Preparing for FDA 21 CFR Part 11 and EU GMP Annex 11

A Technical Compliance Guide for Life Sciences

NiceLabel White Paper

www.nicelabel.com/enterprise

Executive Summary

Since the late 1990's, the Food and Drug Administration (FDA) and the European Union (EU) have been developing regulations to protect the public's health. It has been estimated that erroneous medical device procedures and processes have cost billions of dollars and thousands of lives. Product identification standards have been designed to improve health provider processes, patient safety, and overall quality of medical care. The specific components of these federal regulations pertain to validations, audit trails, electronic signatures, copies of records, and record retention.

FDA 21 CFR Part 11 and EU GMP Annex 11 are two sets of rules that the NiceLabel Label Management Solution (LMS) addresses for pharmaceutical and medical device compliance. The Code of Federal Regulations (CFR) for the United States and Good Manufacturing Practice (GMP) for the European Union share the same intent. These stringent regulations are enforced by hefty non-compliance penalties. As a result, life science companies allocate significant resources to comply and mitigate the potential for errors and fines.

The FDA has led the charge throughout the years by being the first to set regulations in an exponentially growing medical market. These regulations focus on electronic methods to ensure proper data retention and validation. By stepping away from legacy paper-based methods which cause error-prone validations, the FDA has moved to using computer technology to ensure safety and security.

This white paper examines the FDA and EU regulatory standards and outlines how NiceLabel's Control Center Enterprise module ensures proper label lifecycle compliance. You will also learn how the NiceLabel LMS integrates the labeling required for life science regulations with customers' existing workflows and business information systems including Oracle, SAP, and other Enterprise Resource Planning (ERP) systems. This paper will provide companies with varying printing and administrative workflows information on the software tools they need to comply with FDA and EU regulations.

Understanding FDA 21 CFR Part 11 and EU GMP Annex 11 Compliance

Title 21 is the part of the Code of Federal Regulations (CFR) that establishes the United States FDA regulations on electronic records and electronic signatures. Part 11, defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable and equivalent to paper records. Part 11 applies to drug manufacturers, medical device manufacturers, biotech companies, biologics developers, contract research organizations and other FDA-regulated industries. It requires that they implement controls, including audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in processing the electronic data that the FDA predicate rules require them to maintain.

Good Manufacturing Practices (GMP) are practices required to conform to the guidelines recommended by agencies that control authorization and licensing for the manufacture and sale of food, drug, and active pharmaceutical products. These guidelines provide the minimum requirements that a pharmaceutical or a food product manufacturer must meet to assure that the products are of high quality and do not pose any risk to the consumer or public. Annex 11 is the European equivalent to the FDA's 21 CFR Part 11 compliance mandating the use of electronic records and signatures.

Many legacy compliance methods involve human intervention and consist of paper-based record keeping, maintaining multiple copies of records, and manual validation of records by multiple employees. These methods can result in costly and potentially life threating errors and oversights. The FDA has addressed these well-known issues through Part 11 of the CFR.

Organizations that are looking to modernize their systems to comply with FDA 21 CFR Part 11 and EU GMP Annex 11 compliance must have an acute understanding of both the processes and technologies required to meet the requirements. Software alone does not ensure compliance. Using software from a vendor with in-depth knowledge of international labeling regulations gives companies peace of mind when faced with a complex compliance initiative.

NiceLabel's Compliance Solutions for Life Sciences

NiceLabel designed its Control Center Enterprise module with user interfaces and functionality to help life science companies achieve compliance. The NiceLabel LMS is a next-generation label lifecycle management solution that allows business users to design, review, approve, and control label data from a modern HTML5 Web application. It provides data validation, time stamps, maintenance of records, and electronic signature capture in accordance with FDA 21 CFR Part 11 requirements and EU GMP practice guidelines.

Electronic Signatures

FDA 21 CFR Part 11 governs the acceptance of electronic records as authentic and electronic signatures as legally binding. Electronic signatures are considered to be a trustworthy, reliable equivalent to paper-based records.

Part 11 applies to all electronic signatures and records that are submitted to the FDA. The NiceLabel Control Center Enterprise module helps organizations meet the requirement by forcing each electronic signature to have a unique user ID and password combination for each user that accesses label designs or printing. User authentication is configured through an administrative interface that controls access to the entire network. Role-based access control (RBAC) allows the administrator to restrict user access to specific software features. Any label can also be password protected for additional access level security.

