Table 16. (Continued)

Policy	Processes	Procedures
States intent and direction for:	*Activities that transform the intent into action are:*	*Examples (not all inclusive) of documented instructions for:*
Integrity of data transfers and transmissions	• Process to verify data integrity	• Verifying data integrity at initial installation (see Subchapter 3.6) • Verifying data transfer accuracy after equipment maintenance or IT system downtime • Verifying data integrity after changes in equipment or software upgrades • Verifying formula calculations • Changing reference intervals • Electronic only: –Verifying data integrity after restoration of data files –Verifying integrity of system interface transmissions
Provision for information availability during downtime	• Process to manage system downtime	• Archiving and retrieving data • Troubleshooting error or event logs • Communicating significant software malfunctions • Establishing system backup and data storage protocols • Maintaining daily operations during a software malfunction • Incorporating downtime processes into the facility's disaster preparedness plan • Practicing system downtime procedures

Abbreviations: IT, information technology; QSE, quality system essential.

QSE Information Management incorporates the laboratory's commitment to quality and confidentiality in the flow of information. This QSE includes assessing information needs, planning and designing to meet those needs, maintaining the security and integrity of data and information, and disseminating information in a timely and accurate manner while meeting confidentiality requirements. Guidance for computer system hardware and software programs is provided in Subchapter 3.6. Guidance for paper-based recordkeeping systems is provided in Subchapter 3.8.

3.9.1 Planning for Information Needs

Information, and in particular examination results and reports, is the laboratory's final product. The laboratory needs to ensure that it has an effective information management system in place to achieve confidentiality of patient information and accessibility, accuracy, timeliness, and security.

NOTE:

This QSE includes assessing information needs, planning and designing to meet those needs, maintaining the security and integrity of data and information, and disseminating information in a timely and accurate manner while meeting confidentiality requirements.

The flow of information varies depending on the laboratory's scope of examinations and level of technology. Therefore, each laboratory needs to document how paper-based and electronic information moves through the path of workflow. This documentation includes how information is:

- Communicated (eg, available examinations and specimen collection requirements to laboratory customers)
- Received (eg, requests for examinations)
- Generated (eg, examination results)
- Disseminated (eg, release of results and reports)
- Manipulated (eg, transcription or transmission across an interface)

The flow of information related to the QSEs should also be documented, eg, when the laboratory is responding to a manufacturer's recall or customer complaint or preparing for an external accreditation assessment. (**NOTE:** Recalls and complaints are considered NCEs.)

When the laboratory is planning and developing the key elements of paper-based and/or electronic information management systems, some important elements to consider include the requirements for:

- ☑ Unique identifiers for patients and specimens
- ☑ Formatting of request forms and computer screens
- ☑ Logs and worksheets for recording all required results from performing the process or procedure, including amended and corrected results
- ☑ Unique identifiers of laboratory personnel
- ☑ Processes that ensure accuracy of manual data entry, data recording, and transmission, including date and time
- ☑ Protection against loss or unauthorized change of data and information
- ☑ Maintenance of confidentiality of protected patient information
- ☑ Effectiveness of reporting systems
- ☑ Accurate and effective paper and/or electronic reports to allow for proper interpretation of the results
- ☑ Effective and timely communications that are documented according to laboratory procedures

3.9.2 Confidentiality of Information

Laboratories need to incorporate commitment to confidentiality of patient-related information into their processes to manage incoming and outgoing information, whether written or electronic. Laboratories need to establish processes to handle requests for patient information from internal sources, as well as from external sources such as governmental agencies and accrediting organizations. These processes and procedures need to include all of the following:

- Completing confidentiality forms
- Receiving patient records and other materials from internal or external sources
- Handling requests from internal or external sources
- Releasing and transferring patient information or records to internal or external sources
- Managing clinical trial information (when applicable)
- Ensuring that all electronic transfers and transmissions of documents and information over a public network and the Internet have appropriate encryptions for security

3.9.3 Security for Data Access

To protect data and information from unauthorized access and use, the laboratory needs to establish and document processes and procedures for all of the following:

- Identifying which persons or groups are authorized to access and use the data and information
- Responding to external requests for release of information
- Changing access levels
- Defining how security breaches will be identified and the actions needed to prevent such breaches, whether paper or electronic[86]
  - **NOTE:** Breaches of security are considered NCEs.
- Defining the audit trail

The laboratory needs to consider the confidentiality of records with regard to all persons who can enter the laboratory (eg, cleaning and maintenance personnel). Additional consideration is needed for access to records at all off-site laboratory and records storage locations.

