

## FacilitySight 21 CFR Part 11 Compliance

### What is 21-CFR Part 11?

Pharmaceutical companies have historically submitted product applications to the Food and Drug Administration (FDA) on paper. With the advent of technology this is now dominated with electronic data records and electronic submissions. This change in philosophy has meant that in the FDA's efforts to "Protect Human Health", they have had to put controls in place to ensure that this 'new' data is as reliable as the original. The 1997 Electronic Records; Electronic Signatures Rule (21 CFR 11) is the document which defines those controls. 21 CFR 11 stipulates the rules concerning the use of the electronic records and also defines the requirements for data capture, storage, retrieval, maintenance and security of those records when reviewed by FDA inspectors.

Pharmaceutical companies typically produce two things, Drugs and Data. Data is gathered at source and either automatically downloaded onto a database or manually input into a database. As multiple database formats exist with no common security format the requirements for an industry standard became apparent. Data which is not generated, stored or maintained as a permanent electronic record is, by the same provisions, not required to meet the regulations, therefore data stored locally in instrument volatile memory and printed direct to a printer does not need to comply.

The 21 CFR 11 regulations are divided into three subparts, General Provisions, Electronic Records, and Electronic Signatures.

**Electronic Records** – An electronic record is "any data or other information represented in digital form, which is created, modified, maintained, archived or distributed by a computer system."

**Electronic Signatures** – Under the regulation, signatures can either be:

- A handwritten signature "is the legal mark of an individual, handwritten by that individual and executed to present intention to authenticate a writing in permanent form."
- An electronic signature is "a computer datacompilation of any symbol or series of symbols executed, adopted or authorized by an individual to be the legally binding equivalent of the individual's signature."
- A digital signature is an electronic signature based upon biometric measures of the originator's authenticity.

### Computer Systems

Computer systems are divided into two categories, closed systems and open systems.

**Closed System** – A system maintained on a dedicated connection between source and storage where open external access is not permitted.

**Open System** – In an Open System data is gathered from multiple locations and stored to a common central location; access to this database must be rigidly maintained and requires encryption to ensure the source of data is valid. Closed system security requirements specify controls for the authenticity, integrity, and confidentiality of electronic records. This requires that:

- Data can be retrieved for audit, or review in human readable format.
- Audit Trails must exist, be secure, date and time stamped and un-editable. They should record all the system changes applicable to the data collected, stored and retrieved.
- Security controls are in place to ensure
  - No two individuals have the same combination of user name and password.
  - Periodic checks and recalls of identification code or passwords.
  - Loss management and replacement procedures.
  - Safeguards against unauthorized use.

Reporting of unauthorized use in an urgent and immediate manner.

Open system security requirements also have to meet these standards, but with the addition of measures ensuring authenticity, integrity and confidentiality, i.e., document encryption and digital signal standards.

The system above states the rules that apply to software systems. However, as all systems are inherently different they are open to interpretation. The FDA guidelines (Title: Enforcement Policy 21 CFR 11 Electronic Records; Electronic Signatures, CPG7153.17 13-May-1999) for inspectors states "the agency's current thinking on the rule" to that end Particle Measuring Systems has made best efforts to meet all interpretations in the FacilitySight software application.

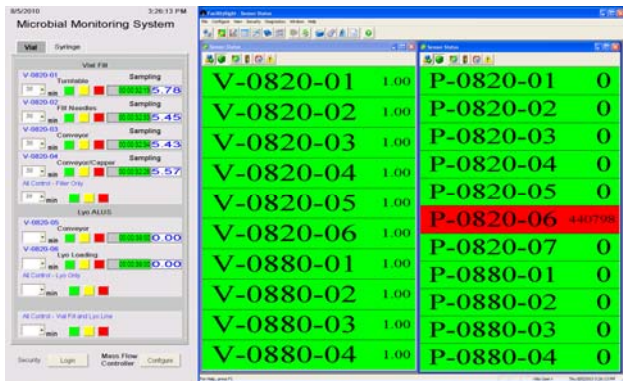
### FacilitySight and 21 CFR Part 11

FacilitySight is the all-encompassing facility monitoring software, offering Windows® based

compatible software package providing collection, storage and analysis of data reported by Particle Measuring Systems instrumentation and other facility monitoring devices. Data from other devices such as third party particle counters, airflow velocity, DI resistivity, dissolved oxygen, temperature, absolute pressure, differential pressure, and relative humidity sensors can be collected with FacilitySight while satisfying 21 CFR Part 11 requirements.

