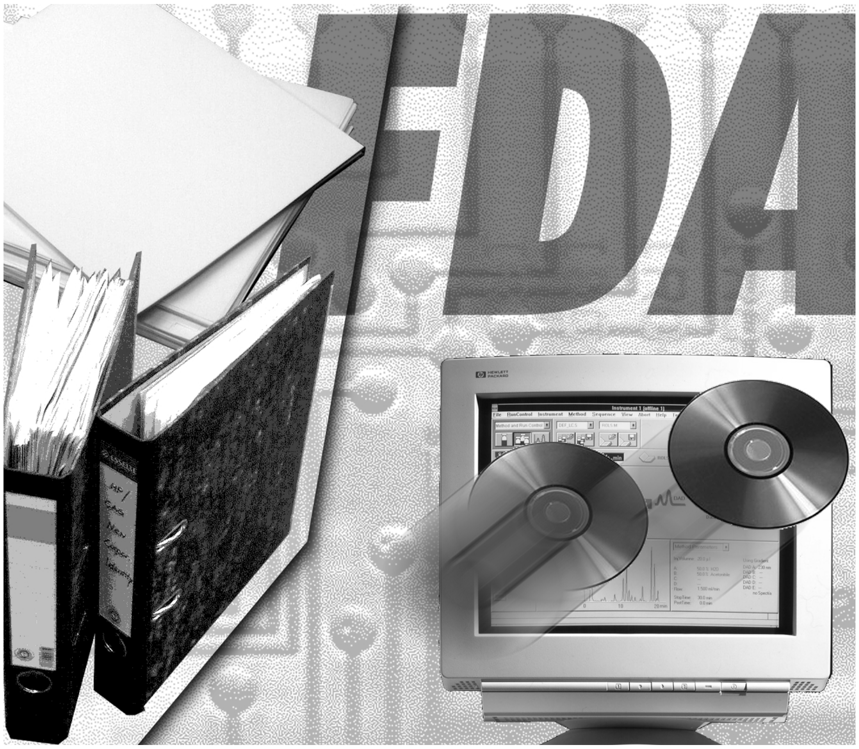
Implementing Electronic Records and Signatures with Agilent's ChemStation Family

Technical Note



Introduction

In a collaboration with representatives of the pharmaceutical industry, the FDA created a task force in 1991 to define the scope, general requirements and implementation procedures for electronic records that the agency would accept instead of the traditional "paper trail". On March 20, 1997, the final ruling on electronic records, signatures and submissions, known as 21 Code of Federal Regulations (CFR), Part 11, was signed and published. The final rule has been effective since August 20, 1997.

This final rule applies to all industry segments regulated by the FDA. Its intention is to improve the speed of submission approval through the use of technology while still protecting the agency's charter to ensure public health.

The use of electronic records will help reduce the cost of business processes that require creating and maintaining extensive paper documentation. For example, approval cycles will be shorter and access to documentation will be faster and more productive. Submissions for new drug approvals (NDA) are the first target for the use of electronic records.

Agilent Technologies
Innovating the HP Way

Electronic Records versus Paper Records

CFR 21 Part 11 regulates the acceptance criteria for electronic documents, electronic signatures and handwritten signatures executed to electronic records to be considered equivalent to paper records and handwritten signatures. For the first time, this determines how paperless record systems can be compliant with cGMP regulations (CFR 21 Part 210 and 211). The intention of CFR 21 part 11 is to explicitly enable and allow technology that was not anticipated when most existing FDA regulations were written without sacrificing the integrity of records and reports.

The ruling supersedes any existing paper record requirements in the sense that electronic records may be used instead of paper records. The rule establishes minimum criteria for electronic records and electronic signatures to be trustworthy and reliable. The intention is to minimize opportunities for record falsification and to maximize chances of detecting falsifications.

The use of electronic records and electronic signatures is voluntary within the regulated industries. Paper records are still fully accepted by the FDA. Companies can decide to replace their paper-based record-keeping with electronic record-keeping processes, provided that the requirements of CFR21 Part 11 are met and that a docket stating this intent has been submitted to the FDA. The FDA advises interested parties to contact the agency on transmission methods, media, file formats and technical protocols and accompanying paper documentation prior to submitting electronic records.

