U.S. ENVIRONMENTAL PROTECTION AGENCY
OFFICE OF INFORMATION RESOURCES MANAGEMENT
RESEARCH TRIANGLE PARK, NORTH CAROLINA 27711

DRAFT

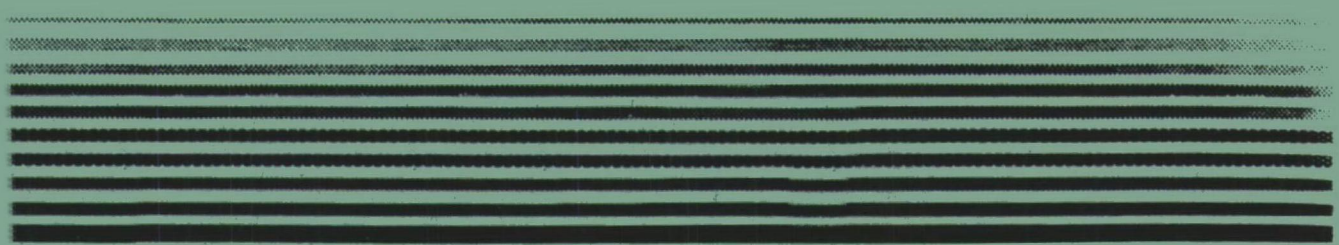
AUTOMATED LABORATORY STANDARDS: EVALUATION OF THE STANDARDS AND PROCEDURES USED IN AUTOMATED CLINICAL LABORATORIES

CONTRACT 68-W9-0037, DELIVERY ORDER 035
MAY 1990

Prepared by:

BOOZ·ALLEN & HAMILTON Inc.

4330 East-West Highway
Bethesda, Maryland 20814-4455
301/951-2200



Automated Laboratory Standards:

Evaluation of the Standards and Procedures Used in Automated Clinical Laboratories

DRAFT

Prepared for:

Office of Information Resources Management
U.S. Environmental Protection Agency
Research Triangle Park, North Carolina 27711

May 29, 1990

Prepared by:

BOOZ•ALLEN & HAMILTON Inc.
4330 East-West Highway
Bethesda, Maryland 20814
(301) 951-2200

Contract No. 68-W9-0037

Table of Contents

Executive Summary

The U.S. Environmental Protection Agency (EPA) has initiated a program to ensure the integrity of computer-resident data in laboratories performing analyses in support of EPA programs by developing standards for automated laboratory processes. The possession of sound technical data provides a fundamental resource for EPA's mission to protect public health and the environment.

This report describes the findings of a review of standards and practices used in existing automated systems in a limited number of laboratories in a clinical setting. These laboratories conduct either standard clinical pathology/clinical chemistry analyses or forensic determination of the presence of illicit drugs in urine specimens for commercial or government (military and civilian) clients. EPA has chosen to study clinical laboratory standards and practices under the assumption that such laboratories generate data of high integrity. Additionally, these laboratories are regulated by a number of Federal and state agencies, as well as being supported or accredited by a number of professional organizations. Both the regulatory agencies and the associations provide a variety of requirements, standards, and guidance for the clinical laboratories to follow in their day-to-day operations.

Representatives of six forensic drug testing laboratories were interviewed to determine the standards, practices, and control techniques used in each facility. Through this evaluation, it was determined that the drug testing program that serves the needs of the U.S. Army, the Department of Transportation, and the Department of Health and Human Services, as well as some private clients, contains standards for procedures and safeguards that could serve as models for EPA's computerized data acquisition and analysis systems. These standards follow the spirit of the Good Laboratory Practice standards already published by EPA for the Federal Insecticide, Fungicide, and Rodenticide Act and the Toxic Substances Control Act. These standards should be considered by the EPA in drafting standards on computer operations, software design, sample custody, and computerized analytical chemistry operations for both EPA laboratories as well as contractors

conducting analytical chemistry work for EPA under any of its environmental monitoring programs.

Additionally, many of the drug testing laboratories surveyed have implemented extensive security practices that help maintain the integrity of their manual and computer-resident data. These include strict chain-of-custody procedures (with a manual record and signatures) as well as a detailed manual audit trail or computer-resident transaction log providing the audit trail. Also, individual terminals could be permanently locked out of certain data sets or could access files only at certain times of the day, corresponding with normal hours of operation. By using these and other control mechanisms, the laboratories have experienced little or no litigation related to data validation and sample custody, and have successfully defended their practices and results in court.

Finally, clinical laboratories in a hospital setting were examined via staff interviews and literature review. Although these laboratories may be less of a role model than are the drug testing laboratories for EPA to follow, due to the importance of data availability over data confidentiality, a variety of techniques for data security were identified that EPA may want to implement. These include unique passwords, a hierarchy of password protection based on the job level of the individual, a record of every password owner that accesses a particular data set, and the ability of a terminal to shut down if unauthorized attempts are made to access the system.

Background

The U.S. Environmental Protection Agency (EPA) has initiated a program to ensure the integrity of computer-resident data in laboratories performing analyses in support of EPA programs by developing standards for automated laboratory processes. The possession of sound technical data provides a fundamental resource for EPA's mission to protect the public health and environment, regardless of the activities of the specific environmental programs. The activities of these environmental programs are diverse, and include basic research at EPA's environmental research centers, environmental sample analyses at EPA's regional laboratories and contractors' laboratories, and product registration relying on analytical data submitted by the private sector.

EPA recognizes that the implementation of an automated laboratory standards program will require each laboratory to allocate resources of dollars and time for the program's execution. Experience has shown that in developing and using a proper standards program, a net savings may be achieved, as acquisition, recording, and archiving of data will be improved with a net reduction in test duplication.

Within EPA, the Office of Information Resources Management (OIRM) has assumed the objective of establishing an automated laboratory standards program. The need for this program is evidenced by several factors. These include the rising use of computerized operations by laboratories, the lack of uniform standards developed or accepted by EPA, evidence of problems associated with computer-resident data, and the evolving needs of EPA auditors and inspectors for guidance in evaluating automated laboratory operations.

