FDA 21 CFR Part 11
Electronic records and signatures – solutions for the Life Sciences Industry

Power and productivity
for a better world™

The Rule 21 CFR Part 11

"Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form."

FDA 21 CFR Part 11

For Life Sciences Industries, electronic signatures were given legal equivalence with traditional "wet ink" signatures on paper in 1997.

The Food and Drug Administration (FDA) rule for electronic records and signatures became effective and enforceable on August 20, 1997. The rule has two main areas of enforcement: electronic records and electronic signatures.

The rule applies to all areas of Title 21 of the Code of Federal Regulation (CFR) for all manufactured drugs and medical products distributed in the United States of America.

Detailed procedural and technical requirements are given for both electronic signatures and electronic records. Some of these include:

- Ability to discern invalid records
- Ability to generate electronic copies of records
- Automatic generation of audit trail
- Access controls
- Secure link of signatures to records
- Use of unique secure signatures

Electronic record keeping and electronic signature use are not mandatory, but if used must comply with the requirements of the rule.

The scope of 21 CFR Part 11 includes operational areas of a pharmaceutical, biotechnology or medical device company such as:

- Manufacturing (for example, production records)
- Maintenance (for example, asset management or calibration records)
- Laboratory (for example, sampling results or product development)

Although this document deals exclusively with 21 CFR Part 11 for the U.S., many other jurisdictions also have directives in place that enable the use of electronic records and signatures.

You've been using electronic records for years

"Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system." **FDA 21 CFR Part 11**

By the 1990's technical ABB solutions existed for generating fully electronic batch records using distributed control systems. Batch management was either handled by a separate software package or fully integrated with the DCS.

This arrangement enabled a production plant to be operated in accordance with the S88 standard or previous national standards, generating working recipes, monitoring inventories, controlling plant equipment and collecting all salient data under a secure access control arrangement.

The DCS had a configurable report package for generating customized batch records and management reports. At the same time, our batch software was becoming available for digital signing of records.

The only item missing in the equation to make fully electronic batch records a possibility was the actual regulation.

21 CFR Part 211.188 states "...records [must be] checked for accuracy, dated and signed." Other clauses of Part 211 such as §186 refer explicitly to "full signature handwritten." These were seen as regulatory blocks on the pharmaceutical road to the digital world.

Moving to fully electronic data handling promised huge cost savings from improved efficiency and reduced physical handling and storage compared to traditional paper records, as well as increased security, traceability and transferability of data.

It is not just in the manufacturing (GMP) area that electronic data handling offers noteworthy benefits. The amount of data generated in analytical laboratories operation under GLP is significant, and since this data requires review and approval signatures, 21 CFR Part 11 promises major improvements in workflows and data handling.

Our commitment

Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Our customers ask for support moving into a paperless world in order to satisfy regulatory requirements as well as business requirements such as ease of use and reduced costs. "Know the market, follow its demands, open up future opportunities for our customers." This is ABB's philosophy to create value for our customers.

21 CFR Part 11 has become an integrated part of our automation technology and system design. The rule is not a "problem" anymore. We help our customers to achieve and maintain 21 CFR Part 11 compliance while minimizing life cycle costs.

Regulatory compliance

The 800xA automation system is a technology platform that can be installed and configured to support to the 21 CFR Part 11 regulation.

Our automation system complies with the rule's requirements with features like system security, secure data management and reporting, and supports electronic records and signatures, and a time-stamped audit trail, for automated electronic recording.

Electronic records and signatures

Our technology combines the efficiency of electronic record keeping with the security of authenticated electronic signatures.

Electronic records in an automation system are easier to keep than manual records. Records generated and maintained by the automation system include:

- Recipe handling
- System configuration
- Device calibration
- Operator input
- Audit trail
- Alarm and event history
- Trends and batch records

The automation system can ask the user to electronically sign records; for example, when new calibration data is released for download into an instrument, a new batch recipe is approved for production or an operator input occurs. The electronic signature act is performed by user or supervisor typing in their User ID and Password.

Security

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

Authorization and access control

We utilize and extend the Microsoft Windows Security system to meet the demands of automation applications for Life Sciences Industries. Access can be controlled down to the object (e.g., motor) and even function (e.g., start the motor). Critical operator actions can be designated for a user authentication action prior to permitting the action to take effect in the process.