The Case for Signing Electronic Records Electronically or by Hand

So, what is an electronic signature?

Subpart C of the FDA rule explains that the signature is considered handwritten (irrespective of the technology used), if the act of signing with a stylus is still preserved. This means that a handwritten signature that is scanned in electronically and incorporated into an electronic document (i.e. an image signature) remains a handwritten signature. However, this mandates that the act of associating the electronic version of the signature to the document can only be done by and is traceable to the person whose signature is being used. Without further provisions, a simple image signature could be easily applied to other electronic documents and it would be impossible to tell that this has happened.

Such electronic versions of handwritten signatures may be applied to electronic records, provided they comply with the requirements outlined in the FDA rule on electronic records. More specifically, a handwritten signature would have to be digitized for each signing and tightly linked with the signed document (for example, by data security standards). In order to facilitate authentication and to ensure that no other individual is faking the handwritten signature, characteristics of the handwritten signature need be stored for each authorized individual. A match between the stored characteristics and the actual handwritten signature has to be determined before accepting the signature.

Today, the technology required to enable the use of handwritten signatures with an electronic pen for electronic records is sophisticated. The required hardware support for pen digitizers is not necessarily built into commercially available operating systems. Software vendors still need to adapt their software applications to enable a secure electronic path for handwritten signatures applied to electronic records.

The FDA Definition of an Electronic Signature

Today, regulated laboratories already have tight security controls in place and the security schemes available with standard operating systems, for example, Microsoft® Windows NT® help fulfill the requirements of the FDA definition of electronic records. It is therefore more straightforward to apply electronic signatures to electronic records. This can be achieved using standard technology that does not require additional hardware devices or customizations of existing software products.

Electronic signatures that meet the requirements of the FDA rule are considered equivalent to full handwritten signatures required by agency regulations.

The FDA defines the following mandatory requirements for an electronic signature:

- The electronic signature must be unique to one individual and not to be reused by, or reassigned to, anyone else (11.100).
- If not based on biometrics (see below), the electronic signature must employ at least two identification components (11.200), for example, a user id and a password.
- An electronic signature executed to electronic records must be linked to the respective record to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means (11.70).

It is important to note that the rule does not require the use of biometrics-based identification methods. Various biometrics-based identification systems are currently being offered in the computer industry. Examples include voice recognition, facial recognition, hand pattern recognition and retinal scans. They typically require additional proprietary hardware and software for each point of access to a computer system. Devices for biometrics-based identification may gradually migrate into standard computer operating systems, thus reducing the effort of installation and validation of those devices.

The FDA clearly states that combinations of user name, user-ID code and a unique password can be accepted as an electronic signature:

"A user name may be an acceptable identification code. What must be unique is the electronic signature, which (if not biometric) typically consists not only of the id code, but also a password. See 11.100(a) and 11.300(a). You can attain the e-sig uniqueness any way you wish. Generally, firms make sure the user id is unique so that if, by coincidence, two people create the same password, the result is not two identical electronic signatures. Furthermore, for e-mail account purposes, firms generally establish unique (but not confidential) id account names. It's a good idea for firms to establish sound password procedures for their staff".[4]

This permits to employ the security scheme of current, secure operating systems like Unix® or Microsoft Windows NT. The combination of a unique user-ID with a unique password only known to this person qualifies as an electronic signature. If the user-ID is chosen to match a user's full name, it complies with the requirement to show the user's printed name along with each signature:

"A code (such as 34588) is not a printed name. If the user id is, in fact the user's full name, then when printed, the userid would meet this requirement because the userid and the printed name would be identical."[4]

What is a Digital Signature?

In the previous section, an electronic signature has been defined as the electronic equivalent of a traditional, handwritten signature. Digital signatures expand this concept by applying cryptographic methods for authentication of the user and integrity of the record accessed by this user. Generally, digital signatures imply the use of personal and public encryption keys. An author uses his personal key to protect the document that he created (by encoding or "scrambling" it using appropriate

User name Carol Smith

Password *******

Figure 1
Definition of electronic signature

encryption software and his personal key). Once encrypted, the protected document can only be modified using this personal key and read by anyone in possession of the public key of its author. The encryption keys provide evidence that the document was really written by the stated author and prevent falsifications of the document.

