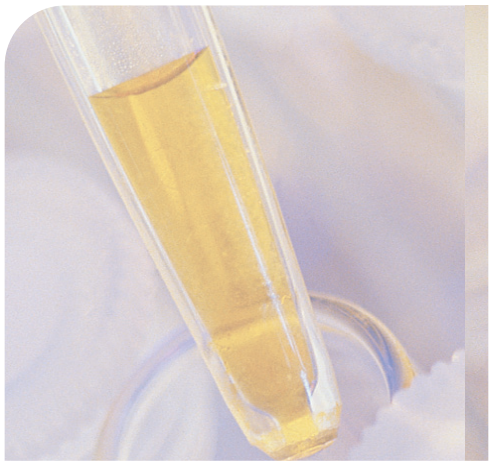

Laboratory Products Focus

DECODING 21 CFR PART 11

S. Raghuraman and Dr. Lai Weng Chuen

The 21 CFR Part 11 was effected in 1997 by the US Food & Drug Administration (FDA) to encourage wider use of electronic data technology. With predicate regulations such as GMP, GLP and GCP as its base, Part 11 delineates a set of criteria to implement control, validation and audit trail on electronic data that are meant to replace written documents as equivalents.

Although necessary to preserve data integrity, Part 11 remains one of the most challenging regulations imposed by the FDA on the biotechnological and pharmaceutical industries, directly affecting all systems that generate, store and use electronic data which fall under the predicate regulations.

In August 2003, after gathering significant industry feedback, FDA released the guidance draft "Industry Guide, Part 11, Electronic Records; Electronic Signatures – Scope and Application". Through this scope and Application Guide, the agency announced a narrowed scope of Part 11 with enforcement discretion exercised on items such as computerised systems validation, time-stamped audit trails, and methods used to reproduce and retain electronic records. This guide remains relevant today, pending a revised version of the Part 11 regulation to be released by FDA.

Author Details:

S. Raghuraman, Engineering Director
and Dr. Lai Weng Chuen, R&D Director
Eutech Instruments
Email: eutech@thermofisher.com
Web: www.eutechinst.com

GUIDANCE PAPER WITH LITTLE GUIDANCE TO FOLLOW

If the magnitude of Part 11 is not enough to stumble the compliance folks, the wide range of interpretations surrounding Part 11 serves to confound the industry.

Despite the Scope and Application Guide, "enforcement discretion" really means "enforce where appropriate", and companies are left to wonder as they design their compliance plans at their discretion, depending on the predicate regulations which they are subjected to. Under such circumstances, it is not uncommon to see companies overwhelm themselves by over-complying.

Confusing as it is, companies looking forward to the promised amendment of Part 11 are unlikely to find more concrete rules to follow. Fundamentally, Part 11 is a regulation that supports the predicate regulations which a company is mandated to comply with. It doesn't specify what data needs to be regulated or for how long – these are dependent on the requirements of the relevant predicate regulations and internal company policies. Because of the myriad of systems and situations which the regulation is applicable to, a certain amount of flexibility in definition is inevitable.

COMPLYING WITH PART 11

So the question is, how much is enough, and how much is too much? Logically, a company will do well to base its compliance plan on the regulation – a federal law, and not just on the guidance paper – a guide that carries no legal force. This said, not all systems and data are subjected to Part 11 regulation. In determining the system and data to include under Part 11 compliance plan, a company may start off with asking the following questions:

- Are these records and signatures required by the predicate regulations?
- Are these records and signatures part of an SOP that is required by the predicate regulations?
- Are these records and signatures relied on to perform regulated activities?

Once the parameters are set, the next step is to identify the points in your system where data is recorded, edited, transmitted and archived, then ensure full audit trail at these junctions to track any actions performed on these data.

Both a closed system and an open system (see *Figure 1* for FDA definition) require full time-stamped audit trail records documenting any data manipulation. An open system also requires document encryption and use of appropriate digital signature standards. This may seem like a daunting amount of documentation, but a good 21 CFR Part 11 software package will simplify your processes significantly.

Definitions

According to the US Food and Drug Administration:

A closed system means as an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

An open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Figure 1. Definitions According to the FDA

21 CFR PART 11 & ELECTROCHEMISTRY

Electrochemistry is widely used in biotechnology and pharmaceutical laboratories, where measurements are typically taken using research bench meters. These measurements are increasingly automated and the reports generated by these instruments will therefore need to comply with 21 CFR Part 11 if the data falls under any of the predicate GxP regulations.

Some electrochemistry research bench meters in the market, like Eutech's CyberScan 6000 series, run on a Windows operating system, enabling the bench meters to perform basic PC functions apart from their usual measurement utility. In other words, researchers can effectively perform measurements, data storage, report generation and go on the internet to do researches or email their report all with one instrument, without hooking up to a computer.

