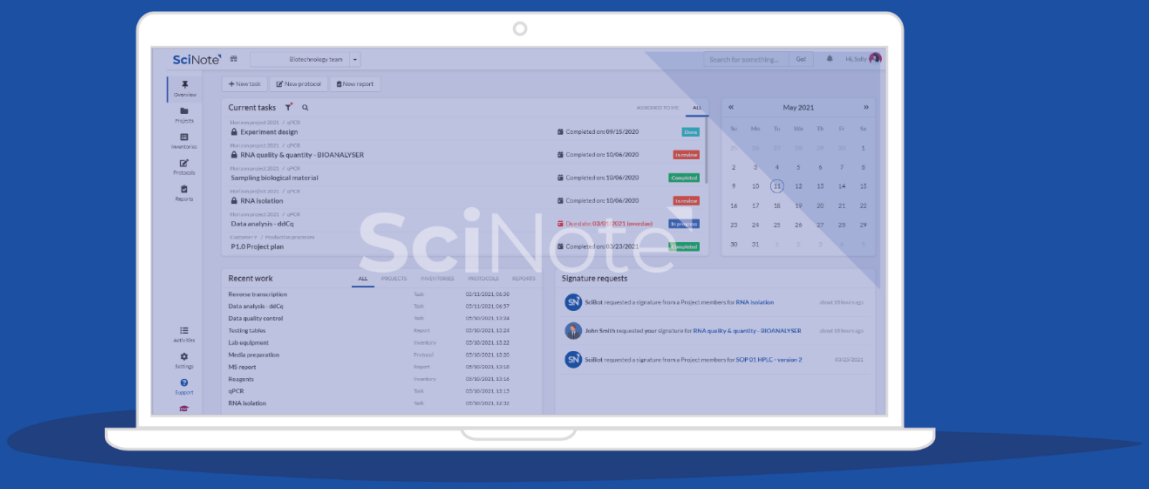
SciNote

SciNote Functionalities Related to GMP and GLP Compliance

Content



Introduction

When your laboratory or company advances from R&D to manufacturing a pharmaceutical product, food, medical device or any other product intended for human or veterinary use, you will inevitably hit the requirement to comply with the GxP guidelines.

GxP is a general abbreviation for the "good practice" quality guidelines and regulations. The "x" represents a particular field, such as laboratory (GLP), manufacturing (GMP), clinical (GCP), etc.

These guidelines ensure that all aspects of the product development process are conducted according to the best methods for safety, efficacy, and quality.

The transition to the regulated environment can be a challenging task. Not only does it require significant financial investment, it also presents a huge bureaucratic burden for the organization.

It also implies implementation of the GxP mindset, that is centered upon traceability (the ability to reconstruct the development history of a product) and accountability (the ability to resolve who has contributed what to the development and when). Documentation management is a critical aspect of the GxP guidelines and documentation compliance may soon result in excessive paperwork.

Many hurdles related to documentation management can be mitigated with the use of an electronic lab notebook (ELN). It should, however, be carefully evaluated, which of the ELN providers best fits the needs of your organization and if it possesses the technical features required by the regulatory guidelines. It is important to emphasize **that ELN itself, as well as any other software or tool, cannot be certified to be GxP compliant.** This is because the compliance does not solely depend on the software system or tool you use, but mostly on how diligently the processes and procedural controls (e.g., document control, SOPs, training etc.) are implemented and handled by the organization that uses electronic data, electronic records that are generated in an ELN or other software tools. It is, however, essential that an ELN offers functionalities that fulfill the requirements of the GxP guidelines and facilitate its implementation within your organization.

Some of the most important GxP guidelines that include the requirements for computerized systems are **GMP** (FDA CFR Title 21 Part 11 and EudraLex Volume 4 — GMP Guidelines, Annex 11) and **GLP**. Below we will explain the specific requirements of those guidelines for ELNs, and also claim how SciNote technical features can support you to achieve GxP compliance.

GMP guidelines

Pharmaceutical and biotechnological companies that manufacture a pharmaceutical product, food, medical device or any other product intended for human or veterinary use, have to comply with the Good Manufacturing Practice (GMP) guidelines. The purpose of the GMP guidelines is to ensure that products are safe and meet stringent quality standards during the production process.

The GMP guidelines that provide technical requirements of computerized data systems, including ELNs, are covered in the CFR Title 21 Part 11 imposed by the FDA in the US and EudraLex Volume 4 — GMP Guidelines, Annex 11 in the EU.

