

DOT
ELECTRONIC TRANSMISSION AND STORAGE OF DRUG TESTING INFORMATION
FEDERAL ADVISORY COMMITTEE
Subcommittee Reports
9/18/2003

OVERVIEW

The Department of Transportation (DOT) established the Electronic Transmission and Storage of Drug Testing Information, Federal Advisory Committee in December 2001. The Committee members were selected, by the Secretary of Transportation, primarily from a list that was developed from individuals and groups who attended two public meetings in June and August of 2000. The Office of Management and Budget, the Department of Transportation and the Department of Health and Human Services sponsored these initial meetings. All nominees expressed an interest in dealing with issues of security related to the transmission and storage of drug testing information.

The Department established the Procedures for Transportation and Workplace Drug and Alcohol Testing Programs, known as **49 CFR Part 40**, in 1989, and added alcohol testing to the rule in 1994. **49 CFR Part 40** provides uniformity across all modal transportation industries on how drug and alcohol tests are conducted, and specifies what documentation is required. One of the statutory requirements is that DOT drug testing must be conducted in laboratories certified by the Department of Health and Human Services, HHS. Currently, there are approximately 53 drug-testing laboratories certified to conduct drug testing for the transportation industry and for federal agencies. Approximately 8.3 million transportation workers are in safety sensitive designated positions requiring drug testing. There are approximately 674,000 employers regulated by these rules. All laboratories report DOT mandated test results directly to a physician designated as a medical review officer (MRO). It is estimated that there are approximately 20,000 MRO's. In the past, laboratory test results were sent by mail or courier, generating substantial paperwork requirements.

The Department made modest changes in the procedures for test result reporting when **49 CFR Part 40** was updated and republished on December 19, 2000. The changes permitted greater use of faxes and scanned computer images. Moreover, these changes permitted laboratories to transmit negative test results only by electronic means to MRO's, provided the laboratory and the MRO ensure that the information is accurate and can be transmitted in such a manner as to prevent unauthorized access or release while it is transmitted or stored. While the rules also permit the electronic transmission of laboratory positive test results, a paper (or faxed) copy of the CCF is still required to be received by the MRO before the MRO takes any action. In the preamble of the December 19th rule, the Department pointed out that the increased use of electronic reporting is both inevitable and beneficial. At the same time, the Department wanted to ensure that there are good, consistent minimum standards for the use of this technology, in order to protect the important integrity and confidentiality requirements of the program.

The purpose of this Committee is to assess the current status of electronic security technology and make recommendations for minimum standards, applicable to employers, laboratories, MRO's, and all other service agents regarding the electronic transmission and storage of drug testing results. The goal is to develop consistent standards that will protect the integrity and confidentiality of the program. Topics reviewed by the Committee include: data format and uniform record layout; storage medium, procedures, and security; transmission methodology and security; interoperability and ease of use; and standards for electronic signatures. Additionally, time permitting; the Committee will examine the procedures used in implementing electronic signature technology within the framework of the DOT drug and alcohol-testing program. The Committee is not charged with developing recommendations for the so-called "paperless

laboratory” or for recommending the initiation of a totally paperless drug testing and reporting process. However, the Committee may need to look at the impact of electronic transmission of drug testing information as it relates to potential legal challenges, as well as the future role of electronic signatures on the program. Also, while the Committee may look at specific methodologies, hardware and software products, the Committee's goal is to recommend a relatively generic process that will address the Department's concerns about security and yet at the same time will be realistic so that it can be implemented by small transportation businesses and at a reasonable cost. Additionally, any process recommended must be flexible enough to be used in the future, even as the technology itself changes. The Department also actively solicited participation by other federal agencies in these meetings and many of them have been represented at the meetings, including the Department of Health and Human Services, the Food and Drug Administration and the Justice Department and many more.

The first meeting of the Committee was held on June 17-18, 2002. At this meeting, there was a review of the current procedures and data elements used laboratories, MRO's and employers; a review of “state of the art” in electronic transmission and security; a review of legal considerations; and a discussion of implementation issues and costs. There were also presentations by the FDA (electronic security methodologies), Justice Department (legal considerations) and the DOT (Federal employer perspective). Three subcommittees were formed to study and make recommendations to the entire Federal Advisory Committee: data elements and record layout; digital signatures and security of the transmission of the drug testing information; and security and storage of drug testing information.

The second Committee meeting was held on April 7-8, 2003. At this meeting, the discussion focused on the preliminary work of the three subcommittees. In addition, there was a discussion of HIPAA security requirements and the HL-7 and how it could be used as the protocol for transmitting drug testing results between different entities – e.g. collection site to lab, lab to MRO, and MRO to employer. There was agreement among the Committee that the subcommittees were making significant process in gathering the information required for the entire Committee to make recommendations to the DOT. There were a number of items identified that required further clarification and investigation for the next meeting. There was recognition that there may not be a “one size fits all” standard for all of the employers, laboratories, MRO's, or TPA's. There was also continued consensus that the final recommendations should be appropriate for the specific data elements and how they are used; that a cost/benefit or risk analysis be a part of the recommendations; and, that the recommendations be technology neutral to permit the DOT to adapt to changing technologies.

The third Committee meeting will discuss the final recommendations from the three subcommittees and solicit active feedback from the public at-large and the stakeholders in this process. Based on these discussions and public comments, the Committee will provide the DOT a final report with its recommendations. The Department anticipates that, following the receipt of the Committee's recommendations and their review; DOT will propose changes to **49 CFR Part 40** through a notice of proposed rule making. This should result in minimum standards for security in transmission and storage of drug testing information and in a more widespread use of electronic technology in the program.

The three Subcommittee reports follow and are organized with an executive summary preceding the in-depth discussion of the issues and recommendations for consideration by the entire Committee:

DATA ELEMENTS AND RECORD FORMAT SUBCOMMITTEE

EXECUTIVE SUMMARY

In the current workplace drug testing environment, a variety of defined 'service agents' provide specific services to employers. These agents must communicate with one another and ultimately to employers to convey data. As workplace drug testing programs have evolved, these entities have increasingly relied upon electronic communication to transmit information. In the current environment, there has been no defined set of standards relied upon to ensure that the communications are accurate and consistent. Rather, individual entities have developed unique standards that are not portable between agents.

One of the goals of the Federal Advisory Committee on Electronic Transmission and Storage of Drug Testing Information is to identify and recommend a set of common standards for electronic communication that will be used by all parties to the program. This includes, but is not limited to, laboratories, medical review officers (MRO's) and third party administrators (TPA's). The committee feels that by standardizing communication formats, data transfers between entities will be more efficient, accurate and consistent. This subcommittee has reviewed current practices to define the needs of a variety of end users, reviewed standards currently available for applicability, and has identified advantages and disadvantages of adopting a current standard or developing new standards.

The subcommittee recommendation for a unified approach to electronic reporting of drug testing results is based upon the adoption and use of standards for formatting electronic messages and for coding of laboratory test names and results. As an accepted industry standard for electronic messaging of health information and the standard for development of the computerized medical record, **Health Level 7 (HL7) version 3.0 (XML)** emerged as the choice of a standard for Drug test results report messaging format. Wide and increasing adoption by laboratories of Logical Observation Identifiers, Names and Codes (**LOINC**) for the specification of the test names made it the choice for coding of laboratory tests.

EXISTING METHODOLOGIES - CURRENT PROCESS

Drug testing data is stored electronically in literally hundreds of different kinds of information systems. To provide service to employers, the data needs to be shared between these systems. Computer to computer interfaces can help make this information available when and where it is needed.

Currently, information may flow between entities in a number of ways. Initiated at the Employer, requests for tests at collection sites may be communicated directly or through a TPA. Specimen information is then sent directly to the laboratory with the specimen and entered into the LIS. Test results from the laboratory are transmitted directly to the MRO who may communicate final results directly to the employer or to the TPA as an intermediary. While the general flow of information is constant, the structure and contents of the information itself vary greatly. Due to the architecture of these disparate computer systems, drug-testing data is transmitted between systems in a multitude of user-defined messages. This requires transmitting and receiving parties to define the content of the messages for one another. Because an individual service agent may work with many different providers, this process has resulted in many sets of client-specific interfaces that require ongoing maintenance. This creates data inconsistencies within these user-defined formats. It also inhibits the portability of information among users within the drug testing community and places unnecessary development and maintenance on all parties.