Laboratories collecting data for EPA's programs have taken advantage of increasing technology to streamline the analytical processes. Initially, automated instrumentation entered the laboratories to increase productivity and enhance the accuracy of reported results. Computers maintaining data bases of results were then used for data management and tracking. These computer systems were integrated into more sophisticated laboratory information management systems (LIMS).

Methods for data reporting include electronic mail, electronic bulletin boards, and direct links between central processing units. Each of these advances necessitates thorough quality control procedures for data generation, storage, and retrieval to ensure the integrity of computer-resident data.

Currently, EPA has no Agency-wide guidelines for laboratory information integrity that laboratories collecting and evaluating computer-resident data must follow. The requirements that must be considered in developing automated laboratory standards come from a variety of sources, including the requirements of the Computer Security Act of 1987 (P.L. 100-235, January 8, 1988) and various EPA program-specific data collection requirements under Superfund, the Resource Conservation and Recovery Act, the Clean Water Act, and the Safe Drinking Water Act, among others. Additionally, OIRM has developed electronic transmission standards and is developing a strategy for electronic recordkeeping and electronic reporting standards that will impact on all Agency activities. The development of uniform principles for automated data in EPA laboratories, regardless of program, will take into account the common elements of all these data collection activities, and provide a minimum standard that each laboratory should achieve.

There is increasing evidence of problems associated with the collection and use of computer-resident laboratory data supporting various EPA programs. To illustrate, as of November 1989, EPA's Office of the Inspector General was investigating between 10 and 12 laboratories in Superfund's Contract Laboratory Program (CLP) for a variety of allegations, including "time traveling" and instrument calibration violations. In "time traveling," sample testing dates are manipulated, by either adjusting the internal clock of the instrumentation performing the analyses or manipulating the resultant computer-resident data. (Hazardous waste samples must be assayed within a prescribed time period or the results may be compromised.) Additionally, calibration standard results have allegedly been electronically manipulated and other calibration results substituted when the actual results did not meet the range specifications of the CLP procedure being followed. If proven, these allegations may be treated as felonies.

Because the introduction of automation is relatively new and still evolving, no definitive guidelines for EPA auditors and inspectors have been developed. Inspectors must be alert to the steps in those procedures used by the laboratories

generating and using computer-resident data where the greatest risk exists. These critical process points indicate the magnitude of control that should be placed on each step of the process. If adequate controls are not present, the remainder of the process cannot correct a deviation, and the entire process will provide no reliable conclusions. Automation introduces many new variables into a system, each with its own set of critical process points. Inspectors must verify that laboratory management has recognized the various risks and has instituted an appropriate risk management program.

As part of EPA's program to ensure the integrity of computer-resident data, EPA reviewed the policies and procedures in place in clinical laboratories, since it was reasoned that the data generated by such laboratories must be of exceptional quality because it impacts directly on the lives and livelihood of individuals. Using data from hospital-based clinical laboratories, medical practitioners must make decisions on patient care that will have a tremendous impact (positive or negative) on patients' health. In relying on the results of clinical laboratories conducting forensic urinalysis for illicit drugs, employers must make significant employment decisions about their workforce. It was hypothesized that some of the standards in place in automated clinical laboratories could be applied to the automated environmental chemistry laboratory environment. As a result of its research in automated clinical laboratories, EPA identified many procedures that could be applied to automated laboratories.

Other areas of evaluation in developing the standards program include a review of current automated technology; a survey of current automated environmental chemistry laboratory practices; an evaluation of standards, methods, and controls used in managing automated financial systems; and an analysis of the applicability of EPA's Good Laboratory Practice regulations to automated laboratories. The findings of each of these evaluations are provided in separate reports.

Our evaluation focused on three types of clinical laboratories: laboratories associated with hospitals, laboratories conducting forensic drug urinalysis, and laboratories screening blood products for antibodies to human immunodeficiency virus (HIV). Each type of clinical laboratory provided differing levels of practical

information. For the purposes of this evaluation, drug testing laboratories provided the best role model for analytical chemistry laboratories supporting EPA programs.

Findings

Practices in Clinical Drug Testing Laboratories

Management, technical, and quality assurance personnel were interviewed at six mid-Atlantic drug testing facilities engaged in urine drug testing for either military or civilian agencies as well as commercial clients. The drug testing programs supported by these laboratories are primarily overseen by the military, by the National Institute on Drug Abuse (NIDA), or by the Department of Transportation (DOT). The interview questions were related to laboratory computer-controlled equipment, computer security, and computer-resident data integrity. The questions and discussions followed a pattern set by the Good Laboratory Practice standards[1] that could reasonably be applied to computers, to computer software, and to analytical chemistry laboratories conducting work using computer-linked instrumentation. The questions focused on several general areas, including personnel and management practices, computer security principles, chain of custody of samples, the type of integrated computer-controlled analytical instrumentation systems that were effective in terms of both sample handling and data security, and data validation and retention.

Answers to the series of discussion questions were tabulated to determine common points of reference or differences between the operations and standards of the laboratories with respect to:

- Organization and personnel
- Laboratory operations, including security and standard operating procedures
- Conduct of each study, including requirements for data entry, data changes, data validation, and chain of custody

[1]Sections below are related to the Good Laboratory Practice standards as published by EPA under the Toxic Substances Control Act (TSCA) at 40 CFR Part 792.

- Requirements for records and reporting

- Standards for operating the drug testing program.

The following discussion addresses the findings in the above order.

Organization and Personnel

Personnel (40 CFR 792.29)

In all cases, the laboratory technicians had a range of educational and work experience that was suitable for their technical assignments in drug testing. Those who had additional background in computer programming, operations, or computerized data acquisition filled those positions where more direct computer work was needed. Personnel in positions of computer operators, programmers, system administrators, or computer maintenance generally had more formal computer training or training with a computer manufacturer, as well as internal training. Computer hardware maintenance and operating systems upgrades were handled by outside computer contractors at the military laboratories and by corporate information systems staff at the NIDA-certified laboratories.