Part 11 and Annex 11 are not completely aligned; however, they share a mutual goal to ensure that electronic records are as secure and reliable as paper records. The regulations provide requirements for the use of electronic signatures, authentication, data integrity, audit trails, data management procedures, access to records in a human-readable form, record retention, and archiving. The requirements for digital signatures and maintaining integrity of the electronic records are extensive and mandate that electronic signatures must be as reliable as hand-signed signatures.

Here are some important technical requirements that an ELN needs to meet to assure your organization can be GMP compliant (according to the CFR Title 21 Part 11):

1. ELN should preferably provide a **closed system by employing restricted access** (with a unique combination of username and password), ensuring that only authorized personnel can access its electronic records. The system should be controlled to ensure the authenticity, integrity, and the confidentiality of electronic records.

2. It should be possible to **create human readable copies of your digital data** at any time in a human readable form (for example in pdf format). In addition, these copies must also be archived for future retrieval.

3. ELN should provide **time-stamped audit trails** to independently record the date and time of users' entries and actions, which cannot be edited or deleted.

4. **Electronic signatures** should be implemented in an ELN in a well-defined manner, including:

    - Signed electronic records should provide the printed name of the signer, the date and time when the signature was executed and the meaning (such as review, approval, responsibility, or authorship) associated with the signature.
    - Each electronic signature shall employ at least two distinct identification components such as an identification code and password. It shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

- Electronic signatures shall be indisputably linked to their respective electronic records in a way to prevent fraudulent use.

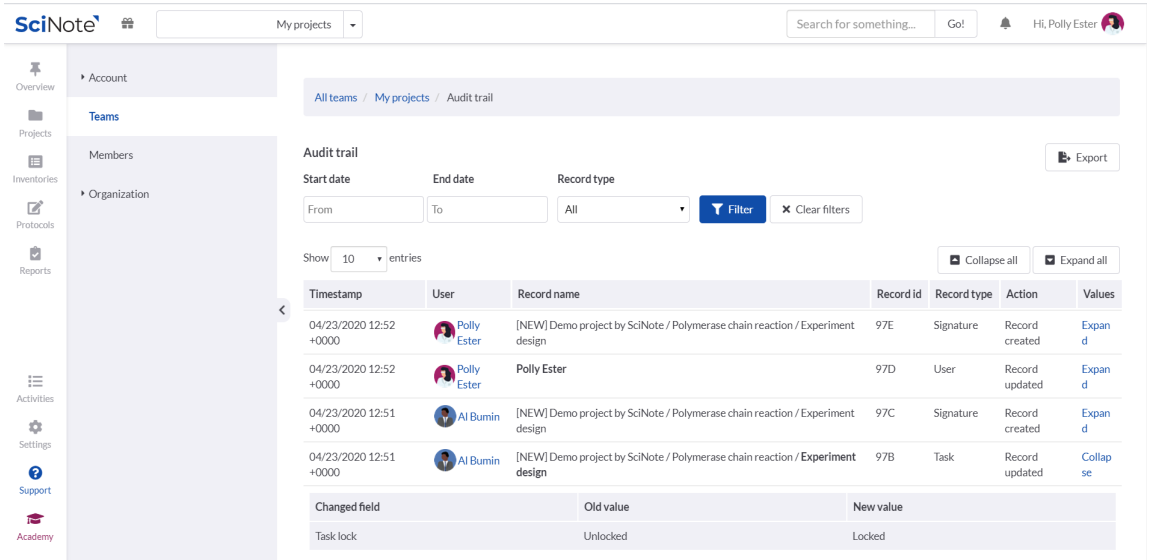
SciNote features for GMP environments

SciNote is a web-based electronic laboratory notebook. According to 21 CFR Part 11 it is categorized as a closed system. SciNote's features and service support all compliance requirements mandated by 21 CFR part 11 for a closed system, while still keeping SciNote flexible and easy to use. In particular it provides the following technical features:

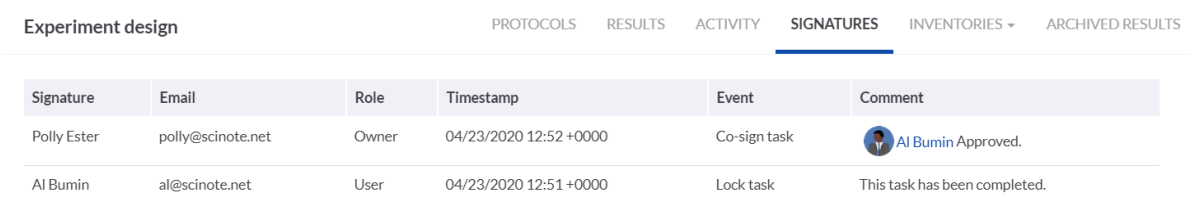
1. SciNote provides a secured **closed system with restricted access**. This is assured by secured system-login, which is unique for each individual SciNote user. The system is controlled to ensure the authenticity, integrity, and the confidentiality of electronic records.

