

AUTO11-A
Vol. 26 No. 33
Replaces AUTO11-P
Vol. 26 No. 5

IT Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard

This document provides a framework for communication of IT security issues between the IVD system vendor and the healthcare organization.

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



AUTO11-A
ISBN 1-56238-621-2
ISSN 0273-3099

Volume 26 Number 33

IT Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard

Andrzej J. Knafel, PhD
David Chou, MD
Bryan Crocker
Randy R. Davis
Eric Olson
Douglas O. Wood
Edwin O. Heierman, PhD

Abstract

Clinical and Laboratory Standards Institute document AUTO11-A—*IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard* specifies technical and operational requirements, as well as technical implementation procedures related to security of IVD systems (devices, analytical instruments, data management systems, etc.) installed at a healthcare organization. The intended users for this standard are vendors (IVD system manufacturers), users (e.g., laboratory personnel), and IT management of the healthcare organizations.

Clinical and Laboratory Standards Institute (CLSI). *IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard*. CLSI document AUTO11-A (ISBN 1-56238-621-2). Clinical and Laboratory Standards Institute, 940 West Valley Road, Suite 1400, Wayne, Pennsylvania 19087-1898 USA, 2006.

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 healthcare 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in technology may affect the procedures, methods, and protocols in a standard or guideline, users should replace outdated editions with the current editions of CLSI/NCCLS documents. Current editions are listed in the CLSI catalog, which is distributed to member organizations, and to nonmembers on request. If 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



Contents

Abstract	i
Committee Membership.....	iii
Foreword.....	vii
1 Scope.....	1
2 Definitions	1
2.1 Acronyms.....	1
3 Delineation of Vendor and HCO Responsibilities	2
4 Technical Design Guidelines Related to Regulatory Requirements	3
4.1 Preventing Unauthorized Application Usage.....	3
4.2 Preventing Unauthorized Data Access.....	8
4.3 Protection From Malicious Software	14
4.4 Security Monitoring.....	17
4.5 Preventing Loss of Data.....	19
5 Process and Operational Requirements.....	20
5.1 IT Security Requirements Engineering and Management	21
5.2 IT Security Hazard Analysis and Risk Management	21
5.3 Vendor System Validation/Verification	21
5.4 Vendor Security Audits/Assessments/Tests	21
5.5 Documents for HCO	21
5.6 Preventive Actions (software patches, virus definitions).....	22
6 Applicability to Device Classes	23
References.....	33
Additional References.....	34
Summary of Delegate Comments and Committee Responses	35
The Quality System Approach.....	42
Related CLSI/NCCLS Publications	43

Foreword

The IT security requirements related to various laboratory systems (devices, analytical instruments, data management systems, etc.) are growing, mainly caused by 1) new international regulations applicable to healthcare organizations,¹ 2) an increase in the degree of integration of the IVD systems in the IT environment of healthcare institutions, and 3) attacks observed in healthcare organizations from a multitude of sources.

The real and potential threats for the systems and the organizations are also growing. Listed below are several examples illustrating how systems could be compromised by malicious software/people:

- changing processed/static data (e.g., test applications, calibration), resulting in the production of incorrect results;
- stealing patient electronic health records by querying the LIS/HIS from compromised laboratory systems (e.g., laboratory instrument with CLSI/NCCLS document LIS2—*Specification for Transferring Information Between Clinical Laboratory Instruments and Information Systems* [formerly ASTM E1394] query protocol);
- stealing or manipulating patient/sample results from the system;
- damaging the IVD system software, requiring reinstallation and resulting in down-time for the user and service costs for the vendor;
- misusing the IVD system as a means for compromising other systems in the healthcare organization's IT environment; and
- misusing the IVD system as a means for entering the vendor's corporate network.

This document provides a framework for communication of IT security issues between the IVD system vendor and the healthcare organization.

Key Words

Access control, authentication, authorization, encryption, hardening, IT security

IT Security of *In Vitro* Diagnostic Instruments and Software Systems; Approved Standard

1 Scope

This standard specifies technical and operational requirements, as well as technical implementation procedures related to IT security of IVD systems (devices, analytical instruments, data management systems, etc.) installed at a healthcare organization. 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 (e.g., laboratory personnel), and IT management of healthcare organizations.

This standard is not intended for use as the final written policy for the healthcare organization. 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 ISO, IEEE, etc.

The suggested best practices contained in this document are based on the current state of technology at the time of publication. These best practices are distinguished from the requirements by 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 healthcare organization and vendor should clearly state in the corresponding contract how the standard would be applied during clinical trials.

2 Definitions

authentication – process of determining that an entity (someone or something) is the one claimed to be.

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

device end user – end user in the HCO familiar with the medical device and its operation.

healthcare organization (HCO) – all components of an organization where the IVD is installed.

IT support – customer support staff familiar with computer hardware, operating system software, commercial off-the-shelf (COTS) software components, and networking environment.

validation – confirmation, through the provision of objective evidence, that requirements for a specific intended use or application have been fulfilled (ISO 9000).²

verification – confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (ISO 9000).²

2.1 Acronyms

BIOS	basic input/output system
COTS	commercial off-the-shelf
CRC	cyclical redundancy check
DBMS	database management system

Related CLSI/NCCLS Publications*

- AUTO3-A** **Laboratory Automation: Communications with Automated Clinical Laboratory Systems, Instruments, Devices, and Information Systems; Approved Standard (2000).** This document provides standards to facilitate accurate and timely electronic exchange of data and information between the automated laboratory elements.
- AUTO9-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.
- LIS2-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.
- POCT1-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.

* Proposed-level documents are being advanced through the Clinical and Laboratory Standards Institute consensus process; therefore, readers should refer to the most current editions.