UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
RESEARCH TRIANGLE PARK, NC 27711
OFFICE OF AIR QUALITY PLANNING AND STANDARDS

Technical Note- Use of Electronic Logbooks for Ambient Air Monitoring

04/20/2016

The use and storage of electronic information is increasing at ever faster paces in our environment. Real time ambient air data is now being posted on PC and smart phones that allows the public instant access to this information. Funding transactions are occurring on smart phones and electronic signatures are legally binding[1]. Virtually all air monitoring programs collect, validate and certify data electronically using new generation data logging and transmittal systems. This demonstrates progress from our analog information management systems where monitoring organizations reviewed strip charts to determine concentrations and evaluate data quality. An area where more progress can be made in the ambient air monitoring program is the entry and storage of logbook information in electronic formats.

Goal

The purpose of this guidance is to establish minimum requirements for documenting and maintaining electronic logbook (e-logbook) information for the Ambient Air Monitoring Program. This document is not intended to be inclusive of all electronic records initiatives presently being conducted in the EPA, but rather is seen as a starting point for an e-logbook practice to ensure some consistency across all the monitoring organizations utilizing e-logbooks for ambient air monitoring in accordance with 40 CFR Part 58.

Adherence and implementation of this e-logbook guidance is the ultimate responsibility of the monitoring organization lead (MOL) with assistance from the quality assurance (QA) manager and records manager[2]. A monitoring program can maintain both paper and electronic information. Storage and archiving of all records are the responsibility of the MOL and must be documented or referenced in the monitoring organizations quality management plan (QMP) and quality assurance project plan (QAPP) and be available for external review.

OAQPS supports the use of electronic data collection systems for the collection of ambient air logbook information in a manner that ensures that:

- The system has adequate levels of security and administration to ensure e-logbook data cannot be tampered with and have adequate levels of backup (i.e., frequency and multiple storage locations)

[1] http://www.gpo.gov/fdsys/pkg/BILLS-106s761enr/pdf/BILLS-106s761enr.pdf
https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/esign-guidance.pdf
[2] QMP or QAPP would identify individuals responsible for managing the e-logbook system.

- Personnel entering or editing information are uniquely identified and have been given authority to enter/edit. A list of the personnel, their authority and access privileges should be included or referenced in the organizations QA documentation (QAPP/QMP) and be available to EPA. E-signatures are strongly suggested for use.
- Every logbook entry/edit (entry session[3]) is date/time stamped and the entry person identified.
- Original entries are recorded and archived. Initial entries are not erased when revisions (edits to previous entries in a different entry session) are made. This ensures an audit trail is available for all entries.

Scope of Document

This guidance document addresses the use of e-logbooks for the Ambient Air Monitoring Program described in 40 CFR Part 58. This document will provide a background of the monitoring program, the traditional use of logbooks, and the minimum features necessary for monitoring organizations to migrate towards an e-logbook system if they so desire. Traditional use of hardcopy logbooks remains an acceptable practice and this guidance simply provides an alternative approach.

Authority

EPA Regional Offices, as part of QMP/QAPP review and implementation of technical systems audits, will be responsible for ensuring that implementation of e-logbooks meet the minimum requirements described in this document.

Background -Ambient Air Monitoring Networks and Monitoring Objectives

Between the years 1900 and 1970, the emission of six principal pollutants increased significantly. The principal pollutants, also called criteria pollutants are: particulate matter (PM10 and PM2.5), sulfur dioxide, carbon monoxide, nitrogen dioxide, ozone, and lead. In 1970, the Clean Air Act (CAA) was signed into law. The CAA and its amendments provide the framework for the protection of air quality. As part of this framework, EPA establishes and periodically revises National Ambient Air Quality Standards (NAAQS) for the criteria pollutants, and the Agency has established requirements for monitoring networks for these pollutants. 40 CFR Part 58, Appendix D requires that monitoring networks be designed for three basic monitoring objectives:

- to provide air pollution data to the general public in a timely manner
- to support compliance with ambient air quality standards (primary and secondary) and emission strategy development
- to support air pollution research studies

Most of the ambient air monitoring sites have been implemented to support NAAQS decisions. The monitoring data and its associated data quality attributes, including logbooks, are used in decisions regarding the status of areas' attainment or nonattainment of the NAAQS and as such our quality systems and record keeping processes must ensure that our ambient air measurements and its associated data quality information are credible, reliable and legally defensible. Much of the documentation that is used to verify that monitoring sites are properly located and maintained and that

