



# FinePointe GLP Features User Guide

## **OVERVIEW**

This user guide provides an overview of the GLP compliant features and tools available in FinePointe, including details on proper use of the system to satisfy 21 CFR part 11 requirements relating to electronic records.



**Data Sciences International**

**119 14TH STREET NW**

**SUITE 100**

**ST. PAUL, MN 55112 USA**


**(651)481-7400 • 1(800)262-9687**

**[www.datasci.com](http://www.datasci.com)**

**PN: 011759-001 REV01**

# Table of Contents

<b>Welcome .....</b>	<b>4</b>
FinePointe Security Options .....	4
Installation and Setup .....	4
Configuring the Controller Server .....	5
Establishing Initial Security Settings.....	6
User Access Levels and Authorization Control .....	9
Creating Users .....	9
Disabling and Enabling Users .....	10
Managing User Roles.....	10
Roles controlling access levels .....	11
GLP roles .....	12
User Access Examples .....	12
GLP Study Creation.....	13
Electronic Signatures.....	14
General Principles of Electronic Signatures .....	14
Signing Items .....	15
Signature Meanings .....	17
Accessing Electronic Signatures .....	17
Audit trails .....	18
Data Management, Archiving and Restoring .....	19
Database Integrity .....	20
Additional Recommended Policies and Procedures.....	21
Username and Password Policy Considerations .....	21
Periodic inspection of audit trails.....	22
Procedures to secure folder permissions.....	22
Special Considerations When Using the Windows Security Option.....	22
Special Considerations When Using the SQL Database Authentication Option .....	22
Appendix A: 21 CFR Part 11; Electronic Records, Electronic Signatures Subpart B - Electronic Records .....	23
Controls for Closed Systems.....	23
Electronic Manifestations .....	27
Components and Controls.....	28



Controls for Identification Codes/Passwords.....	29
Appendix B: GLP Signature Permissions.....	32
Appendix C: Restricted Features Listed by Access level.....	33

## WELCOME

Congratulations on joining the community of users worldwide who rely on DSI's products to perform preclinical physiologic research. Thank you for your interest in DSI products. We are committed to providing you with quality products and services.

The GLP option in FinePointe provides the technology to assist an FDA-regulated organization in achieving compliance with 21 CFR Part 11. The FinePointe system offers security options for limiting system access to authorized individuals, ensuring the integrity of electronic records, and allowing Users to electronically sign records. Utilization of the FinePointe GLP tools should be complemented with Standard Operating Procedures (SOPs), developed and implemented by the User, which comply with 21 CFR Part 11 and its umbrella regulations (GLP regulations).

This manual will help you understand the features available within FinePointe which will assist you in establishing a GLP compliant study environment. In addition, please see Appendix A for a listing of 21 CFR Part 11 requirements and comments on how the FinePointe system addresses or relates to each specific requirement.

## FINEPOINTE SECURITY OPTIONS

### INSTALLATION AND SETUP

When deploying a FinePointe system, it is important to understand you are setting up multiple computers which work together as to create the FinePointe environment. A FinePointe system, is composed of a Controller Server, Member Servers, and Clients. The installation software allows you to select which to install.

**Controller Server:** The FinePointe system must have one computer must be designated as a Controller Server. The Controller Server stores the study databases, maintains the security information, can have a data acquisition station, and manages your license.

**Member Servers:** You can optionally have one or more Member servers. Each Member Server is a data acquisition station which can be used to acquire data for any study stored in the associated Controller Server.

**Clients:** A client is the user interface used to access any of these servers. You can deploy as many clients as you choose, but the Controller Server enforces how many clients can be logged in at any given time.

**Isolated Station:** An Isolated Station is a special type of Member server that is not connected to the network. This may be used when the data acquisition station is isolated from the rest of the network. However, if a standalone workstation is needed, setting it up as a controller server is often the appropriate option. Contact DSI for guidance on which type of server or station is most appropriate.

### INSTALL FINEPOINTE SOFTWARE

The FinePointe installation wizard will guide you through the process of installing program components, drivers, and SQL database components (if applicable). Refer to the FinePointe Installation Guide for additional details. The license dongle must be inserted after installation and must remain inserted at all times in order for the software to function.

## LAUNCHING FINEPOINTE CONTROL PANEL FOR THE FIRST TIME

---

To open the FinePointe Control Panel, a Windows account with local administrator privileges is required. When opening the FinePointe Control Panel for the first time, it is necessary to establish database and server settings. First, the Control Panel will ask which type of server is being installed: Controller Server, Member Server, or Isolated Station.

Select **Controller Server** for the computer that will be used to store the study databases and control security settings for the FinePointe systems. The Controller Server is responsible for enforcing security policies, maintaining study information for all servers, and communication with any clients.

One or more **Member Servers** may also be installed on a network if desired, but the security and GLP features are determined by the Controller Server.

**Isolated Stations** require a security file generated by the Controller Server. After the Controller Server has been set up with the desired security options (see section below), select **Database Management>Save Security Database for Isolated Stations** to generate this file. Then copy the file to the FinePointe data folder on the isolated station server.