In addition to the information above, whenever electronic data systems are in use, the laboratory also needs to establish and document processes and procedures for:

- Identifying personnel who may perform specific functions in the information system
- Establishing appropriate security levels of computer access for each job title or individual user
- Establishing password configuration and frequency of change
- Changing passwords for computer access
- Changing and managing security levels
- Changing computer programs or interfaces
- Modifying software data files
- Amending verified results or interpretations, or supplementing with addenda

NOTE:

To avoid potential breaches of cybersecurity or confidentiality, use of personal e-mail to conduct business should not be allowed.

To avoid potential breaches of cybersecurity or confidentiality, use of personal e-mail to conduct business should not be allowed.

The processes and procedures for developing a cybersecurity network so that confidentiality of protected information can be maintained are described in the following subchapters.

3.9.3.1 Identification Function

The laboratory and organization should identify and manage cybersecurity risk to systems, assets, data, and capabilities. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables the laboratory and organization to focus and prioritize their efforts, consistent with risk management strategy and business needs.

3.9.3.2 Protection Function

The laboratory and organization should develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. This function supports the ability to limit or contain the effects of a potential cybersecurity event.

3.9.3.3 Detection Function

The laboratory and organization should develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. This function enables timely discovery of cybersecurity events.

3.9.3.4 Response Function

The laboratory and organization should develop and implement the appropriate activities to take action regarding a detected cybersecurity event. This function supports the ability to contain the effects of a potential cybersecurity event. When required, the laboratory needs to report a privacy breach to the person(s) whose health information has been breached.

3.9.3.5 Recovery Function

The laboratory and organization should develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired by a cybersecurity event. This function supports timely recovery to normal operations to reduce the effects of a cybersecurity event.

3.9.3.6 Other Information Management System Security Considerations

Computer programs also need to be adequately protected to prevent alteration or destruction by casual or unauthorized users.

Both paper and electronic processes should include an audit mechanism that allows for identification of any individual or system supplier who has entered or modified any data or files contained in the laboratory or its computer programs.

Security access levels define who may change, amend, or make an addendum to a verified result. Procedures for changing verified results are described in Subchapter 4.3.2.2.

One service's computer system (eg, laboratory, pharmacy, imaging, hospital) must not jeopardize the data security of the other services' systems. Therefore, appropriate security measures are needed to prevent unauthorized access to data and information in one computer system that can be accessed from other systems.

NOTE:

Security access levels define who may change, amend, or make an addendum to a verified result.

3.9.4 Integrity of Data Transfers and Transmissions

The laboratory often exchanges data with other paper or electronic systems. Data exchange can be a transfer or transmission, and although these terms are often used interchangeably, they are different. Data transfer implies that there is no direct connection between systems. For example, when a paper record is moved to a new paper source or an electronic document is copied to another file or disk, data are simply transferred to a different location. Data transmission indicates a direct connection between systems, either serial or network. Examples include a one-time download of existing electronic system data to a new electronic system, real-time information sent from an examination system to the laboratory system, and information sent from the laboratory system to an electronic medical record.

The laboratory needs processes to protect data integrity at all times.

In addition to ongoing regular review of data integrity, verification and documentation of data transfers and transmissions and review of calculations performed on patient data are needed in each of the following situations:

- At initial installation (see Subchapter 3.6)
- After equipment maintenance or downtime of laboratory (or other facility) systems
- After equipment changes
- For electronic systems:
  - After restoration of data files
  - After software updates

To detect errors in data entry, transfer, transmission, storage, or processing, data integrity may be verified by comparing patient information on reports and video displays with the original input at defined intervals.

Historical data protection needs to be verified whenever changes are made to laboratory examination parameters such as reference intervals, units, and host codes. When reference intervals or other laboratory tables are also maintained within the hospital information system, any laboratory changes need to be verified in the hospital system, as well.

