EGNYTE

GxP and 21 CFR Part 11 Compliance

Good practices and acceptance criteria

GxP

The GxP refers to the Good x Practices which are a set of regulations and guidelines established by the U.S. Food and Drug Administration (FDA) for addressing the quality and manufacturing of anything FDA regulated. The 'x' stands for particular fields like: Laboratory, Clinical, Manufacturing, and others.

Many regulated companies utilize a GxP system, which typically consists of various processes designed for the purpose of GxP compliance.

Egnyte helps organizations maintain GxP compliance in the cloud and on premises. We provide a platform for life sciences and pharma companies to collaborate, manage and distribute information to their employees and partners, backed by enterprise-grade security and compliance. We simply manage GxP files to meet compliance requirements.

The organizations using Egnyte in GxP systems have the following responsibilities:

- **Management responsibility:** Customers are responsible for how they create and maintain their Egnyte account. Management with executive responsibility within the customer organization should define and communicate an Egnyte account governance policy to ensure that their account(s) used in GxP Systems are tracked and that root account credentials are controlled by qualified individuals who are authorized by the organization. Additionally, a robust password policy should be applied to the Egnyte account.

- **Personnel:** Customers are responsible for ensuring their personnel have proper education, training, and experience to perform their assigned job functions. Egnyte provides training and support for administrators and users in the Egnyte University.

- **Audits:** Content management platforms need to be auditable for GxP system compliance. In order to conduct effective audits, IT auditors should become familiar with the comprehensive audit features within Egnyte.

  Egnyte enables customers to create scheduled audit reports, like:

  1. File audit reports
  2. Permissions audit reports
  3. Login audit reports
  4. User audit reports
  5. Group audit reports

- **Records and logs:** For each GxP system, life sciences organizations are required to identify the retainable records and logs needed as GxP evidence and to maintain the integrity and availability of the records throughout their retention period. When using Egnyte in GxP Systems, the retainable records primarily consist of the customer data within their GxP System, and the system-generated logs and audit trails available within the customer's Egnyte account. This helps to improve data integrity from a GxP data perspective.

  Since the record types and formats associated with automated IT processes are quite different from manually-generated records, GxP customers should make sure to identify the record types and formats they need to retain and to develop their recordkeeping guidelines appropriately.

  Regulatory: Customers may be required to provide information about how the GxP system secures personal information. Customers using Egnyte in GxP systems with files that contain PII should make sure to understand the data residency/sovereignty requirements and, if necessary, describe the security and data locality controls implemented by Egnyte.

  Egnyte enables customers to find and secure all PII and PHI data within the cloud and on-premises repositories being managed by Egnyte. In addition, we enable companies to meet the legal or regulatory requirements imposed on data based on the country or region in which it resides.

While life sciences and pharma companies are benefiting from the use of digital document management as part of their GxP regulated process, they must also comply with the regulatory requirements of the US 21 CFR, Part 11 federal regulation if using electronic records and e-signatures in place of paper-and-ink-based records to comply with FDA rules.

21 CFR Part 11

21 CFR Part 11 defines the criteria for acceptance of electronic documentation and signature submissions to the FDA. This law details FDA regulations for electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper.[1]

Egnyte helps life sciences organizations using electronic signatures meet the following key components:

1. Protection of Electronic records (Subpart b)

2. Electronic signature management (Subpart c)

1. Protection of electronic records

Subpart b – Electronic records

What the regulation requires: Controls for closed systems[2]

The regulation requires that persons who use closed systems (systems controlled by individuals responsible for the electronic content) to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and confidentiality of electronic records, and to ensure the signer cannot readily repudiate the signed record as not genuine. Their procedures and controls should include the following:

Section 11.10(a)

Validation of systems to ensure accuracy, reliability, consistent performance, and the ability to discern invalid or altered records.

How Egnyte Complies	Customer responsibility
Egnyte has achieved SOC 2 Type 2 certification, ensuring that we securely manage customer data to protect the interests of the organization and its privacy. Egnyte is also ISO 27001 certified which ensures that we can enable control over change management, access controls, monitoring, logging, audit trails, encryption and all of the technical controls we have implemented in production. These controls are continuously monitored by production security staff, audited internally in our annual internal audit and also annually by the British Standards Institution (BSI). We also conduct monthly operational reviews for access, scans and other activities to maintain control effectiveness.	The organization using Egnyte is responsible for: • Validating computerized systems used to support regulated activities • Defining the process governing changes to the account configuration and the controlled operation of the system • The initial assessment and periodic re-evaluation of Egnyte's ability to comply with accepted standard best practices regarding system development lifecycle activities, backup management, and system monitoring. This assessment may consist of a periodic review of available third-party reports and certifications (e.g. SOC 2, ISO 27001).