Lower level chemistry or clinical laboratory technicians received training and supervision for the equipment they were assigned to but the amount of computer training was minimal. In general, all laboratories had standard operating procedures (SOPs) that dealt with all aspects of the technicians' or technologists' work.

The Quality Assurance Unit and Computer Operations (40 CFR 792.35)

In general, computer operations are not overseen or examined by the laboratory's QAU. The computer group itself may have a rudimentary QAU with standard operating procedures.

Laboratory Operations

Security

Basic Password/Logon Security (40 CFR 792.61)

All laboratories where personnel were interviewed use a routine hierarchical form of password(s) control, consisting of a simple name-based logon that allows the individual access to the terminal. A unique password then allows the individual access to pre-approved menus or programs. Password control and/or change systems vary from lax (passwords are never changed, or are changed once or twice a year but the technician may continue to use the old password) to strict (passwords are changed monthly on order from the central computer, and existing passwords are retired). One system has the capability of requiring answers to personal identifier questions in addition to the password system.

Additional security is obtained by locking certain terminals out of the system or refusing to accept data outside the authorized work schedule times. Most systems have an automatic sign-off or time-out should the user leave the terminal. This may range from 1 to 15 minutes.

Password access varies among laboratories, from individual access only to maintenance of a complete list of users and their passwords secured in the corporate office. Administrative action for the unauthorized use of a password or password swapping ranges from lax (in a policy statement but not monitored or enforced) to dismissal with no further warning. In general, laboratory personnel deny that password exchange has been a problem.

Facility Physical Security (40 CFR 792.41)

All computers are subject to data loss in the event of a power failure. The extent of the loss will depend on the software and the computer. An uninterruptible power supply (UPS) system (such as a battery or generator) will be of assistance, as will a backup computer system. The UPS will ensure an orderly shutdown to prevent damage to the computer, but some data (i.e., the data in process at the time) will be lost. Each laboratory has a system of determining which

data have been lost and which samples must be rerun. Data generated by hand will be entered at a later time once the computer system has been restarted and is functional. All such data are archived as raw data.

All facilities have some sort of physical security for their computers. This may be a locked computer room or it may be separate and restricted areas throughout the facility. Entrance to any physical area may be restricted to authorized personnel and all entries may be recorded in the computer.

The existence and use of external connections to the computer vary among the laboratories. In general, any modem line will be highly secure. This may be accomplished by physically disconnecting the incoming line until its use is authorized. Modem lines are generally used by maintenance contractors and their use is monitored and recorded.

Most laboratories do not permit "phone-ins" for test results, although one permitted phone access after the client's identification was verified and he/she would then be called back by laboratory personnel with the results.

Operating Procedures

Standard Operating Procedures (40 CFR 792.81)

Most equipment and operations are covered by SOPs. The computer section itself may have SOPs for the equipment and maintenance.

In-House Development of Computer Software (40 CFR 792.61)

The software employed in drug testing laboratories is generally developed in-house due to its specialized nature. In most cases, there is little evidence of following software development life cycle procedures, although this is planned to be part of the next generation of computer software for these laboratories. However, several laboratories claim to use the software development life cycle and have written software that is in the validation documentation stage now. The laboratory's Quality Assurance Unit is not typically involved in the development of the software.

Computer software is not always validated in any formal fashion. As software modifications are developed, in most cases, they are functionally evaluated in a development environment and further tested to make certain that the existing software parameters are unchanged. In addition, some of the laboratories perform parallel runs of current/modified software. Once this is completed the modification can be put into the production environment. There is documentation for this along with a formal procedure for modification to be followed in half of the laboratories where personnel were interviewed.

Conduct of the Study

Audit or Validation of Manually Entered Data (40 CFR 792.130)

All laboratories have some data that must be entered manually. This may be minimal and occur at sample receipt control or it may happen throughout the testing process when special tests are required. All laboratories have some validation procedure, manual or automatic, for these data. Validation of manually entered data may be contemporaneous with the work or it may be retrospective, and may involve one or more people. Data entry validation may be by double entry.

Data Change Controls (40 CFR 792.130)

In clinical testing laboratories (e.g., hospital or clinical contract laboratories), the test results are generally held in the work station computer memory until checked and approved by a supervisor, at which time the data are forwarded to the main computer where no further changes are permitted. The first-level check is to make certain that no result is out of range thus requiring an immediate duplicate test. In these tests, there is no concept of "false positive" or "false negative."

In the drug testing laboratory, however, all data are forwarded immediately upon acquisition to the main computer. In drug testing, a false negative may be permitted but not a false positive. Accordingly a positive result at the screening level leads automatically to a confirmatory test (mass spectrum) on a new aliquot (portion or subsample) of the specimen.

Edit or data change controls vary among laboratories both by the nature of the work and the age or sophistication of the computer software. Read/write/edit access levels depend upon a person's job level, and may entail a technician using several different programs to enter, verify, and release results. In some instances, two or more staff members, none below the supervisory or certified scientist level, are allowed to release the results.

Audit trail procedures depend on the program and on the computer system in use. An audit trail may be computer-resident, on paper, or both. An audit trail must show the date the change was made, who made the change, the original data element, the new data element, and the reason for the change. In one drug-testing laboratory, there is no computer-resident audit trail for changed data, as the system required too much memory and has been turned off; a paper trail has been substituted. In most drug testing laboratories, there is an adequate audit trail, either on paper or in an unchangeable transaction log. Some less secure systems maintain only a log of who accessed the system and not of any changes made. Many times the audit trail only keeps a record of editing, allowing authorized personnel to conduct inquiries without maintenance of a record.