2. It is possible to **create human readable copies of your digital data** at any time. SciNote enables full export of the electronic records in a human readable format with all attachments neatly organized in folders. In addition, SciNote also enables export of electronic signature records, audit trails and system logs into human readable files.

3. It provides **time-stamped audit trails** to independently record the date and time of each user's entries and actions. The audit trails cannot be edited or deleted.



4. It supports time-stamped electronic signatures with the required manifestation, that includes the full name of the signer with date and time when the signature was applied and user configurable field to associate a desired meaning (sign/revoke/reject with a comment). The electronic signature is unique to one individual and indisputably linked to the respective electronic record in a way to prevent fraudulent use.



CFR 21 Part 11 in detail
To read more about SciNote functionalities that support you in meeting CFR 21 Part 11 requirements, get your PDF here.

GLP guidelines

Good Laboratory Practice (GLP) was introduced by the Organization for Economic Co-operation and Development (OECD) and it is imposed in the member countries of the OECD (except USA and Japan). GLP guidelines apply to research laboratories and organizations that conduct non-clinical studies for the assessment of the safety or efficacy of products, including pharmaceuticals, food additives, medical devices, etc. The guidelines include principles that apply in particular to ELNs, which mostly prescribe **how data should be stored, secured and managed**.

Some of the most important GLP principles that apply to electronic data and ELNs are outlined below. These also correspond to technical requirements that can be covered by ELNs.

1. **Data security (physical and logical):** prevention of unauthorized access or changes to the system as well as the electronic data, restricted user permissions

management, robust encryption standards, regular back-ups of the data, exporting of the data, etc.

2. **Data integrity:** Comprehensive data protection from unauthorized access, and changes through access and permission control, a full audit trail that shows all changes to the data, including timestamps and credentials of the person who made the changes, timestamped electronic signatures linked to the electronic records, etc.

3. **Validation:** ELN must be suitable for its intended purpose and have consistent intended performance.

4. **Change Control:** any changes of the electronic data in the operational ELN should be properly documented. Change control procedures should ensure data integrity.

5. **Support mechanism:** It may involve system management, training, maintenance, technical support, and performance assessment to ensure that the ELN is reliable, responsive, and continues to meet stated performance.

6. **Archive:** Electronic data should be stored and archived with the defined access control, indexing and the possibility of retrieval. Electronic records should be stored in a format that is readable for the duration of the applicable record retention period.

SciNote features for GLP environments

SciNote has been incorporating the GLP Principles within its system life cycle to ensure to its users a continuous quality of the software as well as the integrity and security of their research data. Here are some of the SciNote features that cover the most important GLP principles that apply to electronic data and ELNs:

1. **Data security:** SciNote has taken all the measures to ensure state of the art security, confidentiality, authenticity and integrity of data, by employing the following features:
   - Access control to prevent unauthorized access is ensured by secured system-login authentication (with username and password), which is unique for each individual SciNote user.
   - Strict controls for data access, data sharing and data management is ensured with restricted user permissions management (with assigned user roles).
   - Session timeout.
   - Robust encryption standards for the data at rest and in transition.
   - Multiple daily backups of the data.
   - Export of all electronic data in a human readable format.

2. Data integrity: strict access control as well as restricted user permission management are implemented to prevent unauthorized access and changes to the

data. SciNote has a full **audit trail** to show all the actions and changes to the data with a version control, timestamp and the associated person making those changes. Moreover, it enables time-stamped **electronic signatures** indisputably linked to the pertinent electronic records.

3. **Validation**: the software is intensively tested and approved before being released to its users. All testing procedures are well planned and documented, including test set-ups and outcomes.

4. **Change Control**: SciNote employs change control to ensure that any modification of the data is well documented. It provides system **generated time stamped audit trails** to independently record the date and time of each user's entries and actions. The audit trails cannot be edited or deleted.

5. **Support Mechanism:** the system performance is regularly monitored by software tests and overall performance assessment to ensure fully functional performance, reliability and responsiveness. In addition, SciNote provides personalized user onboarding and high-quality technical support for the users.

6. **Archive:** SciNote enables archiving of the electronic data, keeping the original data structure and indexing. Strict access and permission control is applied also for the archived data. Any archived entity can be quickly retrieved by users with defined permissions.

Data Protection White Paper
To read more about SciNote's data protection measures, get your PDF white paper here.

Choose your SciNote plan or schedule your demo & Q&A session with a SciNote specialist here.