



Designation: E 1246 – 01

An American National Standard

Standard Practice for Reporting Reliability of Clinical Laboratory Information Systems¹

This standard is issued under the fixed designation E 1246; the number immediately following the designation indicates the year of original adoption or, in the case of revision, the year of last revision. A number in parentheses indicates the year of last reapproval. A superscript epsilon (ε) indicates an editorial change since the last revision or reapproval.

1. Scope

1.1 This practice describes a system for collecting data, maintaining records, and reporting on the reliability of operating clinical laboratory computer systems.² The reliability measure will be achieved by documenting the number, severity, cause, impact, and duration of the failures that a system experiences. This practice can be implemented with paper forms or computer records. The type of computer systems under consideration are those designed to assist the overall workflow of the laboratory, and generally include some or all of the functions of patient biographical data, test ordering, draw list printing, specimen check-in, workstation work list printing, test result entry, result verification, patient report printing, data archiving, quality control, and management report printing. This practice is applicable to all types of clinical laboratories, including major medical centers, teaching hospitals, community hospitals, referral clinics, emergency centers, health care maintenance organizations, specialty institutions, commercial laboratories, and private practices. The significance of portions of the reliability measure may be different in the different settings, but the measurement procedure is the same. This practice is not intended for computers inside instruments or for those systems designed to support a single workstation, although portions of this practice may be applicable.

1.2 *This standard does not purport to address all of the safety concerns, if any, associated with its use. It is the responsibility of the user of this standard to establish appropriate safety and health practices and determine the applicability of regulatory limitations prior to use.*

2. Referenced Documents

2.1 ASTM Standards:

E 792 Guide for Selection of a Clinical Laboratory Information Management System³

E 1029 Guide for Documentation of Clinical Laboratory

Information Management Systems³

E 1239 Guide for Description of Reservation/Registration-Admission, Discharge, Transfer (R-ADT) Systems for Electronic Health Record (EHR) Systems³

E 1639 Guide for Functional Requirements of Clinical Laboratory Information Management Systems³

E 1715 Practice for Object-Oriented Model for Registration, Admitting, Discharge and Transfer (RADT) Functions in Computer-based Patient Record Systems³

E 2118 Guide for Coordination of Clinical Laboratory Services in an Electronic Health Record Environment and Networked Architectures³

2.2 ISO Standards:

ISO IS 12207 Information Technology-Software Life Cycle Processes

ISO CD3 15288 System Life Cycle Processes

3. Significance and Use

3.1 *Use*—This practice is intended to be used by laboratory personnel on a regular ongoing basis. It is primarily intended for laboratory management to keep records on a system in regular operation. The information produced by this practice will also be useful to regulatory agencies, professional review groups, system maintainers, system manufacturers, and others who may be contemplating purchase of a similar system. It is expected that the reports produced by this standard practice will be saved as a part of the life cycle records for the system. This practice is one part of the activities of a system life cycle (see IS 12207 and CD3 15288) and in particular its operation and maintenance processes. A key part of system maintenance is documentation of defects and their effect upon the enterprise operations. This practice addresses ways to make use of the record-keeping needed to manage system maintenance.

3.1.1 This practice is not intended for those systems or parts of systems that are still in development or testing, and any failures caused by such testing shall not be included in the statistics.

3.1.2 This practice is not intended to cover problems due to system designs that do not meet user needs, either at the time of acceptance or because user needs have changed over time. It is expected that such immediate or potential problems will be identified and solved during verification, validation, and acceptance phases of the project (see CD3 15288).

¹ This practice is under the jurisdiction of ASTM Committee E31 on Healthcare Informatics and is the direct responsibility of Subcommittee E31.13 on Clinical Laboratory Information Management.

Current edition approved Nov. 10, 2001. Published February 2002. Originally published as E 1246–88. Last previous edition E 1246–88(1995).

² Prepared in cooperation with the College of American Pathologists.

³ *Annual Book of ASTM Standards*, Vol 14.01.



3.1.3 If this practice is referenced in a contract, it shall be referred to as the “Standard Practice for Reporting Reliability of Clinical Laboratory Computer Systems.” Vendors agreeing to supply reliability reports in accord with this standard practice shall meet all the requirements described herein, or shall provide a list of exceptions or alterations that is acceptable to the managers of the computer system, along with an explanation of how the purpose and integrity of this standard practice is maintained.