---

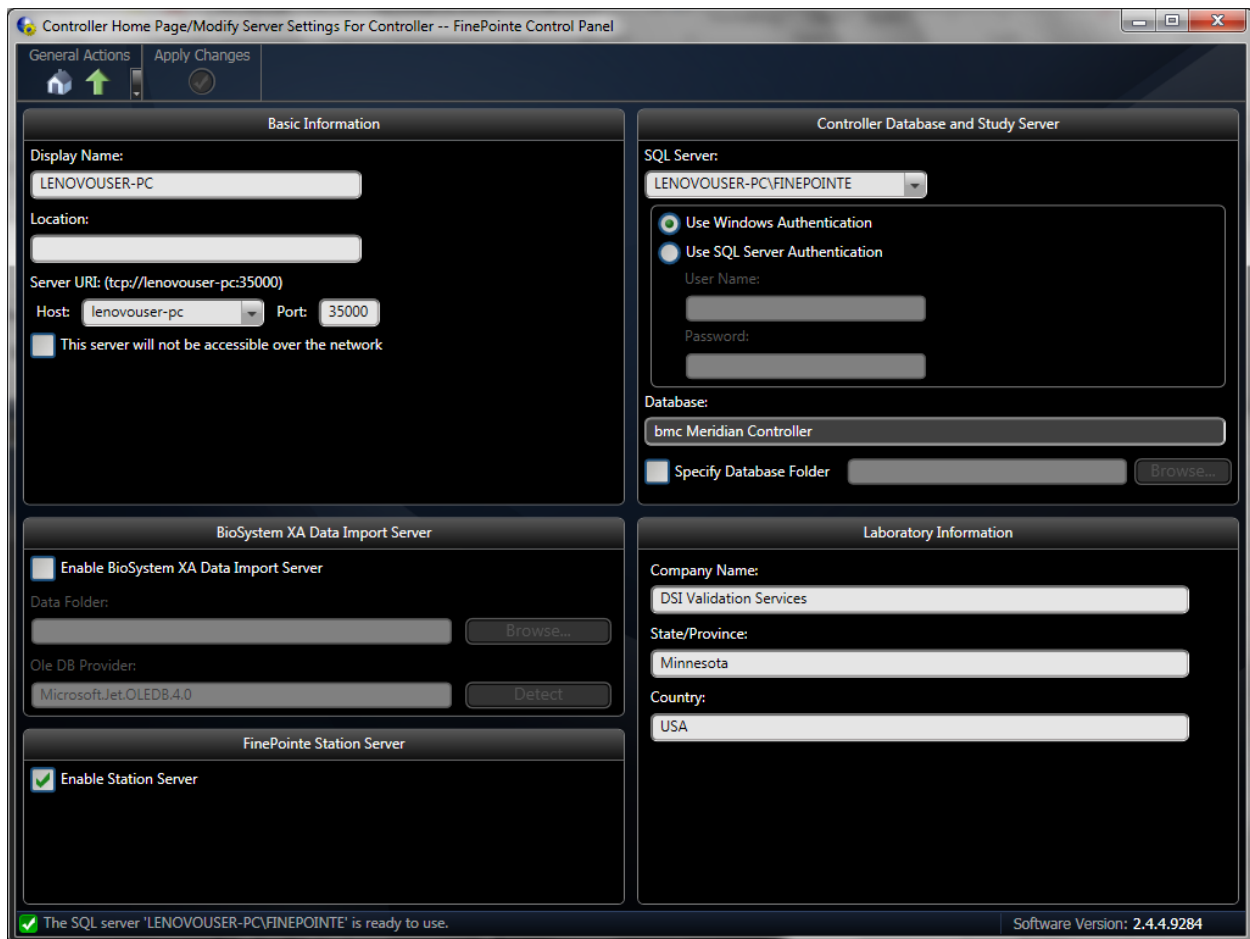
## CONFIGURING THE CONTROLLER SERVER

### MODIFYING SERVER SETTINGS

---

After selecting Controller Server, the FinePointe Control Panel will open and the **Modify Server Settings** tool will be available.

Open this tool, and fill out the Laboratory Information section with a company name and location details. Under the Controller Database and Study Server section, select an authentication method and SQL server. Typically, Windows authentication is used, and the user simply selects the FinePointe server from the dropdown list. However, SQL Server Authentication is also available; refer to the Additional Procedures section below for details regarding this option.



Select **Apply Changes** from the top menu, and the status line at the bottom of the screen will indicate that the server is ready to use. Click the home icon to return to the FinePointe Control Panel Home Page, and the **Log** section will display a message stating that the server self-registered successfully.

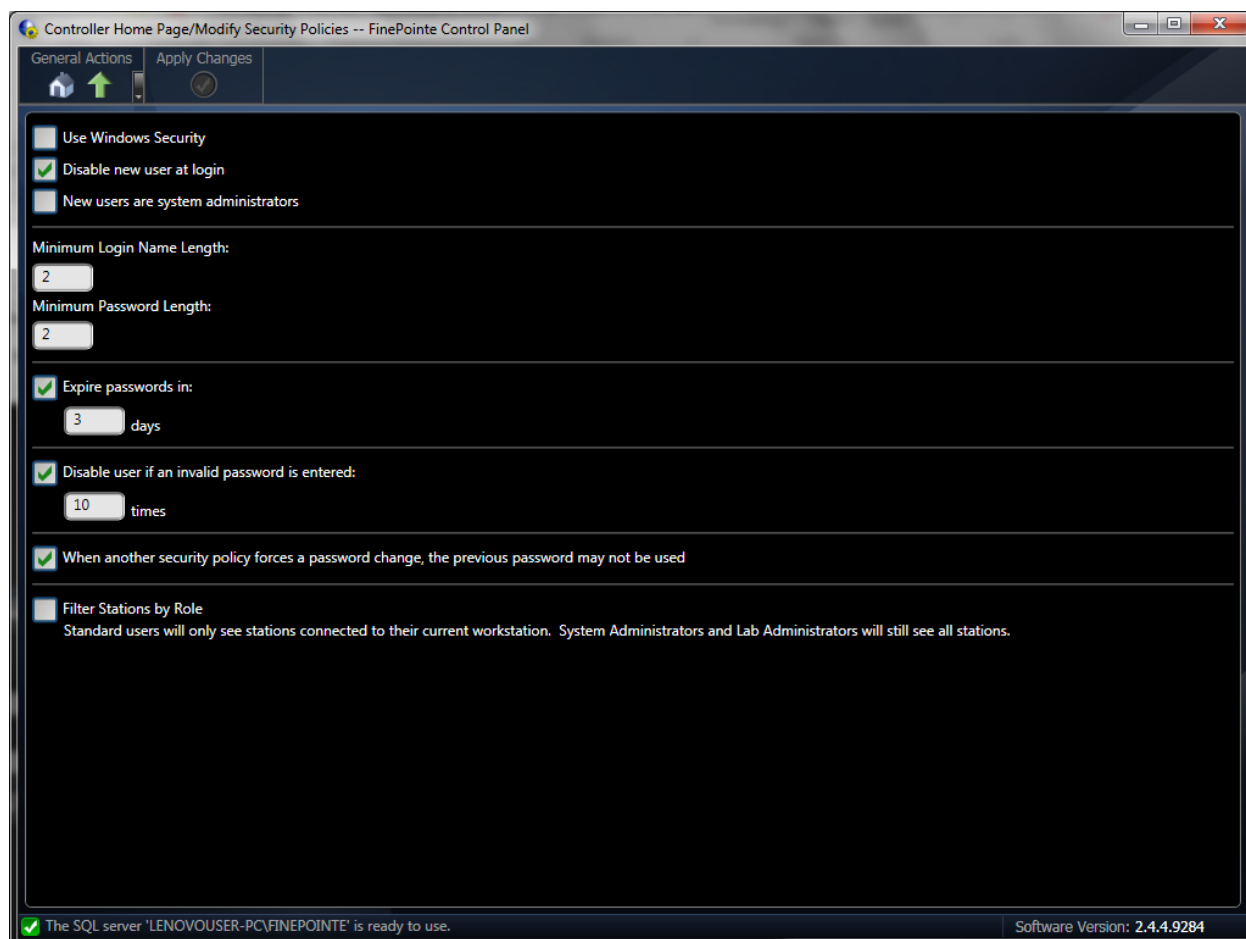
## CONFIRM LICENSE DETAILS

If the license includes this option, the GLP features are automatically enabled and accessible via FinePointe Control panel or FinePointe Review. License file details can be confirmed within FinePointe Control Panel by selecting the **View License Details** tool on the home page. The **Enable GLP** box should be checked. This screen also contains options to install or extend a license, save the license file to the desktop, and re-read the license and update this display. If the **Enable GLP** option is not selected, an updated license file must be obtained to permit access to GLP features.

## ESTABLISHING INITIAL SECURITY SETTINGS

After establishing server and database settings, the FinePointe Control Panel will display additional tools for managing the FinePointe system.

Prior to running GLP-compliant studies, it is necessary to configure security options appropriate for the site and ensure appropriate settings in the Windows environment.



## DEFAULT POLICIES FOR NEW USERS

There are two options for controlling how FinePointe handles new users, controlled by the **Modify Security Policies** tool:

- **Disable new user at login.** By default this option is unchecked, and upon launching FinePointe a “Create New User” icon is available. In a GLP setting, this option must generally be set to “disabled”, unless alternate procedural controls are established to prohibit unauthorized creation of new users.
- **New users are system administrators.** This setting controls whether new users created at the login screen are system administrators by default, however it is always possible to manually change whether a particular user is a system administrator through the FinePointe Control Panel.

## CONFIGURING USERNAME AND PASSWORD POLICIES

FinePointe supports two options for username and password controls: with the FinePointe Control Panel, or with Windows authentication.

If the **Use Windows Security** option is *unchecked*, the system will use **FinePointe** control of login names and passwords. Generally, we recommend using FinePointe control of authentication.