Section 11.10(b)

The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

How Egnyte Complies	Customer responsibility
Egnyte customers can use an Egnyte eSignature partner to apply electronic signatures to a document. The sender and signers can access the signed record via a hyperlink. Egnyte customers have complete visibility and control over all their files and records. All documents can be made available in PDF format and can be viewed with a PDF viewer.	The organization using Egnyte as part of a GxP regulated process is responsible for: • Defining the process for retaining signed records using Egnyte, including provisions to verify that signed documents are validated via the eSignature partner.

Section 11.10(c)

Protection of records to enable their accurate and ready retrieval throughout the records retention period.

How Egnyte Complies	Customer responsibility
All documents managed by Egnyte are encrypted and securely maintained. Egnyte customers have complete visibility and control over all their files and records. Egnyte has achieved SOC 2 Type 2 certification, ensuring that we securely manage customer data to protect the interests of the organization and its privacy. Within Egnyte, customers can set retention policies and access the files as required. Audit trails of all file activity are generated, so customers can monitor the complete history all files during the retention period.	The organization using Egnyte as part of a GxP regulated process is responsible for: • Defining the process for generating backups of records and their audit trials.

Section 11.10(d)

Limiting system access to authorized individuals.

How Egnyte Complies	Customer responsibility
Egnyte allows users with administrative privileges to monitor and control who has access to what content. Only administrators can access and manage the configuration settings area of the system. Compliance is implemented through ISO 27001 controls specific to unique IDs for users, password policy, key management and encryption key lifecycle controls.	The organization using Egnyte as part of a GxP regulated process is responsible for: • Configuring the system in a manner that enforces user authentication to restrict system access.

2. Electronic signature management

Subpart c – Electronic signatures

What the regulation requires: Electronic signature components and controls[3]

Sections 11.200(a)(1)(i), 11.200(a)(1)(ii), 11.200(a)(2), 11.200(a)(3)

a. Electronic signatures that are not based upon biometrics shall:

1. Employ at least two distinct identification components such as an identification code and password
   i. When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.
   ii. When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.
2. Be used only by their genuine owners; and
3. Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

How Egnyte Complies	Customer responsibility
Egnyte has achieved SOC 2 Type 2 certification, and ensures that all documents, data and personal information are protected. Egnyte also has partnerships / integrations with eSignature vendors that are compliant with industry best practices for security and privacy in accordance with SOC 2 Type 2 reporting. The administrator can configure the eSignature solution to require the signer to login with valid credentials containing two or more components, e.g. email address and password; or personal ID number and one-time password. These solutions can also be configured to require signers to provide the same type of valid credentials at the time of signing regardless of the number of signings performed during a continuous period of controlled system access.	The organization using Egnyte as part of a GxP regulated process is responsible for: • Configuring the eSignature solution such that it enforces the use of an identity verification method that employs at least two distinct identification components at the time of signing.

What the regulation requires: Controls for identification codes /passwords[3]

Sections 11.300(a) - 11.300(e

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

a. Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

b. Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

c. Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

d. Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

e. Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

How Egnyte Complies	Customer responsibility
Egnyte has partnerships / integrations with eSignature vendors that are compliant with 21 CFR Part 11. All of these eSignature vendors can be configured to require signers to login using valid credentials before accessing the document for signature. The system can also be configured to require signers to provide valid credentials at the time of signing. Egnyte has achieved SOC 2 Type 2 certification, and ensures that all documents, data and personal information are protected. Compliance is implemented through ISO 27001 controls specific to unique IDs for users, password policy, key management and encryption key lifecycle controls. **How Egnyte complies with controls listed in (a)–(e) above:** a. Because the identifier is the username/email, its not possible for multiple users to have the same identifier and password since their usernames would be different b. Egnyte IT admin can enable password expiration c. It is the customer's responsibility to issue any physical tokens or cards. Egnyte doesn't issue any physical tokens or cards. d. Egnyte enables account lockout with notifications as well as full audits of invalid login attempts e. Egnyte does not have physical tokens nor do we store passwords. This again is the responsibility of the customer.	The organization using Egnyte as part of a GxP regulated process is responsible for: • Initial assessment and periodic reevaluation of service providers to ensure adequate testing processes are followed with regards to password management • Defining the process for user access management including : i. Clear criteria for who can be added to the system as a signer ii. Provisions to force password reset or to revoke access when user credentials have been compromised iii. Specifying the maximum number of incorrect password attempts permitted before a user's account is locked

Conclusion

21 CFR Part 11 compliance is the responsibility of the company (our customers), though as described above, Egnyte provides tools for supporting such compliance efforts. With Egnyte, pharma and life sciences companies can securely collaborate on, manage and distribute regulated laboratory, clinical, and manufacturing content on a single content repository that meets regulatory and compliance standards.

Go here for setup details: https://helpdesk.egnyte.com/hc/en-us/articles/115000779692