Audit Trails

21 CFR Part 11 requires any organization governed by the FDA to track their authentic and electronic signatures. Complete traceability is an essential component of FDA and GMP requirements. The printing audit trail requirement refers to the logging of printed activities. The label lifecycle management capabilities of the Control Center Enterprise module enable administrative management of a label design and printing network; providing complete audit protection. Organizations can conduct full FDA audits showing who printed a label, which label was validated for printing, and which printer the job was sent to all while tracking exactly when each step occurred.

Every activity is centrally logged within the NiceLabel LMS. Reports can be generated and the data can be viewed from a secure web browser. Label revisions and approval workflows can also be viewed and tracked within the NiceLabel LMS, providing a full audit trail for label changes.

Revision Control of Electronic Records

The Control Center Enterprise module includes a centralized document storage server that acts like an electronic label catalogue. This has an HTML5 web based user interface and provides the revision control system for all labels, images, and related files. This allows users to manage multiple versions of files, track changes, revert to a previous revision, and restore deleted files.

Each time the label designer accesses a label file, the file must be checked-out to the user. This locks the file. Other users will only be able to access it in read-only mode. When the designer checks-in the file, the new version is created in the document storage server. All previous revisions of the file are still available in the database. A label designer can always access and activate previous label revisions. For each check-in operation, the user can enter additional comments describing the changes made to the label design.

Two-Step File Approval

The NiceLabel Control Center Enterprise module allows users to enable workflows adjacent to the revision control system. Workflows enable another level of quality control in the label printing process.

Label Production Workflow

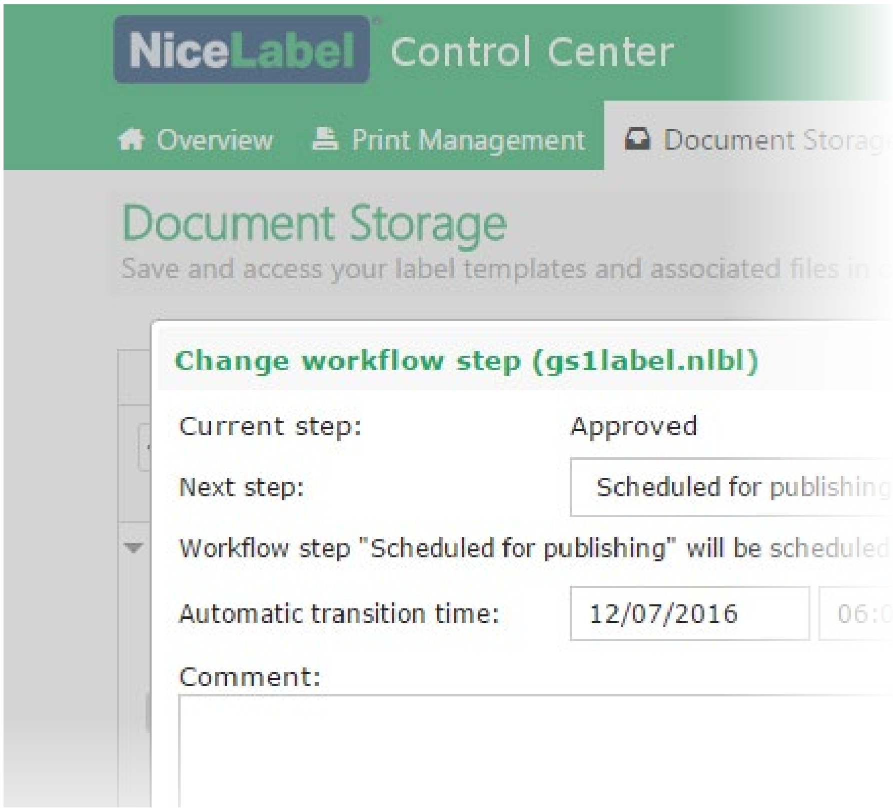
A workflow consists of a sequence of connected steps, which are controlled by the workflow logic. Every step has a start step and a final step. NiceLabel operators will initially enable the multistep approval process.

