

Plateau and 21 CFR Part 11

Electronic Signature and Learning Management

Executive Summary

Life science organizations must rapidly train their employees while at the same time maintaining the highest level of quality control. They must also comply with federal and international regulations relating to safety, quality and accuracy of records. The penalties for failing to comply with these regulations are severe and can result in large fines and interruptions in production and distribution. A Learning Management System (LMS) that manages training data in compliance with regulations and guidelines can be the difference between profitability and a business disaster.

The Plateau is ideally suited to manage training in a highly regulated environment. It allows companies to meet Good Manufacturing Practice (GMP), Good Laboratory Practice (GLP), and Good Clinical Practice (GCP) requirements - as well as general corporate learning needs - with one scalable system.

Plateau has implemented functionality to meet Part 11 requirements as a standard feature of the application. The functionality is based on interviews with FDA representatives, analysis of published FDA documentation and on reviewing the functionality design with existing Plateau life science customers. Currently, Plateau operates as a validated system, managing production data in more than 30 different GMP-covered facilities.

Table of Contents

Section 1: Interpretation.....	4
Section 2: Implementation	6
Section 3: Future Enhancements	11
Appendix.....	12

Section One

Interpretation

Part 11 is a statement of the standards that must be met for software applications to house electronic data that will be accepted by the FDA as official records, in lieu of paper or other physical records. Plateau Learning Management System, as a corporate learning management system, can house records used in operational decision-making and for verifying compliance with training requirements. Depending on a company's interpretation and implementation of Part 11, the LMS could be subject to the requirements of Part 11. In 1997, when Part 11 was released, analysis began on how to modify the LMS application to include electronic signature security as a standard feature.

It is important to note that the FDA does not necessarily require Part 11 to be applied to GxP training records. Application of Part 11 is based on the need for controlled and defined signatures based on previous regulation (collectively called the "predicate rules"). There are no specific predicate rules that require signatures for training records for meeting GxP requirements, so Part 11 may not apply.¹ Of course, each company has broad authority to interpret FDA regulations for their own situations, so Part 11 controls may be desired despite the lack of regulatory requirement.

One of the most difficult decisions that must be made in the development of any generic software application is how to incorporate industry-specific functionality in the application without creating a burden for application users outside of that industry. As the analysis for Part 11 compliance began, it was determined that the first implementation of the functionality would be limited to securing the veracity of the least common denominator of data considered to be required by the company to determine training compliance. This was determined to be any data that related to the completion or attempted completion of a training activity or the assessment of an individual for their knowledge, skill, ability or attitude. By protecting this data, Plateau Systems believes that the crucial link for proving an individual's compliance with regulatory requirements can be established and maintained. Although there are other systems and other data elements that fit together to complete the entire picture of an individual's adherence to applicable requirements, most all other data is less critical than the history of completion and assessment. This is, historically, what the FDA has asked for in compliance audits.

¹ U.S. Food and Drug Administration, Center for Drug Evaluation and Research, Video Conference *The New Scope of Part 11*, September 24, 2003

Plateau Assumptions Regarding Specific Requirements of Part 11

- Plateau will be implemented and managed as a “closed” system.
- Adequate procedural safeguards will be developed by the customer to protect Ids and passwords.
- The “built-in” functionality of the system does not rely on biometric nor token-based authentication. This could be incorporated into the system via custom integration and development, but the “off-the-shelf” functionality is limited to unique username/password combination security.

An area of functionality that was not directly addressed by the FDA in Part 11 was the entry of training history or competency assessments by individuals themselves. Although not a common practice, some companies do allow it. Additionally, any company that allows these records to be automatically entered as a result of an individual’s completion of computer-delivered courseware (CBT, WBT, etc.) will, by definition, be allowing the individual to enter their own events. To satisfy these issues and maintain compliance with Part 11 requirements, it was determined that the overall electronic signature strategy must be applied to these cases as well.