Data integrity

System, engineering and manufacturing data are protected throughout their life cycle from unauthorized access, modification or deletion in order to ensure accuracy, consistency, and completeness. For example:

- User access is controlled by a three-dimensional model: Person x Object x Function. User account passwords age.
- All accesses and changes to system and data are logged and tracked in the audit trail.
- All essential components are designed with redundancy. When redundancy is implemented in the solution, if one component fails, the redundant partner immediately takes over with no interruption of your operations, or loss of data.

Asset monitors use real-time plant and system information as inputs for such tasks as detecting maintenance conditions before failure occurs or to diagnosing a problem.

Network

The system supports client/server architectures. The use of the Microsoft Domain and Networking ensures unique user ID's and maximizes security in the automation system. The "aspect server" is one of the core system services that handles object and asset management, file set distribution and cross references as well as security. Redundancy is also available for the aspect server.

The automation system network is based on TCP/IP over Ethernet. The routing protocol (RNRP) supports redundant network configurations based on standard network components. Detection of a network failure and switch over to the redundant network takes less than one second, with no loss or duplication of data.

Network security considerations depend on whether the system is closed or open. An isolated automation system is an example of a closed system; a system that connects to a corporate intranet or internet is an example of an open system. Proper Information Technology practices should be followed when implementing the network and network security.

21 CFR Part 11 checklist

Our automation technology addresses your 21 CFR Part 11 requirements. This initial checklist for closed system introduces our system support.

The assessment compares the actual regulation test with typical compliant implementation examples using the ABB automation system.

Section	21 CFR Part 11 Regulation Text	800xA Implementation and Application
B-11.10	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:	The end-user and manufacturer is responsible for developing procedures to support automation applications in regulated environments. Our validation experts support a full spectrum of compliancy efforts, including end-user validation, SOP development and risk-based approaches to dealing with 21 CFR Part 11 issues.
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Our customers need to validate their installation. We help by providing project execution and product development methodologies that integrate validation activities throughout the system development life cycle. ABB's automation system supports access control. It registers changes to electronic records as audit trail events. It can be configured to check the validity of input data.
(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Configuration as well as production data, like recorded history, audit trails or batch records, can be exported or archived. The information is available on-line to the authorized operator in either standard or customized displays, or can be printed or exported.
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Our experts help our customers fulfill business and regulatory drivers associated with record retention by defining appropriate procedures for access, archival and retrieval of records. Our automation system also supports long-term archiving.

It is easy to use electronic recording

Section	21 CFR Part 11 Regulation Text	800xA Implementation and Application
(d)	Limiting system access to authorized individuals.	Standard procedures to limit physical access are the responsibility of the customer. System access is managed through the use of a unique User ID and password combination for each user. Additionally, the system supports a number of schemes to prevent the compromising of a user's password including minimum password length, password aging and preventing the re-use of recent passwords.
(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	The audit trail is an integrated system function. Time-stamped audit trail events detail object or file name changes, operator ID, description of change and node. If the change is subject to authorization or electronic signature, then the audit trail will also show the reason and any comment. Audit trail events can be viewed, printed and archived. Change of date and time is access controlled.
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Our automation system supports interlocks and sequential function charts. Our integrated Batch Manager is built to ISA 88 and IEC 61512 standards.
(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	The system restricts access according to the user and user role configuration. The rules relate to the use of system functions, workstations, operator actions, tags or event single tag signals. When the rules are changed, the system automatically generates an audit trail event.
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	The functional scope of system servers or clients is defined during system configuration. In addition, user roles and access can be limited to single or specified nodes.
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	The customer is responsible for ensuring that personnel working with the automation system are qualified. Under ABB's quality system, ABB trains and documents the training of ABB product and system development staff and implementation personnel.

The FDA allows electronic signatures

Section	21 CFR Part 11 Regulation Text	800xA Implementation and Application
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	The system owner is responsible for defining the policy for the manufacturing or production facility. Our consultants support our customers in setting up the required procedures and documents.
(k)	Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents timesequenced development and modification of systems documentation.	The customer's organization is responsible for ensuring change control procedures for operational and maintenance documentation. Our experts are prepared to help our customers. All ABB documentation is fully version controlled in accordance with our quality procedure. On-line help is part of our system. User manuals are included on the distribution media. The product documentation is delivered in PDF files.
B-11.50 **(a)**	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	When electronic records are signed, the system records the following items as part of the electronic signing process: – Date and time stamp – User ID and full name of the signer(s) – Reason for signature, out of a pre-configured list of possible reasons – Optionally, an additional comment by the signer at run-time – PC/node, where the signature was made
(b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	The electronic record includes the signature aspect, which is stored in the same system database. The system allows us to display the electronic signature as described in 11-50 (a) either on the screen or in a report.
B-11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	The signature event, with an explanation of the status or reason (such as "approved" or "maintenance action"), is linked to the electronic record and securely archived with the record and through the audit trail.