- Draft • Request approval • Approved • Rejected

The workflow states that before the label is approved for production printing, two independent approvers must review the document and approve it. All users will provide an electronic signature through each step of the approval process.

The Approved step is the final stage for the label file. Labels cannot be used in production until they are approved. NiceLabel users with print-only permission will only see the labels that are in the Approved stage. The label designer can start working on the new revision of the label file, but the file will not be visible to print-only users until the new revision reaches the Approved state.

The Control Center Enterprise module was built for compliance to regulation and GMP, so organizations are well protected when an FDA inspector conducts an official audit.



Document Storage

Save and access your label templates and associated files in

Change workflow step (gs1label.nlbl)

Current step: Approved

Next step: Scheduled for publishing

Workflow step "Scheduled for publishing" will be scheduled

Automatic transition time: 12/07/2016 06:0

Comment:

Figure 1: Label production workflow

Note: Information presented in this document assumes that the appropriate NiceLabel and system policies have been configured for Electronic Record (ER) and Electronic Signature (ES) support.

Overview

Is the system a Closed System, where the system access is controlled by the individuals who are responsible for the content of the electronic records stored in the system?	YES
Is the system an Open System, where the system access is not controlled by the individuals who are responsible for the content of the electronic records that are stored in system (e.g. a service provider controls and maintains access of the contents of the system, etc.)?	NO
Does the system use an ID/ password combination?	YES
Does the system use tokens?	NO
Does the system use biometrics?	NO

The information below will explain how the Control Center Enterprise module addresses specific requirements within in 21 CFR Part 11.

Subpart B – Electronic Records 11.10 Controls for Closed Systems

	REF		Y/N	Explanation
1.	11.10 (a)	Is the system validated?	YES	NiceLabel Control Center Enterprise is structurally validated and includes a Certificate of Software Validation.
2.	11.10 (a)	Does the validation documentation show that Part 11 requirements have been met and are function correctly?	YES	NiceLabel Control Center Enterprise allows users to be compliant with 21 CFR Part 11, but complete compliance can only occur within a validated electronic record environment. Validation documentation is available for examination during an audit.
3.	11.10 (a)	Is the system able to detect invalid records where applicable (e.g. invalid field entries, fields left blank that should contain data, values outside of limits)?	YES	
4.	11.10 (b)	Is it possible to view the entire contents of the records?	YES	
5.	11.10 (b)	Is it possible to print the entire contents of the records?	YES	
6.	11.10 (b)	Is it possible to generate all the records electronically in a format that can be put on portable medium (e.g. floppy disk or CD) or transferred electronically?	YES	

	REF		Y/N	Explanation
7.	11.10 (c)	Are records protected against intentional or accidental modification or deletion?	YES	The ability to modify or delete data within NiceLabel Control Center Enterprise is limited to specifically assigned privileges.
8.	11.10 (c)	Is data archived off the system? If so, is the meta data (including the audit trail) archived as well? Can all the archived data be accurately retrieved after system upgrades?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
9.	11.10 (c)	Are there different levels of access based on user responsibilities (e.g. user, administrator) (if appropriate)? Is this documented and controlled?	Yes	User access is based on the concept of "profiles". A profile defines a specific level of access based on allowed activities/responsibilities. The ability to create, modify or delete profiles are discrete privileges that may be assigned to specific individuals.
10.	11.10 (d)	Are user access levels approved by the management or the system owner before assignment to a user?	YES	User access levels are set and approved during the process of creating a user. Only an individual who has explicitly been given authority to create or alter a user account can change the access level for a particular user.
11.	11.10 (d)	Is there a controlled, documented process for granting access to a new user, for changing privileges for an existing user and for deleting user accounts?	YES	User creation, modification and deletion are controlled through the configuration module, which is only accessible to authorized users.
12.	11.10 (d)	Is there physical security and procedures to protect the server, database and system components from unauthorized access?	NA	Each organization must develop a controlled, documented procedure for managing system security and protection.
13.	11.10 (e)	Is an electronic audit trail function automatically generated for all operator entries?	YES	There are two audit trails in NiceLabel Control Center Enterprise: print log and Document Storage revision history. Both can be configured only by a designated system administrator.
14.	11.10 (e)	Is the audit trail completely excluded from the control and access of users (except for read-only access of the audit trail file)?	YES	NiceLabel Control Center Enterprise data is stored in a database. A designated system administrator may configure audit trail settings.
15.	11.10 (e)	Is it impossible to disable the audit trail function?	YES	The system audit trail can be disabled only by a designated system administrator.
16.	11.10 (e)	Is the system date and time protected from unauthorized change?	NA	The system date and time are obtained from the server. The ability to change the system date and time is a privilege that is controlled through the computer operating system and not through NiceLabel software.
17.	11.10 (e)	When data is changed or deleted, do all the previous values remain electronically available?	YES	All previous values are stored in the database. When the data is changed, new values are added to the database, and previous information is not overwritten or obscured. The privileges to change or delete data may be limited to specific users.