[3] An entry session is defined as a unique data collection period when e-logbook information is entered into the system either through automated means (i.e., from automated instruments or a data logger) or by a site operator where a date/time stamp and a unique identifier of the entry person is recorded.

field monitors/samplers and analytical instruments are meeting regulations for method implementation and data quality is located in logbooks. These logbooks come in many forms and include:

Site Logbooks -observations upon visiting a site, site evaluations against regulatory siting criteria, scheduled maintenance activities, instrumentation and consumable inventories (i.e., gas standard expiration dates and quantities left etc.).

Instrument logbooks- logbooks associated with each sampler or monitor that contain specific routine maintenance information, repairs, quality control checks, verifications, calibration etc. In many cases this instrument logbook "travels" with the instrument as it is transported to and from monitoring sites for repair or calibration.

Laboratory Logbooks- Similar to logbooks utilized in the field, laboratory logbooks are maintained in analytical laboratories for overall maintenance of the lab, as well as maintenance of analytical equipment, quality control checks, calibrations, and standards.

This guidance does not require separate e-logbooks for each type of logbook used in a monitoring organization. Monitoring organizations may develop e-logbook systems that combine a number of logbook types into one program. In addition, some monitoring organizations may have systems that include both hardcopy and e-logbooks.

A discussion of logbooks can be found in the *QA Handbook for Ambient Air Measurements Systems*[4] including references to a number of good sources of information on how to develop and implement logbooks. Some monitoring organizations use logbooks in a free-form note style to provide a record of the activities that were performed at a site and a lab on a particular day. Some use standardized forms that provide for consistent implementation of specific activities at specific frequencies across all sites in a monitoring network. In either case, the advantage of the logbook is to be able to directly document what has occurred during a work session and be able to review earlier events/activities at a site or with a particular instrument. This can be important for sites that are remote and cannot be accessed through internet or other means. However, with the advent of PCs and tablets and better communication to central office information management (IM) systems, the advantages of having a hardcopy logbook at the site has diminished and they have some of the following drawbacks:

- With only one version (unless scanned frequently), logbooks can be destroyed and damaged to a point of being illegible, and can be lost.
- Data is not available to anyone without traveling to the site.
- Quantitative assessment of logbook data is not easily accomplished without additional data entry which could lead to entry errors.
- Events and dates can be falsified since there is no electronic timestamp on when someone was actually at the site to perform required activities.

Hardcopy logbooks traditionally had some advantages that will need to be satisfactorily addressed with e-logbooks:

- Once written down (non-erasable pen is required) a hardcopy logbook can't be erased and entry errors must be crossed out and initialed. In an e-logbook open entry session[5], entries need to be

[4] http://www.epa.gov/ttnamti1/files/ambient/pm25/qa/QA-Handbook-Vol-II.pdf

[5] Entry session is the time when an E-logbook is open for entry until it is saved. Depending on the sophistication of the system each entry might be initialed and saved or the system might be open for multiple entries before being saved.

developed in a way that they are saved upon entry not just at the end of a full session. This also minimizes any data loss if the log system crashes during an entry session.

- Many types of logbooks are kept at the monitoring site so one can expect that a logbook entry will occur at the site where the work is performed. E-logbooks can achieve this by recording location information of an entry session.
- Logbook pagination allows for one to evaluate the chronology of information collection and can identify when information has been deleted (e.g., a page is missing from the logbook). Using an entry system with date and time stamp will satisfy this issue. Backing up e-logs system (an advantage over hardcopy logbooks) will minimize data loss or deletion as long as there is good security against tampering.
- Handwritten logs (signed/initialed) are difficult (but not impossible) to falsify. Good password secure e-logbooks systems, including use of secondary authenticating factors, can protect electronic data from fraudulent activity.

The goal of this document is to ensure that the salient features of good logbook practices are presented so that e-logbook data is captured and maintained in a manner that is secure, tamper proof, and legally defensible.