Section Two

Implementation

As stated in the above section, Part 11 compliance is currently focused on the protection of two types of information: learning events and assessment events. Information that indicates the completion or an attempted completion of a training-related requirement or activity is called a learning event in the application's terminology. Records of the assessments of how well an individual has mastered a skill or obtained knowledge on a specific topic is called an assessment event in the application's terminology. Therefore, the functionality protected by Part 11 authentication requirements is the creation, deletion and modification of learning and assessment events. The system also incorporates controls to maintain the uniqueness of a user/password combination and to provide the signature manifestations required by the FDA. Also, the system maintains audit trails for all data that would be required to establish the complete set of assignment and history data for an individual.

High-Level Functionality Design

There are several tables, two interfaces and a set of business rules that define the functionality designed for Part 11 compliance. The system provides the following:

- All learning events and assessment events contain a user ID, user name, signature reason, date and time stamp of when the event was created or last modified.
- All learning events and assessment events contain a column that indicates the name of the signer of the record. Data in this column also indicates whether or not a learning event or assessment event was recorded or modified while the electronic signature functionality was active. This allows the organization to easily separate training events that may require further analysis or scrutiny. These names are a part of the data row and cannot be excised by normal means.
- The learning and assessment event transaction audit tables include all data attributes of the training event table plus a column to indicate the nature of the change, either creation, modification or delete. When a row of data is created, modified or deleted from the training event table, a complete duplicate row is created in the learning or assessment event history table.
- Electronic signature functionality is a global switch that affects all learning and assessment event transactions.
- For users to enter learning or assessment events, the user must have a security function assigned to them that allows the recording of learning or assessment events.

- To define uniqueness, the system uses two values: a system username (the same username for system access) and a password (PIN).
- The electronic signature PIN may currently be a different value than the password used to log into the system.
- Electronic signature PINs can be managed by an LDAP or SSL solution.
- PINs can be set to expire within a user (system administrator) specified number of days. If the number of days is exceeded before the user changes the PIN, the system will not allow the user to perform training event transactions until the PIN is changed.
- Each user who will be entering training events must have a PIN to be able to enter learning or assessment events. On initial user creation, the users' electronic signature PIN is blank and the user cannot enter learning or assessment events until the password is created. The user is prompted by the system to create an electronic signature PIN on each login to the system until the password is created.
- The electronic signature PIN is stored as an encrypted value in the database and is linked to each user.
- A system administrator cannot retrieve a user's PIN. A system administrator can only clear a PIN, forcing the user to reset it upon the next login.
- When electronic signatures are active and a user attempts to create, modify or delete a training event, the system intercepts them with a dialog that requires the entry of the current login username and PIN.
- If the user successfully authenticates, the training event activity is committed to the database.
- If the user does not successfully authenticate, the training event activity is not committed to the database. If a user fails to successfully authenticate three times, the system will automatically send an email notification to a specified email address.
- For all protected transaction audit records, the electronic signature data cannot be edited by normal means. The only way to modify this data is through direct programmatic access to the database. The system does not allow external access to the database, even if the individual has an administrative user; access is strictly controlled through the application.
- To bring the electronic signature information to printed human-readable form, custom reports are required.

Interfaces

Administration of the electronic signature functionality of Plateau is managed through the interface below:

Electronic Signature Settings

Disabling electronic signatures will automatically authenticate all unauthenticated learning events.

Enable electronic signatures:

Administrator Email:

Enable PIN Expiration:

PIN Expires After: days
(1000,001)

Count Between Repeated PIN:
(1000,001)

Minimum PIN Change Period: days

Administrator Default Esig Meaning Code:

Student Default Esig Meaning Code:

Administrator Esig Message:

Student Esig Message:

The electronic signature interface has the following controls and functions:

Control	Function
Enable electronic signatures	This switch enables and disables the electronic signature functionality globally.
Administrator email	This is the email address that will receive an email after a third unsuccessful authentication attempt is made.
Enable PIN Expiration	This switch enables and disables the PIN expiration functionality globally. If switched off, e-signature PINs will not expire.
PIN Expires After x Days	This variable sets the number of days a PIN will remain active.
Count Between Repeated PIN	This variable sets the minimum number of different PINs that must be used before the system will allow the use of a previously used PIN.