The security settings allow the administrator to set the following options through the **Modify Security Policies** tool:

- **A minimum login name length.** Because electronic signatures and audit trail entries are associated with the login name, we recommend using login names that are sufficiently long and clear enough to easily differentiate users (for example, using an individual's full name as a login).
- **A minimum password length.** Note that if the minimum password length is not specified as greater than zero, the password field could be left blank. This configuration would not meet GLP requirements for access control and electronic signature components.
- The number of days before expiring passwords, which forces the user to change their password after a specified number of days.
- The number of invalid password entries prior to disabling of the account. As part of limiting access to authorized individuals, we recommend setting this at a reasonable number to prevent an unauthorized user from gaining access by repeatedly attempting to guess a password. This option must be selected and set to some number in order for the system audit trail to properly record unauthorized access attempts.
- An option to disallow the use of the last password when a security policy forces a password change.
- A "Filter stations by role" option is available regardless of the method of user authentication chosen (FinePointe or Windows). When selected, standard users will only see stations connected to their current station, while system administrators and lab administrators will see all stations.

If the **Use Windows Security** option is *selected*, the username and password policy options in FinePointe will not be available. Instead, management of login names and passwords would be accomplished through Windows tools and policies, and the User will need to ensure that the Windows environment settings and SOP's meet GLP requirements (e.g. policies to cover password aging, disabling of users, and monitoring unauthorized access attempts). It is especially important to note that the FinePointe system audit trail **will not** record invalid authentication attempts if Windows Security is selected; rather, the user must develop procedures for detecting and documenting access attempts by using Windows tools.

While the user authentication (usernames, passwords, and associated policies) are controlled via Windows account settings, **User Roles** are still necessary to assign users particular levels of authorization within the FinePointe Review program (see User Access and Authorization section below).

## FOLDER SECURITY PERMISSIONS

---

Access to data management tools within FinePointe, including the ability to delete a study, are controlled by access levels (see User Access Control section below), and the system audit trail tracks events such as study deletion (see Audit Trail section below). However, the User must also secure the FinePointe data folder in order to prevent unauthorized access including potential deletion of records outside of the FinePointe application. It is recommended to secure the data folder from accidental deletion by setting folder permissions within Windows to deny standard users the ability to modify or delete the contents of the FinePointe data folder.

## SQL DATABASE AUTHENTICATION

---

In the FinePointe Control Panel, under the **Modify Server Settings** tool, the User can select whether to use **Windows Authentication** or **SQL Server Authentication** to control database access. The default is Windows authentication, however, if SQL Server Authentication is selected, the User can control database access through a



SQL management utility. If using this option, the FinePointe application requires rights to run as administrator and write to the study database, while Users can be restricted from accessing or modifying the study database. This should be done in consultation with the User's IT department.

## USER ACCESS LEVELS AND AUTHORIZATION CONTROL

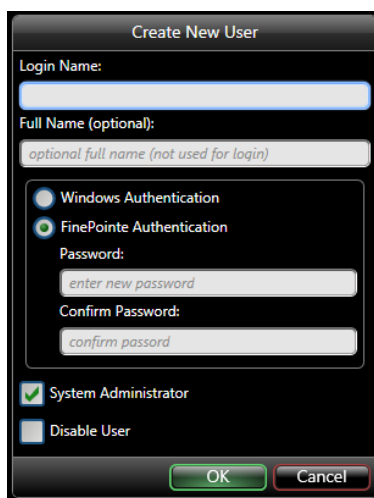
After initial security settings have been established, the next step is typically to create users authorized to access the system. Users are required to enter their username and password when logging in to the system, if they are requesting control of an acquisition, and prior to executing an electronic signature.

### CREATING USERS

The **Manage Users** tool allows an administrator to manage users and their roles on the system level, for a particular laboratory, or for a particular study. Users can be managed through the FinePointe Control Panel, or by selecting the blue **Manage Users** icon from either the laboratory or study level.

In a typical GLP environment, creating users is usually accomplished in the FinePointe Control Panel since **creating New Users at Login** is not enabled under the Security Policies tool.

From the Control Panel Home Page, select the **Manage Users** tool, then **Users Management>New User**. Input the desired login name and initial password (if using FinePointe Authentication). Checkboxes exist for whether the user is a system administrator, and whether a user is disabled.

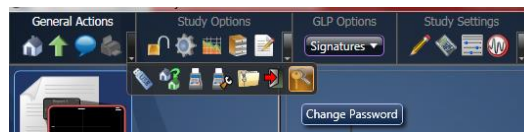


Though optional, we recommend filling out the "Full name" field in addition to a login name, in order to provide an additional record of a user's identity. However, within the electronic signatures and audit trail records, the username but not the full name is stored. Therefore, SOP's must be established to ensure that a user's identity is clearly linked to a specific username, and that historical uniqueness of the username is retained. One option for doing so is to keep a record of usernames along with each individual's verification of their electronic signature equivalence.

## DISABLING AND ENABLING USERS

In the event that a user's access has been automatically disabled (e.g. for too many bad password attempts), the system administrator may use this tool to uncheck the "disable" button to permit the user access again. Conversely, the system administrator may use this tool to disable a user at any time should a user's access need to be revoked or suspended.

Through this tool, the system administrator may also set or reset a user's password. A user may change his or her own password at any time within FinePointe Review by selecting **General Actions>Change Password** at either the laboratory or study level.



## MANAGING USER ROLES

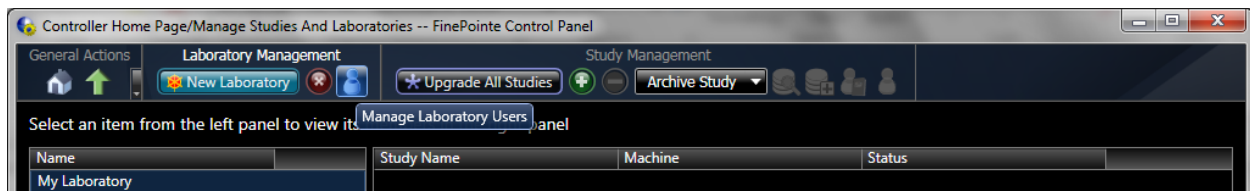
In addition to gaining system access with a valid username and password, access to the functionality of the FinePointe software is controlled by roles. After users have been created, they must be assigned access to the relevant laboratories/studies and assigned appropriate roles.

In order to open any laboratories or studies, users must be assigned a role within that study or laboratory. Several access levels are available, controlling which features are accessible, including which electronic signature types are possible for that user.

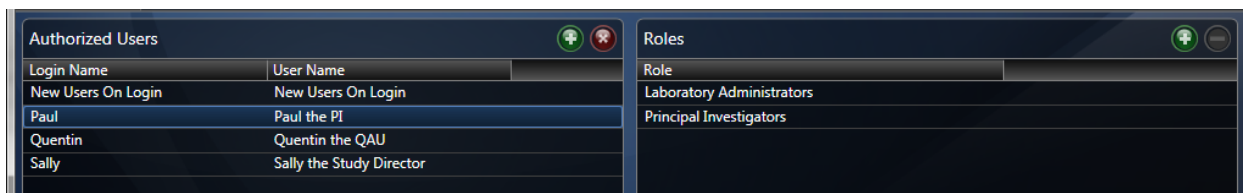
With the exception of the system administrator roles, which provides administrator rights across the entire system, users may be assigned different roles for different laboratories and studies. For example, a user could be a laboratory administrator for one lab, have a PI role on a study within that lab, while only having technician rights for a study within a different laboratory. The flexibility of this system ensures that user access can be controlled at the level of the system, laboratory, or individual study, whichever is appropriate for the particular user environment.

Note that there are user roles which control access levels in addition to GLP roles which provide special signature rights. These two distinct types of roles are explained separately below.