Minimum Requirements

An e-logbook system should meet National Archives and Records Administration (NARA)[6] requirements that pertain to e-logbooks. The e-logbook system should and be able to: 1) collect, organize, and categorize, and 2) facilitate the preservation, retrieval, use, and disposition of records. Attachment A provides the current version (2015) of this federal regulation for informational purposes. Although not all of the regulation pertains to e-logbooks, many of the requirements described are applicable to e-logbooks and are included in the information provided below. EPA acknowledges that monitoring organizations may also have local records policies, and they will need to ensure their system meets the need of both EPA & their own policies.

Much of the information that follows comes from the website: *Basic Requirements of an Electronic Recordkeeping System at EPA*[7] and are the features that must be addressed when developing or evaluating an e-logbook system for data defensibility. This information needs to either be included or referenced in the monitoring organizations QMP or QAPP in order for the EPA approving authority to be able to review and approve the e-logbook process as adequate.

- **Integrity** - The system must ensure the integrity of the records it manages and be able to:
  - Minimize the risk of unauthorized alteration or erasure of the records.
  - Allow only authorized personnel access to the records in the system.
  - Allow only authorized personnel to perform administrative functions such as creating or deleting directories, altering the parameters of metadata fields, and assigning access rights.
  - Ensure system security through the use of rigorous passwords and authenticating factors (challenge questions).
  - Ensure that locational information of entry session is recorded.

[6] National Archives and Records Administration (NARA) regulations at 36 CFR Part 1236 Electronic Records Management including Subparts B and C .

[7] http://www.epa.gov/records/tools/erks.htm

- **Metadata/Identity** - Identify each record sufficiently to enable authorized personnel to retrieve, protect, and carry out the disposition of the records in the system. Appropriate identifying information may include:
    - Organization of origin
    - site ID
    - date
    - code for type of logbook file or form
    - key words for retrieval- i.e., site common name , logbook form name etc.
    - addressee (if any)
    - author- person completing the form (entry session) and unique identifier(s) of that person
    - Record of review/approval of data, if required
    - authorized disposition (coded or otherwise)
    - security classification (if applicable).

- **Backup** -The system must allow for records to be backed up to protect against information loss and be able to:
    - Be backed up on a regular basis (e.g., nightly) to safeguard against the loss of information due to equipment malfunctions or human error.
    - Provide for recovery of the records that have been copied during the backup.
    - Allow duplicate copies of records to be maintained in storage areas separate from the location of the records that have been copied.

- **Organization/Delegations-** The e-logbook system should be documented in a manner that identifies roles and responsibilities for:
    - System development and maintenance
    - System administration and access authority
    - Logbook entry at designated sites and laboratory facilities
    - Logbook review auditing personnel
    - Password codes and protection from unauthorized users

- **Accessibility**- The system should document the process of providing access to various monitoring organization personnel such as site operators, lab personnel, QA staff, independent auditors, management and system administrators, as well as detail the “levels” of access or permissions (read/write authority) each group might have.

- **Retrievability** -The system must retrieve records and be able to:
    - Permit easy retrieval in a timely fashion
    - Ensure that records are accessible by individuals who have a business need for information in the records
    - Provide a method for all authorized users of the system to retrieve desired documents
    - Permit retrieval of both individual records and groupings of related records

- **Migration**-The system must allow records to be migrated and be able to:
    - Retain the records in a universal or similar format for their required retention period and until their authorized disposition date.
    - Ensure that information is not lost because of changing technology or deterioration.
    - Allow for the conversion of storage media to provide compatibility with current hardware and software.
    - Maintain a link between records and their metadata through conversion or migration.

- Ensure that the authorized disposition of the records can be implemented after conversion.

- **Auditability-**The system should be developed and documented in a manner that it can be tested (hardware and software) and reviewed by information technology experts and QA auditing personnel both internal and external to the monitoring agency.

- **American with Disability Act (ADA) Compliance** – The e-logbook system should meet ADA[8] standards.

- **e-Signatures/Legal signatures[9]**- E-signatures are accepted practice[10] and must be considered for use as part of the submission process and the legal defensibility of e-logbook information. The system may be based on the set-up of secure password systems. The system should identify the individuals that are authorized to perform activities that generate e-logbook information.

- **Information Security/Locking -** Once data from an entry session has been generated and transmitted, it must be immediately secured as an official record. It must also comply with EPA and federal requirements for safeguarding information resources and confidential business information, if applicable. Information about the program developers as well as the users should be stored. There should be a log of developer rights and developer changes to the programs.