Digital signatures require additional registration efforts with public agencies to obtain personal and public encryption keys. In addition, encryption and decryption software is needed to access and protect documents.

The FDA does not require digital signatures for signing electronic records in so-called “closed systems”.

Digital signatures are mandatory for environments that fall into a category classified as “open systems” by the FDA. Whether a system is considered “open” or “closed” depends on who controls access to it and who is responsible for the system's contents.

Open and Closed Systems

The FDA defines different measures for so-called open systems and closed systems. The controls are more stringent for open systems. In an open system, record authenticity, integrity and confidentiality have to be ensured by applying cryptographic methods and digital signatures. In a closed system, procedures and controls must be in place to ensure authenticity, integrity (and, when appropriate, confidentiality) of electronic records when creating, modifying, maintaining, or transmitting electronic records.

“Controls are any measures taken to ensure record and signature trustworthiness and reliability. Some of those measure[s] may be procedural, such as physical access limitation, and others are more automated, such as implementing audit trails.”[4]

Definition of a Closed System

“Closed System means an environment in which access is controlled by persons who are responsible for the content of the electronic records that are on the system.” (11.3.5)

Today, a pharmaceutical laboratory is typically considered a closed system under these definitions. Regulated laboratories have stringent access control mechanisms and operating procedures in place. They are in full control and fully responsible for the records they maintain. A regulated laboratory would potentially fall outside the category of closed systems if its its records were stored and transmitted on a public network not secured by the company's firewall implementation. The location of an electronic record and who controls access to that record determine whether a company's network is to be considered an open or closed system:

“You have a closed system if the record is on your firm's network and you control access to that network, even where access is through public telephone lines or T1 lines. The system is open, from your perspective, if your record resides on a network to which you don't control access. If that other system is run by a contractor, but you are responsible for the record itself, the system is open.” [5]

Consequently, implementing a chromatography data system or analytical data management system in a regulated laboratory requires a combination of procedural controls in the laboratory with security functionality inherent to the data system and its underlying operating system.

Necessary Control Mechanisms for Closed Systems

The control mechanisms that the FDA requires for a closed system should guarantee that an individual should not be able to readily say that:

- he or she did not, in fact, sign the record,
- a given electronic record containing the individual's signature was not, in fact, the record that the person signed, or
- the originally signed electronic record had been altered after having been signed.

Requirements for electronic records	How Agilent Technologies helps satisfy the requirements
• The systems used for the creation and maintenance of electronic records must be validated.	☑ The Agilent ChemStation family of products is validated during design and ships with a declaration of conformity to the internal quality processes at Agilent Technologies. ☑ Agilent Technologies offers additional validation services for installation qualification (IQ), operational qualification (OQ) and ongoing performance verification (PV) for hardware and software.
• System access must be limited to authorized individuals.	☑ The Agilent ChemStation family of products ships with Microsoft Windows NT and takes advantage of NT's inherent user access security capabilities. File access privileges can be defined on a per user basis for data files, methods, sequences and results regard less of whether they reside on a client or a server. ☑ In addition, the Agilent ChemStation database system employs user level access security to an Oracle® database used for results organization.
• Secure, computer-generated, time-stamped audit trails must be used.	☑ Agilent ChemStations allow storing raw data, methods and results in a checksum protected binary register. Method history information including a time-stamp and operator name is automatically appended to this register. Transfer logs automatically document data transfer activities in a network server configuration.
• Operational system checks must ensure the system is still fulfilling its intended purpose.	☑ The Agilent ChemStation includes installation verification and ongoing software verification functions that execute tests and reports testifying the integrity of the system.
• The system must allow the creation of accurate and complete copies of the electronic record in human readable as well as electronic format for inspection and review by the FDA.	☑ This is achieved using standard archival tools. The Agilent ChemStation can automatically store a copy of the acquisition method with the acquired raw data. ☑ Additionally, in a networked environment the automatic and traceable transfer of methods and raw data from Agilent ChemStation clients to secure file system or an Oracle database on a central server with user level security provides increasing degrees of security and control.
• Electronic records must be protected.	☑ At the operating system level, use Windows NT file system security to protect integrity and confidentiality of records stored on the computer. ☑ On standalone Agilent ChemStations, use the binary register to reliably document and reconstruct analysis results on the local PC at any time. ☑ In a networked Agilent ChemStation environment, sequence, method and data files are automatically versioned and protected on a central server running Windows NT Server. ☑ When using results organization in conjunction with a database, raw data and results are protected by user level security on the central server running an Oracle database.