From the FinePointe Control Panel, users can be assigned to a laboratory by opening the **Manage Studies and Laboratories** tool, and selecting **Laboratory Management>Manage Laboratory Users**.



Select the desired laboratory, and users may then be added or deleted from the list of authorized users for that lab. Additionally, selecting each user allows the addition or deletion of roles for that user (in the right hand pane).



Users may also be managed within FinePointe Review at the laboratory or at the study level. Using an account with sufficient access level (Study Administrator or above), select **Study Options>Manage Study Users** to assign users roles within a specific study.



## ROLES CONTROLLING ACCESS LEVELS

Users must be assigned at least one of the following roles controlling which features they are authorized to access. Without at least one of these roles assigned, the user will not be able to open a laboratory or study and will not be able to perform any functions in the FinePointe Review software. Users may have multiple roles assigned. Please refer to Appendix C for a full listing of restricted features for each access level.

**System Administrator** – Provides full access to all features, authorizing the user to manage studies and users, including full rights to create, modify, and delete records.

**Laboratory Administrators** – Provides administrator level access to an assigned laboratory, but not to other laboratories to which this user has not been assigned.

**Study Administrators** – Provides administrator level access to an assigned study, but does not allow laboratory level privileges such as creating folders and managing laboratory users (however, a study administrator may still manage users for that particular study).

**Technician** – Provides intermediate level access. Users assigned a technician role can launch studies they are assigned to, perform analysis functions, and create reports. A technician cannot create, rename, delete, or archive studies. They are also restricted from laboratory level activities such as creating folders and managing users.

**User** – The user role provides the most limited access level. A study user has read-only access to studies. In addition to the restrictions of the technician access level, a study user is restricted from: launching or requesting

control of a station, creating, modifying, or deleting subjects, groups, and recordings, changing parameters, changing acquisition settings, changing analysis functions (e.g. chart options, measurements, and events), and calibrating hardware.

**Contract Client** – This is an optional access role for GLP studies, which functions differently than the other access roles. A user with this role can only view content within the study that has been approved with a Contract Client Approve electronic signature.

---

## GLP ROLES

In addition to roles controlling study access, FinePointe includes descriptive roles designed specifically with GLP studies in mind. These special roles are descriptive of a user's contribution to the study and provide access to particular signature types. However, these roles do **not** allow access to a study on their own; they must be accompanied by one of the above access levels in order for the user to open a laboratory or study. Please refer to Appendix B for a full listing of electronic signature privileges controlled by GLP roles.

**Principal Investigators** – All GLP compliant studies must have a designated P.I. The P.I. can generate all types of signatures available.

**Study Director** - All GLP compliant studies must have a designated Study Director. The study director can generate all types of signatures available.

**Quality Assurance Unit** – All GLP compliant studies must have a designated QA unit. This role is designed for quality assurance unit activities. The QA unit has signature rights to: accept or reject a subject, reject a previously accepted recording session, and re-open previously approved studies and reports. Other signature rights, such as authoring, are not available to the QA unit.

**Contributing Specialists** – This is an optional role for descriptive purposes, with no special signature rights.

*Note: User* – See description above. This is an access role can be used for both GLP and non-GLP studies. When used for a GLP study, it does not permit electronic signatures for the purpose of authoring or approving; however a user may reject a subject session or recording.

*Note: Contract Client* – See description above. This access role for GLP studies provides no special signature rights.

---

## USER ACCESS EXAMPLES

Because GLP signature roles do not provide user access on their own, and because access needs may vary across studies, users may require multiple role assignments. Please see the following examples of such cases.

Example 1: Alice is a lead investigator who will be responsible for a set of studies. She will need to create, manage, and potentially delete studies. For a current GLP study, she will be the designated principal investigator and will need authorization to execute various electronic signatures (e.g. authoring and approving).

Appropriate role assignments for Alice would be:

- A System Administrator or Laboratory Administrator level of access, because she will be creating and managing multiple studies. Alternately, she could be assigned Study Administrator level access for each study she is responsible for.

AND

- A Principal Investigator role assigned at the study level for the GLP study, with her user account designated as the Principal Investigator during study setup.

Example 2: Bob is a Study Director for a particular study, and needs the ability to create and modify that study. He may also occasionally conduct acquisition sessions for other studies, but would not need the authority to create or alter those studies.

Appropriate role assignments for Bob would be:

- A Study Administrator level of access for the study he will be directing.  
AND
- A Study Director role assigned at the study level for the GLP study, with his user account designated as the Study Director during study setup.  
AND
- A Technician level of access for other studies he might assist with.

## GLP STUDY CREATION

Please refer to the installation and setup guide for details on establishing an appropriate hardware configuration and calibrating your system.

When creating a study, simply select whether the study follows GLP or not. Selecting “This study follows GLP” opens up several fields. Select users (who have appropriate roles assigned) and designate a Principal Investigator, Study Director, and QA unit. There is also an option to designate a Contributing Specialist. A Principal Investigator location and study objective are also required.

Note: Once a study has been created, FinePointe does **not** allow the user to change the status of a GLP study into a non-GLP study. Other study options, such as measurements, phases, and task sequences may still be modified by opening the **Study Settings** tool, assuming the user has a sufficient access level (Study administrator or above).

GLP studies automatically enable electronic signatures and include audit trails without requiring any additional setup steps. Within a GLP study, the GLP Options menu will be available on the main study screen, and electronic signature options will be enabled for several study components (outlined in the Electronic Signatures section below).

Acquisition of data for a GLP study proceeds in the same fashion as for a non-GLP study.

## ELECTRONIC SIGNATURES

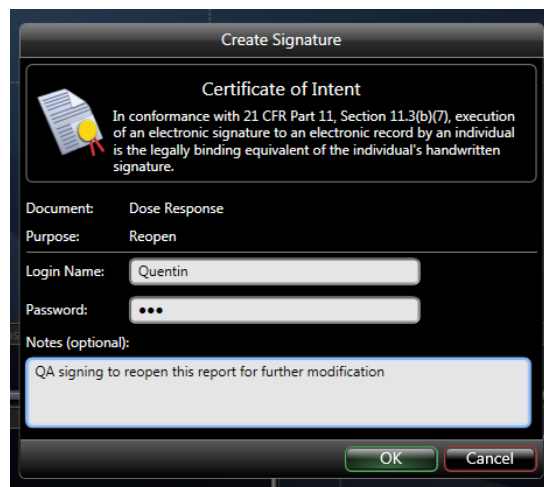
### GENERAL PRINCIPLES OF ELECTRONIC SIGNATURES

GLP compliant electronic signatures must meet several requirements. Signed electronic records must contain the name, date, time, and meaning associated with the signature. The electronic signatures within FinePointe contain the date, time, signature meaning, username, and a notes field, but do not contain the full name provided. Therefore, an additional record of the association between usernames and a user's identity is necessary.

Each signing within FinePointe includes a certification of intent and statement legal equivalence to a handwritten signature stating:

*"In conformance with 21 CFR Part 11, Section 11.3 (b) (7), execution of an electronic signature to an electronic record by an individual is the legally binding equivalent of the individual's handwritten signature."*

Test site procedures and practices should also reinforce this equivalence with a formal written acknowledgement.



When attempting to perform a signing, the **Create Signature** dialog box will open and the User will see the certificate of intent, the name of the document being signed, the purpose, and a field to enter any desired notes.

In addition, the User is required to enter their Login name and Password and the system will authenticate the user prior to completing the signature.

If the User lacks correct permissions to perform the signing, attempting to sign will generate a message stating “User [Login name] is not authorized to sign this document”. If the User’s credentials cannot be authenticated, the system will display an error message stating “User cannot be authenticated: Invalid password or user name”.