Minimum PIN Change Period	This variable sets the minimum number of days that must pass before a user can change his or her PIN. This is designed to prevent a user from rapidly changing PINs in order to continue using a previously used PIN for convenience.
Administrator Default Esig Meaning Code	This variable contains the meaning code an administrator wishes to assign when executing an electronic signature. The system will only allow entry of a valid meaning code. Valid reason codes are entered in a separate interface (see below).
Student Default Esig Meaning Code	This variable contains the meaning code an individual learner wishes to assign when executing an electronic signature. The system will only allow entry of a valid meaning code. Valid reason codes are entered in a separate interface (see below).
Administrator Esig Message	This variable contains text that will be displayed to an administrator when executing an electronic signature.
Student Esig Message	This variable contains text that will be displayed to an individual learner when executing an electronic signature.

In order to prevent the entry of erroneous signature meanings, the system references a user-entered list of valid meaning codes. The following interface is used to enter and manage the meaning codes:

Electronic Signature Meaning Code

> Add New

Add New Electronic Signature Meaning Code Reference

* = Required Fields

* **Meaning Code ID:**

Description:

The electronic signature meaning code interface has the following controls and functions:

Control	Function
Meaning Code ID	This is the unique key value for the code.
Description	This is the description of the meaning of the signature.

In order to authenticate a record, the system presents the following interface:

E-Signature

* = Required Fields

Please enter your electronic signature, and then click apply changes.

* **User Name:**

* **E-Signature:**

* **Meaning Code :**

This interface has the following controls with the following functions:

Control	Function
User Name	This variable allows the user to enter his or her user name.
E-Signature	This variable allows the user to enter a PIN.
Meaning Code	This variable contains the meaning code the user wishes to assign when executing an electronic signature. The system will only allow entry of a valid meaning code.

Section Three

Future Enhancements

Plateau Systems is constantly improving the products we develop, including our functionality for Part 11 compliance. Currently, we are planning to make the following enhancements to our Part 11 compliance functionality:

- Configurable application of electronic signature protection to most data entities
- Assignment of electronic signature protection to be optional, by data attributes (i.e., e-signatures only applicable to certain subject areas, component types or domains)
- Ability to define the minimum length, maximum length and inclusion of a selectable format for a PIN
- Modification of learning history detail interface to optionally include all manifestations of electronic signature
- Selection for specific standard reports to optionally include all electronic signature manifestations

There is no set timetable for the implementation of these areas of functionality. They are incrementally added as development and release schedules allow.

Appendix

Section-by-Section Analysis

In the table below:

(M) = Manufacturer

(P) = Plateau

Clause	Type of Control	Resp	Notes	Plateau Position
Subpart B – Electronic Records Sec 11.10, Controls for closed systems				
11.10	Procedural	(M)	This clause specifies a number of specific controls. Manufacturer will need to demonstrate a system of self- inspection audits to demonstrate compliance with the procedures and controls listed below.	
11.10 (a)	Procedural	(M)	ER/ES systems need to be validated following established policies and practices.	
	Technological	(P)	ER/ES systems should be able to identify changes to electronic records in order to detect invalid or altered records. In practice, this means having an adequate audit trail that can be searched for information. For example, to determine whether any changes have been made without the appropriate authorizations.	Plateau provides a complete transaction auditing capability for all learning events and assessment events, including user, date and time stamps. The training event transaction audit table includes all data attributes of the learning and assessment event tables and a column indicating the nature of the change: creation, modification or deletion. When a row of data is created, modified or deleted from the learning or assessment event table, a complete duplicate row is created in the appropriate learning or assessment history table.
11.10 (b)	Technological	(P)	ER/ES system should allow electronic data to be accessed in human readable form.	Plateau provides a variety of reports and views. Additionally, 3 rd party query and reporting tools can be used to develop custom views and reports.