Implementation Plan for Electronic Records

Implementing electronic records and electronic signatures in the regulated environment requires process and behavioral changes. The implementation should be laid out in steps.

The implementation steps with Agilent Technologies' chromatography data systems running under Microsoft Windows NT are explained on the following pages:

Step 1: Implement appropriate security controls and procedures in the laboratory

Step 2: Configure the Agilent ChemStation for electronic records support

Step 3: Configure network extensions for electronic records support (Agilent ChemAccess)

Step 4: Add Oracle database extentions for automatic and electronic results approval and storage (Agilent ChemStore C/S)

1. Implement Appropriate Security Controls and Procedures in the Laboratory

- Set up NT account system.
- Define and use NT user policies.
- Define and use NT security policy.
- Configure an inactivity timeout
- Define and implement password implementation policy.

The first step requires an evaluation of the current procedures for system access, record creation and modification, record signing, and record archival. The first step reveals which user groups exist in the current organization and what responsibilities and privileges they have. These responsibilities and privileges then have to be mapped into appropriate account system and security policies on the computer systems. Individual accounts must be set up for every user who needs access to the system. Each user requires a unique user-ID and a unique password. Shared user accounts or passwords that can be easily guessed are unlikely to be acceptable to an FDA inspection. Groups of users with similar responsibilities can be assigned group permissions on the system. Standard user groups configured on Agilent ChemStations are for administrators, chemists and service personnel.

It is common in the IT environment to mandate passwords that are at least 8 characters long and require a combination of letters and numbers. Windows NT supports a technique called password aging that will expire user passwords after a defined period and will require a new, different password for the user.

It is advisable to implement so-called NT user policies. NT user policies assign user profiles and secure user directories to each user and can be used to simplify the NT desktop by restricting access to only the programs that the user is authorized to use.

Since Agilent ChemStations typically run in unattended mode, for example, automated sequence mode overnight data acquisition, it is advisable to set inactivity timeouts on the NT desktop. This will prevent unauthorized access to the computer system while the operator responsible for the unattended session is away. A standard operating procedure for securing unattended computer systems is highly recommended.

When step 1 is completed, the procedural controls required for electronic records management in closed systems are in place.

2. Configure the Agilent Chem-Station for Electronic Records Support

- Tie into NT account system security.
- Enforce data security and traceability with the GLPSave register.
- Modifications to the method are tracked in the Method History Log.

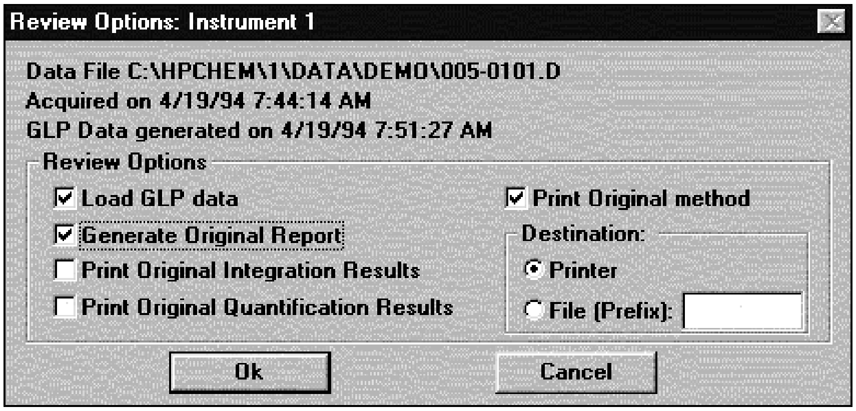
Under Windows NT, the Agilent ChemStation can be configured to retrieve the user-ID of the current logged-in user and store this as the operator. The Agilent ChemStation operator name is automatically stored in the data files acquired by the operator. Changing the operator name then requires a new logon to Windows NT. The advantage is that all system access is validated by the NT operating system. It is not necessary to rebuild the account system in the Agilent ChemStation.