3.2 *Significance*—There are several advantages to the widespread adoption of a common practice for reporting clinical laboratory computer system reliability.

3.2.1 *Comparison of Different Systems*—A practice for reporting system reliability will permit comparison of systems offered by different vendors. When each vendor and each laboratory choose to define downtime differently and to follow different procedures for keeping reliability information, there is no easy way to compare the reliability of different systems. A commonly adopted reliability measure will allow:

3.2.1.1 Prospective buyers to compare reliability of different systems as a part of their selection process.

3.2.1.2 Prospective buyers to realistically determine for the systems under consideration the amount of redundancy, spare parts, and service support they would need to satisfy the reliability requirements of their particular operations.

3.2.1.3 Vendors to evaluate their product against the competition and to identify and correct areas that need improvement.

3.2.1.4 Vendor sales people to accurately represent the reliability of their product to prospective customers.

3.2.2 *System Purchase*—Demonstrated system reliability over an initial trial period is often included as one of the acceptance criteria items during purchase contract negotiations. Availability of a standard practice for reporting reliability will clarify that part of the contract and simplify that portion of the negotiations (Guide E 792).

3.2.3 *System Life Cycle*—All laboratories need to maintain records on system reliability and to periodically make reports on that reliability to institution administrators and outside reviewers (Guide E 1029) as part of the operation and maintenance processes and laboratory management. A standard practice for reporting reliability of the information system offers the laboratory the following advantages:

3.2.3.1 It reduces the planning effort needed to devise a separate reliability reporting scheme at each institution.

3.2.3.2 It results in a more uniform level of quality in the reliability reporting procedures used from institution to institution.

3.2.3.3 It provides the laboratory with an accepted tool to answer critics of information system reliability, both from the administration and from the users of the laboratory services.

3.2.3.4 It permits creation of an accepted definition of the time when repair or other remedial action is needed. When reliability drops below a specified level, then redesign, replacement of older components, retraining of users or repair people, or other corrective action is indicated. If such a definition becomes widely accepted, the laboratory will have less difficulty convincing administrators to allocate funds for upgrade

or convincing vendors to undertake the repairs.

3.2.4 *Reliability Standards and Reviews*—A standard measure of reliability makes it possible to determine national levels of normal or typical reliability of clinical laboratory information systems. This has several advantages:

3.2.4.1 Individual institutions may compare themselves against those standards to decide when to modify the system or alter the operating procedures.

3.2.4.2 Regulatory or professional review groups can use this information as a part of their evaluation.

3.2.4.3 Once national levels of reliability are determined, the medical laboratory community in cooperation with the suppliers can evaluate the average reliability of system components in the field and determine if it should be improved. If so, the data collected might help identify the areas of reliability that are most in need of improvement.

4. Downtime and Intermediate Events

4.1 In order to provide an operational definition of downtime, it is helpful to identify some individual events within a typical failure incident. Each of these events shall be assigned a time and date. The downtime, or time a system is inoperative in any way due to a failure, is defined as the interval from “failure occurrence” (see 4.2) to “resumption of normal operations” (see 4.11). Intermediate milestones make it possible to evaluate the quality of service and identify areas where improved service procedures are needed. The interval from “failure occurrence” (4.2) to “initial service contact” (4.4) is the time the end-user needed to recognize and act on the problem. From there to “start of diagnosis/repair” (4.8) is the service vendor response time. From “start of diagnosis/repair” to “completion of validation” (4.9) is the repair time. The interval from “completion of validation” to “resumption of normal operations” (4.11) is the time needed to recover the system.

4.2 *failure occurrence*—the time and date when the failure occurred marks the beginning of a failure incident. Sometimes the exact time of the failure can only be estimated.

4.3 *failure discovery*—often immediately, but perhaps some time after the failure happened, an operator becomes aware that a problem has developed. “Failure discovery” is the time and date when the system operator determines that there is a failure.

4.4 *failure documented*—the “failure documented” step is the time and date when basic information about the failure occurrence and associated information is recovered in a form useful to communicating to the support or service person. See Fig. 1.

4.5 *initial service contact*—the time and date when the system operator first attempts to secure the assistance of an appropriate service person is the “initial service contact” time. Several initial service contact times may be identified if maintenance is provided in layers. For example, there may be an in-house person who provides low- or intermediate-level service who is contacted first. If that person determines that the problem requires it, the system vendor or outside maintenance organization is subsequently contacted.