Despite the comprehensive functions which allow users to contain their research activities within one instrument, such systems are still considered to be non-compliant without an audit-tracking function.

To assist with Part 11 compliance, Eutech has come up with a software, the CyberComm 6000, that helps to automate audit-tracking when users connect the meter to a computer installed with this programme.

The CyberComm 6000 is a software that transfers the entire meter's interface to a computer system, so users can conduct their researches on the meter through their computer. Like the CyberScan 6000 meter, CyberComm 6000 allows users to create individual password-secured login accounts to collect, analyse and control their research data.

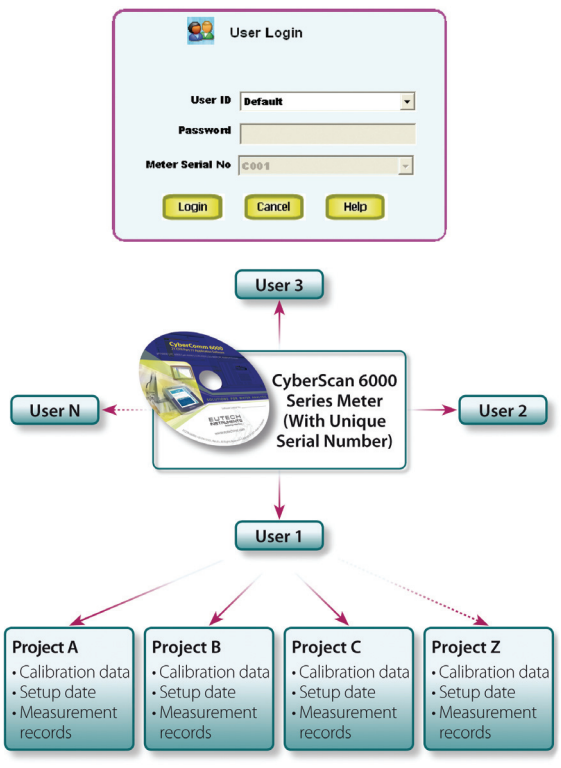

Figure 2. The ID-Password login system is a popular form of electronic signature that is not based upon biometrics, and allows users to utilise the same system in a secured and compliant manner.

The software is equipped with analysis functions like the real-time generated graphs and charts, and data can be protected within the programme under individual accounts, thereby limiting access to the user only.

The added advantage is an audit trail mechanism within the software that automates the audit process entirely: Each data point generated is stamped with time and date; each user access, view or edit creates an entry in the CyberComm 6000 activity log, stamped with time, date, meaning of the action, and the user responsible.

This activity log is accessible only by the administrator account holder. In case of accidental deletion, this log is double backed up within the system, retrievable with the manufacturer's help.

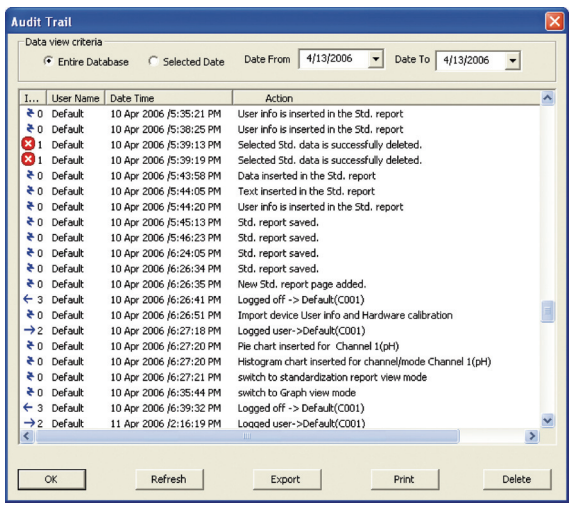

Figure 3. Automated audit trail records all data manipulations with date, time, user and action

A SYSTEM IS MORE THAN JUST SOFTWARE

Using software provided by Instrument manufacturers, with built-in technical controls for Part 11 compliance, is just one part of the entire system compliance plan. For complete Part 11 compliance, users have to ensure that their entire IT systems or Laboratory Information & Management Systems (LIMS) also comply.

For example, the simple act of sending data governed by a predicate regulation through email can complicate your compliance plan significantly as it extends to your email system. Although accessible only by the appointed receiver via ID and password login, an email sent through the Internet usually travels through several servers before reaching the specific users. The email system is therefore, treated as an open system under Part 11; and a document, if sent via email unencrypted, is deemed as insufficiently protected.

In other words, no matter how good a software you use, lack of data-management knowledge on the part of those handling data can deem your research non-compliant. The CyberComm 6000 provides a direct link between the research instrument and the storage/ analysis system; it simplifies the audit trail process by recording all activities within the programme from data generation all the way to storage. Yet, even with the most comprehensive software, a compliance plan is still reliant on how the relevant personnel uses the system, and is only complete when the right tools are used in tandem with proper training, guidance and a comprehensive S.O.P in place.

