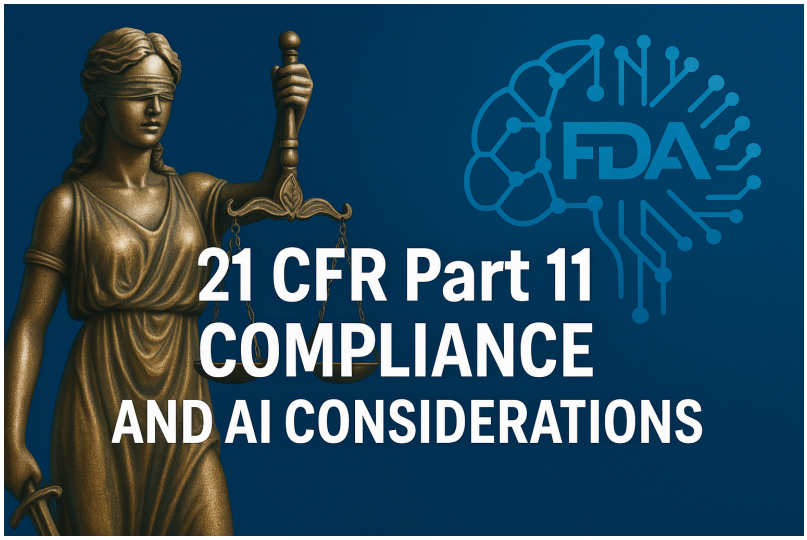
21 CFR Part 11: Electronic Records, Signatures, AI, GxP Compliance

By InuitionLabs.ai • 7/25/2025 • 60 min read

21 cfr part 11 | fda compliance | gxp | electronic records | electronic signatures | artificial intelligence | data integrity | regulatory affairs | quality assurance | system validation



21 CFR Part 11 Compliance in 2025: Electronic Records, Signatures, and AI in GxP

Introduction

In the regulated life sciences industry, **FDA 21 CFR Part 11** remains a cornerstone for ensuring trustworthiness and integrity of digital records and signatures. Enacted in 1997, Part 11 established the criteria under which electronic records and electronic signatures are considered equivalent to paper records and handwritten signatures ecfr.gov linkedin.com. Nearly three decades later, in 2025, this regulation is more relevant than ever as companies embrace cloud computing, Artificial Intelligence (AI), and other digital technologies in Good Practice (GxP) environments. Regulators expect organizations to implement secure, validated, and audit-ready systems to maintain data integrity and product quality dotcompliance.com dotcompliance.com. This report provides an in-depth examination of 21 CFR Part 11's key elements, the latest FDA guidance and enforcement trends, detailed compliance controls, and how emerging technologies – especially AI – should be managed under Part 11. The goal is to equip quality assurance, regulatory, and IT professionals with a comprehensive understanding of Part 11 compliance in today's landscape.

Overview of 21 CFR Part 11 and Scope

21 CFR Part 11 (often just "Part 11") is the FDA regulation that defines how electronic records and electronic signatures can be trusted as much as paper records and ink signatures. Its scope spans all FDA-regulated industries (pharmaceuticals, biotechnology, medical devices, etc.) that choose to use electronic systems to meet record-keeping requirements dotcompliance.com linkedin.com. In essence, **if a record is required by any FDA predicate rule (such as GMP, GLP, GCP regulations) and that record is created, stored, or transmitted electronically, Part 11 applies** ecfr.gov ecfr.gov. This includes records submitted to FDA in electronic form, even if not explicitly called out in other regulations ecfr.gov fda.gov. The regulation was born from the need to ensure that electronic data could be just as accurate, authentic, and reliable as traditional paper records – particularly given how easily digital data can be modified without proper controls linkedin.com linkedin.com. Under Part 11, an electronic record or signature that meets all prescribed requirements is considered equivalent to its paper counterpart ecfr.gov ecfr.gov.

Notably, Part 11 distinguishes **"closed systems"** (where system access is controlled by those responsible for the content) from **"open systems"** (where access is not controlled by the content owners) ecfr.gov ecfr.gov. Closed systems are typical within a company's internal network or validated cloud environment, whereas open systems might involve data exchange over public networks. Part 11 mandates additional measures (like encryption and digital signatures) for open systems to ensure record integrity and confidentiality ecfr.gov. In either case, the overarching goal is the same: electronic records and signatures must be **trustworthy, reliable, and generally equivalent to paper** throughout their entire lifecycle ecfr.gov linkedin.com. The regulation also asserts FDA's inspectional authority over not just the records but also the systems and controls used to manage them (including computer systems, software, and associated documentation) ecfr.gov. In summary, if you generate or maintain GxP records electronically, you must implement Part 11's controls to ensure those records (and electronic sign-offs) are credible and auditable.

Key Requirements of Part 11 (Electronic Records and Signatures)

21 CFR Part 11 lays out a series of **technical and procedural controls** that organizations must have in place for systems handling electronic records. These requirements are designed to preserve record integrity, security, and traceability. The **core elements** of Part 11 compliance include the following:

- ** System Validation:** You must validate any system used to create, modify, or store regulated electronic records to ensure **accuracy, reliability, and consistent intended performance** ecfr.gov dotcompliance.com. In practice, validation means documenting that the software and hardware do what they are intended to do, and can detect any invalid or altered records. This involves defining user requirements, testing the system's functions (under real-world conditions), and maintaining validation status over the system's life. FDA expects validation to be risk-based; higher-risk functions (those impacting product quality or patient safety) should get the most rigorous testing and documentation cooley.com medium.com. Importantly, system validation is not a one-time event – changes (upgrades, patches, configuration updates) must be evaluated and the system re-validated as needed to assure continued compliance dotcompliance.com dotcompliance.com. Effective validation provides confidence that electronic records and signatures are trustworthy from the point of creation onward.

- ** Audit Trails:** Part 11 requires secure, computer-generated, time-stamped **audit trails** to track all changes to electronic records ecfr.gov dotcompliance.com. In other words, the system must automatically record who performed an action, when it occurred (date and time), and what the action was (e.g. creating, modifying, or deleting a record). Critically, audit trails must **preserve prior entries** – no overwriting of old data – so there is a history that can be reviewed to detect improper changes ecfr.gov. Audit trail records should be tightly linked to their corresponding records and retained as long as the records themselves are retained ecfr.gov. They should also be **tamper-evident**, meaning users (even system administrators) cannot alter or erase the audit log without detection dotcompliance.com. During FDA inspections, firms are expected to provide complete audit trail information to reconstruct events in the system's use cooley.com. For example, if a quality control test result is later modified, the audit trail should show the original value, the new value, who changed it, when, and why cooley.com. Robust audit trails are fundamental to data integrity, creating transparency and accountability for electronic recordkeeping.

- **Access Controls and Security:** Only **authorized individuals** may access systems housing GxP electronic records ecfr.gov dotcompliance.com. This means implementing user access controls such as unique user accounts (no shared logins), strict password policies, and role-based permissions. Part 11 calls for **limiting system access** to those who need it, and using **authority checks** to ensure users can only perform functions they are permitted to perform (for instance, only a manager can electronically approve a record) ecfr.gov. System administrators should maintain a current list of authorized users and their permission levels cooley.com. Any changes in user access (e.g. role changes or revoking access) should be documented. Additionally, there should be **device checks** in place to validate the source of data inputs or operational commands when appropriate (for example, ensuring an instrument sending data to the system is recognized and calibrated) ecfr.gov. These security measures, combined with physical and network security controls, protect against unauthorized data access or manipulation. A common compliance gap has been the use of shared login credentials or insufficient permission controls – practices that FDA has repeatedly cited as data integrity risks astrixinc.com. Therefore, strong access management and security policies are essential to Part 11 programs.