For the data acquired by the validated operator, data security and traceability should be enforced by enabling the secure binary register storage option of the Agilent ChemStation method.

This option stores chromatographic signals, spectral data, integration results, quantification results, instrument performance data and data analysis method details in a binary, checksum-protected register. Additionally, a logbook entry testifies that the binary register was stored. Using the appropriate review function, results can be reconstructed at any time.

Modifications to the method parameters are tracked in a method history log that stores the operator name, a computer-generated time-stamp and an optional comment of the operator.

When step 2 is completed, the automatic access verification and audit trail elements for sequences, methods and data files are in place for a single Agilent ChemStation.



Review Options: Instrument 1

Data File C:\HPCHEM\1\DATA\DEMO\005-0101.D
Acquired on 4/19/94 7:44:14 AM
GLP Data generated on 4/19/94 7:51:27 AM

Review Options

☑ Load GLP data
☑ Generate Original Report
□ Print Original Integration Results
□ Print Original Quantification Results
☑ Print Original method

Destination:
● Printer
○ File (Prefix):

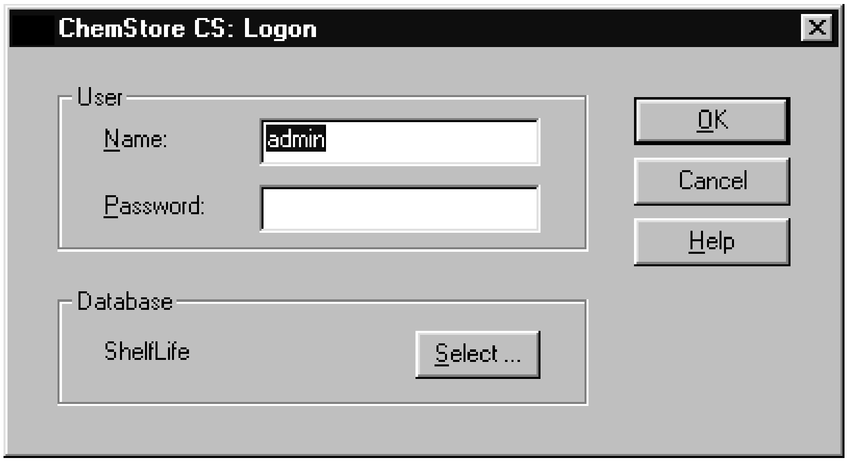
Figure 2
Review GLP data

3. Configure Network Extensions for Electronic Records Support (Agilent ChemAccess)

- Implement security privileges for each chromatographic instrument in the laboratory
- Store secured and versioned raw data centrally

In workgroup based laboratories with an existing network infrastructure, distributed computing can significantly enhance the information flow and reduce the time that it takes to administer the systems in the lab. The Agilent ChemStation extension provides lab-wide status and can centrally store the sequences, methods and data files acquired by a workgroup on an NT server. The system keeps secured and versioned revisions of sequences, methods and data files.

When step 3 is completed, centralized administration and raw data security are in place for a laboratory workgroup.


ChemStore CS: Logon

User

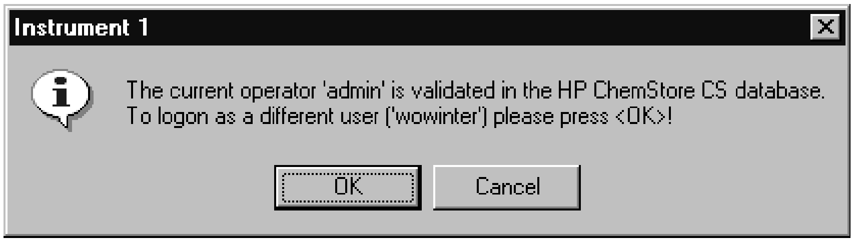
Name: admin

Password:

Database

ShelfLife

Figure 3
Agilent ChemStore validates the currently logged-on user


Instrument 1

The current operator 'admin' is validated in the HP ChemStore CS database.
To logon as a different user ('wowinter') please press <OK>!