Regardless of the continuity of a session, FinePointe requires full authentication for each signing.

---

## SIGNING ITEMS

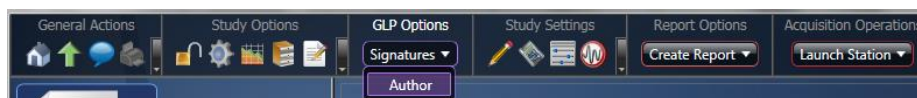
Several different types of items can be signed. While the User is automatically prompted to sign the recording when stopping an acquisition session, the system does not force this signature, and it is up to the User to establish SOP’s determining which signatures will be required.

Only the currently available signature types will display; for example, signing to “Approve” a study will cause the signature option “Reopen” to appear, while all other options will not be available. Similarly, if a “Reject” signature is executed on an item, the option “Accept” will be the only one available, so that “Author” and “Approve” signatures cannot be executed on a rejected item.

---

## STUDY

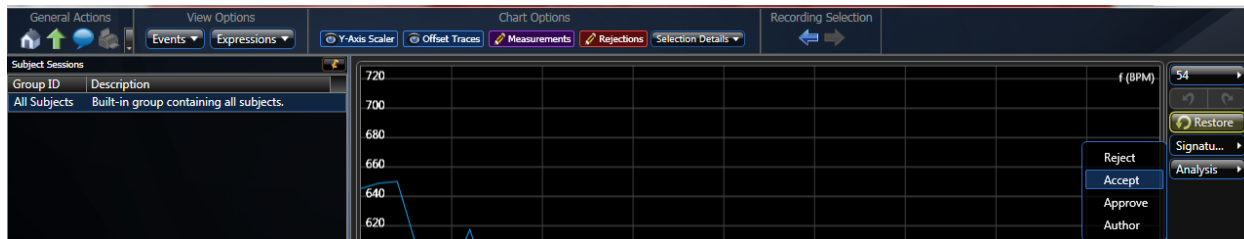
At the study level, signatures can be created to Author, Approve, Contract Client Approve, and Reopen a study. To sign a study, select **GLP Options>Signatures** and select a signature from the drop-down list which contains the currently available signature types.



---

## SUBJECT

At the subject level, signatures can be created to Accept, Reject, Approve, Contract Client Approve, and Reopen a subject. To sign subjects, open **Study Options>View Data and Place Measurements**, then select a subject from the list in the left-hand pane. The far-right pane then displays a **Signatures** drop-down list which contains the currently available signature types.



## GROUP

At the group level, signatures can be created to Author, Approve, Contract Client Approve, and Reopen a group. To sign groups, open **Study Options>Manage Groups and Subjects**, then select a group from the list in the left-hand pane. The **Signatures** drop-down list then displays towards the top of the screen.



## RECORDING

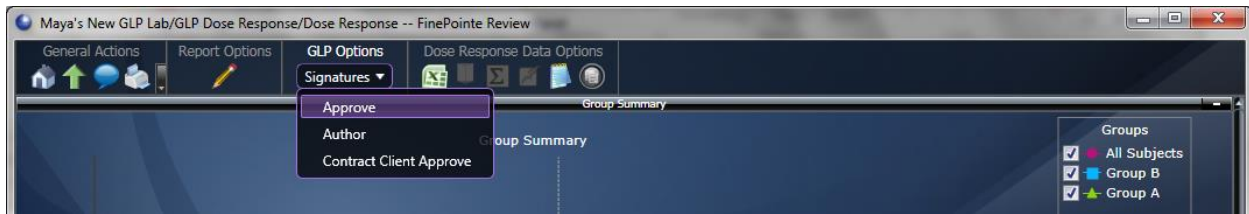
At the recording level, signatures can be created to Accept or Reject a recording. To sign a recording, select the recording on the main study page, and open the **Operations** down list in the far-right column. This list displays options including the available signatures.

Subject ID	Recording Time	Duration	Phase	Source	Status	Open	Operations
11	12/6/2016 12:53:25 PM	1.4 mins	Main	FP Series WBP [DEMO-061] Site1	Complete	Open	Operations
12	12/6/2016 12:53:25 PM	1.4 mins	Main	FP Series WBP [DEMO-061] Site2	Complete	Open	Operations
13	12/6/2016 12:53:25 PM	1.4 mins	Main	FP Series WBP [DEMO-061] Site3	Complete	Open	Operations
14	12/6/2016 12:53:25 PM	1.4 mins	Main	FP Series WBP [DEMO-061] Site4	Complete	Open	Operations

## REPORT

At the report level, signatures can be created to Author, Approve, Contract Client Approve, and Reopen a report. To sign a report, open the report from the study home page, then select **GLP Options>Signatures** and select a signature from the drop-down list which contains the currently available signature types.






---

## SIGNATURE MEANINGS

### AUTHOR

An authorship signature is the user’s confirmation that he or she is the individual performing that action or collection. Multiple signatures of authorship may be executed on the same item (unless that item has already been Approved). It is good practice to establish SOP’s governing when the Study Director and/or Principal Investigator are required to execute an authorship signature.

### ACCEPT/REJECT

An individual or group’s study data may be signed as accepted or rejected. A rejection includes a mandatory “notes” field, while this field is optional when accepting data.

### APPROVAL

In contrast to signing for authorship of a particular action or piece of data, approving a study involves signing the entire study and stopping data collection. Once a study is approved, no additional data can be added to that study. The study can still be archived and restored for future viewing. If additional data needs to be added, an authorized user must perform a “reopen” signature.

### CONTRACT CLIENT APPROVE

After a subject session or recording has been approved, there is an additional option to “Contract Client Approved”. This feature is intended to give a user with only “Contract Client” role access to data.

### REOPEN

This allows a previously approved study to be reopened in order for additional data to be added or changed, or for additional signatures to be added to items. This is only possible for a study or other item that has previously been approved.

---

## ACCESSING ELECTRONIC SIGNATURES

Electronic signature records can be accessed in FinePointe Review by inspecting the **Study Audit Trail** (see Audit Trails section for more details), or by opening a study and selecting **Study Options>View Signatures**.



While the audit trail is organized by date and time, the **View Signatures** dialog is organized by signed item. The top pane shows a list of signed items and their descriptions. Selecting an item displays the full signature history for that item, including the date, time, signer, signature meaning, and any notes provided at the time of signing. The view signatures dialog does not permit export (audit trails may be exported, however).



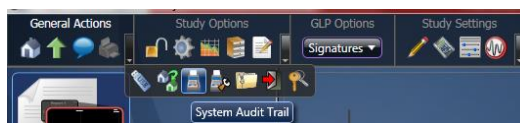
There is no mechanism within FinePointe to modify the electronic signature records (or the audit trails) associated with a study, and signature records are retained by the study throughout any archiving or restoring actions.

## AUDIT TRAILS

The system, calibration, and study have distinct audit trails. The date, time, username, and description is recorded for all audit trail entries. All audit trails are read-only access within FinePointe, however they may be exported as Excel, Open Office, or text files. Audit trails are displayed in a time-sequenced fashion, and subsequent entries do not obscure prior entries.

Audit trails are “read only” within FinePointe and cannot be modified; however, once the audit trail is exported such a document could potentially be modified. Additional protection of exported audit trail documents can be accomplished by setting the exported files as “read only” and/or ensuring they are exported to a secure location in accordance with SOP’s appropriate for the study site.

The **system audit trail** can be accessed in FinePointe Review by selecting **General Actions > System Audit Trail** from within either a laboratory or a study.