Clause	Type of Control	Resp	Notes	Plateau Position
11.10 (b)	Technological	(P)	ER/ES systems need ability to export data and any supporting regulatory information (e.g. audit trails, configuration info relating to ID and status of users and equipment.)	Plateau is compatible with any importing or exporting tool that is compatible with Oracle.
11.10 (c)	Procedural	(M)	Manufacturer should specify retention periods (in accordance with predicate rules) and responsibilities for ensuring data is retained securely for those periods.	
	Procedural	(M)	Manufacturer needs a defined, proven, and secure backup and recovery process for electronic data.	
	Technological	(P)	ER/ES systems should be able to maintain electronic data over periods of many years regardless of upgrades to the software and operating system.	Plateau upgrades do not affect data. Operating system changes are irrelevant to the data in the system.
11.10 (d)	Procedural	(M)	Manufacturer needs procedures defining how access is limited to authorized individuals.	
	Technological	(P)	ER/ES systems should restrict access in accordance with pre-configured rules that can be maintained. Any changes to the rules should be recorded.	In addition to the electronic signature security, the system provides for role-based security, denying access to protected functions from unauthorized users. Specific "rules" governing the behavior of specific security functions are fixed in the application and cannot be changed.
11.10 (e)	Procedural	(M)	Manufacturer needs procedure to maintain the audit trail (see 11.10 © above)	
	Technological	(P)	ER/ES systems should be capable of recording all electronic record create, update, and delete operations. Data to be recorded must include as a minimum: time and date, unambiguous description of event, and identity of operator. This record should be secure from	Plateau provides complete transaction auditing capability for all learning and assessment records including user, date and time stamps. The learning and assessment event transaction audit table includes data attributes of the learning and assessment event tables and a column to indicate the nature of the change, either creation, modification or delete. When a row of data is created, modified or deleted from the learning or assessment event

Clause	Type of Control	Resp	Notes	Plateau Position
			subsequent unauthorized alteration.	table, a complete duplicate row is created in the appropriate learning or assessment event history table.
11.10 (f)	Technological	(M) (P)	Where operations are required in a pre-defined order, for example in batch manufacture, the ER/ES system should enforce that ordering through the system's design.	Both the learning event recording process and the competency assessment event recording process have an enforced sequence.
11.10 (g)	Procedural	(M)	Manufacturer needs procedures defining how the authorization processes are carried out and that staff have been trained in their use.	
	Technological	(P)	ER/ES Systems should restrict use of system functions and features in accordance with pre-configured rules that can be maintained. Any changes to the rules should be recorded.	In addition to the electronic signature security, the system also provides for role-based security, denying access to protected functions from unauthorized users. The specific "rules" governing the behavior of specific security functions are fixed in the application and cannot be changed.
11.10 (h)	Technological	(M)	Where a pharmaceutical organization requires that certain devices act as sources of data or commands, the ER/ES system should enforce the requirement.	Although Plateau can serve as a data source for a variety of systems, integration with other systems is custom integration work and is beyond the scope of the "off-the-shelf" feature set of the application. If Plateau is serving in this capacity, it is incumbent on the manufacturer to develop the requirement and the proper behavior in the interface to adhere to the requirement.
11.10 (i)	Procedural	(M)	A Manufacturer's staff that develops, maintains, or uses electronic record/electronic signature systems must have the education, training, and experience to perform their assigned tasks.	
	Procedural	(P)	Supplier requires a procedure to demonstrate that persons who develop and maintain electronic record/signature systems have the education, training, and experience to perform assigned tasks.	Plateau maintains resumes on the development staff and these are available for inspection by Manufacturer with advance notice.

Clause	Type of Control	Resp	Notes	Plateau Position
11.10 (j)	Procedural	(M)	Policy needed to describe the significance of electronic signatures, in terms of individual responsibility and the consequences of falsification for both the organization and individual.	
11.10 (k)	Procedural	(M)	Manufacturer needs procedures to cover the distribution of, access to, and use of operational and maintenance documentation once the system is in use.	
	Procedural	(M)	Manufacturer must ensure adequate change control procedures for operational and maintenance documentation.	
	Technological	(M)	Where systems documentation is in electronic form, an electronic audit trail should be maintained, in accordance with 11.10 (e) above.	Electronic documentation (help files) for the system can be modified by the customer to suit a particular implementation. However, there is no system-supplied audit trail for system documentation. If operational documentation for the Plateau needs to be protected and version-controlled, Plateau recommends the documentation be entered and managed via the document version control and management system already in place at Manufacturer.
Sec. 11.30, Controls for open systems				
11.30	Technological	(P)	All Technological requirements identified in 11.10 for Closed systems	Plateau is not designed to be used as an open system.
	Technological	(P)	Controls should be in place to ensure authenticity, integrity and confidentiality of e-records from creation to the point of receipt.	Plateau is not designed to be used as an open system.
	Technological	(P)	Encryption technology should be in place to ensure secure distribution of electronic records.	Plateau is not designed to be used as an open system.