	REF		Y/N	Explanation
18.	11.10 (e)	Is the audit trail data protected from accidental or intentional modification or deletion (read-only access)?	YES	All audit trail data is stored in a central database. Configuration is designed to prevent unauthorized access to the database but it is up to the organization to protect the database from unauthorized access.
19.	11.10 (e)	Are the electronic audit trails maintained and retrievable for at least as long as their respective electronic records?	YES	Audit trails in the NiceLabel Control Center Enterprise Document Storage are maintained for as long as the electronic records (i.e. document storage items). Audit trails in NiceLabel Control Center printing history are maintained as part of database backups. If the database is correctly backed up (this is a responsibility of the organization), database restore will also restore electronic audit trails.
20.	11.10 (e)	Are the electronic audit trails readily available for inspections and audits?	YES	Audit trails are available online in NiceLabel Control Center Enterprise Document Storage and printing history.
21.	11.10 (e)	Can selected portions of the audit trail be viewed and printed by inspectors?	YES	
22.	11.10 (e)	Can selected portions of the audit trail be extracted in a transportable electronic format that can be read by regulatory agencies?	YES	
23.	11.10 (e)	If no audit trail is available, can the system detect that a record was altered since its last approval?	NA	Audit trails of changes to documents in NiceLabel Control Center Enterprise Document Storage are stored in the database. Alteration of documents creates new values that are also stored in the database. Records are not overwritten.
24.	11.10 (e)	Are operator name, date, time, and indication or record (or file) creation, modification or deletion recorded in audit trail?	YES	
25.	11.10 (e)	If the predicate regulation requires it, is the reason for a change included in the audit trail?	YES	
26.	11.10 (f)	If the system requires sequenced steps, does it ensure that the actions are performed in the correct sequence?	YES	NiceLabel Control Center enterprise Document Storage uses workflows that ensure proper sequencing.
27.	11.10 (g)	Does the system ensure that only authorized individuals can use the system?	YES	In order to access NiceLabel Control Center Enterprise, individuals must have a user account associated with the permission profile. Without that, no access to the system is allowed. Permission profile defines capabilities that the user has on the system.
28.	11.10 (g)	Does the system (or procedure) verify that an individual has the authority to electronically sign a record before allowing them to do so?	YES	If an individual is not in the right user profile, he or she is not able to change the workflow step.

	REF		Y/N	Explanation
29.	11.10 (h)	If it is a requirement of the system that data input or instructions can only come from specific input devices (e.g. instruments, terminals); does the system check for the correct device?	NA	NiceLabel Control Center Enterprise designates appropriate input based on user authentication and not device authentication.
30.	11.10 (i)	Is there documentation to show that persons who develop the system have the education, training and experience to perform their assigned tasks (including temporary and contract staff)?	YES	Full documentation is available as part of an audit of the NiceLabel software development process.
31.	11.10 (i)	Is there documentation to show that persons who maintain or use the system have the education, training and experience to perform their assigned tasks (including temporary and contract staff)?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
32.	11.10 (i)	Is there documentation to show that persons who use the system have the education, training and experience to perform their assigned tasks (including temporary and contract staff)?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
33.	11.10 (j)	Is there a written policy in place and enforced that holds individuals fully accountable and responsible for actions initiated under their electronic signatures?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
34.	11.10 (k) (1)	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
35.	11.10 (k) (1)	Is access to "sensitive" systems documentation restricted e.g., network security documentation, system access documentation?		NA
36.	11.10 (k) (2)	Is there a Change Control (or equivalent) SOP governing revisions to system documentation?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.