- **Electronic Signature Controls:** When using electronic signatures (e-signatures) in lieu of handwritten signatures, Part 11 imposes specific controls to ensure they are uniquely attributable and legally equivalent to a person's sign-off. Each e-signature must be **unique to one individual** (no two people can share the same signature credentials) ecfr.gov. Before an organization allows an electronic signature, it must verify the person's identity and certify to FDA that the e-signatures are intended to be legally binding (often via a **Letter of Non-Repudiation** submitted to the FDA) ecfr.gov cooley.com. Every signed electronic record must contain information that clearly indicates: the printed name of the signer, the date and time of signature, and the meaning of the signature (e.g. approval, review, authorship) ecfr.gov. The system should **link the signature to the record** such that it cannot be removed or copied to another record fraudulently ecfr.gov. Part 11 also specifies signature execution methods: if not using biometrics, signatures should employ at least two distinct identification components (for example, a user ID and password) for the first signing in a session, and at least one component for subsequent signings in that same session ecfr.gov. If the signing session is broken, all components must be re-entered for a new signature ecfr.gov. Biometric signatures (like fingerprint or iris scan) must be designed so they can only be used by the genuine owner ecfr.gov. Furthermore, **password/PIN security policies** must be in place – ensuring uniqueness of combinations, periodic password changes, and safeguarding of password data ecfr.gov ecfr.gov. In practice, many companies implement e-signatures via username/password prompts that also capture the meaning of the signing (often using a comment or predefined options). These e-signatures, properly managed, carry the same legal weight as handwritten signatures in a paper record linkedin.com cooley.com. Firms must also train employees that an electronic signature is legally binding and not to be used by anyone else – misuse or sharing of e-sign credentials can lead to serious compliance violations.

- **Records Retention and Availability:** Electronic records must be maintained in a manner that protects their **integrity and accessibility for the required retention period** ecfr.gov blog.seavision-group.com. Part 11 requires the ability to generate **accurate and complete copies** of records in both human-readable and electronic form for FDA inspection and review ecfr.gov. In practice, this means you should be able to readily retrieve any regulated record and its audit trail and present it to an inspector in a readable format (screen view or printout). Records should be protected against loss or alteration through effective backup systems and archival processes cooley.com. FDA does not differentiate between electronic and paper records regarding retention; if a rule says retain for X years, that applies equally to electronic formats cooley.com. Therefore, companies need robust data backup and disaster recovery procedures, especially if records exist only electronically cooley.com. For example, FDA expects that all data (including **metadata** like timestamps and audit trails) necessary to reconstruct an event or decision are retained and retrievable during an inspection cooley.com. Failure to produce required records on demand – whether due to poor archiving or system issues – can result in citations. In summary, **data integrity** must be preserved not just at the moment of record creation but for as long as the record must be kept, which could be years after its creation. This requires disciplined records management and IT controls (periodic backup verification, migration to new formats as systems become obsolete, etc.) to avoid data loss over time.

- **Operational and Procedural Controls:** Part 11 also emphasizes the **procedural aspect** of controlling electronic records. Firms must have written **Standard Operating Procedures (SOPs)** and policies that ensure individuals are held accountable for actions under their electronic signatures and that describe proper system use ecfr.gov ecfr.gov. There should be **operational system checks** enforcing the correct sequence of steps in a process where appropriate (for example, a workflow system might enforce that approval can only happen after a record is completed) ecfr.gov. **Authority checks** should confirm that only authorized individuals can perform certain critical operations (like a manufacturing operator cannot release a batch record – only a quality unit person can) ecfr.gov. Training is another key element: personnel who develop, maintain, or use the systems must have adequate education and training to perform their tasks and understand Part 11 obligations ecfr.gov linkedin.com. Additionally, **documentation controls** must be in place for system documentation (e.g. manuals, configuration specifications): distribution of these documents should be controlled, and changes to documentation should be tracked with a change history (essentially an audit trail on the documentation) ecfr.gov. This prevents unauthorized or unknown changes to how the system operates. Taken together, these operational controls create a culture and framework that support electronic data integrity: clear procedures, proper training, and accountability that complements the technical controls. Regulators often ask to see policies on electronic signatures usage, SOPs for system administration, and evidence of training during inspections dotcompliance.com astrixinc.com. Lack of appropriate procedures or neglecting to follow them has led to compliance gaps in many companies. Thus, success under Part 11 is not just about software features – it's equally about people and procedures following good documentation practices.

Table: Summary of Key Part 11 Control Requirements

Control Area	Part 11 Expectations (Closed Systems)
Validation	Validate systems to ensure accuracy, reliability, and consistent intended performance; be able to detect invalid/altered records ecfr.gov. Maintain validation with changes. dotcompliance.com
Audit Trail	Secure, time-stamped audit trail of create/modify/delete actions; cannot obscure previous entries; retain audit logs as long as record ecfr.gov. Tamper-proof and reviewable dotcompliance.com.
Access Control	Unique user IDs; limit access to authorized individuals; use authority checks so only permitted users/functions occur ecfr.gov ecfr.gov. Password and security policies to prevent unauthorized use.
Electronic Signature	Unique to each person; identity verified and on file with FDA (non-repudiation letter) ecfr.gov. Captures signer name, date/time, and meaning for each signature ecfr.gov. Linked to record and cannot be excised ecfr.gov. Uses two-factor authentication (or biometrics) for signing ecfr.gov.
Records Retention & Copies	Records (and audit trails) retained per predicate rules; must be easily retrievable and in human-readable form for inspection ecfr.gov. Backup and archive systems to protect records over time cooley.com.
Operational Checks	System enforces correct sequencing of steps/events where appropriate (workflow controls) ecfr.gov.
Training & SOPs	Users/developers must be trained and qualified for their roles ecfr.gov. Written procedures in place for system operation, maintenance, and security; individuals accountable for e-records/e-signatures under their control ecfr.gov.
Documentation	Control over system documentation: distribution, access, and change tracking (document change audit trail) ecfr.gov.

Note: Open systems must implement all above plus additional measures like encryption and digital signatures to ensure data integrity and confidentiality during transmission ecfr.gov.

FDA Guidance and 2025 Updates

Over the years, FDA has supplemented Part 11 with guidance documents and has adjusted its enforcement approach in response to industry challenges and technological advances. **Initially**, after Part 11 came into effect (1997), industry feedback indicated the rule was overly prescriptive and costly to implement. In response, FDA issued a guidance in 2003 ("Part 11, Electronic Records; Electronic Signatures – Scope and Application") that narrowed the scope of Part 11 enforcement cooley.com. The 2003 guidance introduced a **risk-based approach**, stating that FDA would exercise enforcement discretion for certain requirements (like system validation, audit trails, record copies) **except for records that directly fall under predicate rules or are submitted to FDA** cooley.com. Essentially, FDA indicated it would focus on critical records and not insist on Part 11 controls for every electronic system indiscriminately. That guidance also encouraged industry to base the extent of validation on a system's impact on product quality and patient safety – a principle that has only strengthened over time.

Recent Guidance (2017–2024): Recognizing the rapid evolution of technology (cloud computing, mobile health, etc.), FDA began updating its recommendations. In 2017, the Agency released a draft guidance to expand on the risk-based approaches to electronic system validation first outlined in 2003 cooley.com. Then, after the experience of the COVID-19 pandemic (which greatly increased reliance on remote and digital tools in clinical trials), FDA issued a revised draft in 2023 cooley.com. Finally, in **October 2024, FDA published a *final guidance* titled "Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers."** This 2024 guidance (Revision 1) consolidates and updates FDA's current thinking for clinical trial settings, but many principles apply broadly. It contains a Q&A format with 29 questions on topics such as the scope of Part 11, validation, data integrity, service providers, digital health tech, and e-signatures cooley.com cooley.com. Key takeaways from the 2024 guidance include:

- **Scope Clarifications (Real-World Data and Foreign Trials):** FDA clarified that Part 11 compliance is **not required for electronic health records (EHRs) or other real-world data sources** at the point of origin; the Agency "does not intend to assess compliance of an EHR system or other electronic system that is a source of real-world data with Part 11" fda.gov fda.gov. However, **once data from such sources are transferred into a sponsor's clinical trial electronic data capture (EDC) or other system for use in a regulatory submission, Part 11 applies** fda.gov. In other words, the onus of Part 11 starts when external data enters your regulated system. Additionally, Part 11's applicability is global in reach: if a foreign trial not conducted under an IND will be used to support an FDA application, the electronic records from that study **must still comply with Part 11** requirements cooley.com. FDA explicitly states Part 11 covers "any records required to be kept in electronic format" for studies supporting INDs or marketing applications, even if the study is outside the U.S. and not under FDA oversight at the time cooley.com. Sponsors must ensure such data meets integrity standards (and also meet **21 CFR 312.120** for foreign data acceptance cooley.com). These clarifications underscore that data used for FDA decisions – no matter where or how generated – ultimately needs to be Part 11 compliant once it's part of an FDA submission.