STANDARDIZATION

Standardization of the data elements, codes and the file format for the reporting of DOT drug testing results will accomplish several things:

1. Promote interoperability of systems and the creation of comparable data at different sites.
2. It will eliminate the need for pre-arranging the convention needed to transmit data from one entity to another. Systems will no longer need to know who sent the data before it is able to understand the content of the information.
3. It will eliminate file conversion when data is shared between additional systems. As a drug test moves through the pipeline from its inception to conclusion, it will be expressed in the same format. This ability to plug and play from one system to another allows for seamless movement of the information.
4. It will eliminate the need to interpret and translate information, resulting in greater data integrity and reliability.
5. It will result in cost savings both in hard dollars and resources. The time and money expended to create, maintain and implement ever changing standards will be greatly reduced or eliminated completely.

Selection Criteria –

There are four elements to consider in choosing a file format:

1. Compatibility
 - a. The format meets DOT requirements
 - b. The format has wide platform acceptance
2. Adaptability
 - a. Can be changed to meet future needs
 - b. Extensible
 - i. Allows for reasonable extensibility without revision
 - c. Works with Non-DOT testing
3. Implementation
 - a. Ease of implementation
 - i. Time required to implement
 - ii. Availability of resources
 - iii. Difficulty of technology
 - b. Cost of implementation
 - i. Wholesale change for all existing systems
 - ii. Additional resources
4. Maintainability
 - a. Standard Authority
 - i. Who keeps the standard(s)
 - ii. Will the standards authority cater to DOT needs
 - b. Life cycle of revisions
 - i. How long does it take to make revisions to the standard
 - ii. Does a vehicle exist for revisions

File Format -

Multiple choices exist or can be created for the file format. Almost every lab has one or more file formats that they currently use to transmit drug results to their clients. Established formats by the labs are typically some type of delimited text.

Each of these files relies on the ability of the receiving organization to understand how the file format is arranged. This is done through pre-arranged convention. A file typically contains information for multiple drug tests. A file may contain some type of header information, a group of records and an indicator for the end of the file. Based upon the arranged convention, each record contains data for the results of a drug test. The record may be a fixed length where each data element is contained in a specific segment of the file. Another common method is to separate each data element within a record with a delimiter. This is usually a comma or some other character that begins and ends each data element regardless of its length. Although this works, it can be very error prone. In a fixed length file, the loss of one character can corrupt the whole file. A missing separator (or and additional one) in a delimited file can cause the same catastrophic effect.

With the advent of the Internet, the use of file transfers increased exponentially. Along with this, a new type of data file was created. XML (Extensible Markup Language) started as a way to create smart web pages. Because of its simplicity and extensibility, it is quickly becoming the standard for the bulk of business electronic file transfer.

XML takes the data that is sent in a file and wraps each data element with its definition. Now, instead of the file only containing the data and relying on a prearranged structure, the file contains its own definition. This results in a more robust, less error prone exchange of data.

Format Origin -

There are many approaches, which can be used to choose a file format. Among them are creating a new standard, use an emerging one or use an established format. Each of these has advantages and disadvantages.

Creating A New Standard

Creating a new standard assures us that we will have complete compatibility with all DOT requirements. The standard created will, by definition, have all the necessary fields and nuances that are needed by the DOT. A new standard can be easily tailored to incorporate Non-Dot Testing and the needs of the community at large.

As with any set of data unforeseen or additional fields will be needed in the future. A created standard is easy to change to add new elements as the needs arise.

Once the data fields have been identified, it will take a relatively short time to establish and publish the standard. The control entity need only publish it to be accepted as the standard. This eliminates the time it would take for a third party governance entity to approve the standard.

Maintainability of a created standard is the most serious obstacle to this approach. Maintaining the standard poses several complicated and time consuming obstacles that will need to be overcome.

1. A standard holder will need to be developed to maintain it. The standard holder could take several forms. It could be the DOT, a committee of interested parties or an already established standard holder. Any and all of these is complicated to establish and maintain.
2. A revision methodology will need developed. Once a “committee” is established, a process will need to be put in place to suggest and make changes to the new standard.

Use An Emerging Standard

There are several emerging standards that deal to some degree with drug testing. Various Human Resource organizations are developing standards for use in HR software. Within these standards, drug-testing results are addressed, but not to the extent required by the DOT.

Using an emerging standard should provide us with fair compatibility with DOT requirements. None of the emerging standards completely encompasses the DOT data requirements. Requests to extend the standard would need to be made to the governing entity. The same would be true for Non-Dot Testing requirements.

The use of an emerging standard would be more difficult to change to include new elements. Since the process to change these has are typically emerging with the standard, the revision cycle can be long.

The time necessary to establish the standard would be dependant on the speed in which the governing agency moved to incorporate the additional data elements needed to meet all of the DOT requirements. Although fairly simple, this could take time, possible as long as 18-24 months.

Revisions to the standard would be made through the governing agency. Typical timeframes for revisions are between 12 to 24 months.

Use An Established Standard

There are many established standards that deal with reporting drug-testing results. Nearly all of the laboratories that perform the analysis of DOT drug tests have developed a standard that they use to interface with the MRO. Most of these standards were created by the laboratory based upon the systems that they use. They are, for the most part, a text or data file that reports results in a batch mode. Any of these formats could be used as a standard for DOT testing.

Although these standards exist and are or would be completely compatible with the needs of the DOT, they will be problematic in adapting due to the fact that they were designed to meet the needs of the laboratory and it’s clients. Many of the fields exist to serve the needs of a particular lab or one of its clients. To consolidate multiple formats into one standard would be difficult, if not impossible.

Several of the labs have embraced and extended a standard used within the Health Care industry, HL7. The HL7 framework is appears to be the best choice for unifying a standard for reporting DOT drug testing results for several reasons:

1. It is moderately easy to tailor to incorporate DOT and Non-DOT data elements.
2. It is easy to implement.
3. The standard exists and is supported within the industry.
4. An established governing entity exists.

5. A revision methodology exists through the governing entity.

HL7

"Level Seven" refers to the highest level of the International Standards Organization's (ISO) communications model for Open Systems Interconnection (OSI) - the application level. The application level addresses definition of the data to be exchanged, the timing of the interchange, and the communication of certain errors to the application. The seventh level supports such functions as security checks, participant identification, availability checks, exchange mechanism negotiations and, most importantly, data exchange structuring.

The HL7 structures that are currently in use by labs for drug-testing results encompass all of the existing data elements. Several versions of HL7 are being used. Once the data elements that are being proposed by this committee (appendix 1) have been verified they can be incorporated into this structure. At that point, the data exchange structure can be unified into a single standard.

Costs

The cost to implement a new file format will be roughly equal regardless of the approach. The existing organizations will most likely convert the file after they receive it to work within their existing IT systems. Once processed, the internal file can then be translated to the standard format for any additional transmissions.

The use of XML will reduce the cost of implementation due to the built in ability to present data in multiple ways.

RECOMMENDATIONS

The subcommittee recommendation for a unified approach to electronic reporting of drug testing results is based upon the adoption and use of standards for formatting electronic messages and for coding of laboratory test names and results. As an accepted industry standard for electronic messaging of health information and the standard for development of the computerized medical record, Health Level 7 (HL7) version 3.0 (XML) emerged as the choice of a standard for Drug test results report messaging format.

Wide and increasing adoption by laboratories of Logical Observation Identifiers, Names and Codes (LOINC) for the specification of the test names made it the choice for coding of laboratory tests.

The use of HL7 and LOINC is recommended as the best overall solution for several reasons:

1. They are in use by the laboratory community already and the most universal of the approaches. Although they are not used exclusively, there is an established knowledge pool that can be tapped.
2. They can be extended to allow for changes that may arise as a result of additional needs by the DOT. Both standards allow for revisions and a process to address these revisions exist.
3. They exist as well established standards. Although creating a new file format exclusively for use in reporting of drug testing results would be a perfect solution, which satisfies all of the needs of the DOT, it would create a larger problem with maintainability. The establishment of a governing entity and the associated processes to maintain, review and revise the standard would be a daunting, expensive, time consuming task. Any advantages gained, would be quickly lost.