Figure 4
The Operator designation of the Agilent ChemStation is protected by the database extension

4. Add Oracle Database Extensions for Automatic and Electronic Results Approval and Storage (Agilent ChemStore C/S)

- Use first pass data review and approval to electronically transfer results into the database.
- Second pass data review in the database, for example, by a supervisor).
- Approve/reject results from within the database.
- Assign reanalysis tasks online to a specific operator from within the database.

Authorized users can use the batch review function of the Agilent ChemStation as a first pass data review of acquired data for result accuracy. Data that pass this first review can be automatically uploaded into the database. The relational database allows results organization of all chromatographic data acquired by Agilent ChemStations throughout the laboratory, including chromatogram and spectra graphics, and, optionally, binary copies of the raw data.

A user-level security based networked Oracle database extension to the Agilent ChemStation can then be used for a second pass data review, including tabular and graphical result visualization and optional trend charting. Data that passes the second review cycle, can be approved automatically by authorized users of the database. Data that do not fulfill the quality criteria can be flagged as “rejected”. Rejected results can be assigned for reanalysis by a specified operator. The batch data to be reanalyzed by that operator is downloaded to him electronically.

After identifying and taking appropriate action to fixing the problem by a reanalysis step (for example, by reintegrating the chromatogram), the revised result is uploaded automatically to the database as a new revision of the analysis result, keeping the original revision in the database for traceability purposes.

When step 4 is completed, a lab-wide electronic record system is established for the chromatographic raw and results data. Results data is organized in a secure relational database based on Oracle.

Frequently Asked Questions

What happens to the electronic signature if the respective employee leaves?

Industry representatives worried at first about the possible implications of having to maintain electronic signatures in a system overtime, taking employee turnover into account. The following explanation by the FDA shows that the user account capabilities built into secure operating systems. for example, Microsoft Windows NT can be used to satisfy the requirement.

"It should be easy to link the signature to the record so that folks can't copy the signature to falsify an electronic record by ordinary means. The link must be retained for as long as the record is kept, just as a handwritten signature stays with the paper, long after an employee has departed a company. A user id/password can be removed from a current user database, but still be retained in an archive for purposes of this section."[4]

When an employee leaves the company, the system administrator disables the employee's user account, to prevent misuse by another user. The electronic records already associated with the departed employee's electronic signature are not invalidated.

Do we need to maintain old equipment over the record retention time?

Does this mean that companies who standardize on electronic records will have to maintain obsolete systems for accessing electronic records during the record retention period? The answer is "no". The FDA does not require maintaining obsolete equipment as long as the electronic records are fully transcribed from the old system to the new system.

Suppliers of analytical data management systems must provide viable and functional migration or upgrade paths for equipment reaching the end of its useful life. Agilent Technologies has a proven track record for backwards compatibility. Current Agilent ChemStations control HP 1090 liquid chromatographs manufactured since 1983 and equipped with the appropriate firmware upgrades. Current Agilent ChemStations import data and spectral libraries generated on Pascal ChemStations since 1986. Agilent Technologies is committed to continuous, non-disruptive innovations in the analytical laboratory.

Literature

1.
"Electronic Records; Electronic Signatures 21 CFR Part 11" Department of Health and Human Services Food and Drug Administration Docket No. 92N-0251RIN 0910-AA29"

2.
" Towards the "Paperless" Pharmaceutical Lab" *PEAK 1/1998, page 5 Agilent Technologies*

3.
Prof. Dr. H.-D. Unkelbach Fachhochschule Wiesbaden "Electronic Signature Presentation, PTS Seminar" September 19, 1997, Düsseldorf, Germany

4.
Paul Motise (FDA) "Responses to questions posed by the PhRMA Computer Systems Validation Committee about Electronic Records and Signatures regulation (responses received April 21, 1997)"

5.
Paul Motise (FDA) "Responses to questions posed by the PhRMA Computer Systems Validation Committee about Electronic Records and Signatures regulation (responses received June 12, 1997)"

For the latest information and services visit
our world wide web site:
http://www.agilent.com/chem

Publication Number 5966-2315E

Agilent Technologies
Innovating the HP Way