- **Data Integrity and Record Retention Expectations:** The FDA's 2024 guidance emphasizes there is **no leniency for electronic data vs. paper when it comes to recordkeeping obligations**. During inspections, firms will be expected to **provide all records and associated data needed to reconstruct the trial or process**, including **metadata** and **audit trails**, whether those records are electronic or paper cooley.com. For example, metadata like timestamps of original data acquisition and any changes made are crucial for reconstructing what happened and must be available cooley.com. If records exist only electronically, you must have adequate backup and recovery procedures in place to prevent loss cooley.com. This reflects FDA's broader focus on **data integrity**: regulators have repeatedly flagged issues where companies could not produce complete data or where audit trails revealed unreported changes. In fact, between 2014 and 2018, around **50% of FDA drug manufacturing inspection 483s cited data integrity problems**, and **79% of warning letters** in that period included data integrity deficiencies astrixinc.com astrixinc.com. Common findings include uncontrolled deletion or modification of electronic data, failure to review audit trails, and lack of backups astrixinc.com astrixinc.com. Rather than citing "21 CFR 11" directly, investigators often cite predicate rules like 21 CFR 211.68 (requiring backup and controls for electronic equipment) or 211.194 (complete data in lab records) when Part 11-type controls are lacking astrixinc.com. The takeaway is that **FDA expects complete, accurate, and tamper-proof records**, and they will enforce these expectations under any applicable rule. Companies should therefore treat audit trails and data retention as non-negotiable, routinely auditing their own systems to ensure compliance.

- **System Validation and Documentation:** The 2024 FDA Q&A guidance reiterates that **electronic systems should be validated before use in a clinical investigation** (or any regulated activity) cooley.com. Sponsors and investigators are expected to document the **system features and requirements** and be prepared to provide FDA with evidence of validation, staff training, and standard operating procedures that govern system use cooley.com. Specifically, during inspections FDA may ask for documentation of: what systems were used to create/manage records for a given trial, the intended system requirements or functionality, proof that those systems were tested and perform as intended (validation reports), records of personnel training on those systems, and SOPs or controls in place for things like user access, data entry, data modifications, backups, and contingency plans cooley.com cooley.com. This aligns with long-standing expectations – a system isn't just the software, but also the procedures and people around it. If a company uses a vendor or contract IT service for the system, the **regulated company remains responsible** for compliance and should have oversight of the vendor's activities cooley.com. Regulators have indicated that outsourcing does not absolve a sponsor or manufacturer from ensuring Part 11 requirements are met cooley.com. In summary, firms should maintain a **validation package** and usage documentation for every GxP-critical system and be "inspection-ready" to show those on request.

- **Security, Access, and Audit Trail Controls:** In line with Part 11 rules, the FDA guidance stresses implementing **safeguards** like limiting system access to authorized users, and maintaining a list of all individuals with access (and documenting changes to their permissions) cooley.com. Audit trails should capture user access and actions in the system, with **each record change showing date/time, who made the change, and the reason** for the change cooley.com. The inclusion of a "reason for change" is a notable point – while Part 11's text does not explicitly demand capturing the reason, in practice FDA expects Good Documentation Practices such as requiring users to enter a justification when modifying critical data. Modern systems often enforce a comment for significant changes, or link the change to a corrective action record if needed. The guidance also implies that simply having audit trail functionality is not enough; **procedures must exist to review audit trails and ensure they are not being manipulated** cooley.com. In fact, a number of FDA warning letters have cited firms for not reviewing audit trail data or for staff having abilities to turn off or alter audit trail logs astrixinc.com astrixinc.com. Thus, companies should establish routine audit trail review as part of their quality system (especially for critical data like manufacturing batch records or clinical data changes).

- **Digital Health Technologies (DHT) and Remote Data:** FDA acknowledges the growth of digital health tools (wearables, mobile apps, remote monitoring devices) in trials and manufacturing. The 2024 guidance provides specific recommendations for ensuring data from DHTs remains Part 11 compliant cooley.com cooley.com. Each data point collected via a DHT should be attributable to a **"data originator"** – meaning the system should record who or what generated the data (it could be a person, device, or instrument) cooley.com. Sponsors should maintain a list of authorized data originators (for example, a list of all devices or users that are permitted to transmit data into the system) and supply that to FDA if requested cooley.com. Data from DHTs must be **secure from unauthorized manipulation**: the devices or apps should be designed so that participants or others cannot alter the raw data (e.g. a wearable should prevent editing of its stored readings) cooley.com. Participants need to be trained on proper use of these technologies, and that training documented cooley.com. When transferring data from a DHT into the central electronic record repository (such as uploading from a wearable to the sponsor's database), the transfer process must be **validated and include an audit trail** recording the time/date of transfer cooley.com. Essentially, the chain-of-custody of data from its point of capture to the official electronic record must be secure and traceable. These principles apply equally in manufacturing: if using IIoT (Industrial Internet of Things) sensors or other automated data capture, one should ensure the data pipelines are validated and tamper-proof. The guidance demonstrates FDA's expectation that even cutting-edge digital tools adhere to classic data integrity principles: attributable, legible, contemporaneous, original, accurate (ALCOA), plus metadata capture and traceability (often called ALCOA+).

- **Electronic Signatures Best Practices:** The FDA Q&A also revisits e-signatures, echoing the regulation's requirements. The **elements of an e-signature** (signer name, timestamp, and meaning) must be present and linked to the record cooley.com. FDA does not mandate any specific technology for signatures – **various methods** such as user ID/password, biometric scans, digital certificates, or other secure tokens are acceptable, so long as they meet the requirements of uniqueness and security cooley.com. The guidance reminds firms that each e-signature user must send FDA a certification of their intent (the letter stating that their electronic signature is the legally binding equivalent of their handwritten signature) cooley.com. This letter is often submitted as part of initial Part 11 implementation or when a new system comes online, and typically it's a one-time submission per user or per company listing all users. In current practice, many companies have a procedure to send a "Letter of Nonrepudiation" to FDA's designated address or email when they implement a Part 11 system; the guidance references that requirement to ensure it's not overlooked cooley.com. FDA's flexibility on e-sign methods means companies can take advantage of new authentication technologies, but any method chosen must be documented and proven to fulfill Part 11's intent (e.g. if using fingerprint readers, ensure they truly distinguish unique individuals and cannot be fooled).

Overall, **FDA's 2024 guidance reinforces that Part 11's core principles still apply, even as technology evolves**. It encourages a risk-based approach (focus on what matters for data integrity) and provides clarity on newer use cases like real-world evidence and remote data collection. Notably, the guidance team explicitly *avoided* expanding into certain hot topics – one being **artificial intelligence**, which we will address shortly. It's clear that **compliance enforcement** remains vigorous: FDA inspectors are keen on data integrity issues, whether under Part 11 or parallel regulations. Companies continue to receive observations for failures like unvalidated spreadsheets, uncontrolled user access in lab systems, or missing audit trails – issues fundamentally tied to Part 11 requirements. In fact, FDA has often called Part 11 *"the data integrity rule,"* and while inspectors rarely cite Part 11 by number, they expect firms to implement those controls as part of GMP/GCP compliance astrixinc.com. A firm that "goes paperless" without robust controls is at high risk of regulatory action. The trend in 2025 is that **hybrid systems** (mix of electronic and paper processes) are also under scrutiny, as gaps often occur when data moves between manual and electronic systems dotcompliance.com dotcompliance.com. FDA has made it clear that if any part of your record management lacks validation, security, or traceability, it's a compliance liability dotcompliance.com dotcompliance.com. Therefore, organizations should continuously assess their systems against Part 11 standards, even as they adopt innovations.