Clause	Type of Control	Resp	Notes	Plateau Position
Sec. 11.50, Signature manifestations				
11.50	Technological	(P)	<p>ER/ES Systems must ensure signed electronic records contain information associated with the signing that clearly indicates all of the following:</p> <ol style="list-style-type: none"> (1) Printed name of the signer; (2) Date and time when the signature was executed; (3) Meaning such as review, approval, responsibility, or authorship associated with the signature. <p>These items are subject to the same controls as other electronic records. The info can be stored within the electronic record or in logically associated records, but must always be shown whenever the record is displayed/printed.</p>	The system records all of this data for each record. Because of the limitations of screen display and the ubiquitous use of the data involved, the system will provide select views of the data that contain all of the manifestations of the signature. This requirement can be currently met by modification of the existing views and reports.
Sec. 11.70, Signature/record linking				
11.70	Technological	(P)	<p>ER/ES systems must provide a method for linking e-signatures, where used, to their respective electronic records, in a way that prevents the signature from being removed, copied or changed to falsify that or any other record.</p>	Data associated with electronic signatures are an integral part of the row of data of the training event and cannot be “de-linked”. The only way to modify any aspects of the manifestation of the electronic signature is through direct editing of the data row, requiring knowledge of the administrative application security structure and authentication information.
Subpart C – Electronic Signatures				
Sec. 11.100 General requirements				
11.100 (a)	Procedural	(M)	<p>Manufacturer must ensure uniqueness of electronic signature, and that they are not re-used or re-allocated.</p>	

Clause	Type of Control	Resp	Notes	Plateau Position
	Technological	(P)	ER/ES System should enforce uniqueness, prevent reallocation of electronic signature, and prevent deletion of information relating to the electronic signature once it has been used.	<p>To define uniqueness, the system uses two values: a system username and a password (PIN). The e- signature PIN may currently be a different value than the password used to log into the system. Esig PINs can be set to expire within a user (system admin) specified number of days. If the number of days is exceeded before a user changes the PIN, the system will not allow the user to perform training event transactions until the PIN is changed. Each user entering learning or assessment events must have a PIN to enter the events. On initial user creation, the e-signature PIN for a user is blank and the user cannot enter learning or assessment events until the password is created. The user is prompted by the system to create an e-signature PIN when logging into the system until the password is created. The e-signature PIN is stored as an encrypted value in the database and is linked to each user.</p> <p>User Ids are unique and cannot be reused. They can be inactivated if: a user leaves the company, violates system policies or has an extended leave of absence, but do not have to be deleted from the system. If a user is deleted, a transaction history table insures that the ID remains unique by preventing a duplicate.</p>
11.100 (b)	Procedural	(M)	Manufacturer needs to verify the identity of individuals being granted access to ER/ES system.	
11.100 (c)	N/A	N/A	Signature use certification with FDA	
Sec. 11.200, Electronic signature components and controls.				
11.200 (a)(1)	Technological	(P)	ER/ES systems providing non-biometric electronic signatures need at least two distinct components.	<p>To define uniqueness, the system uses two values: a system username and a password (PIN). The electronic signature PIN may currently be a different value than the password used to log into the system. The electronic signature PIN is stored as an encrypted value in the database and is linked to each user.</p>

