Using Agilent ChemStation to make sure UV-visible spectroscopy data complies with FDA 21 CFR Part 11

Technical Note

Introduction

Effective August 20, 1997, the U.S. Food and Drug Administration (FDA) released and published a new rule to enable pharmaceutical companies to approve their results with electronic signatures and to transfer paper-trail documentation into electronic records. This rule is known as 21 Code of Federal Regulations, Part 11 (refereed to as 21 CFR Part 11) and applies to all industry segments regulated by the FDA.

The requirements on electronic records of 21 CFR Part 11 are not new to the industry as they only summarize several predicate rules. But, 21 CFR Part 11 places high emphasis on the implementation of all measures to protect and secure electronic records.
In addition to this rule on electronic records, other general requirements for computerized systems are brought to the auditor's attention. These rules cover the basic requirements of validation, limiting data access, and ensuring data integrity and data traceability.

This note outlines how the Agilent ChemStation for UV-visible spectroscopy in combination with the advanced or dissolution mode and security pack can help to meet the demands on data security, data integrity and audit-trail. However the ChemStation solution for compliance with 21 CFR Part 11 is designed for and supported in a closed system only.

21 CFR Part 11 requirements

To fulfill the FDA rules and guidelines for compliant electronic records and computerized systems, the most important basic aspects of secure data handling are:

- data security—physical protection of data by limiting access to the system and preventing unauthorized access
- data integrity—protecting raw and meta data and preventing these from unauthorized modification, and linking raw data and results to reproduce the original results at any time, for example, in an audit
- audit traceability—documenting who did what to the results and when, and tracing the user changing meta data such as method parameters

The following evaluation of the FDA rules deals exclusively with closed systems and explains how the Agilent ChemStation for UV-visible spectroscopy helps to address these requirements for closed system, and, finally, how to sign-off measured data and results electronically by applying electronic signatures.

Agilent Technologies
Innovating the HP Way

Agilent ChemStation for UV-visible implementation of FDA requirements for data security, data integrity and audit trail

Data security—limited system access and password policy

The rule requires that all users must be positively identified by having a unique user ID and a personal, secret password before being able to gain access to any computer or computer network and critical application software as verified against the security table at log-in.

The ChemStation for UV-visible access control is based on the user administration of Windows NT (user groups called ChemStationOperator or ChemStationManager) and allows only users with granted permission and a proper identification to logon to the ChemStation and perform specific actions. One of the most important requirements for limited system access is that only the individual users know their passwords and even the system administrator can only manage the users and their user IDs but not their passwords.

The implementation in the software is a two-step approach. First, the Windows NT administrator sets up user identifications and appropriate permission rights for the individual users. Second, when the users first log on to the application, a log-on screen prompts for specification of the individual password. This two step approach ensures that only the individual user knows their password.

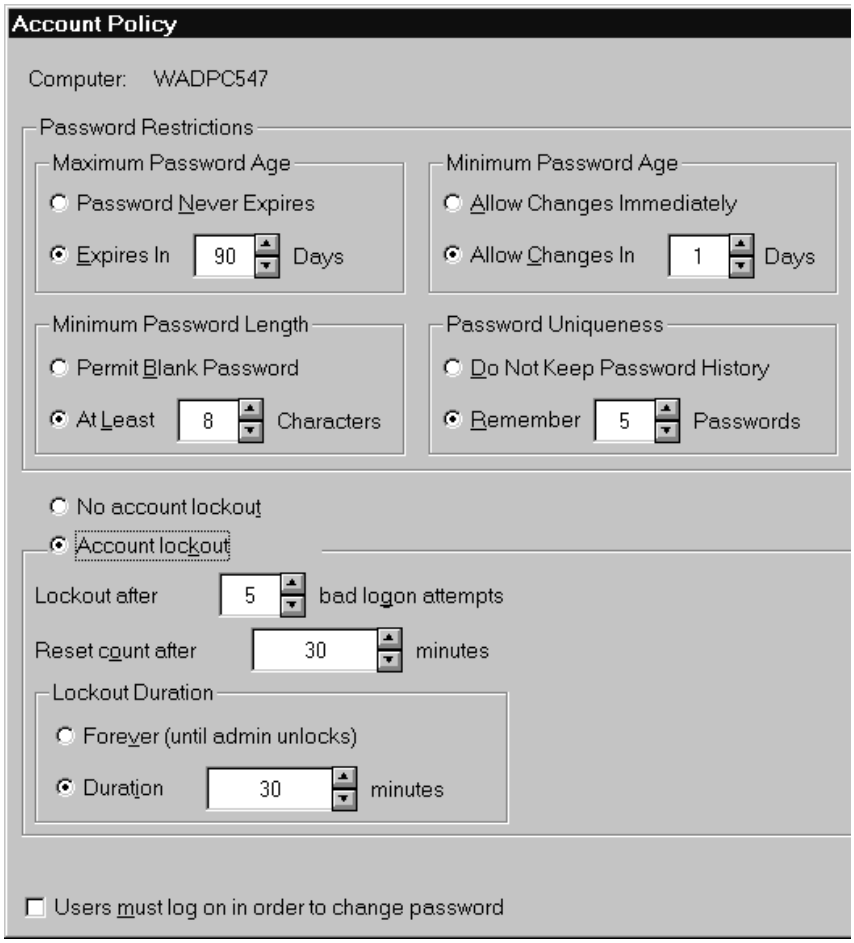

Figure 1
Windows NT account policy

To periodically check and revise the password, Windows NT password-administration function has to be set to apply the company's individual password policy for minimum password length, expiry date, session lock-out, and so on. This is shown in figure 1.