Upcoming/Proposed Changes: While Part 11's text has remained mostly unchanged (aside from minor updates, e.g. in 2023 FDA amended the rule to allow electronic submission of signature certification letters ecfr.gov ecfr.gov), the Agency is modernizing its guidance on software validation. A significant development is FDA's **Computer Software Assurance (CSA)** initiative. CSA is a risk-based validation paradigm that emerged from the medical device quality system regulation but is influencing pharma and biotech as well. The FDA issued a draft guidance on CSA in September 2022, aiming to replace the traditional CSV (Computer System Validation) approach with a streamlined, critical thinking-driven process medium.com. Under CSA, validation efforts are scaled to the risk a software poses to quality; for high-risk functions,

rigorous scripted testing is still expected, whereas low-risk tools can be qualified with supplier documentation and unscripted testing medium.com medium.com. The draft guidance is expected to be finalized by late 2025 (it's on FDA's "B-list" agenda for FY 2025) medium.com medium.com. Inspectors have already signaled expectations aligned with CSA – for example, focusing on whether companies have justification for what they test and not just voluminous paperwork medium.com. CSA doesn't negate Part 11; in fact, it complements it by encouraging manufacturers to **prioritize validation on systems that impact product and patient safety and to leverage automation and vendor qualifications where possible** medium.com medium.com. Firms adopting CSA still must ensure their systems meet Part 11 (one CSA "pitfall" noted is forgetting to enable audit trail or e-sign functions in new software medium.com). The benefit is a more efficient compliance process that can keep up with rapid software changes (which is especially relevant for AI-driven systems or continuous cloud deployments). As of 2025, many companies are piloting CSA approaches in anticipation of FDA's final guidance. Quality units and IT should stay tuned to these developments, as they represent FDA's evolving stance on how best to ensure software reliability *and* encourage innovation.

Implementation Guidance and Controls for Compliance

Achieving and maintaining 21 CFR Part 11 compliance requires a comprehensive approach that blends technology controls, quality system procedures, and a culture of data integrity. Below are detailed implementation guidelines and best practices, aligned with Part 11 requirements, that organizations should consider:

1. Establish a Risk-Based Compliance Plan: Not all systems and records carry equal weight for patient safety or product quality, so begin by **inventorying your systems and classifying their risk**. Identify which electronic records are GxP-critical (e.g. batch production records, analytical data, clinical trial data) and which systems create or manage those records. Conduct a **risk assessment** for each: ask how a failure or data integrity issue in the system would impact product quality, trial subject safety, or regulatory decisions medium.com medium.com. This will help prioritize resources. High-risk systems (for example, an electronic batch record system controlling manufacturing steps) demand very stringent controls and validation, whereas a lower-risk system (perhaps a training records database) might be managed with a lighter touch (still compliant, but not over-engineered). FDA's ethos – reinforced by guidance and CSA – is to use *critical thinking* and focus on controlling meaningful risks rather than blindly applying the same level of effort to every application cooley.com medium.com. As part of planning, ensure that you have management support and cross-functional involvement (IT, QA, operations, etc.), since Part 11 compliance is not solely an IT issue but an organizational responsibility.

2. Develop and Document SOPs Covering Part 11 Controls: A robust set of Standard Operating Procedures is fundamental. Specific procedures should cover at minimum: **System Validation Lifecycle** (how you validate new systems and maintain validation through changes), **User Account Management** (how accounts are created, modified, deleted; password policies;

periodic review of access lists), **Electronic Signature Use** (rules for when e-signatures are required, how users sign, how meaning of signature is indicated, and the process for issuing/withdrawing electronic signature credentials including the FDA certification letter), **Data Backup and Recovery**, **Change Control** for configurations and system updates, **Audit Trail Review**, and **Incident/Deviation Handling** for system issues. Each procedure should assign responsibilities (e.g. IT manages user accounts but QA reviews and approves access for GMP systems; QA reviews audit trails for critical changes monthly; etc.). Regulators will often ask to see these SOPs to verify that procedural controls exist on paper – and then look for evidence they are being followed. Make sure the SOPs also address Part 11's **policy-level requirements**, such as holding individuals accountable for actions initiated under their electronic signatures ecfr.gov. For instance, companies often have employees sign an agreement (or include in training) that they will not share passwords and understand the legal significance of their electronic signature. This can be referenced in the SOP and captured in training records.

3. Implement Technical Controls in Systems Configuration: When configuring or selecting software for GxP use, ensure it has the technical capability to meet Part 11. Key features include: **Audit Trail functionality** – the system should automatically log create/edit/delete actions with user ID, timestamp, and ideally the reason for change (either prompted or via linked change forms). Make sure the audit trail cannot be disabled or altered by end-users; if the software allows turning off the audit trail, that function should be administratively controlled and never used in production. **Security and Permissions** – set up unique user accounts (no generic logins) and assign roles with the principle of least privilege (users only get access to what they need). For example, analysts can enter data but not delete it; only supervisors can electronically sign approval; admin rights are restricted to IT or QA personnel not involved in record content. Ensure **password policies** are enforced (e.g. minimum length, complexity, expiration, lockout on repeated failures) ecfr.gov. Many enterprise systems allow configuration of password rules and account lockout settings – align these with both Part 11 and your IT security policies. **Electronic Signatures** – configure the system so that any electronic signature applied will automatically record the signer's name, date/time, and a statement of meaning. Often this means setting up signature roles (like "Approved By" or "Verified By") in forms, so that when a user signs, the role (meaning) is attached. If using biometrics or single-sign-on tokens, ensure they comply with uniqueness and security requirements ecfr.gov ecfr.gov. Additionally, link the e-signatures firmly to the records (for instance, once signed, the record should show signature details and not allow the content to be changed without invalidating or creating a new signature). **Record protection** – verify that records, once saved, cannot be accidentally modified or deleted without triggering the proper audit trail. Where applicable, enable features like check-sums or PDF locks for exported reports to detect any tampering. Lastly, ensure the system can **produce copies of records** in human-readable form easily (this might involve generating PDF reports or providing read-only inspection accounts). Testing these configurations should be part of your validation.

4. Perform Thorough Computer System Validation (CSV) / Assurance Activities: Based on the risk and complexity of the system, create a validation plan that outlines what needs to be tested and documented to establish fitness for use. High-risk, custom, or bespoke systems will

need a full validation effort: user requirements documented, functional specifications, test protocols (IQ/OQ/PQ or similar) with traceability to requirements, and a validation summary report. For lower-risk or standardized systems (like a well-known commercial software), a streamlined approach might be justified, leveraging vendor documentation and focusing testing on your specific use configuration (this aligns with the emerging CSA guidance) medium.com medium.com. In all cases, **document everything**: FDA may not explicitly require seeing all validation documents, but if there's ever an issue or an audit, robust documentation is your evidence that the system was properly verified. Include challenge tests for key Part 11 functions (e.g., verify that an audit trail entry is created when data is changed; verify that only authorized roles can perform certain actions; simulate an unauthorized login attempt to see if the account locks). Also test **data integrity scenarios**: e.g., if the system time is changed or communication to an instrument is lost, what happens? Ensure backup/restore is tested (retrieving data from backups). Once in production, maintain a **change control process**: any updates or patches should be assessed for impact on Part 11 functionality and validated accordingly before fully implemented. Remember, maintaining the validated state is a continuous process, not a one-time checkbox dotcompliance.com medium.com. FDA's inspectors have cited firms for "inadequate software validation" when changes were made without due re-testing medium.com.