Sample Custody and Results Validation (40 CFR 792.107)

In view of the significance of drug test results it is not surprising that the chain-of-custody procedures in drug testing laboratories are both elaborate and time consuming. Chain-of-custody paperwork starts when the specimens are produced, and the paperwork always accompanies the specimens as they are moved to the testing laboratory and through the screening and confirmation procedures. Logging the specimens into the testing laboratory is frequently done by double-entry manual systems or via bar coding. Specimens are always held in a secure area separated from the testing areas. Aliquots of the specimens are signed out to the technicians for analyses. The original specimens are retained in the secure area for one to two weeks for negative results, and one year for positive findings. A full accounting is retained showing every activity related to each specimen with accompanying mandatory manual signatures at each step. The final results are matched back against the entire chain-of-custody history of the specimen before the results are released.

The chain-of-custody procedures as well as the analytical procedures are sufficiently secure and auditable that there has been little if any litigation based on the assumption of sample identity errors or handling errors in the laboratory over the several years that the urine testing procedure has been in place.

Records and Reporting

Data Retrieval and Data Retention (40 CFR 792.190; 40 CFR 792.195)

There are no guidelines as such for data recovery from storage; this may be set by policy at each laboratory.

Data retention standards are often set by clients or by legal guidelines. In the NIDA-approved laboratories, data retention extends from 30-day to 3-year on-line maintenance to 2-month maintenance of tape backups, to 5 to 7 years for worksheets, and to the indefinite maintenance of microfiche and magnetic tape.

Data Storage and Data Backup Procedures (40 CFR 792.190)

All computer systems are backed up on a schedule to disks or tapes depending on the laboratory and the computer hardware. Backup schedules can range from daily to monthly. Storage of data is not standardized nor is any regular attempt made to determine if the tapes or disks are still readable. Since the stored data continue to be retrievable, the assumption is that the tapes have not as yet deteriorated. Some laboratories contract storage out to tape management firms.

In drug testing laboratories storage of the paper hard copies is also common (most often on microfiche after some period of time). This is required as the hard copies have the chain-of-custody information, including signatures.

Information Security Practices in Other Clinical Laboratories

Intrinsic to the operation of hospital laboratories is an urgency for availability of information – a patient's health, and even his or her life, depends on the treating

physician's access to important information to make immediate decisions concerning patient treatment. For this reason, some data security issues, such as confidentiality, are given lower priority than data availability in the hospital setting. Additionally, due to the variety of specialists that might have an interest in the records of a particular patient, most hospital healthcare workers are granted access to read any patient record. Many hospitals are currently grappling with this issue of ease of access (see Gardner, 1989a, with companion sidebars, and Romano, 1987). Findings obtained in interviews with hospitals lead to similar conclusions with the Gardner series (1989).

Security procedures in place in various hospital laboratories include the use of individual, password-type controls, including two-step sign-on codes and passwords, selected by the user and changed every few months (Gardner, 1989b) or assigned passwords, changed every six months (Gardner, 1989c). Additionally, physicians may have a separate password serving as electronic signature for orders and attestations. (Gardner, 1989b) Hospitals may use a hierarchy of user levels and associated authorized access levels. [However, **all** physicians, nurses, and medical students may have access to **all** clinical data (Gardner, 1989c).]

Additionally, hospital systems may involve the hardware in security systems. Some systems can limit the availability of each patient's data to particular terminals (Gardner, 1989b) or particular times (Gardner, 1989a). For example, a pharmacist might only be able to sign on to terminals in the pharmacy during its normal hours of operation. Additionally, some hospital systems have the ability to "freeze" (lock out) a terminal if a user repeatedly enters an incorrect password or tries to access information beyond the user's clearance level; data processing staff must be called to unfreeze the terminal. (Gardner, 1989c)

Some systems provide "celebrity" protection to well-known patients, which records the identity of each user who examines the patient's data, or permits a user to abort the attempted access without leaving a record (Gardner, 1989c). Other systems control remote access of computer-resident information by using dial-back verification to verify that a request for access is from an authorized physician (Gardner, 1989c). [However, other hospitals are not using the dial-back mechanism to protect against the call-forwarding feature of many phone systems (Gardner, 1989d).]

Policies regarding computer security in hospitals and elsewhere are only as useful as their implementation permits them to be. Forbidding users to "borrow" passwords can only be successful if the system is capable of minimizing the temptation to "borrow" passwords in the first place. One hospital in Florida has instituted a policy of immediate access to system passwords 24 hours per day for legitimate newcomers. The arrangement has been very useful, especially for medical students and interns, who rotate frequently (Gardner, 1989e). Another hospital reported that its staff had such difficulty remembering access codes that printed directions and all staff members' passwords were posted on the computer terminal (Romano, 1987). Clearly, password protection must not be too cumbersome to use.

If a hierarchical access system is instituted, the levels of access must be thoroughly planned, or access might be misunderstood at best, and abused at worst. For example, one hospital reportedly allowed licensed practical nurses (LPNs) to access medication charting even though LPNs are not permitted to give medications. Because of this access privilege, LPNs interpreted the situation as a change in hospital policy and began providing medications to patients (Romano, 1987). Access to medication charting should not have been granted to the LPNs in the first place.

A current concern in hospitals is the use of "cross-patient searching," in which a user can aggregate information across patient records, such as all instances of adverse drug interaction when a certain combination of drugs is provided. Although this ability is a benefit to epidemiologists and medical researchers, the potential for abuse is prevalent (Gardner, 1989a). It is thought that the current lack of standardization across the many systems used among different hospitals is actually enhancing patient record security (Gardner, 1989a).

Detecting and correcting errors in computer-resident data is important, but has received less attention than it should. Basden and Clark (1980) examined two kinds of errors, syntax and context errors, occurring in the use of a hospital information system, CLINICS™, at a teaching hospital. Syntax error concerns the credibility of entries, such as blood pressure being outside a certain range or a month containing greater than 31 days. Context error, on the other hand, concerns the

relationship between a particular datum and other entries. In the medical field, examples of context error include the date of a test authorization not being a date the patient was registered, or an indication that the patient has a sex-linked disease (such as prostate cancer) not appropriate to the individual's sex. The authors concluded in their study that syntax checking alone would reduce the error rate to around 7 percent, which was still felt to be unacceptable. To reduce the error rate further, the authors recommended implementing a system to check context as well as a system to validate the entries themselves (Basden and Clark, 1980).