Windows NT automatically tracks all violations of access and a lock-out for incorrect logon is configurable. Especially in a production environment, the user often starts a series of measurements and continues to work on another task. In this case it is important to control also the access during the execution of a sequence of measurement. To address this need, the ChemStation can be either locked manually by the user, or automatically after a given period of time.

Data Integrity

To assure data integrity, it is important, that both raw and meta data are protected from unauthorized modification. It is also important that a link exists between raw data, method parameter and results to enable the user to reproduce the original results at any time, for example, in an audit.

The simplest way to demonstrate the concept of data integrity implemented in the ChemStation for UV-visible is to look at the way results are generated and stored from an operator's point of view. First, the operator starts the ChemStation and logs in with their user ID and password. As an operator, they only can load predefined methods from the local hard disk or a server. The measurement sequence will take place in a *closed* loop and requires always the storage of a result file on exit of this sequence.

Within the sequence the operator can only measure blanks, sample and standards. In case of a wrong measurement, the spectrum can be *deleted* and the operator has to give a comment to document the reason for deletion. The *deleted* spectra are not removed from the raw data set, but stored in a specific data block. They are still accessible later on and labeled with information on operator, time, date and reason.

After finish of a sequence of measurements, the result file is saved. This single file includes the complete method, all raw data (complete spectra), the deleted spectra, a run logbook and a signature logbook. By this, all results can be reproduced during an audit from the raw data and the logbook gives information on the actions during generation of the original results, who did what and when, for example measuring this samples or a statement on deletion of a spectrum. In the case of a deleted spectrum, the reviewer even can recall it later and add it to the data set again. Figure 2 shows an example of a logbook of a result file.

It is worth mentioning the advantage of having always the complete spectra of all measurements available and not just a single absorbance value. Looking at the spectrum can often explain the reason for an ambiguous result, for example, a wrong sample, disintegration, background due to an impurity, or an air bubble. The spectrum can also be important to justify a result as to be an outlier.

The result file itself is protected against manipulation or deletion using Windows NT file access permissions. The belonging of a user to one of the ChemStation user groups controls the permission for all future file access using either the ChemStation or other applications like the Windows Explorer. For example, the ChemStation operator has only the permission to create a result file once during the outlined procedure and after that time he can not modify, move, delete or rename it anymore.

Run Logbook

Date	Time	Message
10-Apr-00	14:36:57	Signature was executed on result file C:\HPCHEM\1\DATA\SB_LFS.AR
10-Apr-00	14:34:55	1 Sample deleted.
22-Mar-00	20:31:23	Signature was executed on result file C:\HPCHEM\1\DATA\SB_LFS.AR
22-Mar-00	20:30:13	1 Spectrum restored.
22-Mar-00	10:36:20	1 Sample deleted.
22-Mar-00	10:33:42	--> Data Analysis Parameter
22-Mar-00	10:33:42	Method MODIFIED by Stephan Bayerbach
22-Mar-00	10:33:41	Method CALIBRATED
22-Mar-00	10:33:06	--> Changed Standard(s)
22-Mar-00	10:33:06	Method MODIFIED by Stephan Bayerbach

Signature Logbook

Date	Time	Reason	Signed By
10-Apr-00	14:36:57	Result approved	Stephan Bayerbach
22-Mar-00	20:31:23	Result reviewed	Stephan Bayerbach
22-Mar-00	10:36:58	Result saved	Stephan Bayerbach

Figure 2
Example of a result file logbook

Audit traceability

As mentioned earlier, result files can not be overwritten or modified by the operator. The same is true for method files. If a method is changed, it has to be saved in a different file. Each method includes a logbook, which is automatically attached to the method, with the history of the method as well as a comment explaining the changes. The logbook allows a tracing of all predecessors of each method by the name and location on the filing system.
A versioning based on the logbook is implemented for result files. In this case, a reprocessing with changed parameters will append the logbook with information on the actions done during reprocessing. If the result is stored again, the result file includes the changed method, all raw data and spectra as well as a copy of the actual logbook.

Electronic Signatures

The operator can sign a result before storing it by giving their user ID and password. Existing results can be reviewed by the manager and signed off for review with their user ID and password.

All signatures have a single line of user-definable text for the purpose (for example, result created, result reviewed) and are documented in the signature logbook of the result file with date, time, reason and full name of the person who signed.

Different modes of the ChemStation and support of 21 CFR part 11

The different modes of the ChemStation for UV-visible offer different features depending on the application. For full support of 21 CFR part 11, the advanced and/or the dissolution-testing mode are required. Table 1 gives an overview on the available features of the security pack in combination with the different application modes.

	Software Mode			
Feature	**Standard**	**Advanced**	**Dissolution**	**Kinetic*** **
Raw data protection	Yes	Yes	Yes	–
Storage of raw and meta data	No	Yes	Yes	–
Mandatory log-on	Yes	Yes	Yes	–
Versioning on the ChemStation side	No	Yes	Yes	–
Electronic sign-off	No	Yes	Yes	–
Application lock*	Yes	Yes	Yes	–
Audit-trail method	Yes	Yes	Yes	–
Audit-trail raw/meta data	No	Yes	Yes	–
Archiving built-in**	No	No	No	–
Password policy part 11	Yes	Yes	Yes	–
Data recovery tools	No	No	No	–

* Not mandatory for part 11 compliance, but highly recommended for data security and lomg-term data storage. These tasks have to be done by the IT department.
** Not mandatory for part 11 compliance, but important in production environments.
*** Not supported.

Table 1
Overview of features available in the ChemStation security pack

Publication Number 5980-1051E

Agilent Technologies
Innovating the HP Way