5. Ensure Data Integrity in Practice (Routine Reviews and Monitoring): Having the technical capability for audit trails and security is necessary but not sufficient. **Routine monitoring and review** of system records is crucial. For example, establish a schedule for QA or a data integrity team to review a sample of audit trail records for critical systems on a periodic basis (e.g. weekly or monthly depending on usage). Look for any unusual patterns, such as frequent data modifications or attempts to access functionalities beyond a user's role. FDA has explicitly recommended independent audits of data integrity; some warning letters even "strongly recommend" hiring a third-party to evaluate data practices astrixinc.com. Whether internal or external, conducting periodic **data integrity audits** can catch issues like users sharing accounts, or incomplete metadata capture. Another best practice is to implement **system alerts** for certain events – e.g. if an audit trail shows someone disabled an audit logging (if the software permits it) or if there's an unusual spike in data changes at odd hours. Modern systems or overlay tools can send such alerts to management for investigation. **Review of electronic signatures** can be part of batch or study record review: ensure that all required signatures are present and valid, and that timestamps make sense chronologically. By actively monitoring, a company demonstrates control over the electronic system. In case of any deviations (like an audit trail review finds an unauthorized change), investigate under the quality system (similar to how you'd investigate a lab OOS or a manufacturing deviation) and take corrective action, including retraining or procedural fixes as needed. This approach closes the loop on Part 11 compliance, proving that it's an active program.

6. Vendor Management and Cloud Considerations: Many companies use cloud-based software or external IT service providers for hosting GxP systems. Part 11 compliance in such cases demands careful delineation of responsibilities. If using a **Software-as-a-Service (SaaS)** provider or cloud host, ensure that the provider's infrastructure meets high security standards

(look for certifications like ISO 27001, SOC 2, etc., which FDA also views favorably compliancequest.com compliancequest.com). Establish in writing who is responsible for what: for instance, you might handle user administration and validation of your processes, while the vendor manages server maintenance and backup – but you need to confirm the vendor's procedures (like how they back up data, how they restrict their own staff's access) also support compliance. **Audit your vendors** or review their third-party audit reports. Cloud does not remove your accountability: FDA can and will hold the company accountable for Part 11 even if a contractor was involved cooley.com. It's wise to have quality agreements in place with any third-party detailing compliance requirements (e.g. the vendor will not make changes to the system without notification, will allow you to retrieve all your data, etc.). On the technical side, cloud-based systems might offer **built-in compliance features** – use them. For example, many cloud eQMS or LIMS platforms have modules for electronic signature and audit trails, but they may need to be configured or turned on. After deployment, maintain evidence like **access logs from the cloud** and **configuration settings** as part of your validation package. If the cloud environment is dynamic (auto-scaling servers, frequent updates), consider the guidance from CSA: adopt continuous validation techniques, automated testing, and close supplier coordination to ensure changes don't inadvertently break compliance compliancequest.com compliancequest.com. The bottom line is, whether on-premises or cloud, the same Part 11 principles apply – data must be secure and controlled. Companies just need to adapt their approaches to the cloud's shared responsibility model.

7. Training and Culture: Human factors remain one of the biggest risk areas. All users of Part 11 systems should receive initial and periodic **training on proper use of electronic systems and on data integrity expectations**. Training should cover practical instructions (how to log in, how to sign records, what not to do – e.g. don't share passwords, don't leave a terminal unlocked) as well as the regulatory importance (why these rules exist, the potential consequences of non-compliance). People are more likely to comply if they understand the "why" and not just the "how." Establish a culture where data integrity issues can be raised without fear – for example, if someone discovers an audit trail was accidentally turned off or a record went missing, they should report it immediately so that it can be fixed and investigated, rather than feeling pressure to hide it. Management should periodically communicate the importance of accurate electronic record-keeping and that **data integrity is part of everyone's job**. This cultural aspect is often what separates companies that consistently comply from those that run into issues. FDA inspectors often interview personnel to gauge their understanding of procedures and their attitude toward electronic record controls. Confident, knowledgeable staff who take ownership of data integrity make a strong positive impression; conversely, if an operator seems unaware of how their actions are logged or a supervisor doesn't know they should review audit trails, it raises red flags. Therefore, invest in ongoing education (including updates when regulations or guidance change) for all stakeholders – from IT administrators to end users and even contractors who might use the systems.

By following these implementation strategies, companies can build a robust Part 11 compliance program. It's essentially about **designing quality and integrity into the electronic systems**

from the start, and sustaining that state through vigilant oversight. The effort is significant, but the cost of failure (warning letters, product recalls, or even consent decrees) is far worse. Moreover, a well-controlled electronic system yields business benefits: reliable data for decision-making, efficiency gains from reduced errors, and readiness for digital innovation such as AI integration. Speaking of which, we next examine how **Artificial Intelligence technologies intersect with Part 11 compliance** – an area of growing importance.

Artificial Intelligence (AI) in GxP: Interaction with Part 11 Compliance

As the life sciences industry increasingly experiments with **Artificial Intelligence (AI) and Machine Learning (ML)** in regulated activities, questions arise about how these technologies fit under 21 CFR Part 11. AI has potential to revolutionize data analysis, process automation, and decision support in GxP environments – from using computer vision to inspect products, to machine learning algorithms predicting process deviations, to AI chatbots assisting in clinical trial data coding. However, integrating AI into GxP processes must be done carefully to **ensure that electronic records handled or generated by AI meet the same Part 11 requirements for integrity, traceability, and accountability**. Below we explore key compliance considerations when using AI in domains subject to Part 11.

AI-Generated Records and Data Integrity: One fundamental issue is that Part 11 was written assuming **humans create, modify, and sign records**. The regulation does not explicitly address what happens when an algorithm – not a person – generates or changes an electronic record linkedin.com. Despite this, FDA's expectation is that **regulated entities remain responsible for records and decisions, even if derived from AI or automated sources** linkedin.com. In practice, this means if an AI system creates a result (for example, an AI analyzes a medical image and produces a diagnostic measurement that goes into a study dataset), that result is an electronic record under Part 11. The company must ensure the record is attributable (who is the "author" – likely the system, but under supervision of a person), and that it's accurate and auditable. One approach is to treat the AI like any other instrument: you would identify the system in the metadata (e.g. algorithm name/version as the data originator) and have an audit trail of its actions cooley.com. For instance, if an AI application updates a value in a database, the audit trail should record that "System X (AI algorithm v2.3) changed value Y to Z at time T". Many systems allow use of service accounts or system IDs to log automated actions – these should be configured so that AI operations are not lumped under generic admin accounts but uniquely identified. Additionally, **procedures should specify human oversight**: e.g. a scientist or clinician reviews AI-generated outputs, especially if they are critical, and "accepts" them into the record formally. In a clinical trial context, FDA has signaled that humans must take responsibility for any data used in submissions, even if an AI helped produce it linkedin.com. Therefore, companies should have controls to review and approve AI-generated data (similar to how one might review data transcribed by an instrument). This ensures that ultimate

accountability remains with qualified personnel and that any blatantly incorrect AI outputs can be caught and corrected before they become official records.

System Validation for AI Algorithms: Validating AI-based systems poses unique challenges compared to traditional deterministic software. However, **regulatory requirements for validation still apply** – perhaps even more stringently, given AI's complexity. FDA expects that any software used in production (manufacturing or trials) is validated for its intended use cooley.com, and AI software is no exception. A risk-based validation strategy is critical here: define the **intended use** of the AI clearly (e.g. "This AI model will screen HPLC data for anomalies" or "This ML model will predict which batches might fail to meet a spec, as a decision-support tool"). Based on risk, determine what aspects need evaluation: model accuracy, reliability, and consistency are analogous to "accuracy, reliability, consistent performance" in Part 11 ecfr.gov. For an AI model, you might conduct performance testing using a validation dataset and see if it meets pre-defined acceptance criteria (for example, >95% sensitivity in detecting a defect it was trained to detect). Also, test the system's ability to **discern invalid or altered records** ecfr.gov: if the AI is ingesting data, can it recognize out-of-range or corrupted inputs? If the AI outputs are fed into other systems, ensure any hand-off is correct and captured in audit trails. Another aspect is **model version control**: an AI model can "learn" or be updated over time, but from a compliance perspective, you should treat each model version like a new software version that requires change control and possibly re-validation. For example, if you retrain a machine learning model with new data and it changes its behavior, that's analogous to a software update – you need to document the change, verify that the new model still meets requirements, and keep an archive of the old model and its training data (in case you need to investigate how a previous decision was made). Incorporating AI into a validated state may involve additional documentation like **data lineage** (tracking training data sources), **testing for overfitting or bias**, and establishing **acceptance criteria** for model outputs (e.g., if the AI flags a sample as "suspect," does a human then do further testing?). Regulators will likely expect that companies know the limits of their AI – meaning you have defined where it's reliable and where it isn't, and have mitigations for the latter.