This audit trail records:

- All access attempts, both valid and invalid, as well as users logging out.
- All password changes, whether by the user or system administrator.
- User management activities including the creation and deletion of users, modification of user roles and disabling and re-enabling of users.
- Other system activities such as server/client connections.

Note: While unauthorized access attempts are recorded in the audit trail, the system does **not** automatically notify the system administrator of such attempts. Therefore, we recommend establishing a procedure for periodically inspecting the records to ensure that the system administrator and other appropriate parties are aware of unauthorized access attempts. Timely detection and reporting of such events is a requirement of 21 CFR Part 11:11.300(d).

The **calibration audit trail** can be accessed by selecting **General Actions > Calibration Audit Trail**.



This audit trail records:

- The date, time, username and description of all calibration sessions.

The **study audit trail** can be accessed in FinePointe Review by selecting **Study Options > View Study Audit Trail** from within the study.



The study audit trail is linked to the study, so that the audit trail is included in any archive of the study, and is maintained if the study is restored from archive. This audit trail records:

- The creation, deletion, and modification of study data and information, such as study settings, recordings, measurements, and reanalysis of recordings.
- The creation, deletion, and modification of study components such as reports, subjects and groups.
- Electronic signatures created for the study.
- User connections and disconnections from the study.

## DATA MANAGEMENT, ARCHIVING AND RESTORING

The archiving feature allows studies to be archived for storage. Studies can be archived multiple times if desired, and can be easily restored at any time. All audit trails and signatures are retained with the study through any archiving and restoring.

To access the archiving tools in the FinePointe Control Panel, select **Manage Studies and Laboratories> Study Management>Archive Study**, then select either the **Archive** or **Restore** option. To access these functions from FinePointe Review, right click on a study and select **Archive**.



To restore a study, open the desired laboratory and select **Laboratory Options>Restore Study From Archives**, then select the desired study from the list.



Archiving and restoring functions are limited by the user's access level. A system administrator can perform archiving and restoring functions for any study, a laboratory administrator may archive and restore any study within that laboratory, and a study administrator can only archive and restore the study they are assigned an administrator role to.

Within the **Manage Studies and Laboratories** tool, the user may also add and remove studies from a laboratory. Note that adding and removing studies from a particular laboratory is *not* the same as deleting the studies from the server. After removing a study, it will not be accessible from within a laboratory, but it will still be available to be added to a laboratory using this tool.

The **Manage Data** tool in the FinePointe Control Panel can be used to view, delete, or begin processing tasks.

Additionally, under **Database Management** in the FinePointe Control Panel, there is an option to delete the entire database. Only select this option if it is necessary to start from scratch with an entirely new database; all data, archives, study information, and user information will be lost and cannot be recovered.

## DATABASE INTEGRITY

The FinePointe includes a cyclical redundancy check (CRC) to detect unauthorized data manipulation or data corruption. Under **Database Management** in the Control Panel, or from the **Study Options** menu within a study, any user can select **Verify Database Integrity**. The integrity check will then run, and will tell the user whether any errors have been detected.



An option to **Repair Database** also exists if the user has sufficient access level. If errors are detected and the records repaired, the study audit trail will include entries documenting the records repaired.



FinePointe also automatically runs an integrity check whenever data is transferred to the server, and network traffic is encrypted during such transfers.

## ADDITIONAL RECOMMENDED POLICIES AND PROCEDURES

It is important to note that no piece of software can ensure GLP compliance on its own. Appropriate procedural and administrative controls must also be established to ensure that the system's operation meets GLP requirements.

### USERNAME AND PASSWORD POLICY CONSIDERATIONS

Electronic signatures and audit trail records reference the login name (username), but not the user's full name. Therefore, SOP's must be established to ensure that a user's identity is clearly linked to a specific username, and that historical uniqueness of the username is retained. One option for doing so is to keep a record of usernames along with each individual's verification of their electronic signature equivalence.

When creating a new user, procedures must be established to ensure that the system administrator does not have knowledge of the password that will be used for access and electronic signatures. The password is obscured while typing and remain obscured in the user management tools; however if a system administrator is the person to establish the initial password then the password would be known by more than one person. Aside from the general password expiration policies, there is not a mechanism in the software to force the user to change the initial password. Options for ensuring password privacy include ensuring the new user is present to select and input the initial password during account creation, or establishing SOP's requiring the new user to change his or her password upon initial login and prior to using the password in any electronic signature actions.

#### PERIODIC INSPECTION OF AUDIT TRAILS

The FinePointe system controls access through role based security, will not allow users to login without an appropriate username and password combination, and logs any invalid attempts to log on in the audit trail (when FinePointe authentication is used). However, GLP requirements dictate that unauthorized access attempts be detected and reported to the appropriate management in a timely fashion. Therefore we recommend the system administrator periodically review the audit trails in order to monitor any unauthorized access attempts.

#### PROCEDURES TO SECURE FOLDER PERMISSIONS

The FinePointe Data folder and database location should be secured Through Windows policies. One option is to disable access to the folder location for non-administrator users. Windows group policies may also be used to control access and/or permissions level for groups or specified individual windows users.

---

#### SPECIAL CONSIDERATIONS WHEN USING THE WINDOWS SECURITY OPTION

The system provides a choice of whether to use FinePointe or Windows authentication. If Windows authentication is used, any user that has administrator privileges in Windows will have administrator privileges within FinePointe. Additionally, it would be necessary to work with the organization's IT group to establish username, password, and user access policies that meet GLP requirements. Windows policies and/or other procedural controls must be established outside of FinePointe to ensure the following: uniqueness of login names (including historical uniqueness), policies to cover password aging, procedures for disabling users, and procedures for detecting and reporting unauthorized access attempts. Note that when Windows authentication is selected, the FinePointe system audit trail does not record access attempts with invalid credentials.

---

#### SPECIAL CONSIDERATIONS WHEN USING THE SQL DATABASE AUTHENTICATION OPTION

This option exists for customers who desire to control database access through SQL database authentication controls. Implementing this option is typically done in consultation with a test site's IT department. If this option is desired, the system owners will need to use a SQL management utility to ensure the FinePointe service is run as a user with full access to the specified database and data folders, as well as establishing appropriate access controls for other users or groups (e.g. read-only access for standard users).

## APPENDIX A: 21 CFR PART 11; ELECTRONIC RECORDS, ELECTRONIC SIGNATURES SUBPART B - ELECTRONIC RECORDS

The following section is an outline of the FDA's 21 CFR Part 11 requirements and how the FinePointe application addresses each requirement.

---

### CONTROLS FOR CLOSED SYSTEMS

#### CLOSED SYSTEMS

---

*Section 11.10 of the regulation requires, "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."*

This document assumes that operation of the FinePointe System falls under the controls specified for Closed Systems. FinePointe is accessed by individuals (FinePointe Users) who are responsible for the content of electronic records that are on the system through the use of an authorized login name and password combination.

If the FinePointe System is being used to create, modify, maintain, or transmit electronic records that fall under the requirements of the FDA, then the User should comply with 21 CFR Part 11 Electronic Records, Electronic Signatures regulations. The User is responsible for developing and implementing Standard Operating Procedures (SOPs) to prevent falsification of such records by complying with the following regulations for closed systems:

#### VALIDATION OF SYSTEMS

---

*Section 11.10 (a) of the regulation requires, "validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records."*

The User is responsible for validating the FinePointe System within their computer, laboratory and regulatory environment.

DSI provides a Validation Solution Package to assist FinePointe Users with validating FinePointe Systems. Please contact DSI for more information.