Signature components and control

Section	21 CFR Part 11 Regulation Text	800xA Implementation and Application
C-11.100 **(a)**	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The system security is based on Microsoft Windows Security. All user identification and password combinations are unique.
(b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	The customer organization is responsible for assigning access rights to operators and other users, which allow them to use our system.
(c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	Our customers are responsible for submitting a certification to the agency that the electronic signatures used in their system are intended to be the legally binding equivalent of traditional-handwritten signatures.
C-11.200 **(a)**	Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	For security, our system requires two components for authorization and electronic signatures, the user identification and password.
	(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.	The system distinguishes between an electronic signature assigned and linked to an electronic record, and an authorization for controlled system access, e.g., to open a valve or to schedule a batch recipe. The user must enter his or her user ID and password for each separate signature action.

Unique users and signatures

Section	21 CFR Part 11 Regulation Text	800xA Implementation and Application
C-11.200 (a)	(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.	Each signer must identify him or herself with unique user ID and password, irrespective of the type of signature requested: 1st or 2nd signatures from an individual or a member of a user group.
	(2) Be used only by their genuine owners; and	Our customers need to set up appropriate procedures and policies.
	(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.	The pharmaceutical organization is responsible for installing appropriate procedures and policies. Password data cannot be retrieved from the system. Security and access control limit access to electronic records and audit trail information.
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Our security and access controls are built around standard Microsoft security features.
C-11.300 (a)	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Every combination of user identification and password is unique.
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	In addition to organizational procedures, the system technology supports password aging and minimum password length and prevents the reuse of a configurable number of prior passwords.
(c)	Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Our customer is responsible for defining procedures for handling forgotten or lost passwords. If you need help in this process, please contact your local ABB.
(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.	The system utilizes Microsoft security, which allows the system to disable a user's account after consecutive failed logins. Failed attempts to login, authorize or electronically sign records are logged as audit trail events by the system.
(e)	Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	This is the responsibility of the system owner. Our experts can support this effort.

Your validation and compliance partner

Compliant System 800xA solutions are delivered and supported by our validation project execution organizations, ensuring seamless integration into regulated and quality controlled processes.

Our automation system can integrate third-party units as well, and process electronic recording and signatures for product-related data for the complete plant area. Many legacy units were not constructed for full 21CFR Part 11 support.
The rule is imposing a considerable burden on pharmaceutical companies to comply.

To address criticism of 21 CFR Part 11, especially from the owners of legacy systems, the FDA issued a statement about the “risk-based approach to GMP” and later, in August 2003, issued a guidance “Scope and Application,” stating that Part 11 will be interpreted “narrowly.”

“Risk Based” Approach

ABB has developed a pragmatic and risk based approach to dealing with 21 CFR Part 11. The main characteristics of the model are consistency, rationale and risk reduction:

- Assessments are brief and directed towards the highest risk.
- No assessment is complete until the remediation is identified.
- Regulatory, inspection and business criticality are determined.
- Prioritization is based on criticality, cost and economic life cycle.

All corrective actions are justified with a rationale, both those that are to be implemented and those that are not.

An overview of System 800xA products and services for the Life Sciences Industry

Analysis and Instrumentation Equipment

- Raw material identification
- On-line monitoring of API manufacturing process, and solvent recovery process
- On-line moisture analysis
- At-line analysis of powder blend homogeneity, and solid dosage from content uniformity

Automation

- Discrete control and visualization systems
- Process control systems
- Fieldbus technology and asset management
- Engineering and optimization software
- Batch control and management

Manufacturing Execution Systems (MES/EBR)

Robot-based Manufacturing

- End-of-line packaging cells
- Robots to pick, pack and palletize

Validation and Compliance Services

- Risk assessment
- Computer systems validation
- Laboratory systems validation
- Equipment and facilities qualification
- Business systems validations
- Quality systems and standard operating procedures

Contact us

ABB AB
Control Technologies
www.abb.com/800xA
www.abb.com/controlsystems

3BSE077527 en

Power and productivity
for a better world™