To meet compliance with the general provisions and ensure that the electronic records (data) can be verified as genuine, trustworthy and as reliable as the original, the database that is used in FacilitySight is binary format, encrypted in a Borland Database. Three files per database per day are generated and three are required to retrieve the data. This prevents any alteration of the data outside of FacilitySight.

FacilitySight software is installed on a local computer (Server). This computer communicates to the field sensors using Ethernet 10BaseT, Serial RS-485 or Serial RS-232 direct commands. The data is returned from the field sensors into the FacilitySight software for display, alarm alerts, and data storage. The only access into this database is through FacilitySight; this follows the rules applying to **Closed Systems**.

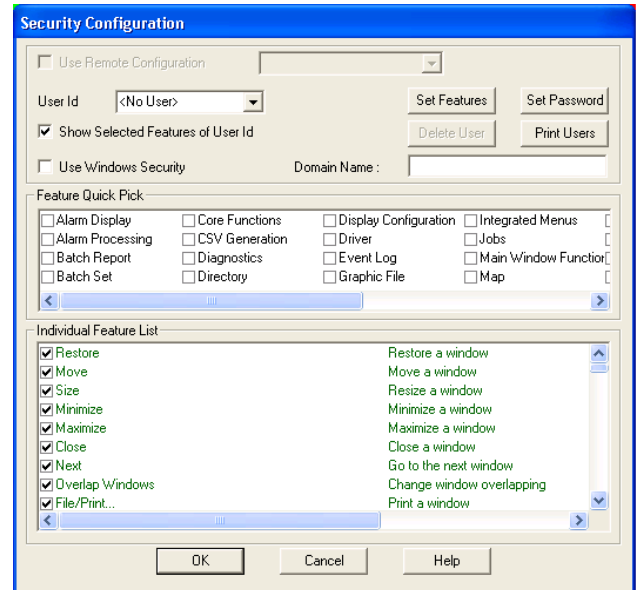


**Figure 1. FacilitySight interface**

If the system is to be networked across a site network, a firewall between the Particle Measuring Systems segment of the network and the corporate network is recommended.

To ensure that access to the stored data meets all the controls required for closed systems the following systems have been put in place.

A full **audit trail** monitors all system-generated events, including threshold alarms and warnings, hardware alarms, security changes, configuration changes, user logins/outs and all other user events.



**Figure 2. Security Configuration window**

In the **Security Configuration** window each user is assigned specific tasks that are defined by the security administrator and every user is configured with a unique user name and password. On first login the user is prompted to change password. For ease of validation, the complete security configuration settings can be printed – excluding passwords! Passwords are retrieved every 90 days for review and change; this time period can be changed by the security administrator.

Should any unauthorized login attempts be made, a system alarm communicates this alarm via a configured pager or email alert. After 5 attempts, an entry is also made into the Audit log. For large integrated network systems the operators at the network terminals are assigned security from either the local network computer or controlled from the respective server.

Author: Bryan Young, Particle Measuring Systems

Windows® is a registered trademark of the Microsoft Corporation.

GAMP® is a registered trademark of ISPE. To learn more about GAMP to place an order, visit [www.ispe.org](http://www.ispe.org)

© 2010 Particle Measuring Systems. All rights reserved.

Reproduction or translation of any part of this work without the permission of the copyright owner is unlawful. Requests for permission or further information should be addressed to Particle Measuring Systems, Inc. at 1-800-238-1801