4.6 *end of service contact*—the time and date when the provider of service acknowledges a request for repair.



LABORATORY COMPUTER SYSTEM FAILURE REPORT

Institution name: _____

Computer system name: _____

Prepared by Name: _____

Job title: _____

FAILURE CATEGORY	TIME AND DATE HISTORY
Total loss of all function ☐	Failure occurrence _____
Loss of any primary function ☐	Failure discovery _____
Any primary function impaired ☐	Failure documented _____
Loss of any secondary function ☐	Initial service contact _____
Any secondary function impaired ☐	End of service contact _____
Loss of redundancy ☐	Initial service response _____
	Start diagnosis/repair _____
	End of diagnosis/repair _____
	Completion of validation _____
	Restart of operations _____
	Resume normal operations _____

DURATION OF THE FAILURE

PROBABLE CAUSE:

Hardware failure ☐	Software failure ☐	User/site problem ☐	Unknown cause ☐
---	---	--	--

Service Person _____ Job Title _____

Affiliation _____

Symptoms of the Problem: _____

Repairs Made: _____

Comments: _____

FIG. 1 Example Failure Report

next milestone. This may be considerably later than the initial service contact if busy telephones, answering services, or other communication problems are encountered. There may be more than one end of service contact time if maintenance is provided in layers.

4.7 *initial service response*—the time and date when an authorized service representative of the hardware/software maintenance provider contacts the user regarding the problem. This is the time when the nature of the problem is first discussed with a service person. It may or may not coincide with end of service contact (4.6).

4.8 *start of diagnosis/repair*—after being made aware of the problem, there will be a time and date when the service provider commences the evaluation of the reported failure and begins the diagnosis and repair.

4.9 *end of diagnosis/repair*—the next milestone is the time and date when the service provider reports to the user that the problem has been repaired. In the case of layered service, this may be the time when an in-house group reports that the problem requires the attention of an external service provider. In this case, there may be more than one pair of start and end times (4.8 and 4.9) for diagnosis and repair.

4.10 *completion of validation*—the next time and date identified is when diagnostic routines or application programs indicate that the problem has been corrected. This milestone represents the time at which all functions have been restored and validated. There still may be additional effort required of the user to restore and validate data that may have been lost or corrupted because of the failure.

4.11 *restart of operations*—when the user is able to exercise all previously disabled functions and execute application-dependent backup procedures. For some systems, this may mean reloading the backup database and reapplying records from the transaction log to the database. In other cases, the transactions lost since the last backup may be reentered manually.

4.12 *resumption of normal operations*—the failure event is over at the time and date when all normally scheduled tasks can be executed in their regular time frame. If the failure event was of long duration, it may require many hours from the “restart of operations” until database recovery is complete and normal operation is possible.

5. Classification of Failures

5.1 In the measurement of computer system reliability, it is important to recognize that some failures are more serious than others. Some failures only degrade performance or affect only a noncritical function, and do not require the laboratory to seek alternative methods to continue to accept test orders and turn out results. To achieve the objectives in Section 4, it is desirable to account for the more serious and the less serious failures separately. In this way, the standard reliability statistics can more properly reflect the impact of failures on the operation of the laboratory, which is the important objective of a standard measure of reliability. In this section, failures are classified into several types depending on whether they involve loss of primary function, secondary function, or redundancy.

5.2 *Primary Functions*—The primary purpose of a clinical laboratory system is to enhance patient care by providing measurement information about patients’ health conditions, including clinical decision support. It can do this by keeping records, assisting laboratory workflow, and improving communications by maintaining continuing information flow from the laboratory to the practitioner in all settings of care. A primary function is therefore any function directly related to providing patient care. Primary functions include:

- 5.2.1 Patient registration,
- 5.2.2 Test ordering,
- 5.2.3 Specimen collection,
- 5.2.4 Work list generation,
- 5.2.5 Result acquisition,
- 5.2.6 Result verification, including any quality control reports needed to help verify patient results,
- 5.2.7 Patient result reporting and posting,
- 5.2.8 Charge capture, but not charge reporting,
- 5.2.9 Inventory functions in blood bank,
- 5.2.10 Word processing functions in anatomical pathology,
- 5.2.11 Supply chain management,
- 5.2.12 Human resource management, and
- 5.2.13 Transaction logs or audit trails that backup the changes made to the database.