Audit Trails and Logging in AI Systems: Audit trails become even more important when a system, not a person, is making decisions or changes. If an AI system automates actions (for instance, auto-adjusting a process parameter or auto-verifying a record), it is vital to **log those actions with the same rigor as human actions**. Ensure that whenever the AI writes a result to a database or triggers an event, a record of that event (with timestamp) is created. In some cases, AI might operate in real-time streaming data scenarios, generating huge volumes of log data. It may be impractical to review all of it, but you should still store it securely and have means to review slices when needed (for example, if investigating a particular outcome). As noted earlier, capturing **who/what made a change** is essential – so configure your systems to record the identity of the AI module or bot. In regulated labs, there is emerging use of robotic process automation (RPA) or AI bots to transfer data between systems; these bots typically use a dedicated account and every action they perform is captured in audit trails just like a human user would be linkedin.com. Review of such logs might be part of periodic system checks.

Another point: AI algorithms might produce **intermediate data or summary reports** that are not directly user-edited but are used for decision making. If those are part of regulated decision processes, consider retaining them as part of the record (or be able to regenerate them). For example, if an AI flags 5 out of 1000 data points as outliers and those five get investigated, the fact those five were flagged should be evident in the audit trail or report logs. **Data integrity for AI inputs** is also crucial – if an AI's input data is erroneous, its output will be too. Thus, Part 11 controls upstream (ensuring source data is reliable and traceable) are indirectly a control on AI output integrity. In summary, **traceability** from input to AI to output should be maintained. Some companies use the concept of a **"model card"** or log file that accompanies each AI decision, summarizing what model version was used, what data went in, and what result came out erasciences.com. This kind of approach can greatly aid auditability and explainability of AI decisions.

Explainability and Reproducibility: One of the oft-cited challenges of AI, especially complex machine learning or deep learning models, is that they can be a "black box," making decisions that are not easily explainable to humans. While Part 11 doesn't explicitly demand explainability of algorithms, in a GxP context **explainability becomes part of building trust and ensuring appropriate use of AI**. For instance, if an AI suggests rejecting a batch or identifies a clinical trial anomaly, regulators (and your internal QA) will want to know the basis. **Explainable AI (xAI)** techniques can be leveraged – these might include simplifying the model's reasoning into human-interpretable terms, or identifying which input factors were most influential in the outcome ispe.org ispe.org. Embracing explainability is a good practice because it ties into Part 11's goal of ensuring you can **verify and justify** electronic records. If an AI output is entirely opaque, it becomes difficult to validate or defend in an audit. Some industries have started requiring a level of explainability for high-stakes AI (for example, the EU's draft AI Act leans that direction). In pharma, an example approach could be: if an ML model classifies microscope images to check cell culture health, accompany its output with a heatmap or key feature that influenced the decision, so a scientist can review whether that makes sense. **Reproducibility** is another concern – if you feed the same input data into the AI, do you consistently get the same output? For deterministic software this is usually yes, but for AI it might not be if the model has randomness or if it's continuously learning. For GxP, you typically do *not* want an algorithm that changes on the fly in uncontrolled ways. A best practice is to **freeze the model** for use (no learning during production use unless validated) and only update via a controlled process. This way, given the same input, the output is reproducible. Reproducibility is crucial if an FDA inspector or a quality investigator says "show me how this result came about" – you should be able to rerun the model (the same version) on the same data and get the same result to demonstrate reliability ispe.org ispe.org. It also ties into investigating deviations: if an AI decision is questioned, having the ability to recreate the outcome with the archived model and data is invaluable. Therefore, manage your AI models under version control like code, and archive each version and training dataset.

AI System Governance and Change Control: Companies venturing into AI should extend their quality systems to include **AI governance**. This means formalizing how AI models are developed,

tested, approved, monitored, and retired. Borrowing from ISPE's recommendations, an **AI governance framework** might involve multi-disciplinary oversight (IT, QA, data science, ethics) and cover policies for data management, bias prevention, transparency, accountability, and validation of AI systems ispe.org ispe.org. For example, **data management** policies should ensure that training data for AI is high quality, representative, and stored with the same care as any GxP raw data ispe.org ispe.org. If an AI is making decisions that could be biased (e.g., diagnosing patients), a procedure to assess and mitigate bias should be in place ispe.org ispe.org. From a Part 11 perspective, one concern is **data integrity of training data** – if the model was trained on faulty or unverified data, its output could be consistently flawed (a case of "garbage in, garbage out"). Thus, treat training datasets used for GxP AI like test records – verify their integrity and maintain a record of their source. **Change control** for AI models is critical: just as any GxP process change must be reviewed, a model update (retraining, algorithm change) should go through change control, with impact assessment on any records it generates or affects. If the model is embedded in a device or system, one might have to file a regulatory notification, depending on significance (more relevant in devices with AI). Another aspect of governance is **continuous monitoring**: AI performance can drift over time, especially if the input data characteristics change (model degradation). Establish metrics and periodically evaluate the AI's output against expected results or known standards. If performance drifts below an acceptable threshold, that's analogous to a calibration going out of tolerance – it should trigger an investigation and retraining or other corrections. In FDA's device realm, there's discussion of "Predetermined Change Control Plans" for algorithms that retrain, but in drugs/biologics, the concept is nascent content.govdelivery.com. For now, a prudent strategy is to lock down AI models in GxP use and only change them with full validation, unless you've engaged FDA on some adaptive algorithm approach explicitly.

Human Oversight and Accountability: Both regulatory expectations and common sense dictate that AI should be used with human oversight in GxP areas. Part 11's requirement that individuals are accountable for electronic records still applies – so if an AI system aids in decision-making, the decision should ultimately be confirmed by a responsible person. For example, if AI software flags a lab test as suspect, a human reviewer should examine that and decide whether to invalidate the test or not, documenting their reasoning. The **role of the human-in-the-loop** should be clearly defined in procedures. Depending on the AI's role, oversight might be required for each individual action (for high criticality tasks) or batched/periodic review for lower risk uses. The key is you cannot abdicate quality decisions entirely to a black-box algorithm under current regulations. Even if an AI is extremely accurate, you should initially treat its outputs as "recommendations" that need human approval. Over time, if confidence grows and if possibly regulatory thinking evolves, more autonomous use might be allowed, but it would likely require demonstration of the AI's reliability and perhaps regulatory buy-in. As of 2025, FDA has not issued detailed guidance on AI in Part 11 or drug manufacturing, but the assumption is any **use of AI is subject to the firm ensuring compliance with all applicable regulations** cooley.com cooley.com. In other words, you can use AI, but if something goes wrong (inaccurate records, overlooked errors), your company is fully accountable. A good practice is to document the rationale for using AI for a task, including expected benefits and how

risks are mitigated, as part of your validation or technical file. If an inspector sees AI was involved in, say, reviewing clinical data, they might ask how you validated it and how you ensure it didn't miss anything – be prepared with that justification.