4. The cost of implementation is equivalent to any other solution.

Electronic exchange of drug testing information is now a common process in the drug testing industry. Choosing a standard for the messaging exchange of this information is an important step in this process. Improved information models, the use of standard message format, and the use of standard vocabularies should lead to increased plug-and-play compatibility on interfaces in the future.

One of the next steps necessary to define a standard will be the creation of an Industry Working Group. The focus of the group will be to propose a file format based upon the conclusions of the committee.

DATA ELEMENTS - See Appendix A

Appendix A: Data-Elements

The subcommittee (Data-Elements and Record format) has identified the following list of data elements to support effective sharing of data related to drug and alcohol testing.

Data Elements	BAT	Collection Site	SAP	MRO	Laboratory	Additional Description
	Y – Required data element					
Performing Laboratory						
Lab ID					Y	Laboratory SAMHSA ID
Lab Name					Y	Laboratory Name
Lab Address					Y	Should include 2 line address, city, state and zip code
Lab Accession Number					Y	Laboratory internally assigned accession number
Employer						
Employer ID/Account Number	Y				Y	Client account number
Employer Name	Y	Y	Y	Y	Y	Company Name
Employer Address						Should include 2 line address, city, state and zip code
Employer Phone Number						Area Code + Phone Number
Employer Fax Number						Area Code + Phone Number
Employer Site ID or user definable					Y	User defined field identifying the employer. Can consist of one or more delimited fields
Medical Review Officer						
MRO Name		Y			Y	
MRO Address		Y			Y	Should include 2 line address, city, state and zip code
MRO Phone Number		Y			Y	Area Code + Phone Number
MRO Fax Number		Y			Y	Area Code + Phone Number
MRO CCF Copy 2 Received Date				Y		
MRO Review Date				Y		
MRO Reported Date				Y		
MRO Responsible Person name				Y		
Requisition						
CCF/Specimen ID				Y	Y	Specimen Identifier
Reason for test				Y	Y	From table 1
Collection Date & time				Y	Y	

Specimen Type				Y	Y	From table 2
Donor ID						
Employee ID	Y	Y		Y	Y	Can be employee ID or driver license number
Social Security Number	Y	Y		Y	Y	
Donor Name	Y	Y	Y	Y		Donor lastname, first name, middle initial
Collection Site						
Collection Site ID		Y			Y	Collection Site Lab assigned ID
Collection Site Name		Y			Y	
Collection Site Address		Y				Should include 2 line address, city, state and zip code
Collector's Name		Y			Y	Collector last name, first name, middle initial
Collector's Phone Number		Y			Y	Area Code + Phone Number
Collector's Fax Number		Y			Y	Area Code + Phone Number
Ordered Test Panel						
Panel Code					Y	Laboratory specific panel number which identifies the type and the number of drugs to be tested
Panel Name					Y	Description of the panel
Panel Type (DOT/Non DOT)					Y	Yes/No
Drug Test result						
Date sample received at the laboratory					Y	
Date certifying scientist released the results					Y	
Certifying scientist name					Y	Certifying scientist last name, first name, middle initial
Recoverable Remarks					Y	Laboratory remarks about the information to be recovered and the status
Laboratory Remarks					Y	Additional information from the laboratory about the sample/requisition.
Laboratory Report Date					Y	
Overall Test Result						
Negative				Y	Y	Yes/No Field
Positive				Y	Y	Yes/No field
Dilute				Y	Y	Yes/No field
Substituted				Y	Y	Yes/No Field
Adulterated				Y	Y	Yes/No Field
Invalid				Y	Y	Yes/No Field
Rejected				Y	Y	Yes/No field
Refusal				Y		Yes/No field

Canceled				Y		Yes/No field
Overall Test result Notes					Y	
Performed Tests						This record is a reoccurring one multiple times. There is one record for each drug screened with its corresponding LOINC code. There is one record for each positive drug confirmation with its corresponding LOINC code. There can be additional record for any other tested analytes i.e. Specific Gravity or Creatinine
Test Code					Y	LOINC Code of the test performed. Specific LOINC code for a drug screen result or Specific LOINC Code for a drug confirmation result
Test Name					Y	Performed test name
Test Result					Y	Test result value
Unit of measure					Y	
Reference Range					Y	
Screen Cutoff Value					Y	
Confirmation Cutoff Value					Y	
Result Status					Y	Final/partial

Table Definitions

Table 1 Reason for Test (Table accepted 9/27/2000 – naming not approved)

Entry	Description
Blank	Unknown/Other – Need to include message comment to explain further
PA	Post Accident
RD	Return to Duty
FU	Follow-up
PE	Pre-Employment
RA	Random testing
RS	Reasonable Suspicion/Cause
PM	Periodic Medical
PR	Pre-site Access
NI	Not Indicated
PP	Pre-placement

Table 2 Specimen Type

Entry	Description
Blank	Unknown/Other – Need to include message comment to explain further
BL	Blood
EB	Breath
HR	Hair
OF	Oral Fluid, STT, Saliva
UR	Urine
SW	Sweat

DIGITAL SIGNATURES AND SECURITY OF TRANSMISSION

EXECUTIVE SUMMARY

The objective of this subcommittee is to provide the Department of Transportation with recommendations concerning the use of electronic methods for reporting drug and alcohol results information. Due to the rapid proliferation of electronic communication, it is important that the DOT provide more specific guidance to employers and service providers than exists in the current regulations. The most pertinent parts of the existing requirements are listed below:

49CFR Part 40. 40.97: What do laboratories report and how do they report it?

(iii) The results report may be transmitted through any means that ensures accuracy and confidentiality. You, as the laboratory, together with the MRO, must ensure that the information is adequately protected from unauthorized access or release, both during transmission and in storage.

(d) As an exception to the reporting requirements of paragraph (b) and (c) of this section, the MRO may report negative results using an electronic data file.

(1) If you report negatives using an electronic data file, the report must contain, as a minimum, the information specified in paragraph (c) of this section, as applicable for negative test results.

(2) In addition, the report must contain, your name, address, and phone number, the name of any person other than you reporting the results, and the date the electronic results report is released.

(e)..... If you use the electronic data file to report negatives, you must maintain a retrievable copy of that report in a format suitable for inspection and auditing by a DOT representative.

While the need exists for clearer direction, any future DOT regulations must also be flexible enough to permit employers and service providers the ability to adapt their use of information technology to the degree that makes sense. There is a wide spectrum of sophistication and resources among the DOT-covered population. When combined with the extremely rapid evolution of information technology, and the relatively slow process of rule making, it makes sense that the greatest emphasis be directed towards establishing appropriate objectives and standards rather than mandate specific methods or technologies. The challenge lies in providing enough flexibility while still allowing employers and service providers sufficient information to answer the ever present question: Does it meet DOT requirements?

As stated above in Part 40.97, the need exists to protect results information “during transmission and storage.” The charge of our subcommittee was to address these two states of electronic information specifically as they pertain to the resulting process. The transmission or transfer of data from one system to another is defined as “data in transit”, while data stored in a manner that permits another party to view it is defined as “remote data access.” Regardless of the state of the electronic information, the objective is the establishment of standards that ensure that accuracy and confidentiality of results information is maintained.

Standards are needed because results in a digital format are subject to different exposures, problems, and threats than those reported with physical media, such as paper or analog fax. Existing regulations were derived from industry standards that have withstood numerous legal challenges, and it is likely that the electronic methods of results reporting will be subject to the same level of scrutiny. Only by anticipating and examining potential problems and exposures can standards be established that will withstand future challenges. In today’s world of data theft, computer viruses, worms and “denial of service” attacks, the industry should take appropriate precautions to ensure that electronic data is adequately protected.

Once potential pitfalls have been identified, it is possible to establish guidelines for policies and procedures for that govern data in transit and remote data access. Employers and service providers need to establish policies that govern their use of electronic information in a manner consistent with the objectives of confidentiality and accuracy. Policies for electronic reporting should incorporate procedures specific to technologies utilized by the employer or service provider.

A wide variety of electronic reporting methods are being used in the drug testing industry today. It is important to examine these approaches and ascertain their strengths and weaknesses so that appropriate standards can be developed without forcing specific technologies or approaches on employers or service providers.