#### ACCURATE AND COMPLETE COPIES OF RECORDS

---

*Section 11.10 (b) of the regulation requires, "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."*

All data can be exported from FinePointe in hardcopy format. In addition, a special report type, the Source Data Report, can also be used to generate an exportable hard copy of the raw data from which any measurements were derived.

Appropriate use and control of audit trail, FinePointe files, user names and passwords, the Verify Database function and secured directories (for control of FinePointe files) through the Windows system can technologically assist the User with producing accurate and complete copies of electronic records for inspection, review, and copying by the FDA.

- FinePointe Audit Trails provide who, what, where, and why information associated with an electronic record.
- FinePointe study data includes the signature records and audit trails within each study, so that the User can verify the link between an electronic signature and the signed item.
- Username and password policies allow the User to control access to the FinePointe System, and therefore, inhibit the obstruction of electronic records by un-authorized Users.
- Securing the data directory and/or the SQL database allows control over the level of access to electronic records outside of the FinePointe application.
- Altered or invalid records can be discerned using the Verify Database function in FinePointe. A cyclical redundancy check is performed to verify database integrity, and the results are displayed to the user. This manual operation can be performed at any time, however the system also automatically performs this check when data is transferred to the server.

## PROTECTION OF RECORDS

---

*Section 11.10 (c) of the regulation requires, “protection of records to enable their accurate and ready retrieval throughout the records retention period.”*

The User is responsible for establishing systematic archiving and backup procedures to ensure that electronic records are stored in a manner where they can be retrieved over an extended period of time. Determining a record’s retention period is also the responsibility of the organization.

The FinePointe system offers tools for archiving studies and restoring studies from archive, which automatically include the retention of associated audit trails and electronic signature records.

## LIMITING SYSTEM ACCESS

---

*Section 11.10 (d) of the regulation requires, “limiting system access to authorized individuals.”*

The User is responsible for controlling which individuals have access to the System and the degree of authority they have on the System (Access Levels).



With regards to the FinePointe System, only individuals who are granted usernames and passwords and are set up on the system as authorized users of a particular system, laboratory, or study are permitted to gain access to the FinePointe application. The degree of authority that the User has on the System is further defined by use of Access Levels. Any user requesting control of a currently running session must re-authenticate with valid credentials before control of the session is granted by the System.

## AUDIT TRAILS

---

*Section 11.10 (e) of the regulation requires, “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.”*

FinePointe generates Audit Trail information (see section on Audit Trails). Audit Trails include a computer-generated time stamp and the required information (who, what, where, and why) for GLP compliance. Audit trails may be exported but cannot be altered within FinePointe and subsequent entries in the Audit Trail do not obscure previous entries. If FinePointe’s Archive/Restore tool is used, each study’s Audit Trail is automatically included in any archived or restored study.

The User is responsible for establishing SOPs that prohibit Users from obscuring recorded information and determining the retention period and maintenance of the audit trail so that the FDA may review and copy all pertinent records.

## OPERATIONAL CHECKS

---

*Section 11.10 (f) of the regulation requires, “use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.”*

The User is responsible for developing SOPs that establish conformance amongst Users who operate the system to enforce sequential execution of steps or events, as appropriate. When collecting study data, study subjects must be specified and task sequences (including the duration of each task) must be defined by the user prior to acquisition of any data.

## AUTHORITY CHECKS

---

*Section 11.10 (g) of the regulation requires, “use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation of computer system input or output device, alter a record, or perform the operation at hand.”*

To prevent un-authorized access to the FinePointe System or unauthorized execution of an electronic signature, the System performs the following checks:

- Verifies that the login name and password used to log-on the system represents a valid User. A security policy within FinePointe can control the number of invalid password entries before the account is disabled.

- Verifies that the logged on User is authorized to open the laboratory or study within the FinePointe application (system checks that the Login name is listed on the laboratory or study's list of authorized users).
- Verifies that the logged on User is authorized to carry out particular functions within the application (FinePointe application checks the User's Access Level permitted for that particular System). If a FinePointe User is restricted from using certain functions, then those functions either will be grayed so that the User cannot select the function or the application will display a warning message notifying the User that they are not allowed to perform those actions.
- Verifies that the logged on User is authorized to execute electronic signatures by checking the Login name and Password prior to executing the electronic signature. The System also determines if the User is permitted to sign files according to their Access Level defined on the System.

## DEVICE CHECKS

---

*Section 11.10 (h) of the regulation requires, "use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction."*

A valid hardware setup must be specified in order for each data acquisition session to begin, and incompatible configurations (e.g. an incompatible apparatus or species) will not run. To assist the User with tracking the source of data, the system audit trail records the name of the System establishing a connection to the server. When transferring data from the client to the server, a cyclical redundancy check (CRC) is performed to ensure database integrity.

## EDUCATION, TRAINING, AND EXPERIENCE

---

*Section 11.10 (i) of the regulation requires, "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 User is responsible for determining the extent of education, training, and experience a User requires to be deemed proficient in operating the FinePointe system.

DSI provides training courses on FinePointe systems. Please contact DSI for more information.

## ACCOUNTABILITY OF ELECTRONIC SIGNATURES

---

*Section 11.10 (j) of the regulation requires, "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 User is responsible for developing procedures that hold Users responsible for their electronic signatures. Each electronic signature executed within FinePointe also contains a certificate of intent to reinforce this accountability.

## DOCUMENTATION CONTROL

---

*Section 11.10 (k) of the regulation requires, “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 and (2) revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.”*

The User is responsible for establishing procedures for revision and change control regarding development and modification of systems documentation.

---

## ELECTRONIC MANIFESTATIONS

---

### SIGNATURE INFORMATION

*Section 11.50 (a) (1, 2, and 3) of the regulation requires, “signed electronic records shall contain information associated with the signing that clearly indicates all of the following: printed name of the signer, the date and time when the signature was executed and meaning (such as review, approval, responsibility, or authorship) associated with the signature.”*

The Study Audit Trail includes a record of each electronic signature executed. Signature information organized by item signed can also be viewed by selecting the View Signatures tool within a study. The username, date and time of signature, and reason for the signature is indicated for each signed item. The View Signatures dialog also indicates text information (notes) that the User entered upon executing the electronic signature.

---

### ELECTRONIC SIGNATURE CONTROLS

*Section 11.50 (b) of the regulation requires that the information stated in section 11.50 (a), “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 signature records are included as part of the study and are retained within the study even if the study has been archived and/or restored.

Information from the View Signatures dialog exists in a human-readable electronic display, allowing the FinePointe User to tie electronic signature information with the electronic record. Additionally, the Study Audit Trail is linked to each electronic study record, and may be displayed electronically or exported.

---

### SIGNATURE/RECORD LINKING

*Section 11.70 of the regulation requires. “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 signatures are stored with a study and cannot be excised from the study. In addition, there is no mechanism to import signatures into an existing or newly created study. Copying, archiving, and restoring a study does not alter the signature record.

Subpart C - Electronic Signatures

## GENERAL REQUIREMENTS

---

*Section 11.100 (a) of the regulation requires, “each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.”*

The User should establish procedures to prohibit multiple Users from utilizing the same Login name and Password required in gaining access to the System and executing electronic signatures; each electronic signature should represent only one individual.

The FinePointe system does not permit multiple instances of the same Login name. However, to maintain historical uniqueness, even if a user has been deleted, it is recommended that the User develop procedures to prevent Login name re-use (for example, disabling instead of deleting users and/or maintaining a separate record of all Login names assigned over the life of the system).

It is recommended that the User develop SOPs to ensure that each User utilizes their own unique Login name and Password and maintains control over the use of these components so that no other individual can employ falsified operations on the System.