Some salient technical controls to look out for when choosing your software:

- ***Ability to generate accurate and complete records in human readable and electronic format for agency review and copying***
- ***Data archiving and protection to enable ready and accurate retrieval of records for reviews by the agency***
- ***Security mechanism with electronic signatures that limits distribution of, access to, and use of data only to the relevant personnel***
- ***Mechanism to maintain the uniqueness of combined ID and password, so no two researchers have the same combination of ID and password, or in the case of biometric electronic signatures, a mechanism to ensure the signature cannot be utilised other than the genuine owners***
- ***Automatic audit trail recording mechanism that generates a record, stamped with date, time, action and user ID stamping, each time a data point is created, modified or deleted***
- ***New entries should not obscure previous records, and the audit log should be kept archived, accessible only by the administrator***
- ***Document encryption ability, in the case of Open Systems***

Figure 4. Choosing your software

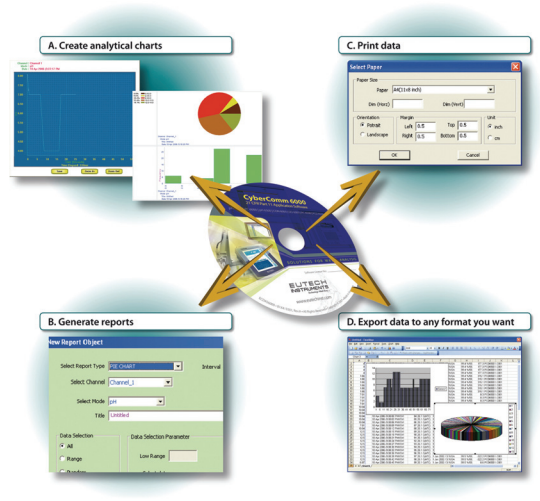

Figure 5. The Eutech CyberScan 6000 Series allows users to perform basic PC functions such as Create Analytical Charts, Generate reports, Print data and Export data to any format you want.

ABOUT EUTECH CYBERCOMM 6000

The CyberComm 6000 is a software designed for use with Eutech CyberScan 6000 Bench meters, the World's first full-colour CE Windows Touchscreen Research Meters. Available for simultaneous multi-parameter measurements of pH, Ion, Conductivity, Resistivity, TDS, Salinity, Dissolved Oxygen, BOD and Temperature.

REFERENCES:

"Guidance for Industry Part 11, Electronic Records; Electronic Signatures – Scope and Application", Pharmaceutical CGMPs, August 2003

"21 CFR Part 11: Electronic Records; Electronic Signatures; Final Rule; Electronic Submissions; Establishment of Public Docket; Notice",

Food and Drug Administration (Department of Health and Human Services), March 1997

"Pharmaceutical cGMPs for the 21st Century – A Risk-based Approach, Final Report" Food and Drug Administration (Department of Health and Human Services), September 2004

Tammala D. Woodrum, JD, "21 CFR Part 11: The Role of Predicate Regulations and Associated Internal Policies", Drug Information Journal, V37, 2003.

Easy Biological Wastewater Analysis with CyberScan DO 6000's Automatic 5-Day BOD Test

The five-day BOD, OUR (Oxygen Uptake Rate) and SOUR (Specific OUR) are important test procedures employed in industrial biological wastewater management. The five-day BOD test measures the amount of dissolved oxygen required to biodegrade waste pollutant in five days, and is EPA-mandated in many industries to maintain environmental law compliance, such as animal feed lots, paper mills, refineries and chemical plants; OUR and SOUR, on the other hand, are rapid tests used to evaluate how toxic or biodegradable a wastewater sample is within two to five minutes.

Whether it's BOD, OUR or SOUR analysis, **Eutech**'s CyberScan DO 6000 series is equipped for accurate, in-depth dissolved oxygen measurements complete with detailed analysis charts. Designed for advanced lab research, the DO 6000 comes with an automatic 5-day BOD testing function with on-screen prompts and a self-stirring probe. BOD, OUR and SOUR testing simply is a breeze with this research meter.

The CyberScan 6000 research-grade benchmeter series is also available for multiparameter measurements of pH, pH FET, ORP, Ions, Conductivity, TDS, Salinity, Resistivity and Temperature. With advanced communication features, every CyberScan 6000 benchmeter comes with internet capabilities so users can go online with the meter directly and send their research data to any computer.

Figure 1. Automatic five-day BOD test with sample ID and self-stirring probe that complies with EPA method requirements

Figure 2. Extensive Communications Capabilities: RJ45 Internet/Intranet; SD Card; USB; Wireless IrDA; RS232 and Audio Inputs