The topic of signing documents electronically is of particular concern, due to the confusion that exists between digital certificates used in public key infrastructure and digitized signatures, commonly used in other common transactions such as credit card purchases. Although digitized signatures provide a human-recognizable signature as a form of authorization or consent, they do not provide any protection of the electronic data itself. Public key infrastructure, or PKI, incorporates digital certificates to “sign” electronic data providing for its accuracy and integrity. When combined encryption techniques, data “signed” in this fashion is recognized as legally binding (Electronic Signatures in Global and National Commerce Act, June 2000).

Finally, the standards established by the Department of Transportation must be consistent with the efforts of other federal agencies with similar objectives and requirements. The Food and Drug Administration, as well as the Department of Health and Human Services, have already made significant progress in establishing regulations for how electronic information should be handled. GSA and NIST have served as a resource for federal agencies as they struggle to move to paperless environment.

THREATS AND EXPOSURES TO DIGITAL DRUG TESTING INFORMATION

The electronic movement of drug testing information and results between testing labs, medical review officers, and trading partners by way of computer networks provides a number of advantages to the industry but this comes with additional risks that compromise data integrity, confidentiality, and non-repudiation. This in turn calls into question the legal defensibility of the drug test result if brought in to court. The following provides some background on the types of major threats and or attacks that must be considered prior to discussing method of protecting this data.

Major Threats -

The following is a list of typical threats to information security in the distribution of data across network environments.

- ***Unauthorized Access to Data:*** This class of threat is essentially concerned with a user gaining access to data for which he/she has no authorization. This often happens when a user is only supposed to have authorization to certain data for company A but penetrates into company B’s data. For example, the DER for company A may end up seeing results that belong to company B.
- ***Loss and/or Destruction of Data:*** Computer viruses, parasites, and worms can potentially destroy critical drug testing information and obstruct the timely reporting of results data that could have an impact on safety.

- ***Unauthorized Information Flow:*** By information flow, we mean that the flow of information between two parties must be suitably restricted so as not to violate a prescribed set of distribution policies or a partner agreement. For instance, a laboratory may send drug test results to a medical review officer via an electronic interface, however, the laboratory is not authorized to view or download results information from the medical review officer
- ***Theft and Fraud:*** This threat is similar to an unauthorized information flow. It is often, however, aimed at stealing other valuable information from a network node. Valuable information that could be the object of theft or fraud includes databases of donors, results, and employers.
- ***Violation of Data Integrity:*** Under this threat, a user retrieves or sends data or documents to a participant, but the data is intercepted and tampered with while en route to its destination. The user receives either partial or falsified information as a result. Obviously, any tampering or altering of drug test results could have disastrous consequences.

Attacks -

Forms of Attacks

Network-based service attacks come in two forms: one against data, the other on control systems. The first type of attack involves attempts to steal or corrupt data and deny services. The vast majority of Internet and other computer attacks have fallen into this category. Control-system attacks attempt to disable or take power over operations used to maintain physical infrastructure.

The primary attacks that should be of concern to this audience should be attacks against data and hence are mentioned below. (Physical and Logical Security Subcommittee is addressing control-system attacks.)

Replay Attack

A replay attack occurs when an attacker intercepts a message with a valid security token, and sends it again and again to the network node. This "replay attack" doesn't require any knowledge of the message contents. The goals of such attacks are to gain access to or disrupt normal operations.

The Authenticate messages, has the highest risk for replay attacks. The attacker may intercept a request message or response message and replay it to gain access to a network node at a latter time.

Replay attacks can be prevented if there is a timestamp in the message and there is an expiration time imposed by the receiver. A replay of such a message at a later time will be invalid and rejected by the service. Using a secure communication channel, such as Secure Socket Layer (SSL) can also reduce the risk of replay attack. The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes. It would be hard to intercept an encrypted message and to replay it entirely.

Eavesdropping

Communications between two network nodes are carried typically through public Internet networks. This makes eavesdropping possible. Information remains intact during eavesdropping.

Hackers usually want to intercept information using eavesdropping techniques. Once intercepted, hackers can take them offline to analyze and to decrypt.

It has been proven that even low SSL encryption, such as 54 bit encryption, can be cracked using fast computer systems. Therefore, to prevent eavesdropping, symmetric encryption with 128 bit key and public key encryption with a 1024 bit key is required. As technology progresses, it will be important to keep encryption standards current with those recommended by NIST or an equivalent standards organization.

Dictionary Attack

Dictionary attack is a common form of attack against password-based authentication schemes. It occurs when an attacker captures the messages exchanged during a legitimate run of the protocol and uses that information to verify a series of guessed passwords taken from a precompiled "dictionary" of common passwords. This works because users often choose simple, easy-to-remember passwords, which invariably are also easy to guess.

The attacker can perform attacks directly on a network service by calling the Authenticate method (Login) repetitively using a known user name and a set of passwords from a dictionary. In an Internet environment, eavesdropping on a TCP/IP network can be carried out easily unless authentication information is sent through SSL or some other Virtual Private Network (VPN) technology. VPN's are networks that combine public network infrastructure (internet, phone systems) with various hardware and/or software technologies to create a secure network connection between two or more parties.

Message Insertion and Deletion

This happens when a hacker intercepts a network message and makes changes to the message before relaying it to the recipient. The integrity of the message is compromised in this case.

Attacks of this nature can be defended against using SSL, VPN, or PKI technology.

Man In the Middle

The "man in the middle" (MITM) attack is subtler. The hacker captures the request message and stops it from going any farther. They generate their own request message with suitable modifications and send it along to the Web service. When the response message arrives, he transmits a modified response to the original sender, who has no idea there's anything wrong.

MITM is a common form of attack because a request message travels through many devices such as routers, gateways and bridges before reaching its final destination.

MITM attacks can be reduced through SSL encryption. It is difficult for a middleman to relay SSL encrypted messages.

MITM attacks can be prevented using digital signatures. A signed message from the sender guarantees the integrity of its contents. It is extremely hard, if possible, to tamper with the message without being detected.

Impact on Legal Defensibility of Drug Testing -

The effects of how data is managed and transmitted across networks to business partners can greatly impact the legal defensibility in court. The above attacks and threats show how a prosecutor can call into question the reliability of the test results. How do you know that the test results are the same as produced at the lab and reviewed by the MRO and ultimately received by the business partner? In order to have a legal defense it is critical to be able to demonstrate that the test results are accurate and provide proof that there are proper controls that prevent the data from being tampered without detection.

Each of the above threats or attacks can be minimized, or prevented through the use of security measures and proper policy/procedures.

The level or robustness of the security services will vary, depending on the level of security needed, across processes and or methods of transmitting data. Security measures can be characterized into the following five categories; all of which provide pieces to the overall integrity of the data.

- Confidentiality
- Authorization (Access Control)
- Authentication
- Integrity
- Non-repudiation

Confidentiality

Confidentiality, in an e-Business sense, can be viewed from three perspectives; confidentiality of an identity, confidentiality of a credential, and confidentiality of data. The Software Engineering Institute of Carnegie Mellon defines confidentiality as *“the nonoccurrence of the unauthorized disclosure of information”*. When conducting an e-Business transaction in the drug testing industry, the primary confidentiality concerns are centered on the identity of the donor. Keeping the donor’s identity and associated results information protected requires confidentiality be maintained in two areas:

1. Confidentiality of credentials. This means that all service providers must prevent unauthorized disclosure of their access control and authentication components.
2. Confidentiality of data. Keeping test results and donor information protected is critical. This applies to the data “at rest” or in storage, and data in transit.

The primary means of establishing confidentiality in an e-Business transaction is cryptography, where encryption algorithms and keys are employed and commonly understood between the entity wanting to provide confidentiality of the data and the entity wanting to be ensured of the confidentiality of the data. For data in transit, a secure communication channel, such as the SSL protocol, ensures data confidentiality and data integrity in communications between clients and servers on the Web.

