Polarion Software®

Medical Device Solution

Polarion Customers Achieve
FDA CFR 21 Part 11 Compliance

Europe, Middle-East, Africa: Polarion Software GmbH
Lautlinger Weg 3 — 70567 Stuttgart, GERMANY
Tel +49 711 489 9969 - 0
Fax +49 711 489 9969 - 20
www.polarion.com - info@polarion.com

Americas & Asia-Pacific: Polarion Software, Inc.
406 Tideway Dr. Alameda, CA 94501, USA
Tel +1 877 572 4005 (Toll free) or +1 510 995 8955
Fax +1 510 814 9983
www.polarion.com - info@polarion.com

Overview

The US Food and Drug Administration (FDA) is similar to many organizations embracing software to automate while forced to maintain legacy processes. **FDA ruling 21 CFR Part 11** specifies how electronic records and electronic signatures can be used as a substitute for paper records and handwritten signatures. It is directly applicable to Polarion customers involved with developing and manufacturing pharmaceuticals, medical devices, and research and testing thereof. Here we describe in detail the most challenging requirements of the FDA regulation and how our customers achieve compliance using Polarion without having to remodel or upset their organization's process, or methods.

According to the FDA, an "electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system." Polarion refers to these electronic records as artifacts. All electronic records/artifacts managed by Polarion are maintained in accordance with FDA published rules and guidelines. Here we narrow the focus of this publication to electronic records which the FDA specifies must have electronic signatures.

Electronic signatures are intended to be binding digital equivalents of handwritten signatures. The FDA states that an "electronic signature is a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature." FDA rules specify that each electronic signature shall be unique to one (1) individual and shall not be reused by, or reassigned to, anyone else. The FDA specifically does not equate an electronic signature with proprietary digital signatures provided by vendors such as VeriSign or Adobe.

The intent of this FDA ruling is to ensure there is clear accountability and an irrefutable record of each and every change made during the lifecycle of an artifact. Polarion customers enjoy the benefits of application lifecycle management (ALM) and understand how electronic records are maintained, tracked, and managed throughout their lifecycle of use, reuse, and derivatives thereof. Polarion website (http://www.polarion.com) detail **ALM and Requirements Management**; here we review how our customers use Polarion to achieve FDA 21 CFR Part 11 compliance.

How to achieve FDA 21 CFR Part 11 compliance with Polarion

1. Security practices that limit access to authorized users and hold them accountable for their actions. Access is limited to authorized users by positively identifying user through a unique user name and password. This information is controlled and centrally managed via secure Polarion license server. **Every single user change is recorded and immutable.**

2. Polarion uses **advanced analytics and reporting** capabilities in the form of template and customized reports to help increase management oversight. Records can only be read or modified by users with security access and permissions established by administrator on project and/or global basis.

3. Configurable and secure workflow reduces cycle time by automating routing and approval and incorporating escalation for overdue tasks. Polarion workflow rules manage change and approval routing per your organization's process, ensuring only those users and/or only those electronic records with clearance, permission, or pre-requisites achieved are able to receive approval to progress. Work items or electronic records collaboration move along a pre-defined workflow, from one department to the next. Overdue tasks, bottlenecks, resource issues automatically escalate in real time status project plans and **notifications**.

4. Automatic document **control for revisions** to ensure that only the current version of a standard operating procedure is available Full and immutable **change history** is recorded for each and every electronic record change/approval, with side by side compare, and full search and query for audit report generation.

5. The username and password used at login positively, and undeniably, identifies the user. After login, changes and approvals are **authenticated using electronic signatures**.

6. Accurate traceability maintained for all electronic records, throughout the entire lifecycle, including electronic signatures used for changes and approvals.

7. Polarion's "**import-export round trip**" **with MS Office** is light years beyond all competitors for document control, version management, issue tracking, ease of use and **fast adoption**.

8. Polarion's **management of electronic records** is second to none. Electronic signatures for whatever process, artifacts, work items, or documents you choose are **completely automated**.

9. Polarion uniquely integrates and **manages any electronic record**, document type, or format from CAD through UML to MS Office, regardless of the software used to create them.

10. Polarion is **Web-based** so that it can connect all employees, partners, suppliers involved from virtually anywhere. Polarion provides a **centralized repository** for easy access and **collaboration** by all authorized users. Polarion also provides **off-line clients** at no additional charge!

11. Polarion is **totally open via API and Web Services.** Please check out the POP (http://extensions.polarion.com) site to see examples of how easy it is for Polarion customers to **integrate with any third party application** or create their own **extensions** and **customizations**.

