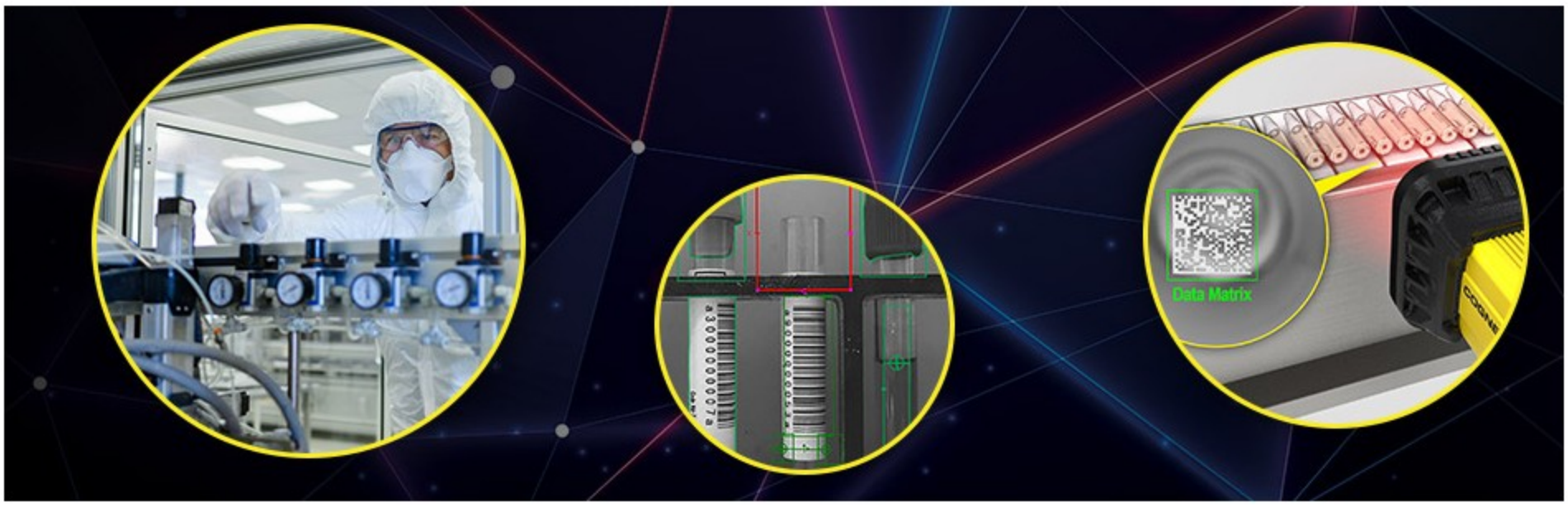
THREE KEY ELEMENTS FOR ENSURING CFR-21 PART 11 COMPLIANCE



In the last post, we covered the basics of 21 CFR Part 11 and the parallel EU Annex 11 as they apply to vision systems, why pharma and medical device manufacturers are often apprehensive about meeting these requirements, and why they really shouldn't be.

To see why not, it's worth looking at a few particular aspects of 21 CFR Part 11 compliance in a bit more detail, with a specific focus on vision systems.

Download 21 CFR Part 11 Whitepaper

Audit trails

While changes to paper records are often detectable, it is possible to manipulate electronic records in ways that are harder to trace. So 21 CFR Part 11 requires that, in a compliant vision system, the record-keeping be set up in such a way that any change to a setting or piece of data creates a timestamped record, a record that can't be changed or erased.

An audit trail is a real-time, sequential log that identifies events or changes by specific user, timestamp, and other identifying information that can be provided to an auditor on request.

A compliant audit trail has several key characteristics:

- Even when a change has been made, any previously recorded information is available for examination. There should be no way to overwrite or delete it. When required, the reason for the change must also be recorded.
- Security ensures that the clock that establishes the timestamps can't be altered. It is recommended that time zone information be clearly documented
- Security ensures that the audit trail can't be edited or deleted by any user.
- The audit trail is retained for as long as the electronic record itself is required to be retained.

These changes can include changes to parameters of barcode readers, labelers, and other equipment. Such an audit trail provides proof of compliance and operational integrity, an example of how regulation and good practice go hand in hand. Automatically linking the audit trail application to a SQL database makes it much easier to maintain these records and retrieve them as needed.

Login credentials

A compliant vision system must have a secure authentication mechanism to prevent unauthorized access. The best solution is a link to the manufacturer's active directory account to verify users and issue the proper certificates. Any user or login changes must be logged and appear in the audit trail.

Different users, such as those allowed to make changes to the application or inspection task, and those who can view the operator panel, should have different default views into the vision system. Passwords need to be changed regularly.

If an unauthorized person does somehow gain access to the system, there must be a method for automatically reporting that breach to whoever is in charge of IT security, and a documented process for handling it.

Validation

A vision system needs to demonstrate that the results it generates are in fact those that it should, by validating against test samples with known results. This ensures that the system operates according to the intended specifications and that it is qualified per 21 CFR Part 11. While vendors can supply a system that meets requirements, it is the responsibility of the customer to validate the system in the user's environment according to their workflow. As in any chain of custody, the information in the record is only as secure as the least secure part of its journey.

Vendors can certainly assist in the validation process, providing documentation and technical assistance for the three phases of validation:

- Installation Qualification (IQ), which tests to ensure that the software has been installed correctly
- Operational Qualification (OQ), which tests to see if the software operates as it should and can meet all regulatory requirements
- Performance Qualification (PQ), which tests whether the system works as it should in the production environment

A manufacturer may choose to bring in a third-party integrator to help with the documentation around IQ and OQ, while the vision system provider provides the features necessary in the software to complete PQ.

Catching up with 21 CFR Part 11

Many production lines know that a review will reveal many inconsistencies with 21 CFR Part 11 requirements. The most common problems are with login credentials. User interfaces on barcode readers and other devices will share group logins, simple passwords, or have no login security at all. Manufacturers fear the difficulty, costs, and time it would take to work with a number of vendors to upgrade these devices, or, if necessary, to replace them with compliant devices.

Fortunately, compliance can be achieved during upgrades, with sophisticated image-based barcode readers, barcode verifiers, or deep learning technology that improve productivity at the same time as they provide the necessary support for compliance.

And, if that is not yet possible, systems integrators such as CXV Global, a Cognex partner, can install its LineDirector product on all lines, providing full, secure control of all production line peripherals from a central access point. This wraps all the devices on each line in compliance, complete with full IQ/OQ/PQ documentation sets that enable the manufacturer to achieve compliance with all user authentication and audit trail requirements of 21 CFR Part 11/Annex 11.

Compliance and operational efficiency go together

In a regulated industry like life sciences, compliance and operations cannot be separated. The audit trail, login credential, and validation requirements are those that any well-run operation would be implementing in their automation system anyway. As manufacturers automate their processes with the help of vision systems, they can improve production and compliance simultaneously.

Download 21 CFR Part 11 Whitepaper

Tags: Medical Devices, Pharmaceutical