Access Control

Access Control is the process by which a software system protects system functions or services from being denied to the user or facilitates the selective use. Within e-Business, access controls grants a user the right (privilege) to conduct a transaction based upon authentication, or denies

that use based on lack or failure of authentication. In the case of electronic access, a user would be granted access to view, retrieve or modify information in a system once they satisfy the system's access control requirements. A system may use a variety of technologies to manage access, such as Personal Identification Numbers (PIN's), passwords, PKI tokens (i.e. smart cards), or biometric scanning devices (i.e. retinal scan, fingerprint scan. A user would be given the appropriate token based upon authentication requirements. Access controls must be flexible enough to allow for the incorporation of additional users and privileges and to allow for the revocation of privileges. Access controls should be commensurate with security requirements of the system or process being controlled. "High value" e-Business transactions would have correspondingly greater access control requirements than those of less strategic value to the organization.

Authentication

Authentication is the association of an identity with an entity. In the physical world, a signature can be used for authentication in a transaction and be legally binding, although some transactions may require a notary for stronger authentication. The notary will physically sight additional forms of identification. In the spectrum of e-business, the identity of an entity will be authenticated through some form of an "electronic signature". This electronic form may be a PIN and password, a physical token (such as a Smart Card), a biometric, a PKI certificate or a combination of the above. The authentication process must be non-refutable and involve the combination of security and authentication technologies, infrastructure, policies and procedures. The ability to build a community with trusted rights and privileges begins with establishing the highest authentication of the identity that may be required to perform the specific process. This is the foundation of any electronic process. If the identity cannot be trusted then any mechanism to secure the authentication is unfounded.

Integrity

Integrity is the assurance of non-alteration, i.e., that data, in transit or in storage, has not been undetectably altered. When a recipient receives a registered letter or FedEx package, he or she can see if the seal has been broken or the document has been physically altered and have some assurance of the integrity of the document. Undetectable changes to documents are more easily made in an electronic medium and thus processes must be established to ensure the integrity of data and transactions. One such process is signing electronic data with digital certificates, which provides a means of ensuring that unauthorized parties have not altered the electronic data being transmitted or shared.

Non-Repudiation

Repudiation is defined as "the rejection or refusal of a duty, relation, right or privilege". If an e-Business transaction is viewed as a binding contract between two parties, a repudiation of the transaction means that one of the parties' refuse to honor their obligation to the other as dictated by the contract. Thus non-repudiation can be defined as "*the ability to deny a false rejection or refusal of an obligation with irrefutable evidence.*" (SANS Institute) A good example of a non-repudiation of submission is the service that the USPS provides when you send a registered letter. You are given a receipt that contains an identification number for that piece of mail. If the recipient never receives the mail and claims that you have not sent it, the receipt is the proof that provides the non-repudiation of submission. If the USPS has the receipt of delivery that contains the recipient's signature, they have provided the proof for the non-repudiation of delivery service.

The USPS provides the non-repudiation of transport service by acting as the trusted third party in the transaction.

Within e-Business, non-repudiation provides the ability to tie an action to a responsible party. PKI is one of the architectures that can provide non-repudiation for electronic transactions analogous to the USPS example. In PKI, the USPS is replaced by an entity called the Certificate Authority (CA), which manages the issuance and utilization of all digital certificates for a specific group of e-business partners. When a sender digitally signs a document or transaction, the CA checks the validity of the sender's certificate and provides a "trusted third-party" witness to the signing. When the recipient accesses the document, the CA also verifies the receiver's certificate, and in doing so, witnesses the receipt. In this example, the CA acts as the trusted third party that provides proof for the non-repudiation of the document's delivery.

Policy Approach -

Policies are a critical component to the protection and security of drug testing data. The use of policies provides a basis of documented requirements for the handling of data as it is generated, stored and transported electronically. This in turn will lead to the documentation of a set of procedures and controls and even contract infrastructure to ensure that the methods used in handling the drug testing data and results are processed and transported accurately to only authorized personnel.

Policies and Procedures -

Policies and procedures are critical to the protection of drug testing data and results. Properly written policies and supporting procedure and controls define the security and handling of the data. This in turn provides the basis of legal defensibility of the data as well as its handling.

Therefore a policy framework of sorts should be developed which defines the minimum-security measures that will be utilized for the management and transports of the drug testing data. The degree or level of these policies is determined on a case-by-case basis within the drug testing industry. Risk analysis can determine how to best to insure the confidentiality, integrity, non-repudiation, authentication and authorization of drug test data. Any entity engaging in the electronic transmission of DOT drug testing information should conduct an accurate and thorough assessment of the risks involved in their respective systems and those of their business associates.

This in turn allows for the definition of clear procedures for the management of the data as well as controls that make it possible to ensure those procedures are correctly followed and managed.

Policies and procedures for drug testing data transmission between trading partners and participants should cover the five basic security components at a minimum:

Confidentiality – Test results, donors, employers

Authorization – Service provider personnel and DER's

Authentication – Validating identities of authorized personnel

Integrity – Accuracy of test results, specifically the content of the transmission

Non-repudiation – Making sure results information got where it was supposed to go

Covered entities should include appropriate training, workforce security, and sanction actions in their policies and procedures.

CURRENT PRACTICES AND DATA PROTECTION PROFILE DISCUSSION

The following discusses the currently perceived methods of transmitting drug testing data and results today. Each one of these are then reviewed to provide guidance as (Protection Profiles) which attempt to clarify general usage of these transports and the level of security components (Confidentiality, Authorization, Authentication, Integrity, and Non-repudiation) that are natively provided as shown in the tables for each protocol.

Email -

The use of email to transmit Drug testing data and results may be utilized but this data MUST be encrypted. This may be accomplished through several means. The first two are S/MIME standards. The later two later two options require additional development and particular effort to ensure the proper protection of results data

- The test result MAY be provided within the body or as an attachment to an encrypted S/MIME email message. Note that this requires Public Key Infrastructure (PKI) based encryption digital certificates issued to each email recipient. The use of asymmetric keys SHALL have a minimum key size of 1024 bit for public/ private keys, or whatever current standard is recognized as industry “best practice” by NIST or an equivalent standards organization.
- Signing the S/MIME message with the senders’ private key can additionally provide the data Integrity and Non-repudiation.
- Test data integrity may be established with the use of either a separate checksum or hash mechanism but MUST being distributed separately from the results data.
- Symmetric key encryption MAY be used to encrypt results data that is then attached to and S/MIME email message. The use of symmetric key for encryption SHALL at minimum utilize 3DES keys or new technologies such as AES. Note that symmetric key distribution SHOULD be documented in a policy/procedure and SHALL NOT be distributed within the same email message as results data.

Note the Authentication and Authorization is naturally provided with the proper implementation and issuance of the public key based digital certificates. If non-PKI based email distribution of test data is utilized, authentication and authorization MAY only be accomplish only through strict implementation and management of policies and procedures, contract infrastructure properly provide authentication and authorization of email address information.

S/MIME Email	Signed & Encrypted	Signed	S/MIME Encrypted Attachment	Symmetric Encryption	Checksum or Hash
Confidentiality	X		X	X	
Authorization	X		X		
Authentication	X		X		
Integrity	X	X			X
Non-repudiation	X	X			

Web Access -

Web based access, MUST utilize secure socket layer (SSL) to transmit drug test data and results. SSL provides a high level of Confidentiality and Authentication, options that are easily implemented through the use of encryption and client/server authentication and allows for Authorization to be centrally managed.

SSL provides symmetric key base encryption of all data passed through an SSL channel. The symmetric key exchange between client and server is accomplished automatically within the protocol and requires at a minimum of the SSL server certificate, which utilizes a PKI base digital certificate issued to the server. Although care MUST be taken, when SSL connections transition from an end point to final storage where data may be left in an unencrypted state as it is moved to an internal database for further processing.

Authentication with SSL can be provided by various means. The best is mutual authentication, where the web server identifies itself with a digital SSL server certificate to the client and the client in turn identifies its self to the web server with a user's digital certificate that the server can validate and grant access based on local access controls called authorizations. The secondary method would be the utilization of the web server authenticating itself to the client machine and then the server requesting the user to authenticate himself with a User ID and Password, which the server authenticates to with its local access controls.

Integrity and Non-repudiation are not a native part to the Web SSL protocols, although that addition can be facilitated by digitally signing the data with digital certificate prior to providing the data for access.