## UNIQUE SIGNATURES

---

*Section 11.100 (b) of the regulation requires, “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 User is responsible for establishing SOPs that verify the identity of an individual who executes an electronic signature on the FinePointe System.

## CERTIFICATION OF ELECTRONIC SIGNATURES

---

*Section 11.100 (c) of the regulation requires, “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”. Section 11.100 (c) (2) also requires “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.”*

It is the responsibility of the User to certify that electronic signatures are equivalent to traditional handwritten signatures and that FinePointe Users who execute electronic signatures are aware that their actions are the legally binding equivalent of the User’s handwritten signature.

To assist the organization, a statement appears in appropriate dialogs notifying Users that electronically signing a file is considered legally binding.

---

## COMPONENTS AND CONTROLS

## USE OF TWO DISTINCT IDENTIFICATION COMPONENTS

---

*Section 11.200 (a) of the regulation requires, “electronic signatures that are not based upon biometrics shall: (1) employ at least two distinct identification components such as an identification code and password.”*

Electronic signatures (and the ability to gain access to the system) require use of a unique Login name (component 1) and Password (component 2).

## USE OF COMPONENTS WITHIN A SINGLE SESSION AND MULTIPLE SESSIONS

---

*Section 11.200 (a) (1) (i) (ii) of the regulation requires, “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 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. 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.”*

To enter the FinePointe application, the User will be required to input their Login name (component 1) and Password (component 2).

When the System is able to recognize both components as valid, the User is then granted control over the System and then may continue to execute electronic signatures. Upon each signing, regardless of whether the signing is the first or a subsequent signing, the User is required to re-authenticate with their Login name and Password.

## USE OF COMPONENTS BY THEIR GENUINE OWNER

---

*Section 11.200 (a) (2) of the regulation requires that signature components, “be used by only their genuine owners.”*

The User should establish procedures so that each FinePointe User has their own unique Login name and Password, these should not be shared amongst multiple FinePointe Users, and only the User should know the Password.

## MISUSE OF COMPONENTS

---

The User is responsible for developing SOPs to prevent misuse of components that are required for executing an electronic signature (and gaining access to the system).

## CONTROLS FOR IDENTIFICATION CODES/PASSWORDS

---

### US OF UNIQUE IDENTIFICATION CODE/PASSWORD

---

*Section 11.300 (a) of the regulation requires, “maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.”*

The FinePointe system does not permit multiple instances of the same Login name (the identification code) to be created; if the User attempts to create an account with an already existing Login name, the system will not permit the creation of the second account.

However, if a Login name has been previously used, but that account was later removed from the system, the Login name would be able to be reused. The User is responsible for establishing SOP's to ensure the historical uniqueness of each Login name.

## PERIODIC CHECK, RECALL, OR REVISION OF IDENTIFICATION CODES/PASSWORDS

---

*Section 11.300 (b) of the regulation requires, "ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging)."*

The User is responsible for establishing SOPs to verify the control and integrity of Login names and Passwords amongst FinePointe Users.

In the FinePointe application, the FinePointe Administrator can force FinePointe Users to periodically change their Password and prevent Password re-usage.

## LOSS MANAGEMENT PROCEDURES

---

*Section 11.300 (c) of the regulation requires "following loss management procedures to electronically de-authorize 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."*

No devices or physical tokens are used. However, to assist the User in preventing un-authorized use of the System, potentially compromised accounts can be disabled by the system administrator. In addition, the system administrator can specify a maximum number of invalid password attempts before the user is automatically disabled.


## SAFEGUARDS TO DETECT AND PREVENT MISUSE OF IDENTIFICATION CODES/PASSWORDS

---

*Section 11.300 (d) of the regulation requires, "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 User is responsible for establishing SOPs regarding safeguards to prevent unauthorized use of Login names and Passwords and determining how the organization will address reporting and detection of unauthorized use of the System.

To assist the User with safeguards to prevent unauthorized use of components employed to access the System or execute electronic signatures, the FinePointe System can be configured to automatically disable an account after a specified number of invalid login attempts.



The System Audit Trail maintains a record of both valid and invalid access attempts.

### PERIODIC TESTING OF DEVICES

---

*Section 11.300 (e) of the regulation requires, “initial and periodic testing of devices, such as tokens and 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.”*

No devices or physical tokens are used.

## APPENDIX B: GLP SIGNATURE PERMISSIONS

Note: As described in the User Access section, User Access Roles are distinct from the special GLP roles enabling most signature types. All users require one or more User Access Roles assigned in order to gain access to the FinePointe system, while not all users will necessarily be assigned GLP roles.

Signature Type	User Access Role					GLP Role		
	System Administrator	Lab Administrator	Study Administrator	Technician	User	QA Unit	Study Director	Principal Investigator
<b>Study Signature</b>								
Unsigned -> Signed							X	X
Approved->Reopened							X	X
<b>Group Signature</b>								
Unsigned->Signed							X	X
Approved->Reopened							X	X
<b>Report Signature</b>								
Unsigned->Signed							X	X
Approved->Reopened							X	X
<b>Subject Session or Recording Session Signature</b>								
Unsigned -> Rejected					X		X	X
Unsigned->Accepted						X	X	X
Unsigned->Approved							X	X
Rejected->Accepted							X	X
Accepted->Rejected						X	X	X
Accepted->Approved							X	X
Approved->Rejected						X	X	X



## APPENDIX C: RESTRICTED FEATURES LISTED BY ACCESS LEVEL

<b>Restricted Features for: System Administrator</b>
The system administrator is not restricted from any features.
<b>Restricted Features for: Laboratory Administrator</b>
The user is restricted from opening a laboratory they are not assigned to.
<b>Restricted Features for: Study Administrator</b>
The user is restricted from opening a laboratory they are not assigned to.
The user is restricted from modifying a laboratory.
The user is restricted from creating a new folder.
The user is restricted from managing laboratory users.
The user is restricted from opening study they are not assigned to.
<b>Restricted Features for: Technician</b>
The user is restricted from opening a laboratory they are not assigned to.
The user is restricted from modifying a laboratory.
The user is restricted from creating a new folder.
The user is restricted from managing laboratory users.
The user is restricted from opening study they are not assigned to.
The user is restricted from managing study users.
The user is restricted from deleting a study.
The user is restricted from renaming a study.
The user is restricted from creating a study.
The user is restricted from creating a study based off of the existing study.
The user is restricted from archiving a study.
The user is restricted from repairing a database.
The user is restricted from modifying study settings.

<b>Restricted Features for: Study User</b>
The user is restricted from opening a laboratory they are not assigned to.
The user is restricted from modifying a laboratory.
The user is restricted from creating a new folder.
The user is restricted from managing laboratory users.
The user is restricted from restoring a study from archive.
The user is restricted from opening study they are not assigned to.
The user is restricted from managing study users.
The user is restricted from deleting a study.
The user is restricted from renaming a study.
The user is restricted from creating a study.
The user is restricted from creating a study based off of the existing study.
The user is restricted from archiving a study.
The user is restricted from repairing a database.
The user is restricted from exporting an acquisition configuration.
The user is restricted from calibrating a station.
The user is restricted from adding, modifying, or deleting subjects or groups.
The user is restricted from modifying study settings.
The user is restricted from reanalyzing recordings.
The user is restricted from including or excluding a reanalysis.
The user is restricted from modifying, deleting or creating new parameters for an existing study.
The user is restricted from changing the algorithm settings for the analyzer used in the study.
The User is restricted from creating new reports.
The User is restricted from editing the chart options for measurements and rejections.
The User is restricted from editing measurements.
The User is restricted from adding events.
The User is restricted from restoring original measurements.
The User is restricted from launching a station session.
The User is restricted from modifying recordings.