- **Data entry/data revision/correction-** An entry session may be recalled and revised. However, those capable of revising the entry should be limited and be identified in the software system (i.e. originator, manager). In addition, the revision cannot overwrite the original information which must be maintained in the record.

- **Version Control**- E-logbooks will change and be revised over time. Version control of e-logbook software must be maintained. Each program or file should have a version number so that updates can be tracked over time. Agency personnel must be aware of the version that is current and in use at all times especially if the software is not located on a central IM system. A process of keeping users aware about versions in use must be developed. As software (i.e., MS Office) continues to be updated, there are often times compatibility issues. Monitoring organizations need to be vigilant about this if a system/program/file is developed in a constantly changing environment.

[8] http://www.section508.gov/summary-section508-standards http://www.ada.gov/

[9] Valid electronic signature refers to an electronic signature on an electronic document that has been created with an electronic signature device. The identified signatory is uniquely entitled to use the signature device for signing that document provided that this device has not been compromised, and where the signatory is an individual who is authorized to sign the document by virtue of his or her legal status or his or her relationship to the entity on whose behalf the signature is executed.

[10] http://www.gpo.gov/fdsys/pkg/BILLS-106s761enr/pdf/BILLS-106s761enr.pdf

Attachment A

National Archives and Records Administration (NARA) regulations at 36 CFR Part 1236 Electronic Records Management including Subparts B and C .

The following section represents the 2015 version of this document which can be found on e-CFR[11] . This regulation does not pertain exclusively to electronic logbooks but since electronic log books are part of an electronic information systems, some of the features/requirements described below are considered in the guidance above for the development of an acceptable e-logbook system.

[11] http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title40/40tab_02.tpl

PART 1236—ELECTRONIC RECORDS MANAGEMENT

Contents

Authority: 44 U.S.C. 2904, 3101, 3102, and 3105.

Source: 74 FR 51014, Oct. 2, 2009, unless otherwise noted.

Subpart A—General

§1236.1 What are the authorities for part 1236?

The statutory authority for this part is 44 U.S.C. 2904, 3101, 3102, and 3105. OMB Circular A-130, Management of Federal Information Resources, applies to records and information systems containing records.

§1236.2 What definitions apply to this part?

(a) See §1220.18 of this subchapter for definitions of terms used throughout Subchapter B, including part 1236.

(b) As used in part 1236—

Electronic information system means an information system that contains and provides access to computerized Federal records and other information.

Electronic mail system means a computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, and word processing documents not transmitted on an e-mail system.

Metadata consists of preserved contextual information describing the history, tracking, and/or management of an electronic document.

Unstructured electronic records means records created using office automation applications such as electronic mail and other messaging applications, word processing, or presentation software.

§1236.4 What standards are used as guidance for this part?

These regulations conform with ISO 15489-1:2001. Paragraph 9.6 (Storage and handling) is relevant to this part.

§1236.6 What are agency responsibilities for electronic records management?

Agencies must:

(a) Incorporate management of electronic records into the records management activities required by parts 1220-1235 of this subchapter;

(b) Integrate records management and preservation considerations into the design, development, enhancement, and implementation of electronic information systems in accordance with subpart B of this part; and

(c) Appropriately manage electronic records in accordance with subpart C of this part.

Subpart B—Records Management and Preservation Considerations for Designing and Implementing Electronic Information Systems

§1236.10 What records management controls must agencies establish for records in electronic information systems?

The following types of records management controls are needed to ensure that Federal records in electronic information systems can provide adequate and proper documentation of agency business for as long as the information is needed. Agencies must incorporate controls into the electronic information system or integrate them into a recordkeeping system that is external to the information system itself (see §1236.20 of this part).

(a) Reliability: Controls to ensure a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

(b) Authenticity: Controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

(c) Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.

(d) Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

(e) Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record;

(f) Context: Mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending upon the business, legal, and regulatory requirements of the business activity; and

(g) Structure: controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

§1236.12 What other records management and preservation considerations must be incorporated into the design, development, and implementation of electronic information systems?

As part of the capital planning and systems development life cycle processes, agencies must ensure:

(a) That records management controls (see §1236.10) are planned and implemented in the system;

(b) That all records in the system will be retrievable and usable for as long as needed to conduct agency business (i.e., for their NARA-approved retention period). Where the records will need to be retained beyond the planned life of the system, agencies must plan and budget for the migration of records and their associated metadata to new storage media or formats in order to avoid loss due to media decay or technology obsolescence. (See §1236.14.)