Quality of the data entered can be enhanced by instituting policies of data ownership. Each professional must enter his or her own data directly into the data base, using the password assigned to the professional, and no other (Romano, 1987). Additionally, integrity of data can be protected by insisting that entry of information on the computer be performed as close as possible to the source of information to avoid transcription errors.

The Special Case of Blood Screening

Laboratories involved primarily in screening blood products for antibodies against the virus responsible for causing acquired immunodeficiency syndrome (AIDS) were unwilling to discuss their information management procedures. Attempts were made to interview representatives of the Whitman-Walker Clinic (Washington, D.C.), the American Red Cross (Washington, D.C.) Alpha Therapeutic (Memphis, Tennessee), and Baxter Healthcare Corporation (Deerfield, Illinois), all of which conduct extensive serological testing. The consensus seems to be that the first line of security for a data system is not to discuss the system at all with those outside the ones who need to know. Although EPA's programs could probably benefit from the experience of this industry, their security is too valuable to be disclosed inadvertently.

Indeed, AIDS antibody testing is a highly sensitive issue in clinical laboratories in general. Hospital laboratories surveyed indicated that results of the various AIDS assays are never entered into the hospital information system, but are kept only as paper records to restrict access to the information. This practice is apparently typical of most hospital laboratories (Gardner, 1989f).

Standards Applicable to Clinical Laboratories

Standards for the operation of clinical laboratories come from a variety of sources, including professional organizations such as the American Society for Testing and Materials (ASTM), the College of American Pathologists (CAP), and the Joint Commission on Accreditation for Healthcare Organizations (JCAHO), from legislation, such as the Clinical Laboratory Improvement Act, and from government agencies, such as the National Institute on Drug Abuse (NIDA). Depending on the types of analyses conducted, any individual laboratory will be encouraged or required to follow the standards of one or more of these organizations.

The American Society for Testing and Materials (ASTM) has developed a series of more than 8,000 voluntary standard guides for a variety of disciplines, including clinical laboratory computer system operations. Examples of these automation standards include the following:

E 1029, Guide for Documentation of Clinical Laboratory Computer Systems

E 792, Guide for Computer Automation in the Clinical Laboratory

E 1246, Reporting Reliability of Clinical Laboratory Computer Systems.

These standards were developed using existing ASTM standards for computer systems and by consulting representatives of the College of American Pathologists.

Additionally, the College of American Pathologists (CAP) has developed standards for laboratory accreditation (CAP, 1988). CAP is a national medical speciality society offering member services, quality assurance programs, and management resources designed to enhance and improve laboratory services for physicians and the public. CAP has developed five standards that specify the minimum requirements to achieve and maintain accreditation. These cover requirements for the director and other personnel in the pathology service or medical laboratory, resources and facilities, quality assurance, quality control, and inspection requirements. The standards do not distinguish between manual and

automated operations in their statement or subsequent interpretation in the document. For example, the standard for resources and facilities is as follows:

> The pathology service shall have sufficient and appropriate space, equipment, facilities, and supplies for the performance of the required volume of work with accuracy, precision, efficiency, and safety. In addition, the pathology service shall have effective methods for communication to ensure prompt and reliable reporting. There shall be appropriate record storage and retrieval. (CAP, 1988, p. 5)

Additionally, CAP has prepared a series of formal inspection checklists that are used for either yearly self-evaluations or on-site inspections conducted by CAP every two years. Selected checklists cover the following aspects of laboratory operation:

Section I, Laboratory General
Section II, Hematology [e.g., blood cell counts]
Section III, Clinical Chemistry [e.g., serum cholesterol testing]
Section III-A, Urinalysis [e.g., glucose or occult blood testing]
Section III-B, Clinical Toxicology/Therapeutic Drug Monitoring
Section IV, Microbiology
Section V, Transfusion Medicine [e.g., blood banking]
Section VI, Diagnostic Immunology and Syphilis Serology
Section VII, Nuclear Medicine [radiolabeled diagnostic procedures]
Section VIII, Anatomic Pathology and Cytology
Section IX, Cytogenetics [e.g., amniocentesis]
Section X, Clinical Histocompatibility [e.g., tissue typing for transplants]
Section XXV, Limited Service Laboratory
Section XXX, Ancillary Testing

The Laboratory General checklist, for example, contains six pages of questions concerning laboratory computer services, and includes specific questions on the type of computer system used, the extent of its use, the operating environment for the hardware, the qualifications of the computer operators, procedures for data entry and reporting, for data retrieval, for data storage, and for maintenance.

The Joint Commission on Accreditation of Healthcare Organizations (JCAHO) is a private, not-for-profit accreditation agency formed to encourage the voluntary attainment of uniformly high standards of healthcare. The organization is constituted of membership from the American College of Surgeons, the American College of Physicians, the American Hospital Association, and the American Medical Association. The JCAHO develops standards, surveys healthcare facilities (not only the laboratory operations, as does CAP), and may grant three-year, renewable accreditation to hospitals and other healthcare facilities. The standards address all facets of healthcare, including a chapter on "Pathology and Medical Laboratories," which focuses on quality issues related to decentralized laboratory testing. JCAHO standards apply to clinical laboratories, but do not directly address the quality of laboratory automation, except as it pertains to the instrumentation and/or facilitates the functions of the laboratory. In general, JCAHO endorses CAP accredited laboratories, except in the areas of safety and blood banking, which must be reviewed separately by JCAHO.