3.9.5 Provision for Information Availability During Computer Downtime

Routine maintenance of the electronic information system should be scheduled in a way that minimizes interruption of patient care. Processes are needed to ensure that the laboratory's work operations and availability of patient results and reports will not be compromised should hardware or software failure occur. Such downtime processes and procedures need to be documented and periodically practiced. These processes should include development of a:

- Secure system to back up laboratory data
- Means to label and store data backup media to protect them from damage or unauthorized access and use
- Means to archive and retrieve data
- Notification process to alert the organization whenever significant hardware or software downtime occurs
- Process to maintain daily operations during a software or hardware malfunction
- Method for determining the cause of system downtime (eg, using the system log files to identify problem areas)
- Process to handle downtime on other systems

The laboratory's downtime process needs to be integrated into the overall organizational disaster preparedness plan (see CLSI document AUTO11[87]).

A flow diagram of how information moves through the laboratory and additional details about information management are provided in CLSI document QMS22.[88]

REMINDER:

See CLSI document QMS22[88] for guidance on information management in the laboratory.

3.10 Nonconforming Event Management

QSE Nonconforming Event Management describes processes to detect and document nonconformances, manage products and services that do not meet specified requirements, classify nonconformances for analysis, and correct the problems they represent. Table 17 summarizes the major requirements for QSE Nonconforming Event Management.

Table 17. Major Requirements for QSE Nonconforming Event Management

Policy	Processes	Procedures
States intent and direction for:	*Activities that transform the intent into action are:*	*Examples (not all inclusive) of documented instructions for:*
Reporting and investigation of each NCE	• Process to identify, report, and record an NCE	• Reporting and recording an NCE
	• Process to investigate an NCE	• Defining responsible personnel for conducting an NCE investigation • Recording and investigating a customer complaint
	• Process to make external notifications of NCEs	• Notifying clinicians and users of nonconforming examinations • Notifying regulatory agencies of NCEs when required
	• Process to respond to NCEs related to the manufacturer's products	• Notifying manufacturers of NCEs as necessary • Defining responsibilities for handling recalls • Removing nonconforming product from laboratory inventory • Recording action taken on recall of a nonconforming service • Completing the defective medical device reporting form • Completing the blood supplier's form for retrospective records review
Classification, analysis, and trending of the collected data and information	• Process to classify, analyze, and trend the aggregate NCE data and information collected	• Classifying an NCE • Tracking and trending NCE data • Analyzing NCE data
	• Process to report NCE information to management	• Preparing the NCE component of the quality report for management review

Abbreviations: NCE, nonconforming event; QSE, quality system essential.

REMINDER:

See CLSI document QMS11[89] for guidance on developing a laboratory NCE management program.

NCE management is linked to the laboratory's and the larger organization's risk management program, because it provides information on systematic service problems that could pose legal or financial risk for the organization.

The laboratory needs to maintain and use processes and procedures when it detects any aspect of its operations that does not conform to regulatory and accreditation requirements, its own procedures or QMS requirements, or agreed-on customer requirements. Reporting also includes NCEs that were identified and corrected before any harm occurred (ie, a "near miss").

An effective NCE management program records and analyzes information from NCEs to identify systematic problems for which continual improvement initiatives can be prioritized, resources allocated, and improvements implemented. Each laboratory needs processes to detect and document NCEs, classify them for analysis, and correct the problems they represent. CLSI document QMS11[89] provides guidance on developing a laboratory NCE management program.

3.10.1 Nonconforming Event Report and Investigation Process

Laboratory leadership needs to foster a culture that supports quality as the foundation for laboratory work. This culture needs to actively support open communication so that personnel at every level of the organization know how to report NCEs and feel comfortable doing so.

Open communication enables:

- Understanding and promoting a nonpunitive environment for reporting
- Linking the analysis of events to process improvements that will improve patient safety and patient care
- Providing education on the concepts of NCE management
- Increasing morale, which helps sustain ongoing, open communication

3.10.1.1 Managing an Individual Nonconforming Event

A nonconformance can be identified through any of the following means:

- Practitioner, patient, donor, or customer complaints
- Nonconforming QC or calibration results
- Nonconforming PT results
- Nonconforming patient examination results and reports
- Nonconforming instruments, reagents, or consumables
- Personnel comments or complaints
- Service alerts, manufacturer recalls, or field corrections
- Findings from internal or external audits
- Management reviews

Every person in the laboratory has a responsibility to report an identified NCE. A defined paper or electronic form provides for uniform reporting.