12. Polarion out of the box provides **industry proven processes to get you going fast**. These **templates and modules** may be reused, customized or used as examples to create your own. There is a **powerful template for IEC 62304 compliance** on the POP site (http://extensions.polarion.com).

13. Polarion's award winning Lucene on steroids hybrid search engine is part of all our products. A search window is available throughout the application. All reports may be saved on a project or global basis for others to use.

14. Polarion provides a secure, time-stamped audit trail far exceeding all requirements for IEC 62304 and FDA 21 CFR Part 11 compliance.

The following chart provides a detailed assessment of how Polarion satisfies the electronic signature requirements for FDA 21 CFR Part 11, Subpart C.

11.100 General requirements.

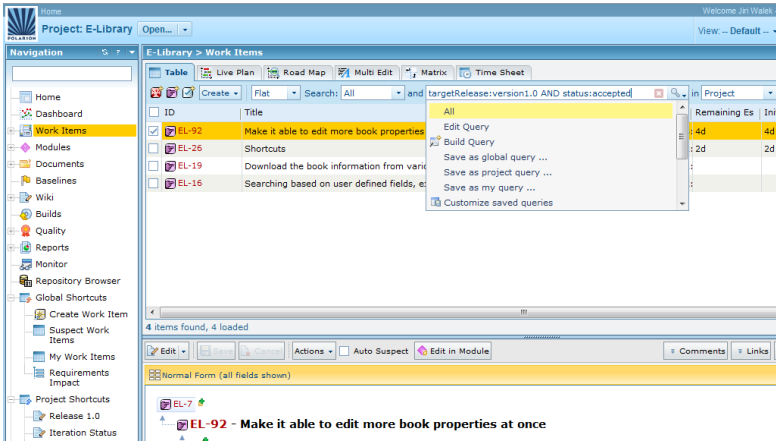|	
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The unique username and password combination required by Polarion ensures the user is authenticated when logging in. All records created by a user are permanently linked to the user and recorded and versioned by Polarion. The Administrator can configure the system so that passwords cannot be reused. Many customers also integrate Polarion with their LDAP/Active Directory.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	The customer is responsible for this requirement, not Polarion.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	The customer is responsible for this requirement, not Polarion.
(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.	The customer is responsible for this requirement, not Polarion.
(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.	The customer is responsible for this requirement, not Polarion.

11.200 Electronic signature components and controls.

(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.	Polarion requires the user name and password combination to uniquely identify the user logging into the system. Privileges and access to actions are controlled by the security settings applied to the user. The security settings to which the user belongs are determined by an administrator who has appropriate security access to manage such groups.
(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.	Polarion requires the user initiate a continuous period of controlled system access with a username and password combination. Each action that the individual executes within this period creates a historical record that contains information about the action and user. The username and password used at login positively, and undeniably, identifies the user. In subsequent signings, the Administrator can specify whether the password alone is sufficient for electronic signatures or that the username and password are both required.
(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.	Polarion requires the user initiate a continuous period of controlled system access with a username and password combination. Each action that the individual executes within this period creates a historical record that contains information about the action and user.
(2) Be used only by their genuine owners; and	The customer is responsible for this requirement, not Polarion.
(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.	Polarion Administrators can set strong password rules, password can be encrypted, and Polarion may be integrated with LDAP for additional controls and authentication.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	The customer is responsible for this requirement, not Polarion.

11.300 Controls for identification codes/passwords.

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.	Polarion Administrators can set strong password rules, password may be encrypted; no two individuals may have the same combination of user name and password. Polarion may also be integrated with LDAP for additional controls and authentication.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Polarion Administrators can manage and reset user names and passwords. Polarion may also be integrated with LDAP for additional controls and authentication.
(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.	Polarion Administrators can manage and reset user names and passwords. Polarion may also be integrated with LDAP for additional controls and authentication
(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.	Polarion can detect, block, and report unauthorized access attempts. Polarion may also be integrated with LDAP for additional controls and authentication.
(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.	The customer is responsible for this requirement, not Polarion.

visit www.polarion.com/products/medical/ for more information

Customers

Here are a few examples of our customers in the Medical Devices, Biotechnology and Pharmaceuticals sectors:

Partners

These partner companies have contributed their knowledge and expertise in the field of medical device development and standards. They have "done the legwork", so you don´t have to:

Did You Know?

Polarion Software's integrated ALM solutions manage requirements engineering, team collaboration, bug tracking, version control, CMMI compliance, Agile process, and more for many kinds of projects with **over 1,000,000 users world-wide** in broad range of industries.