Web Access	Certificate Mutual Authenticated SSL (HTTPS)	User ID/Password Authenticated SSL (HTTPS)	Certificate Sever Authenticated SSL (HTTPS)	Web with no protection (HTTP)
Confidentiality	X	X	X	
Authorization	X	X		
Authentication	X	X		
Integrity				
Non-repudiation				

Electronic Data Interchange -

Electronic Data Interchange (EDI) provides for the transport of data between trading partners. It is a common practice where data is exchanged between trading partners with point-to-point communications. Traditionally, authentication is accomplished with contract infrastructure between trading partners. It does not traditionally provide native support to authenticate an individual who has the authority to view the information.

EDI can be properly secured with the addition of mechanisms such as encryption and digital signing, which provide confidentiality, data integrity, and even non-repudiation. The ANSI X.12 and Internet Engineering Task Force (IETF) has been working to improve basic EDI to add support of Extended Markup Language (XML) as well as leveraging existing internet transport protocols to provide authentication, authorization, confidentiality, data integrity, and non-repudiation. These are documented in the IETF EDIINT working group and include a number of Applicability Statements AS1, AS2 and AS3 (AS3 is still in the early drafts) to define EDI over 3 common internet protocols including S/Mime Email, HTTP, and FTP respectively all three of the applicability statements leverage MIME types and its security components to improve EDI security.

Electronic Data Interchange (EDI)	Traditional Point to point EDI transmission	EDIINT S/Mime with Mime types Transport (AS1)	EDIINT HTTP Transport (Mime types) (AS2)	EDIINT FTP Transport with Mime types) (AS3?)
Confidentiality	X	X	X	X
Authorization		X	X	X
Authentication	X	X	X	X
Integrity		X	X	X
Non-repudiation		X	X	X

Dial-up -

The traditional direct dial-up access of data generally provides a level of security given that password-based authentication is provided as a security component to obtaining the data for download. Dial-up connections are not a direct point-to-point connection and are subject to eavesdropping with in the telecom infrastructure. Therefore, dial-up to view data SHOULD NOT be performed if the data cannot be protected from eavesdropping techniques without hardware assisted encryption modems.

Generally the additional security measures can be added to provide confidentiality with either symmetric key encryption or a password based encryption method. Integrity and Non-repudiation can additionally be added within the digital signing of the information prior to the encryption of the data.

The use of the Internet and ISPs can allow the use of any of the previously discussed methods of transporting drug testing data (S/Mime/ Web access and even EDI) more inexpensively then attempting to add additional security to general dialup methods.

Dialup Access	UserID/Password Authenticated	Certificate Authenticated
Confidentiality		X
Authorization	X	X
Authentication	X	X
Integrity		X
Non-repudiation		X

ELECTRONIC SIGNATURES AND THEIR APPLICABILITY IN DRUG TESTING

A series of events has unfolded that make it important to discuss the use of electronic signatures in drug testing transactions. First, the Government Paperwork Elimination Act that went into effect in 1998, created an expectation that all federal forms would be required to have an electronic counterpart within 5 years. Many from within the drug testing industry wondered if the Federal Custody and Control Form would be covered by the Act. Second, laboratories and then Medical Review Officers, increasingly engaged in the practice of reporting drug test results using various electronic means. In practice, the Custody and Control Form and alternate paper reporting documents, while still required, became less and less involved in the actual receipt and utilization of results data. Finally, the Department of Transportation's amendments to 49CFR Part 40 in 2001 addressed the electronic reporting issue. The requirement to use a paper reporting document for negative results was removed, provided the electronic report met DOT criteria. Paper results documents are still required for all non-negative results reporting. Many industry service agents have made attempts to produce an electronic report that provides the same level of comfort long established with the paper counterparts. Perhaps the most common is the use of digital faxing, where a reporting entity provides results data in field format to a fax rendering system, which then constructs a human-readable graphics file, then dials the recipients fax number, and transmits the image. The image received looks like a paper original in every respect, even including a signature graphic scanned from a hand-written original. This type of signature, called a digitized signature, is often confused with the process of "signing" a document or data electronically. In the application mentioned above, it is the electronic equivalent of a rubber stamp, which is an acceptable method of "signing" negative results documents. It should never be considered, however, an equivalent to the actual paper document containing a wet signature.

Digitized signatures can provide a human-legible indication of consent or authorization, provided they are applied at the time of each transaction. This has become a relatively common practice with credit card transactions at many retailers. However, digitized signatures do nothing to protect the integrity of the data involved in the transaction.

Many service providers and employers have also envisioned a "paperless chain of custody", where the Federal Custody and Control Form has a permissible digital counterpart. In order to make that a reality, the functions of the form would have to be replicated in an electronic fashion. Historically, the functions of the form have been:

1. Affidavits (donor, collector, certifying scientist, MRO)
2. Consent (donor)
3. Chain of custody (collector to courier to lab)
4. Results reporting (lab to MRO, MRO to employer)

Of all of these functions, results reporting is the easiest to replicate, especially in the case of negatives. The overriding concern to be addressed is ensuring that the electronic report cannot confuse the identity of the donor. Since most laboratory systems generate results first on a computer, which is then transcribed to paper, maintaining the link between the sample ID number, and thus the donor's identity, a relatively straightforward process for electronic reporting.

Electronically signing results improves the reporting functionality of the custody and control form. Technologies such as PKI and its use of digital certificates for signing data, offer an opportunity to revisit the requirement for use of a paper document for non-negative results. One notable advantage is removing the need for manual transcription of the result obtained from the laboratory computer system, and any discrepancies that could occur in this process. For medical review officers, a similar model could exist, where electronic data, signed and received from the laboratory, is in turn signed by the medical review officer, then provided to the DER.

Paperless chain of custody becomes more problematic in the areas of affidavits. Very little legal precedence exists to support the use of electronic signing forensic documents similar to the DOT CCF. And while consent precedence exists for use of digitized signatures, it is focused in consumer transactions rather than forensic situations. Notwithstanding, electronic signing technologies in use today, such as PKI, are widely supported legislatively at both the federal and state level. From a technical perspective, it is possible to construct electronic systems that would emulate the consent and affidavit functions of the current CCF.

The issue of chain of custody is most difficult, due to the fact that a specimen bottle is physically transported from the point of collection to a certified laboratory. Even if the collection facility is co-located on the laboratory premises, physical transfer from collector to laboratory personnel mandates chain of custody procedures be followed. In the current paper model, the CCF is the recognized means of linking a given specimen to the identity of the donor. While alternative methods are technically available, it remains to be seen if they can be practically deployed, supported, and defended.

GOVERNMENTS AND INDUSTRY DIRECTION

Federal Government -

A number of Federal Government Agencies have been transitioning to Electronic transactions with the public and other government agencies. This is a fairly recent phenomenon driven by a number of legislative and governmental policies changes as well as the growth of the Internet and newer standards that allow the Internet technologies to streamline government operations while raising the level of security and privacy for these transactions.

Industry -

The transmission of data securely within industry has been transitioning over the last several years from clear text transmission with little or no authentication to encrypted transmission with authentication at a minimum using UserID and password but more recently leveraging more and more direct usage Public Keys and PKI. This is primarily due to the increased standardization of newer security protocols of S/MIME, WEB access and even XML's incorporation of PKI.

REFERENCES

This is a list of reference material that may be of use to larger organizations that have IT personnel.

National Institute of Standards and Technology (NIST)

- NIST, *Federal Information Processing Standards (FIPS)*
- FIPS PUB 73, "Guidelines for Security of Computer Applications," NIST, June 1980.
- FIPS PUB 83, "Guideline on User Authentication Techniques for Computer Network Access Control," NIST, September 1980
- FIPS PUB 87, "Guidelines for ADP Contingency Planning," NIST, March 1981
- FIPS PUB 102, "Guidelines for Computer Security Certification and Accreditation," NIST, September 1983
- FIPS PUB 112, "Password Usage," NIST, May 1985
- FIPS PUB 140-1, "Security Requirements for Cryptographic Modules," NIST, January 1994
- FIPS PUB 180-1, "Secure Hash Standard (SHS)," NIST, April 1995.
- FIPS PUB 186-1, "Digital Signature Standard," NIST, December 1998.
- FIPS PUB 191, "Guideline for the Analysis of Local Area Network Security," NIST, November 1994
- NIST Special Publication (SP) 800-2, *Public Key Cryptography*
- NIST SP 800-7, *Security in Open Systems*
- NIST SP 800-9, *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*
- NIST 800-26, *Security Self-Assessment Guide for Information Technology*, November 2002
- NIST 800-30, *Risk Management Guide for Information Technology Systems*, October 2001
- NIST 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002

National Security Telecommunications and Information Systems Security Committee (NSTISSC)

- NSTISSC *Policy 200 on Controlled Access Protection*, July 15, 1987
- NSTISSC *Policy 300 on Control of Compromising Emanations*, November 29, 1993
- NSTISSC *Directive 500 on Telecommunications and Automated Information Systems Security (TAISS) Education, Training, and Awareness*, February 25, 1993
- NSTISSC *Directive 600 on Communications Security (COMSEC) Monitoring*, April 10, 1990, Page B-12 *Practices for Securing Critical Information Assets*
- NSTISSC *Directive 1000 on National Information Assurance Certification and Accreditation Process (NIACAP)*, April 2000.
- NSTISSI 4005, *Safeguarding COMSEC Facilities and Material*, August 1997.
- NSTISSI 4009, *National Information Systems Security Glossary*, January 1999.

