies the determination, or

- The data do not include any of the following 18 identifiers (of the individual or his/her relatives, household members, or employers) that could be used alone or in combination with other information to identify the subject:
  - Names
  - Geographic subdivisions smaller than a state (including zip code)
  - All elements of dates except year (unless the subject is greater than 89 years old)
  - Telephone numbers
  - Fax numbers
  - E-mail address
  - Social Security numbers
  - Medical record numbers
  - Health plan beneficiary numbers
  - Account numbers
  - Certificate/license numbers
  - Vehicle identifiers including license plates
  - Device identifiers and serial numbers (patient care devices)
  - URLs
  - Internet protocol addresses
  - Biometric identifiers (fingerprint, retina scan)
  - Full face photos and comparable images
  - Any unique identifying number, characteristic, or code

  NOTE 2: Even if the above identifiers are removed, the HIPAA Privacy Rule states that information will be considered identifiable if the covered entity knows that the identity of the person may still be determined.

device end user – end user in the health care organization familiar with the medical device and its operation.

SAMPLE

 ©Clinical and Laboratory Standards Institute. All rights reserved.

The Quality Management System Approach

Clinical and Laboratory Standards Institute (CLSI) subscribes to a quality management system (QMS) approach in the development of standards and guidelines, which facilitates project management; defines a document structure via a template; and provides a process to identify needed documents. The QMS approach applies a core set of "quality system essentials" (QSEs), basic to any organization, to all operations in any health care service's path of workflow (ie, operational aspects that define how a particular product or service is provided). The QSEs provide the framework for delivery of any type of product or service, serving as a manager's guide. The QSEs are as follows:

Organization	Personnel	Process Management	Nonconforming Event Management
Customer Focus	Purchasing and Inventory	Documents and Records	Assessments
Facilities and Safety	Equipment	Information Management	Continual Improvement

AUTO11-A2 addresses the QSE indicated by an "X." For a description of the other documents listed in the grid, please refer to the Related CLSI Reference Materials section on the following page.

Organization	Customer Focus	Facilities and Safety	Personnel	Purchasing and Inventory	Equipment	Process Management	Documents and Records	Information Management	Nonconforming Event Management	Assessments	Continual Improvement
						X AUTO09 LIS02		LIS02 POCT01			

Path of Workflow

A path of workflow is the description of the necessary processes to deliver the particular product or service that the organization or entity provides. A laboratory path of workflow consists of the sequential processes: preexamination, examination, and postexamination and their respective sequential subprocesses. All laboratories follow these processes to deliver the laboratory's services, namely quality laboratory information.

AUTO11-A2 does not address any of the clinical laboratory path of workflow steps. For a description of the documents listed in the grid, please refer to the Related CLSI Reference Materials section on the following page.

Preexamination				**Examination**			**Postexamination**	
Examination ordering	Sample collection	Sample transport	Sample receipt/processing	Examination	Results review and follow-up	Interpretation	Results reporting and archiving	Sample management
							LIS02 POCT01	

SAMPLE

 ©Clinical and Laboratory Standards Institute. All rights reserved.

Related CLSI Reference Materials*

AUTO09-A **Remote Access to Clinical Laboratory Diagnostic Devices via the Internet; Approved Standard (2006).** This document provides a standard communication protocol for instrument system vendors, device manufacturers, and hospital administrators to allow remote connections to laboratory diagnostic devices. The remote connections can be used to monitor instruments' subsystems; collect diagnostics data for remote system troubleshooting; and collect data for electronic inventory management.

LIS02-A2 **Specification for Transferring Information Between Clinical Laboratory Instruments and Information Systems; Approved Standard—Second Edition (2004).** This document covers the two-way digital transmission of remote requests and results between clinical laboratory instruments and information systems.

POCT01-A2 **Point-of-Care Connectivity; Approved Standard—Second Edition (2006).** This document provides the framework for engineers to design devices, work stations, and interfaces that allow multiple types and brands of point-of-care devices to communicate bidirectionally with access points, data managers, and laboratory information systems from a variety of vendors. A CLSI-IFCC joint project.

SAMPLE

* CLSI documents are continually reviewed and revised through the CLSI consensus process; therefore, readers should refer to the most current editions.

©*Clinical and Laboratory Standards Institute. All rights reserved.*

CLINICAL AND LABORATORY STANDARDS INSTITUTE®

Explore the Latest Offerings from CLSI!

As we continue to set the global standard for quality in laboratory testing, we're adding initiatives to bring even more value to our members and customers.

THE Key TO Quality™
from the Clinical and Laboratory Standards Institute (CLSI)

Power Forward with this Official Interactive Guide

Fundamentals for implementing a quality management system in the clinical laboratory.

Find Membership Opportunities

See the options that make it even easier for your organization to take full advantage of CLSI benefits and our unique membership value.

CLSI U
Laboratory Standards Education Center

Visit the CLSI U Education Center

Where we provide the convenient and cost-effective education resources that laboratories need to put CLSI standards into practice, including webinars, workshops, and more.

Shop Our Online Products

Including eCLIPSE Ultimate Access™, CLSI's cloud-based, online portal that makes it easy to access our standards and guidelines—*anytime, anywhere.*

For more information, visit www.clsi.org today.

SAMPLE

SAMPLE

CLINICAL AND
LABORATORY
STANDARDS
INSTITUTE®

950 West Valley Road, Suite 2500, Wayne, PA 19087 USA

P: 610.688.0100 **Toll Free (US):** 877.447.1888 **F:** 610.688.0700

E: customerservice@clsi.org **www.clsi.org**

PRINT ISBN 1-56238-979-3

ELECTRONIC ISBN 1-56238-980-7