Clause	Type of Control	Resp	Notes	Plateau Position
11.200 (a)(1) (i)	Procedural	(M)	Manufacturer needs to establish how it will ensure that both components of electronic signature are entered if session has not been continuous (this can be through system design, or operating procedure if necessary).	
	Technological	(P)	ER/ES system should enforce that both components are entered at least at the first signing, and following a break in the session.	Plateau enforces that both parts of the electronic signature are required for each signing.
11.200 (a)(2)	Procedural	(M)	Manufacturer must ensure staff only use their own e-signature, not anyone else's even on their behalf, as that would be falsification (see 11.10 (j))	
11.200 (a)(3)	Procedural	(M)	Manufacturer needs procedure that users do not divulge their electronic signature (e.g. passwords)	
	Technological	(P)	ER/ES System should not provide any ordinary means of accessing electronic signature information.	There is no user interface that can manipulate electronic signature information. Additionally, the PIN for a user's electronic signature is encrypted in the database.
11.200 (b)	Technological	(M)	Biometric controls should be implemented in such a manner as to ensure the electronic signature is used exclusively by the owner.	The "built-in" functionality of the system does not provide for biometric nor for token-based authentication (this can be incorporated as custom integration and development).
Sec. 11.300 Controls for identification codes/passwords				
11.300 (a)	Technological	(P)	The system should enforce the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	To define uniqueness, the system uses two values: a system username and a password (PIN). The e-signature PIN may currently be a different value than the password used to log into the system. Esig PINs can be set to expire within a user (system admin) specified number of days. If the number of days is exceeded before the user changes the PIN, the system will not allow the user to perform training event transactions until the PIN is changed. Each user entering learning or assessment events must have a PIN to be able to enter the events. On initial user creation, the e-

Clause	Type of Control	Resp	Notes	Plateau Position
				<p>signature PIN for a user is blank. The user cannot enter learning or assessment events until the password is created. The user is prompted to create an e-signature PIN when logging in until the password is created. The e-signature PIN is stored as an encrypted value in the database, linked to each user.</p> <p>User IDs are unique and cannot be reused. IDs can be inactivated if: a user leaves the company, violates system policies or has an extended leave of absence. IDs do not have to be deleted from the system. If an ID is deleted, a transaction history table insures the ID remains unique by prohibiting a duplicate.</p>
11.300 (b)	Procedural	(M)	<p>Manufacturer needs procedures to cover: removal of obsolete users; changing of profiles as user roles change; periodic checking of ID codes; passwords for inconsistencies with current users and periodic changing of passwords.</p>	
	Technological	(P)	<p>System should force passwords to be periodically changed and also enable id/password combinations to be rendered inactive without losing the record of their historical use.</p>	<p>Esig PINs can be set to expire within a user (system admin) specified number of days. If the number of days is exceeded before a user changes the PIN, the system will not allow the user to perform training event transactions until the PIN is changed. Each user entering learning or assessment events must have a PIN to enter events. On initial user creation, the e-signature PIN is blank and the user cannot enter learning or assessment events until a password is created. The user is prompted by the system to create an e-signature PIN on each attempt to enter learning or assessment events until the password is created. The e-signature PIN is stored as an encrypted value in the database and is linked to each user.</p>
11.300 (c)	Procedural	(M)	<p>Manufacturer needs a procedure for management of lost passwords.</p>	
11.300 (d)	Procedural	(M)	<p>Manufacturer needs a procedure to describe how response to attempted or</p>	

Clause	Type of Control	Resp	Notes	Plateau Position
			actual unauthorized access is managed.	
	Technological	(P)	System should provide notification of attempted unauthorized access.	When e-signatures are active and a user attempts to create, modify or delete a learning or assessment event, the system intercepts them with a dialog that displays the current user name and a field for entry of the PIN. When a user successfully authenticates, the event activity is committed to the database. If a user does not successfully authenticate, the event activity is not committed to the database. If a user fails to successfully authenticate 3 times, the system automatically sends an email notice to a specified address.
11.300 (e)	Procedural	(M)	Manufacturer should define how any devices or tokens that carry user/id or password information are periodically tested and renewed.	

PLATEAU™

Plateau
4401 Wilson Blvd.
Suite 400
Arlington, VA 22203
703-678-0000
www.plateau.com

2004 Plateau Systems Ltd. All rights reserved. All brand names and product names are trademarks or registered trademarks of their respective holders.

Information in this document is confidential and proprietary to Plateau Systems, Ltd., is subject to change without notice, and does not represent a commitment on the part of Plateau Systems, Ltd. No party of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the express permission of Plateau Systems, Ltd. Plateau does not make any express warranty