GSA Security Policy and Guidelines

- GSA ORDER CIO 2105.1 11/29/02: GSA Information Technology (IT) Security Policy
- IT Security Procedural Guide: Password Generation and Protection, CIO-IT 01-01 (1/26/01)
- Windows 2000 Professional Hardening Guide (3/14/2002)
- Guide for Developing Security Plans for Information Technology
- GSA Information Technology Security Action Plan (2/99)
- GSA Windows NT Hardening Policy, CIO-IT 01-13 (5/14/01)
- GSA IIS Hardening Policy, CIO-IT 01-14 (5/14/01)

THE PHYSICAL AND LOGICAL SECURITY OF ELECTRONICALLY STORED DATA

EXECUTIVE SUMMARY

The FACA Subcommittee involving the Physical and Logical Security of Electronically Stored Data prepared this Document and presented it to the full committee as background information and for the full committee's use in developing and recommending to DOT security storage standards for electronic drug testing records. The recommendations contained in this document apply to any Laboratory, Collector, Third Party Administrator, Medical Review Officer, and Employer who chooses to store data and information related to Federally Mandated Drug Testing Results in an electronic format in lieu of the storage of the hard copy document.

For clarification purposes, this subcommittee has defined electronic data storage as the retentions of data in any electronic form for the purposes of orderly retrieval, review and documentation.

The subcommittee discussed a number of components associated with the physical and logical security of electronically stored data. These components entailed the use of physical access controls to limit unauthorized access to the electronically stored data; the potential of the interception of data; the use of mobile and portable systems such as laptop computers; how to retire obsolete hardware or media; the identification of a user to the computer system and how this user's identity can be authenticated; measures to protect this authentication process such as limiting log on attempts and the requirement to frequently change passwords.

The subcommittee also considered a number of issues related to logical access control, which can also be described as not only who or what is to have access to a specific system resource, but also the type of access that is permitted. Areas discussed under the logical access control group included access criteria and access control mechanisms.

In addition to the above areas, the sub-committee also discussed the need for audit trails, which are intended to maintain a record of system activity by system or application processes and by user activity, and what information should be contained in these audit trails and that the security for these audit trails must be of the same level as the information it is protecting. A requirement for a review of the audit trail process and related information and data was also discussed. The areas of backups and disaster recovery of electronically stored data was also reviewed by the sub-committee along with the requirements for an annual review of the security audits and an assessment of the security procedures used including a compliance review to ensure that the covered entities are in compliance with the existing regulations.

ELECTRONIC DATA STORAGE

The retention of data in any electronic form for the purposes of orderly retrieval, review and documentation.

PHYSICAL AND LOGICAL SECURITY

The system must be physically and functionally secure to limit unauthorized access to the data. Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The system should also have specifications and requirements for disaster recovery.

Physical Access Controls –

Physical access controls restrict the entry and exit of personnel (and often equipment and media) from any area, such as an office building, suite, data center, or room containing the data server, central storage unit or other computer used for data storage functions.

- *Physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation.*
- *It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied, or occupied by administrative, maintenance, housekeeping or other non-IT, yet essential support personnel.*
- *Multiple levels of access shall be established and the access will be limited according to an individual's duties.*
- *It shall be verified that functional access has been appropriately delegated and that individuals use only their own access codes and passwords.*
- *An individual's access to a restricted area shall be revoked when that individual leaves the company or transfers to another job position that does not require access to the restricted area.*

Interception of Data -

Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. Organizations should be aware that there are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

- *Interception by direct observation occurs when an unauthorized individual(s) casually or intentionally views protected information in any form.*
- *Interception of data transmission can be either direct (i.e. via fax line interception) or via a wireless mechanism (i.e. scanning wireless transmission).*
- *Electromagnetic interception occurs when electromagnetic energy emanating from a cathode ray tube computer monitor is collected and organized in such a fashion as to replicate the human readable contents of the screen.*

The organization must evaluate the potential for such data interception and take reasonable precautionary measures.

Mobile and Portable Systems -

The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks. Organizations must use:

- *Secure storage of laptop computers when they are not in use.*
- *Employ encryption technology where available, as a precaution against disclosure of information if a laptop computer is lost or stolen.*

Retirement of Obsolete Hardware or Media -

Hardware or media that has been retired must be subjected to a process in which previously stored data is made inaccessible and unrecoverable.

IDENTIFICATION AND AUTHENTICATION

Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on *least privilege*, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

Identification -

Identification is the means by which a user *provides* a claimed identity to the system. The most common form of identification is the user ID. The following should be considered when using user IDs:

- ***Unique Identification:*** An organization should require users to identify themselves uniquely before being allowed to perform any actions on the system.
- ***Correlate Actions to Users:*** The system should internally maintain the identity of all active users and be able to link actions to specific users. (See audit trails below.)
- ***Maintenance of User Ids:*** An organization should ensure that all user IDs belong to currently authorized users. Identification data must be kept current by adding new users and deactivating former users.
- ***Inactive User Id's:*** User IDs that are inactive on the system must be deactivated.

Authentication -

Authentication is the means of establishing the *validity* of this claim. There are three means of authenticating a user's identity, ***which can be used alone or in combination:***

- something the individual ***knows*** (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key);
- something the individual ***possesses*** (a token -- e.g., an ATM card or a smart card);
- something the individual ***is*** (a biometric -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint). The following should be considered:

Require Users to Authenticate

An organization should require users to authenticate their claimed identities on IT systems. It may be desirable for users to authenticate themselves with a single login. This requires the user

to authenticate themselves only once and then be able to access a wide variety of applications and data available on local and remote systems.

Restrict Access to Authentication Data

An organization should restrict access to authentication data. Authentication data should be protected with access controls and one-way encryption to prevent unauthorized individuals from obtaining the data.

Secure Transmission of Authentication Data

An organization should protect authentication data transmitted over public or shared data networks. When authentication data, such as a password, is transmitted to an IT system, it can be electronically monitored. This can happen on the network used to transmit the password or on the IT system itself. Simple encryption of a password that will be used again does not solve this problem because encrypting the same password will create the same cipher text; the cipher text becomes the password.

Specific recommendations for addressing the security of electronically transmitted data have been developed by the Digital Signature and Security of Transmission Sub-Committee. The same criteria must be applied to ensure the security of electronically transmitted data.

Limit Log-on Attempts

Organizations should limit the number of log-on attempts to no more than 3 attempts. Many operating systems can be configured to lock a user ID after a set number of failed log-on attempts. This helps to prevent guessing of authentication data.

Establish Time Intervals

Organizations should set appropriate time intervals where by if there is no activity from the user, the system will automatically log off the user.

Secure Authentication Data as it is entered

Organizations should protect authentication data as it is entered into the IT system, including suppressing the display of the password, as it is entered and orienting keyboards away from view.

Administer Data Properly

Organizations should carefully administer authentication data and tokens including procedures to disable lost or stolen passwords or tokens and monitoring systems to look for stolen or shared accounts.

Passwords

If passwords are used for authentication, organizations should:

- ***Specify Required Attributes:*** Secure password attributes such as a minimum length of six, inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID should be specified and required.