The National Committee on Clinical Laboratory Standards (NCCLS) is affiliated with the American National Standards Institute (ANSI). Its members include government agencies, professional societies, clinical laboratories, and industrial firms with interests in clinical laboratory testing. The purpose of NCCLS is to promote the development of national voluntary standards for clinical laboratory testing and to provide a consensus mechanism for defining and resolving problems that influence the quality and cost of laboratory work performed. It publishes standards and guidelines, including ANSI/NCCLS ASI-1, Preparation of Manuals for Installation, Operation, and Repair of Laboratory Instruments, published in 1981. ANSI/NCCLS have published eight additional standards, all of which concern specific laboratory assays and performance standards.

The Clinical Laboratories Improvement Act of 1967 (CLIA), as amended by the Clinical Laboratory Improvement Amendments of 1988 (CLIA '88), concerns laboratories accepting specimens in interstate commerce. Under CLIA, clinical laboratories are licensed on a yearly basis and are subject to on-site inspections. CLIA's implementing regulations, found at 42 CFR Part 74 (Clinical Laboratories), include provisions for obtaining a license, quality control, personnel standards, proficiency testing, and general provisions, such as records, equipment, and facilities. The regulations address quality control and proficiency testing from the

perspective of assay validation and instrument calibration, not the general perspective of information handling. With the exception of references to instrumentation, the regulations do not directly address automation.

Recently, the Health Care Financing Administration of the Department of Health and Human Services developed a final rule (currently in the comment period) that will consolidate CLIA's implementing regulations contained in Part 74 with other regulations concerning Medicare and Medicaid programs under a new part, 42 CFR Part 493, which will be effective September 10, 1990 (U.S. Department of Health and Human Services, 1990).

The National Institute on Drug Abuse (NIDA) has published Mandatory Guidelines for Federal Workplace Drug Testing Programs (U.S. Department of Health and Human Services, 1988). As stated in the preamble to those guidelines (U.S. Department of Health and Human Services, 1988, p. 11970), the guidelines can be distinguished from the CLIA certification requirements by the following:

- Rigorous chain-of-custody procedures for collection of specimens and for handling specimens during testing and storage;

- Stringent standards for making the drug testing site secure, for restricting access to all but authorized personnel, and providing an escort for any others who are authorized to be on the premises;

- Precise requirements for quality assurance and performance testing specific to urine assays for the presence of illegal drugs; and

- Specific educational and experience requirements for laboratory personnel to ensure their competence and credibility as experts on forensic urine drug testing, particularly to qualify them as witnesses in legal proceedings which challenge the findings of the laboratories.

The NIDA guidelines do stress documentation and records retention [section 2.4(m)] and the importance of a quality assurance program (section 2.5). Similar to the CLIA regulations, however, with the exception of references to instrumentation, the guidelines do not address automation directly.

The Department of Transportation has developed Procedures for Transportation Workplace Drug Testing Programs (49 CFR Part 40; Department of Transportation, 1989), which apply to transportation employers (including self-employed individuals) conducting drug urine testing programs pursuant to agencies of the Department. This rule closely follows the "Mandatory Guidelines" published by NIDA.

In the drug testing laboratories that conduct work for the U.S. Army, the following standards are applied:

- Army Standard 380-380 for computer security
- Army regulation 600-85 for chain of custody in the drug abuse program
- Army Surgeon General's standard operating procedures for drug testing.

These standards formed the basis for NIDA's mandatory guidelines.

In addition, several states have additional standards for firms conducting drug testing on samples obtained from within their state jurisdiction whose results are reported back to that state.

Conclusions

At this time, EPA has no Agency-wide protocols that laboratories collecting and analyzing computer-resident data must follow. In addition, there is mounting evidence of real and potential problems with computer-resident data used to support various EPA programs. In developing its program to ensure the integrity of computer-resident data, EPA has studied the standards and practices used in other disciplines. EPA may draw on the experience of several types of laboratories, on experience with several levels of data security, and on the standards used in a number of industries to design standards for computer security and data integrity in EPA laboratories and for EPA analytical chemistry contractors. These standards are achievable in today's instrument and computer software market, and they should be given consideration for rapid implementation in the EPA system.

EPA has studied the standards and practices used in other types of laboratories, including clinical pathology/chemistry and forensic drug testing laboratories. Upon review of the literature and interviewing of laboratory personnel and others, it was determined that the "human" laboratories (clinical and forensic) adhere to strict guidelines and standards related to data integrity, for both manual and computer-based data. This is due to the highly sensitive nature of the tests and the laws and standards related to patient/client confidentiality.

In another paper in this series, EPA looked closely at the data security and integrity issues of the financial industry. That industry recognized many years ago that financial operations needed to be computerized, but that the computerized operations had to embody no greater risks to data integrity than the traditional manual procedures and auditing safeguards. There is no question that this has been accomplished for this industry.

Standards of accountability and security are also very high in the drug testing industry. Clearly, the client cannot permit data manipulation to change a positive result to a negative result. Testing individuals for evidence of the use of illicit drugs cannot permit questionable sample handling that leads to to affixing an identification label erroneously. Although a bank's data error is covered by insurance, the data error in a drug testing program is not.

Legal as well as practical forces have drawn the attention of the health care industry to the integrity of computer-resident data and computer security. Although the healthcare industry appears to be willing to accept a higher percentage of errors or a lower degree of computer security than the financial industry, the risks permitted are in general manageable. The argument in the healthcare industry, which is not applicable to the financial industry, is that speed and access to laboratory data may be critical to a life, but billings to a patient account can wait. Accordingly, the occasional loss of patient data security may be tolerated.

The data acquisition needs of EPA have elements of both the rigid and the tolerant systems. Environmental monitoring studies have an impact directly on dollars and may have an effect on human health and safety. Health and safety data on chemicals, required by several EPA offices, have an impact on corporate earnings and on human health.

In order to assess the risks attendant on environmental release of chemicals, and in order to protect the health of the population and the environment, EPA must rely on each data element presented for analysis. The validity of the data may rest on the accuracy of the test used, but the integrity of the data rests on an unimpeachable sample custody procedure, on secure computers, on auditable data editing, and on the integrity and professionalism of laboratory and management personnel.