Use Cases of AI Supporting Part 11 Compliance: Interestingly, AI can also be a tool *to enhance* Part 11 controls. Some companies have started using AI-driven features to strengthen authentication and monitoring. For example, **biometric authentication** with AI – an e-signature process might use facial recognition or voice recognition to verify the signer's identity (in addition to or in place of password) cooley.com. If implemented properly, this could exceed the security of traditional methods, though it must be validated for accuracy (false accept/reject rates) and meet biometric signature requirements (only used by genuine owner) ecfr.gov. Another use is **AI for audit trail review**: manually sifting through audit logs is tedious, but machine learning can be trained to detect anomalous patterns or potential fraud (e.g., logins at odd times, sequences of data changes that are unusual) cooley.com. Such tools can alert compliance officers to investigate. This doesn't replace the need for audit trails, but augments their usefulness. In pharmacovigilance, AI text mining is used to scan scientific literature for adverse events; while not directly Part 11, it supports compliance with post-market reporting. **AI in data cleaning** is common in clinical trials – algorithms help identify outliers or discrepancies in data. Again, the outputs (queries raised, data changed) should be logged and then addressed by humans as needed cooley.com. We also see AI being embedded in **digital health tech (DHT)** devices – for example, a wearable might use an algorithm to decide if a sensor reading is valid or to summarize raw data. If those decisions affect what data is stored, they need to be validated and transparent. In summary, AI can both pose compliance questions and help solve compliance challenges. The guiding principle is to *apply the existing Part 11 and data integrity requirements to AI use*, and where there is ambiguity, err on the side of maintaining human responsibility and rigorous control.

Case Studies and Industry Applications of AI under Part 11

While the use of AI in fully regulated production is still emerging, several early applications provide insight into how companies can successfully integrate AI while staying compliant:

- **AI-Powered Visual Inspection (Manufacturing):** One pharmaceutical manufacturer implemented an AI-based **line clearance** system on their packaging line to ensure no stray tablets or components remained from the previous batch. Traditionally, line clearance is a manual check, but this firm used a combination of cameras and AI algorithms to automatically detect any unwanted materials, speeding up changeovers. To comply with Part 11 and EU **Annex 11**, the system was developed following **GAMP 5** guidelines (a risk-based computerized system lifecycle) and thoroughly validated before use blog.seavision-group.com blog.seavision-group.com. Key Part 11 controls were built in: the AI system's software was validated for accuracy (it was challenged to detect objects of various sizes/materials in various positions to ensure reliability), secure audit trails recorded each clearance inspection event (with time, who initiated it, results), and only authorized technicians could override or reset the system blog.seavision-group.com blog.seavision-group.com. The system produced **digital evidence and reports** for each batch changeover, complete with images of the line and confirmation that it was clear blog.seavision-group.com blog.seavision-group.com. These reports were treated as electronic records. During regulatory audits, the manufacturer provided these records along with the validation documentation, demonstrating that the AI reduced human error and was under control. The outcome was improved efficiency (faster line clearance) while maintaining compliance – the AI essentially acted as a vigilant secondary checker. This case highlights the importance of **validating AI like any equipment**, and the benefit of generating comprehensive audit trails and reports to satisfy inspectors.

- **AI in Clinical Data Management:** A biotech company faced massive volumes of clinical trial data from electronic sources and leveraged an **AI-based cloud platform** to manage and analyze the data. The solution involved a data lake and ML algorithms to automate data processing and flag anomalies. From the outset, compliance was a central design criterion: the cloud infrastructure was chosen for its robust security certifications (HIPAA, ISO 27001, etc.), and the platform was built to be **Part 11 compliant (audit trails, user controls) and GxP qualified** ardigen.com ardigen.com. In the implementation, they ensured every data transaction was logged, and that any data cleaning performed by AI was either reversible or at least transparently logged. A "single source of truth" paradigm was used – all raw data and processed data stayed in a unified repository with full processing history, facilitating traceability ardigen.com. For example, if the AI merged two similar patient records or corrected a typographical error, the original and changed values were both retained and audit-trailed. The **results** were promising: the company achieved an integrated platform that enabled efficient AI/ML analysis on clinical data while maintaining compliance with 21 CFR Part 11 and other data regulations ardigen.com ardigen.com. The FDA (during an inspection related to a new drug application) was provided with documentation on how the AI algorithms were validated for their specific tasks (like adverse event coding assistance), including test cases showing the AI's output versus manual double-check. Moreover, the platform's audit logs were readily available to show that no unauthorized data manipulations occurred. This case underscores the need to **blend AI with a solid data management strategy** – using AI to handle scale and complexity, but within a controlled, well-documented framework. It also shows that using modern cloud tools (like Databricks, as was the case here) can be done in a compliant way if configured correctly ardigen.com ardigen.com.

- **E-Signature Authentication with AI:** In the realm of electronic signatures, some organizations have started exploring AI-driven **biometric authentication** to enhance security. For example, a clinical research company introduced an eConsent system for trial participants that uses **AI-based facial recognition** to verify identity each time a participant logs in to sign documents. The system was qualified to ensure the false match rate was below a strict threshold and that it could tell live people from photos (liveness detection). Under Part 11, this falls under biometric electronic signatures, so it had to be designed such that it's unique to the individual and cannot be used by anyone else ecfr.gov. The company submitted a non-repudiation letter to FDA for participants' electronic signatures and documented the algorithm's accuracy testing. Each signature event still created a traditional audit record (with participant ID, date/time, and signature meaning such as "consent given"), but the method of identity verification was AI-based. During a routine GCP inspection, FDA was particularly interested in how the system ensured that the person signing was truly the subject and not an impostor. The firm provided the validation reports of the facial recognition AI and logs showing successful verification and any failed attempts (none of which resulted in a false acceptance). Because there was still an underlying unique credential tied to the participant (the biometric template), and the system met Part 11's biometric controls, the approach was accepted. This example demonstrates that AI can strengthen compliance (arguably harder to forge a face than a password) provided it's well-controlled. It also highlights the importance of **testing AI thoroughly in the identity context** – the risk of false positives/negatives directly affects compliance here.

- **Manufacturing Process Control AI (Prototype):** In a forward-looking pilot, a pharma manufacturing site tested an AI-driven **predictive maintenance and process control** system for a critical production line. The AI analyzed sensor data in real time to predict equipment wear and subtly adjust certain process parameters to optimize yield. While this was not yet a full production system, the company worked closely with its quality unit and even consulted FDA liaisons to design compliance into the project. They created a **model risk assessment**: since the AI could influence process conditions, it was deemed high risk. They put in place hard limits (the AI could only adjust within pre-approved ranges, otherwise it would alert an operator for manual decision). Each adjustment by the AI was logged with rationale (e.g. "temperature increased by 0.5°C based on model prediction to maintain potency") and tagged as provisional until the batch was completed and QA reviewed the logs. Validation involved retrospective testing: running the AI algorithm on historical batch data to see if it would have made correct adjustments and not caused deviations – essentially a non-inferiority test compared to human operations. The **explainability** challenge was tackled by having the AI provide a confidence score and top factors for each recommendation, which the process engineer could review. Though still experimental, this case illustrates how an **augmented intelligence approach** can be taken – AI assists but does not fully control without oversight. To satisfy Part 11 principles, every action was captured, the model was locked during a batch, and operators retained final authority to accept or override AI suggestions. If such a system were to go live, the company planned to have a real-time monitoring dashboard for QA and to require a second person (remote process expert) to oversee what the AI was doing in critical operations. This kind of application will likely become more common, and regulatory comfort will grow as industry demonstrates that they can keep AI "on a leash" that ensures quality is not compromised.

These case studies and examples collectively show that **AI can be deployed in compliance with Part 11, but it requires forethought and rigorous controls**. Companies must validate AI tools, integrate them with robust data infrastructure, and maintain transparency of AI actions. Many organizations are publishing white papers and concept papers on "AI in GxP" to share best

practices. For instance, the International Society for Pharmaceutical Engineering (ISPE) has discussed frameworks for AI governance and the importance of explainability in GxP settings ispe.org ispe.org. Early adopters often report that having a strong foundational electronic compliance program (good Part 11 discipline) is what makes layering AI feasible. On the other hand, those without mature data integrity practices may find AI magnifies problems (e.g., automating bad processes gives bad results faster). Regulators have so far been cautiously receptive – there isn't an "anti-AI" stance, rather an expectation that **all the existing quality and compliance principles apply** even if the technology is novel cooley.com. As one FDA representative noted in a conference, *"You can outsource or automate activities, but not responsibility."* Companies should thus approach AI in GxP with both enthusiasm for innovation and respect for the compliance framework that safeguards patient safety and data integrity.