- **Unique:** Passwords must be unique to an individual and allow identification to an individual user. These passwords must be linked to an individual not a group.
- **Change Frequently.** Passwords should be changed periodically. The criteria for system password changes and the frequency of these changes need to be determined by the size of the organization. For example, an office with one Medical Review Officer may not need to routinely change the password used to access confidential information/data while an office with multiple Medical Review Officers may need to change this password every 3-6 months.
- **Train Users:** Teach users not to use easy-to-guess passwords, not to divulge their passwords, and not to store passwords where others can find them.

LOGICAL ACCESS CONTROL

Access is the ability to do something with a computer resource (e.g., use, change, or view). Logical access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted.

Organizations must implement logical access control based on policy made by a management official responsible for a particular system, application, subsystem, or group of systems. The policy should balance the often-competing interests of security, operational requirements, and user-friendliness. In general, organizations should base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions.

Access Criteria -

Organizations can control access to resources based on the following access criteria, as appropriate:

- **Identity (user ID):** The identity must be unique in order to support individual accountabilities.
- **Roles:** Access to information may also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access. The process of defining roles should be based on functional responsibility and a need to know basis.
- **Location:** Access to particular system resources may be location based. For example a local office may have access to local data only while the headquarters' office may have access to all data.
- **Time:** Time-of-day and day-of-week/month restrictions are another type of limitation on access. For example, use of confidential personnel files may be allowed only during normal working hours.
- **Transaction:** Another criteria can be used by organizations handling transactions. For example, access to a particular account could be granted only for the duration of a transaction, e.g., in an account inquiry a caller would enter an account number and pin. A service representative would

be given read access to that account. When completed, the access authorization is terminated. This means that users have no choice in the accounts to which they have access.

- **Service Constraints:** Service constraints refer to those restrictions that depend upon the parameters that may arise during use of the application or that are pre-established by the resource owner/manager. For example, a particular software package may be licensed by the organization for only five users at a time. Access would be denied for a sixth user, even if the user were otherwise authorized to use the application. Another type of service constraint is based upon application content or numerical thresholds. For example, an ATM machine may restrict transfers of money between accounts to certain dollar limits or may limit maximum ATM withdrawals to \$500 per day.
- **Access Modes:** Organizations should consider the types of access, or access modes. The concept of access modes is fundamental to access control. Common access modes, which can be used in both operating and application systems, include read, write, execute, and delete. Other specialized access modes (more often found in applications) include create or search. Of course, these criteria can be used in conjunction with one another.

Access Control Mechanisms -

An organization must have both internal and external access control mechanisms. *Internal* access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. *External* access controls are a means of controlling interactions between the system and outside people, systems, and services. When setting up access controls, organizations can consider the following mechanisms:

- **Access control lists (ACLs):** ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular system resource and the types of access they have been permitted.
- **Constrained User Interfaces:** Access to specific functions are restricted by never allowing users to request information, functions, or other resources for which they do not have access.
- **Encryption:** Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management.
- **Port Protection Devices:** Fitted to a communications port of a host computer, a port protection device (PPD) authorizes access to the port itself, often based on a separate authentication (such as a dial-back modem) independent of the computer's own access control functions.
- **Secure Gateways/Firewalls:** Secure gateways block or filter access between two networks, often between a private network and a larger, more public network such as the Internet. Secure gateways allow internal users to connect to external networks while protecting internal systems from compromise.
- **Host-Based Authentication:** Host-based authentication grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. Many network applications in use today use host-based authentication to determine whether access is

allowed. Under certain circumstances, it is fairly easy to masquerade as the legitimate host, especially if the masquerading host is physically located close to the host being impersonated.

Organizations must carefully administer access control. This includes implementing, monitoring, modifying, testing, and terminating user accesses on the system. The host system should know whether the party requesting access is authorized based on the physical IP address.

Organizations should avoid using passwords as a means of access control, which can result in a proliferation of passwords that can reduce overall security. Password-based access control is often inexpensive because it is already included in a large variety of applications. However, users may find it difficult to remember additional application passwords, which, if written down or poorly chosen, can lead to their compromise. Password-based access controls for PC applications are often easy to circumvent if the user has access to the operating system (and knowledge of what to do).

AUDIT TRAILS

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish *several* security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails must be used for the following:

- ***Individual Accountability:*** The audit trail supports accountability by providing a trace of user actions. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis can be used to examine their actions.
- ***Reconstruction of Events:*** An organization should use audit trails to support after-the-fact investigations of how, when, and why normal operations ceased.
- ***Intrusion Detection:*** If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Intrusions may be detected in real time, by examining audit records as they are created, or after the fact, by examining audit records in a batch process.
- ***Problem Identification:*** Audit trails may also be used as online tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring.
- ***Data Integrity:*** Audit trails must also be able to track any changes to the stored information and data.

Contents of Audit Trail Records -

An audit trail must include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail should be done carefully to balance security needs with possible performance, privacy, or other costs. In general, an event record should specify:

- **Type of Event:** The type of event and its result, such as failed user authentication attempts, changes to users' security information, and organization- and application- specific security-relevant events.
- **When the Event Occurred:** The time and day the event occurred should be listed.
- **User ID Associated With the Event**
- **Program or Command Used to Initiate the Event**

Audit Trail Security -

Organizations must protect the audit trail from unauthorized access. The following precautions should be taken:

- **Audit Trail Security:** The audit trail must have the same level of security as the information it is protecting.
- **Audit Trail Storage:** The audit trail must be kept for the same time frame as the original data or documents.
- **Control Online Audit Logs:** Access to online audit logs should be strictly controlled.
- **Separation of Duties:** Organizations should strive for separation of duties between security personnel who administer the access control function and those who administer the audit trail.
- **Protect Confidentiality:** The confidentiality of audit trail information also needs to be protected if, for example, it records personal information about users.

Audit Trail Reviews -

Application owners, data owners, system administrators, data processing function managers, and computer security managers must determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities. The following should be considered when reviewing audit trails:

- **Recognize Normal Activity:** Reviewers should know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like.
- **Contain a Search Capability:** Audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.
- **Follow-up Reviews:** The appropriate system-level or application-level administrator should review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

- **Automated Tools:** Organizations should use the many types of tools that have been developed to help reduce the amount of information contained in audit records, as well as to distill useful information from the raw data.

BACKUP AND DISASTER RECOVERY

- **Data Storage Requirements:** The data backup and retrieval system must demonstrate the retrievability of archived data in a format that preserves the original information for a time frame that is consistent with the storage requirements for the original hard copy data.
- **Frequency:** The organization should determine the level/frequency of back-ups sufficient to meet the needs of the organization.
- **System Verification:** The back-up/disaster recovery system should be tested to ensure/demonstrate that the back-up/disaster recovery system functions as intended.
- **Protection of Media** Special considerations should be considered to ensure that the back-up media is protected against destruction by disaster, natural or otherwise. This may include offsite storage or fireproof containers appropriate for the stored media.
- **Application Considerations:** The backup programs must also include the application and operating system environment to ensure accessibility to the backup data/information.

ANNUAL REVIEW

There should be at minimum an annual review of the security audits and an assessment of the security procedures used, including a compliance review to ensure that the covered entities are adhering to the regulations.

The security audit should assess the effectiveness of the program to ensure that it not only meets the minimum-security requirements but should also incorporate a Quality Assurance component to look at the effectiveness of the security program and data storage protection.

SOFTWARE VALIDATION

All software changes must be tested prior to the implementation on any “live” operating system. This test must include running scenarios designed to assess the software changes and determine if the software revision achieved the desired result without impacting on existing programs and data.

REFERENCES

The following documents were used as references in the creation of this document:

- National Institute of Standards and Technology Publication 800-14. “Generally Accepted Principles and Practices for Securing Information Technology Systems.

- National Institute of Standards and Technology Publication 800-18. “Guide for Developing Security Plans for Information Technology Systems.”
- National Laboratory Certification Program. Guidance Document for Laboratories and Inspectors. OMB No. 0930-0158. November 2000 Revision.
- National Laboratory Certification Program. General Laboratory Inspection Report. OMB No. 0930-0158. July 2001 Revision.
- National Laboratory Certification Program. Guidance Document for Laboratories and Inspectors. OMB No. 0930-0158. November 2002 Revision.
- National Laboratory Certification Program. General Laboratory Inspection Report. OMB No. 0930-0158. November 2002 Revision.