(c) The transfer of permanent records to NARA in accordance with part 1235 of this subchapter.

(d) Provision of a standard interchange format (e.g., ASCII or XML) when needed to permit the exchange of electronic documents between offices using different software or operating systems.

§1236.14 What must agencies do to protect records against technological obsolescence?

Agencies must design and implement migration strategies to counteract hardware and software dependencies of electronic records whenever the records must be maintained and used beyond the life

of the information system in which the records are originally created or captured. To successfully protect records against technological obsolescence, agencies must:

(a) Determine if the NARA-approved retention period for the records will be longer than the life of the system where they are currently stored. If so, plan for the migration of the records to a new system before the current system is retired.

(b) Carry out upgrades of hardware and software in such a way as to retain the functionality and integrity of the electronic records created in them. Retention of record functionality and integrity requires:

(1) Retaining the records in a usable format until their authorized disposition date. Where migration includes conversion of records, ensure that the authorized disposition of the records can be implemented after conversion;

(2) Any necessary conversion of storage media to provide compatibility with current hardware and software; and

(3) Maintaining a link between records and their metadata through conversion or migration, including capture of all relevant associated metadata at the point of migration (for both the records and the migration process).

(c) Ensure that migration strategies address non-active electronic records that are stored off-line.

Subpart C—Additional Requirements for Electronic Records

§1236.20 What are appropriate recordkeeping systems for electronic records?

(a) General. Agencies must use electronic or paper recordkeeping systems or a combination of those systems, depending on their business needs, for managing their records. Transitory e-mail may be managed as specified in §1236.22(c).

(b) Electronic recordkeeping. Recordkeeping functionality may be built into the electronic information system or records can be transferred to an electronic recordkeeping repository, such as a DoD-5015.2 STD-certified product. The following functionalities are necessary for electronic recordkeeping:

(1) Declare records. Assign unique identifiers to records.

(2) Capture records. Import records from other sources, manually enter records into the system, or link records to other systems.

(3) Organize records. Associate with an approved records schedule and disposition instruction.

(4) Maintain records security. Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.

(5) Manage access and retrieval. Establish the appropriate rights for users to access the records and facilitate the search and retrieval of records.

(6) Preserve records. Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business and to meet NARA-approved dispositions. Agencies must develop

procedures to enable the migration of records and their associated metadata to new storage media or formats in order to avoid loss due to media decay or technology obsolescence.

(7) Execute disposition. Identify and effect the transfer of permanent records to NARA based on approved records schedules. Identify and delete temporary records that are eligible for disposal. Apply records hold or freeze on disposition when required.

(c) Backup systems. System and file backup processes and media do not provide the appropriate recordkeeping functionalities and must not be used as the agency electronic recordkeeping system.

§1236.22 What are the additional requirements for managing electronic mail records?

(a) Agencies must issue instructions to staff on the following retention and management requirements for electronic mail records:

(1) The names of sender and all addressee(s) and date the message was sent must be preserved for each electronic mail record in order for the context of the message to be understood. The agency may determine that other metadata is needed to meet agency business needs, e.g., receipt information.

(2) Attachments to electronic mail messages that are an integral part of the record must be preserved as part of the electronic mail record or linked to the electronic mail record with other related records.

(3) If the electronic mail system identifies users by codes or nicknames or identifies addressees only by the name of a distribution list, retain the intelligent or full names on directories or distributions lists to ensure identification of the sender and addressee(s) of messages that are records.

(4) Some e-mail systems provide calendars and task lists for users. These may meet the definition of Federal record. Calendars that meet the definition of Federal records are to be managed in accordance with the provisions of GRS 23, Item 5.

(5) Draft documents that are circulated on electronic mail systems may be records if they meet the criteria specified in 36 CFR 1222.10(b) of this subchapter.

(b) Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system.

(c) Agencies may elect to manage electronic mail records with very short-term NARA-approved retention periods (transitory records with a very short-term retention period of 180 days or less as provided by GRS 23, Item 7, or by a NARA-approved agency records schedule) on the electronic mail system itself, without the need to copy the record to a paper or electronic recordkeeping system, provided that:

(1) Users do not delete the messages before the expiration of the NARA-approved retention period, and

(2) The system's automatic deletion rules ensure preservation of the records until the expiration of the NARA-approved retention period.