GLOSSARY

Application controls - one of the two sets or types of controls recognized by the auditing discipline. They are specific for each application and include items such as data entry verification procedures (for instance, re-keying all input); data base recovery and roll back procedures that permit the data base administrator to recreate any desired state of the data base; audit trails that not only assist the data base administrator in recreating any desired state of the data base, but also provide documentary evidence of a chain of custody for data; and use of automated reconciliation transactions that verify the final data base results against the results as reconstructed through the audit trail.

Application software - a program developed, adapted, or tailored to the specific user requirements for the purpose of data collection, data manipulation, data output, or data archiving [Drug Information Association].

Audit trail - records of transactions that collectively provide documentary evidence of processing, used to trace from original transactions forward to related records and reports or backwards from records and reports to source transactions. This series of records documents the origination and flow of transactions processed through a system [Datapro]. Also, a chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results [NCSC-TG-004].

Auditing - (1) the process of establishing that prescribed procedures and protocols have been followed; (2) a technique applied during or at the end of a process to assess the acceptability of the product. [Drug Information Association]; (3) a function used by management to assess the adequacy of control [Perry]. That is, auditing is the set of processes that evaluate how well controls ensure data integrity. As a financial example, auditing would include those activities that review whether deposits have been attributed to the proper accounts; for example, providing an individual with a hard-copy record of the transaction at the time of deposit and sending the individual a monthly statement that lists all transactions.

Automated laboratory data processing - calculation, manipulation, and reporting of analytical results using computer-resident data, in either a LIMS or a personal computer.

Availability - see "data availability."

Back-up - provisions made for the recovery of data files or software, for restart of processing, or for use of alternative computer equipment after a system failure or disaster [Drug Information Association].

Change control - ongoing evaluation of system operations and changes during the production use of a system, to determine when and if repetition of a validation process or a specific portion of it is necessary. This includes both the ongoing, documented evaluation, plus any validation testing necessary to maintain a product in a validated state [Drug Information Association].

Checksum - an error-checking method used in data communications in which groups of digits are summed, usually without regard for overflow, and that sum checked against a previously computed sum to verify that no data digits have been changed [Drug Information Association].

Cipher - a method of transforming a text in order to conceal its meaning.

Confidentiality - see "data confidentiality."

Control - "that which prevents, detects, corrects, or reduces a risk" [Perry], and thus reasonably ensures that data are complete, accurate, and reliable. For instance, any system that verifies the sample number against sample identifier information would be a control against inadvertently assigning results to the wrong sample.

Computer system - a group of hardware components assembled to perform in conjunction with a set of software programs that are collectively designed to perform a specific function or group of functions [Drug Information Association].

Data - a representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automatic means [ISO, as reported by Drug Information Association].

Data availability - the state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user [NCSC-TG-004-88]' the state where information or services that must be accessible on a timely basis to meet mission requirements or to avoid other types of losses [OMB]. Data stored electronically require a system to be available in order to have access to the data. Data availability can be impacted by several factors, including system "down time," data encryption, password protection, and system function access restriction.

Data Base Management System (DBMS) - software that allows one or many persons to create a data base, modify data in the data base, or use data in the data base (e.g., reports).

Data base - a collection of data having a structured format.

Data confidentiality - the ability to protect the privacy of data; protecting data from unauthorized disclosure [OMB].

Data element (field) - contains a value with a fixed size and data type (see below). A list of data elements defines a data base.

Data integrity - ensuring the prevention of information corruption [modified from EPA Information Security Manual]; ensuring the prevention of unauthorized modification [modified from OMB]; ensuring that data are complete, consistent, and without errors.

Data record - consists of a list of values possessing fixed sizes and data types for each data element in a particular data base.

Data types - alphanumeric (letters, digits, and special characters), numeric (digits only), boolean (true or false), and specialized data types such as date.

Electronic data integrity - data integrity protected by a computer system; automated data integrity refers to the goal of complete and incorruptible computer-resident data.

Encryption - the translation of one character string into another by means of a cipher, translation table, or algorithm, in order to render the information contained therein meaningless to anyone who does not possess the decoding mechanism [Datapro].

Error - accidental mistake caused by human action or computer failure.

Fraud - deliberate human action to cause an inaccuracy.

General controls - one of the two sets or types of controls recognized by the auditing discipline. These operate across all applications. These would include developing and staffing a quality assurance program that works independently of other staff; developing and enforcing documentation standards; developing standards for data transfer and manipulation, such as prohibiting the same individual from both performing and approving sample testing; training individuals to perform data transfers; and developing hardware controls, such as writing different backup cycles to different disk packs and developing and enforcing labelling conventions for all cabling.

Integrity - see "data integrity."

Journaling - recording all significant access or file activity events in their entirety. Using a journal plus earlier copies of a file, it would be possible to reconstruct the file at any point and identify the ways it has changed over a specified period of time [Datapro].

Laboratory Information Management System (LIMS) - automation of laboratory processes under a single unified system. Data collection, data analysis, and data reporting are a few examples of laboratory processes that can be automated.

Password - a unique word or string of characters used to authenticate an identity. A program, computer operator,or user may be required to submit a password to meet security requirements before gaining access to data. The password is confidential, as opposed to the user identification [Datapro].

Quality assurance - (1) a process for building quality into a system; (2) the process of ensuring that the automated data system meets the user requirements for the system and maintains data integrity; (3) a planned and systematic pattern of all actions necessary to provide adequate confidence that the item or product conforms to established technical requirements [ANSI/IEEE Std 730-1981, as reported by Drug Information Association].