An NCE report form includes space for:

- Tracking number
- Date and time the NCE occurred
- Date and time the NCE was discovered
- Identity of person who discovered the NCE
- Description of what happened
- Immediate action taken
- Investigation into how and why the NCE occurred
- Additional actions, if any
- Assessment of the effectiveness of action(s) taken
- Classification of the event

An electronic spreadsheet or database facilitates documenting, sorting, tracking, and trending NCEs. Commercially available NCE management software is also available for laboratory use.

IMPORTANT NOTE:

Every person in the laboratory has a responsibility to report an identified NCE.

When the NCE involves nonconforming examination results, additional activities are needed, such as:

- Consideration of the medical significance of any nonconforming examinations
- Notification of the requesting health care practitioner
- Halting of nonconforming examinations, withholding of reports, and review/revision of results already released
- Recall or identification of any nonconforming examination results, when necessary
- Definition of additional actions to take
- Designation of personnel responsible for resolving the problem
- Definition of responsibility for resuming examination

The course of action taken in response to the NCE depends on the severity of the issue and the risk to patients, customers, or personnel. A risk assessment helps direct resources to where they are most effective and determines what actions are needed. A high-risk NCE might necessitate an RCA to ensure the root cause is identified and removed to reduce or eliminate recurrence.

REMINDER:

See CLSI document QMS11[89] for guidance on responding to medical device notifications.

NOTE:

Problems identified by the laboratory with equipment or other medical devices need to be reported to the manufacturer and, as applicable, to the appropriate governmental or accreditation organization.

3.10.1.2 Nonconforming Events Related to Manufacturer's Products

Externally generated notifications of medical device hazards and recalls require special handling processes and procedures. The process to handle these notifications is similar to responding to an individual NCE. CLSI document QMS11[89] provides guidance for the laboratory to respond to medical device notifications. Examples include a manufacturer's recall of instruments or reagents and a blood supplier's recall of blood products.

A process is needed to recall the laboratory's products or services as soon as the laboratory becomes aware of a problem. Examples include:

- NCEs related to blood products issued by the laboratory
- Recalls of erroneous information in a guide to laboratory services
- Recall of laboratory-provided specimen collection kits

Problems identified by the laboratory with equipment or other medical devices need to be reported to the manufacturer and, as applicable, to the appropriate governmental or accreditation organization. The equipment needs to be taken out of service, labeled as out of service, and decontaminated before shipping when appropriate, and the actions need to be recorded. When a medical device NCE involves examination results, the steps described in Subchapter 3.10.1.1 need to be followed.

3.10.2 Classification, Analysis, and Trending of the Data and Information Collected

Identifying, investigating, and classifying NCEs leads to rapid identification of:

- A lack of documented processes, procedures, or instructions
- Documented processes or procedures not being followed
- The QSE or path of workflow processes that are causing the most problems

Classification of NCEs is necessary to generate information that facilitates performance improvement. By using a standardized classification system, information can be compared across time. For example, NCEs could be classified by the preexamination, examination, or postexamination process in which they occurred. Specimen NCEs could be subclassified as wrong container type, mislabeled, unlabeled, etc.

The NCEs can be sorted according to their classifications, and the sorted information can be presented in pie charts, Pareto charts, or other graphical formats. NCE data are also meaningful when presented as a ratio of numerator (eg, number of occurrences, number of unacceptable specimens) to denominator (eg, number of examinations, number of patients, or number of specimens received).

Data can be tracked and analyzed in several different ways, such as:

- Across time (eg, by quarter or year)
- Laboratory discipline
- Severity level
- Location
- Type of event
- Classification of event
- Date, time, and shift of occurrence
- Location vs event type
- Location vs person involved
- Action taken

Summary reports of information derived from analyzing NCEs need to be regularly reviewed by laboratory management. The laboratory needs to record the decisions made and actions taken in these management reviews. Decisions needed include both prioritizing problems to resolve and allocating resources for the problem resolution efforts, which, in turn, leads to recommending process improvement projects. CLSI document QMS06[85] provides an overview of methods commonly used for making quality improvements in laboratory processes to increase the likelihood of desired outcomes.

REMINDER:

See CLSI document QMS06[85] for an overview of methods commonly used for making quality improvements in laboratory processes.