(d) Except for those electronic mail records within the scope of paragraph (c) of this section:

(1) Agencies must not use an electronic mail system to store the recordkeeping copy of electronic mail messages identified as Federal records unless that system has all of the features specified in §1236.20(b) of this part.

(2) If the electronic mail system is not designed to be a recordkeeping system, agencies must instruct staff on how to copy Federal records from the electronic mail system to a recordkeeping system.

(e) Agencies that retain permanent electronic mail records scheduled for transfer to the National Archives must either store them in a format and on a medium that conforms to the requirements concerning transfer at 36 CFR part 1235 or maintain the ability to convert the records to the required format and medium at the time transfer is scheduled.

(f) Agencies that maintain paper recordkeeping systems must print and file their electronic mail records with the related transmission and receipt data specified by the agency's electronic mail instructions.

§1236.24 What are the additional requirements for managing unstructured electronic records?

(a) Agencies that manage unstructured electronic records electronically must ensure that the records are filed in a recordkeeping system that meets the requirements in §1236.10, except that transitory e-mail may be managed in accordance with §1236.22(c).

(b) Agencies that maintain paper files as their recordkeeping systems must establish policies and issue instructions to staff to ensure that unstructured records are printed out for filing in a way that captures any pertinent hidden text (such as comment fields) or structural relationships (e.g., among worksheets in spreadsheets or other complex documents) required to meet agency business needs.

§1236.26 What actions must agencies take to maintain electronic information systems?

(a) Agencies must maintain inventories of electronic information systems and review the systems periodically for conformance to established agency procedures, standards, and policies as part of the periodic reviews required by 44 U.S.C. 3506. The review should determine if the records have been properly identified and described, and if the schedule descriptions and retention periods reflect the current informational content and use. If not, agencies must submit an SF 115, Request for Records Disposition Authority, to NARA.

(b) Agencies must maintain up-to-date documentation about electronic information systems that is adequate to:

(1) Specify all technical characteristics necessary for reading and processing the records contained in the system;

(2) Identify all inputs and outputs;

(3) Define the contents of the files and records;

(4) Determine restrictions on access and use;

(5) Understand the purpose(s) and function(s) of the system;

(6) Describe update cycles or conditions and rules for adding, changing, or deleting information in the system; and

(7) Ensure the timely, authorized disposition of the records.

§1236.28 What additional requirements apply to the selection and maintenance of electronic records storage media for permanent records?

(a) Agencies must maintain the storage and test areas for electronic records storage media containing permanent and unscheduled records within the following temperature and relative humidity ranges:

(1) Temperature—62° to 68 °F.

(2) Relative humidity—35% to 45%.

(b) Electronic media storage libraries and test or evaluation areas that contain permanent or unscheduled records must be smoke-free.

(c) For additional guidance on the maintenance and storage of CDs and DVDS, agencies may consult the National Institute of Standards and Technology (NIST) Special Publication 500-252, Care and Handling of CDs and DVDs at http://www.itl.nist.gov/iad/894.05/papers/CDandDVDCareandHandlingGuide.pdf, contact phone number (301) 975-6478.

(d) Agencies must test magnetic computer tape media no more than 6 months prior to using them to store electronic records that are unscheduled or scheduled for permanent retention. This test should verify that the magnetic computer tape media are free of permanent errors and in compliance with NIST or industry standards.

(e) Agencies must annually read a statistical sample of all magnetic computer tape media containing permanent and unscheduled records to identify any loss of data and to discover and correct the causes of data loss. In magnetic computer tape libraries with 1800 or fewer tape media, a 20% sample or a sample size of 50 media, whichever is larger, should be read. In magnetic computer tape libraries with more than 1800 media, a sample of 384 media should be read. Magnetic computer tape media with 10 or more errors should be replaced and, when possible, lost data must be restored. All other magnetic computer tape media which might have been affected by the same cause (i.e., poor quality tape, high usage, poor environment, improper handling) must be read and corrected as appropriate.

(f) Before the media are 10 years old, agencies must copy permanent or unscheduled data on magnetic records storage media onto tested and verified new electronic media