Subpart B—Electronic Records 11.30 Controls for Open Systems

	REF		Y/N	Explanation
37.	11.30	What controls ensure record authenticity, integrity, and confidentiality?	NA	NiceLabel Control Center Enterprise is a closed system.
38.	11.30	Is data encrypted?	NA	NiceLabel Control Center Enterprise is a closed system.
39.	11.30	Are digital signatures used?	NA	NiceLabel Control Center Enterprise is a closed system.

Subpart B—Electronic Records 11.50 Signature Manifestations

40.	11.50 (a)(1)	Do all electronically signed records contain the following information associated with the signing: Full printed name of the signer	YES	The administrator must configure the user name to include the full name for it to appear on the report.
41.	11.50 (a)(2)	Do all electronically signed records contain the following information associated with the signing: Date and time of signing	YES	
42.	11.50 (a)(3)	Do all electronically signed records contain the following information associated with the signing: Meaning of signature (e.g. review, approval)?	YES	When the two-step approval is used, default meanings include draft, request first approval, request final approval, approved and rejected.
43.	11.50 (a)	Are the date and time stamps applied automatically (vs. being keyed in by the user)?	YES	
44.	11.50 (a)	Are date and time stamps derived in a consistent way in order to be able to reconstruct the sequence of events?	YES	Date and time are obtained in UTC (Coordinated Universal Time) format on the server at the location where the signature was executed.
45.	11.50 (b)	Is the above information subject to the same controls as electronic records (audit trail, access control etc.)?	YES	Date and time stamps cannot be modified by users.
46.	11.50 (b)	Are changes to signatures included in the audit trail?	YES	Signatures may not be altered. New signatures may be added to a record if a workflow in NiceLabel Control Center Enterprise Document Storage is configured in such a way (approval workflow requires more than one approver).
47.	11.50 (b)	Do the printed name, date, time, and signature meaning appear in every human readable form of the electronic record? (e.g. all screens and printed reports)	YES	All screens containing information about changes to a document in NiceLabel Control Center Enterprise Document Storage contain information about a user that caused a change to the document. This information includes name, date and time. There are not printed reports available.

Subpart B—Electronic Records 11.70 Signature/Record Linking

	REF		Y/N	Explanation
48.	11.70	If handwritten signatures are executed to electronic records, are the handwritten signatures linked to the electronic record(s)?	NA	
49.	11.70	If the electronic record is changed, is the signer prompted to re-sign (via either manual procedures (SOP) or technical means)?	YES	Every time a workflow step changes the user is required to re-enter his credentials.
50.	11.70	Are the e-signatures linked (via technology, not procedures) to their corresponding electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?	YES	

Subpart C—Electronic Signatures 11.100 General Requirements

51.	11.100 (a)	Is each e-signature unique to a single individual?	YES	
52.	11. 100 (a)	Are e-signatures ever reused, by or reassigned to, anyone other than the original owner?	NO	
53.	11. 100 (b)	Is the individual identity adequately verified prior to issuance of an electronic signature?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
54.	11. 100 (b)	Is there a procedure for reissuing forgotten passwords that verifies the requestor's identity?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
55.	11. 100 (c) (1)	Has certification of the intent to use electronic signatures been submitted to the agency in paper form with a traditional handwritten signature?	NA	Each organization must submit their written intent for compliance with this requirement.
56.	11.100 (c)(2)	Can additional certification or testimony be supplied to show that an electronic signature is the legally binding equivalent of the signer's handwritten signature?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.

Subpart C—Electronic Signatures 11.200 Electronic Signature Components and Controls