Raw data - ". . . any laboratory worksheets, records, memoranda, notes, or exact copies thereof, that are the result of original observations and activities of a study and are necessary for the reconstruction and evaluation of that study. . . "Raw data" may include photographs, microfilm or microfiche copies, computer printouts, magnetic media, . . . and recorded data from automated instruments." [40 CFR 792.3] Raw data are the **first** or **primary** recordings of observations or results. Transcribed data (e.g., manually keyed computer-resident data taken from data sheets or notebooks) are **not** raw data.

Risk - "the probable result of the occurrence of an adverse event..." [Perry]. An "adverse event" could be either accidental (error) or deliberate (fraud). An example of an adverse event would be the inaccurate assignment of an accessionary number to a test sample. Risk, then, would be the likelihood that the results of an analysis would be attributed to the wrong sample.

Risk analysis - a means of measuring and assessing the relative vulnerabilities and threats to a collection of sensitive data and the people, systems, and installations involved in storing and processing those data. Its purpose is to determine how security measures can be effectively applied to minimize potential loss. Risk analyses may vary from an informal, quantitative review of a microcomputer installation to a formal, fully quantified review of a major computer center [EPA IRM Policy Manual].

Security - the protection of computer hardware and software from accidental or malicious access, use, modification, destruction, or disclosure. Security also pertains to personnel, data, communications, and the physical protection of computer installations [Drug Information Association].

System - (1) a collection of people, machines, and methods organized to accomplish a set of specific functions; (2) an integrated whole that is composed of diverse, interacting, specialized structures and subfunctions; (3) a group of subsystems united by some interaction or interdependence, performing many duties but functioning as a single unit [ANSI N45.2.10, 1973, as reported by Drug Information Association].

System Development Life Cycle (SDLC) - a series of distinct phases through which development projects progress. An approach to computer system development that begins with an evaluation of the user needs and identification of the user requirements and continues through system design, module design, programming and testing, system integration and testing, validation, and operation and maintenance, ending only when use of the system is discontinued [modified from Drug Information Association].

Transaction log - also **Keystroke, capture, report, and replay** - the technique of recording and storing keystrokes as entered by the user for subsequent replay to enable the original sequence to be reproduced exactly [Drug Information Association].

Valid - having legal strength or force, executed with proper formalities, incapable of being rightfully overthrown or set aside [Black's Law Dictionary].

Validity - legal sufficiency, in contradistinction to mere regularity (being steady or uniform in course, practice, or occurrence) [Black's Law Dictionary].

References

Basden, A., and E.M. Clark (1980), Data Integrity in a General Practice Computer System (CLINICS), *International Journal of Bio-Medical Computing* 11:511-519.

Black, Henry C. (1968), *Black's Law Dictionary*, Revised Fourth Edition (West Publishing Co., St. Paul, Minnesota).

Clinical Laboratory Improvement Act of 1967 (P.L. 90-174, December 5, 1967).

Clinical Laboratory Improvement Amendments of 1988 (P.L. 100-578, October 31,1988).

College of American Pathologists (1988), *Standards for Laboratory Accreditation* (Commission on Laboratory Accreditation, College of American Pathologists, Skokie, Illinois).

Datapro Research (1989), *Datapro Reports on Information Security* (McGraw-Hill, Inc., Delran, New Jersey).

Department of Transportation (1989), *Federal Register*, Procedures for Transportation Workplace Drug Testing Programs; Final rule. Vol. 54, No. 230, December 1, 1989, 49854-84,

Drug Information Association (1988), *Computerized Data Systems for Nonclinical Safety Assessment: Current Concepts and Quality Assurance* (Drug Information Association, Maple Glen, Pennsylvania).

Gardner, Elizabeth (1989a), Computer Dilemma: Clinical Access vs. Confidentiality, *Modern Healthcare* (November 3), pp. 32-42.

Gardner, Elizabeth (1989b), Secure Passwords and Audit Trails (Sidebar), *Modern Healthcare* (November 3), p. 33.

Gardner, Elizabeth (1989c), System Assigns Passwords, Beeps at Security Breaches (Sidebar), *Modern Healthcare* (November 3), p. 34.

Gardner, Elizabeth (1989d), System Opens Access to Physicians, Restricts it to Others (Sidebar), *Modern Healthcare* (November 3), p. 38.

Gardner, Elizabeth (1989e), 'Borrowed' Passwords Borrow Trouble (Sidebar), *Modern Healthcare* (November 3), p. 42.

Gardner, Elizabeth (1989f), Recording Results of AIDS Tests can be a Balancing Act (Sidebar), *Modern Healthcare* (November 3), p. 40.

National Bureau of Standards (1976), *Glossary for Computer Systems Security* (U.S. Department of Commerce, FIPS PUB 39).

National Computer Security Center (1988), *Glossary of Computer Security* (U.S. Department of Defense, NCSC-TG-004-88, Version 1).

Office of Information Resources Management (1987), *EPA Information Resources Management Policy Manual*, Chapter 8 (U.S. Environmental Protection Agency, Washington, D.C.).

Office of Information Resources Management (1989), *EPA Information Security Manual* (U.S. Environmental Protection Agency, Washington, D.C., December 15, 1989).

Office of Management and Budget (1988), *Guidance for Preparation and Submission of Security Plans for Federal Computer Systems Containing Sensitive Information*, OMB Bulletin No. 88-16 (Office of Management and Budget, Washington, D.C., July 6, 1988).

Perry, William E. (1983), *Ensuring Data Base Integrity* (John Wiley and Sons, New York).

Romano, Carol. A. (1987), Privacy, Confidentiality, and Security of Computerized Systems: The Nursing Responsibility, *Computers in Nursing* (May/June), pp.99-104.

U.S. Department of Health and Human Services (1988), *Federal Register*, Mandatory Guidelines for Federal Workplace Drug Testing Programs; Final Guidelines. Vol. 53, No. 69, April 11, 1988, 11969-11989.

U.S. Department of Health and Human Services (1990), *Federal Register*, Medicare, Medicaid and CLIA Programs; Final Rule with Comment Period. Vol. 55, No. 50, March 14, 1990, 9537-610.