	REF		Y/N	Explanation
57.	11.200 (a)(1)	Is the signature made up of at least two distinct identification components, such as an identification code and password?	YES	A signature comprises of a user name and a password.
58.	11. 200 (a)(1)(i)	If continuous signing sessions are used, are two (or more) e-signature components required for the initial signing?	YES	The user name and password are required for the initial signing.
59.	11. 200 (a)(1)(i)	If only one e-signature component is required for subsequent signings:		
60.	11.200 (a)(1)(i)	If a user leaves the workstation, do procedures and/or automatic controls ensure that it is treated as a non-continuous session?	YES	If NiceLabel Control Center Enterprise is configured to use Forms authentication it automatically ends the signing session after a period of time. If Windows authentication is used, the operating system needs to be configured to allow that—this is the responsibility of an organization running NiceLabel Control Center Enterprise.
61.	11. 200 (a)(1)(ii)	Are two (or more) e-signature components required for each signing during a non-continuous signing session?	YES	The user name and password are required for each signature during a non-continuous signing session.
62.	11.200 (a)(2)	Are non-biometric signatures only used by their genuine owners (e.g. by procedures or training reinforcing that non-biometric e-signatures are not "loaned" to co-workers or supervisors for overrides)?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
63.	11.200 (a)(3)	Are non-biometric signatures administered and executed so that unauthorized use requires the collaboration of two or more individuals?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
64.	11.200 (b)	Are biometric e-signatures designed to ensure that they can be used only by their genuine owners?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.

Subpart C—Electronic Signatures 11.300 Controls for Identification Codes / Passwords

	REF		Y/N	Explanation
65.	11.300 (a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals can have the same combination of identification code and password?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
66.	11. 300 (a)	Are controls (procedural or technical) in place to prevent the re-use of identification codes?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
67.	11. 300 (b)	Is the issuance of identification codes and passwords periodically checked, recalled, or revised (e.g. to cover such events as password aging)?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
68.	11.300 (b)	Do passwords periodically expire and need to be revised?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
69.	11.300 (b)	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
70.	11.300 (c)	Is an SOP in place directing action to be taken to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices used to carry or generate e-signature components?	NA	NiceLabel Control Center Enterprise does not use tokens, cards, or other devices to carry e-signature components.
71.	11.300 (c)	Does this SOP contain procedures for managing and controlling temporary or permanent token/ card replacements?	NA	NiceLabel Control Center Enterprise does not use tokens, cards, or other devices to carry e-signature components.
72.	11.300 (d)	Are any attempts to unauthorized use detected and reported immediately to the system "security unit" (e.g. a system administrator is notified automatically by console message or paper) and, as appropriate, to organizational management?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
73.	11.300 (e)	Are there procedures covering the initial and periodic testing of devices, such as tokens or cards that bear or generate identification code or password information?	NA	NiceLabel Control Center Enterprise does not use tokens, cards, or other devices to carry e-signature components.
74.	11.300 (e)	Does the testing include checks for proper functioning, performance degradation, and possible unauthorized alteration?	NA	NiceLabel Control Center Enterprise does not use tokens, cards, or other devices to carry e-signature components.

Conclusion

The NiceLabel LMS provides life sciences companies with a cost effective label lifecycle management solution to enable compliance.

The NiceLabel LMS allows companies to go beyond barcode label template design to drive enterprise printing networks to mitigate risk, optimize process and improve agility. NiceLabel has invested heavily into documentation and security measures to make the NiceLabel Control Center Enterprise module an ideal solution for FDA 21 CFR Part 11 and GMP Annex 11 regulated companies. NiceLabel's Control Center Enterprise modern web interface has built in risk mitigation capabilities including sleek navigation, customization options and the ability to enforce administrative rules. A complete toolset allows customers to centralize electronic records, maintain proper audit trails, validate with electronic signatures, and restrict access through administrative approvals.

The NiceLabel Professional Services Group (PSG) works with customers to ensure a rapid software implementation that delivers a quick ROI. From implementation to maintenance, the NiceLabel support team provides the final insurance that any issue will be alleviated through web, phone, chat, or on-site support.

Some of the world's leading life sciences companies like Abbott, Pfizer, Baxter, NuVasive, Bio Rad, Cardinal Health, Merck, Roche, B Braun, GSK and many others trust NiceLabel to help them streamline label printing while achieving compliance. To learn how NiceLabel can help you comply with FDA 21 CFR Part 11 and GMP Annex 11 requirements, visit www.nicelabel.com/enterprise.

This technical guide is for general information purposes only and does not contain or constitute legal or other advice. Euro Plus expressly disclaims any and all liability for the statements set forth in this technical guide and any reliance thereon.

Americas
+1 262 784 2456
sales.americas@nicelabel.com

EMEA
+386 4280 5000
sales@nicelabel.com

Germany
+49 6104 68 99 80
sales@nicelabel.de

China
+86 21 6249 0371
sales@nicelabel.cn

www.nicelabel.com