Conclusion

21 CFR Part 11 remains a vital regulation in 2025, anchoring the trustworthiness of electronic records and signatures in an era of digital transformation. Its core tenets – from system validation and audit trails to secure user authentication and record integrity – provide a proven framework to ensure that electronic data can stand up to scrutiny just as paper records have for decades. FDA's recent guidance and enforcement trends reaffirm that while technology evolves, the **principles of data integrity are constant**: records must be complete, accurate, and attributable; signatures must be genuine and accountable; and systems must be under a state of control. Organizations should stay abreast of the latest FDA guidances (such as the 2024 Q&A and forthcoming CSA validation approach) and adapt their compliance programs accordingly, embracing risk-based methods to work smarter and more efficiently.

At the same time, the rise of **Artificial Intelligence and machine learning** in life sciences is ushering in both opportunities and new questions for compliance. As we've detailed, AI can be harmonized with Part 11 by treating AI-driven processes with the same rigor as any critical system – validating algorithms, capturing their actions in audit trails, managing changes, and retaining human oversight. Concepts like explainability, reproducibility, and AI governance are becoming essential parts of the quality assurance vocabulary. Companies that successfully integrate AI will likely be those who expand their quality systems to include data science expertise and who foster collaboration between traditional QA/QC and IT/AI teams. The message from regulators is clear: you may leverage cutting-edge tools (AI, cloud, etc.), but you cannot compromise on the control and transparency of GxP records. If an AI helps generate or evaluate data used in regulatory decisions, you must **be able to defend that data and the process by which it was produced**. This includes showing auditors the what, why, and how of your AI's involvement, backed by documentation and verifiable logs.

In practical terms, companies should approach Part 11 compliance in 2025 as both a **technical and cultural effort**. Technically, ensure every GxP software system is assessed for Part 11 gaps and fixed (most modern systems can meet these requirements, but only if configured and used

properly). Procedurally, reinforce training and SOPs that instill good data integrity practices. Culturally, treat data as a critical asset – something to be safeguarded like product inventory or intellectual property. Encourage employees to be vigilant about data accuracy and to speak up if they see potential issues, whether it's a suspicious audit trail entry or an AI model result that "doesn't look right." With regulatory authorities worldwide focusing heavily on data reliability, a strong Part 11 program is not just about avoiding FDA citations; it's about ensuring the **foundation of trust** in all the digital data that drives modern healthcare innovations.

In conclusion, 21 CFR Part 11 provides the guidance to navigate the complex landscape of electronic record-keeping. Its enduring relevance, even 28 years on, stems from technology-neutral principles that can flex to new modalities linkedin.com linkedin.com. Firms that master Part 11 compliance position themselves to confidently embrace digital transformation – including AI – while maintaining the rigorous standards of quality and accountability that regulators and patients expect. By combining solid compliance practices with forward-looking adaptation, life science organizations can ensure that as their tools get smarter, their data stays trustworthy, and their operations remain in a state of control. The path to innovation is wide open, as long as it's built on a strong bedrock of compliance.

Sources:

1. Code of Federal Regulations, **21 CFR Part 11 – Electronic Records; Electronic Signatures**, U.S. Food & Drug Administration (FDA) ecfr.gov ecfr.gov.
2. FDA Guidance for Industry, **"Electronic Systems, Electronic Records, and Electronic Signatures in Clinical Investigations: Questions and Answers"**, Final Guidance (October 2024) fda.gov fda.gov.
3. Cooley LLP analysis of FDA Part 11 Guidance, **"FDA Finalizes Guidance on Use of Part 11 Electronic Systems, Records and Signatures in Clinical Investigations"** (Oct 24, 2024) cooley.com cooley.com.
4. Dot Compliance Blog, **"FDA 21 CFR Part 11 Compliance: What You Need to Know in 2025"** by B. Percy (June 5, 2025) dotcompliance.com dotcompliance.com.
5. Astrix Inc. Blog, **"Enforcement Trends in FDA Data Integrity 483s and Warning Letters"** (Feb 16, 2020) astrixinc.com astrixinc.com.
6. LinkedIn Article by D. Janzen, **"21 CFR Part 11 – Relevance of a 28 Year Old Regulation in Modern Cloud and AI Settings"** (2023) linkedin.com linkedin.com.
7. SEA Vision Whitepaper, **"Line Clearance Solutions: Ensuring Compliance with 21 CFR Part 11 and Annex 11 GAMP 5"** (June 10, 2025) blog.seavision-group.com blog.seavision-group.com.
8. Ardigen Case Study, **"Transforming Clinical Trial Reporting: A Scalable and Compliant Data Platform"** (July 1, 2025) ardigen.com ardigen.com.
9. ISPE Pharmaceutical Engineering, **"Artificial Intelligence Governance in GxP Environments"** (July/Aug 2024) ispe.org ispe.org.

10. ISPE Pharmaceutical Engineering, **“The Road to Explainable AI in GxP-Regulated Areas”** (Jan/Feb 2023) ispe.org ispe.org.

11. Medium (Vital Compliance), **“Mastering FDA’s Computer Software Assurance (CSA) Framework”** by D. James (June 16, 2025) medium.com medium.com.

12. FDA CFR Title 21 Part 11, **Electronic Code of Federal Regulations (eCFR)** current to 2025 ecfr.gov ecfr.gov.

IntuitionLabs - Industry Leadership & Services

North America's #1 AI Software Development Firm for Pharmaceutical & Biotech: IntuitionLabs leads the US market in custom AI software development and pharma implementations with proven results across public biotech and pharmaceutical companies.

Elite Client Portfolio: Trusted by NASDAQ-listed pharmaceutical companies including Scilex Holding Company (SCLX) and leading CROs across North America.

Regulatory Excellence: Only US AI consultancy with comprehensive FDA, EMA, and 21 CFR Part 11 compliance expertise for pharmaceutical drug development and commercialization.

Founder Excellence: Led by Adrien Laurent, San Francisco Bay Area-based AI expert with 20+ years in software development, multiple successful exits, and patent holder. Recognized as one of the top AI experts in the USA.

Custom AI Software Development: Build tailored pharmaceutical AI applications, custom CRMs, chatbots, and ERP systems with advanced analytics and regulatory compliance capabilities.

Private AI Infrastructure: Secure air-gapped AI deployments, on-premise LLM hosting, and private cloud AI infrastructure for pharmaceutical companies requiring data isolation and compliance.

Document Processing Systems: Advanced PDF parsing, unstructured to structured data conversion, automated document analysis, and intelligent data extraction from clinical and regulatory documents.

Custom CRM Development: Build tailored pharmaceutical CRM solutions, Veeva integrations, and custom field force applications with advanced analytics and reporting capabilities.

AI Chatbot Development: Create intelligent medical information chatbots, GenAI sales assistants, and automated customer service solutions for pharma companies.

Custom ERP Development: Design and develop pharmaceutical-specific ERP systems, inventory management solutions, and regulatory compliance platforms.

Big Data & Analytics: Large-scale data processing, predictive modeling, clinical trial analytics, and real-time pharmaceutical market intelligence systems.

Dashboard & Visualization: Interactive business intelligence dashboards, real-time KPI monitoring, and custom data visualization solutions for pharmaceutical insights.

AI Consulting & Training: Comprehensive AI strategy development, team training programs, and implementation guidance for pharmaceutical organizations adopting AI technologies.

Contact founder Adrien Laurent and team at https://intuitionlabs.ai/contact for a consultation.

DISCLAIMER

The information contained in this document is provided for educational and informational purposes only. We make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability of the information contained herein.

Any reliance you place on such information is strictly at your own risk. In no event will IntuitionLabs.ai or its representatives be liable for any loss or damage including without limitation, indirect or consequential loss or damage, or any loss or damage whatsoever arising from the use of information presented in this document.

This document may contain content generated with the assistance of artificial intelligence technologies. AI-generated content may contain errors, omissions, or inaccuracies. Readers are advised to independently verify any critical information before acting upon it.

All product names, logos, brands, trademarks, and registered trademarks mentioned in this document are the property of their respective owners. All company, product, and service names used in this document are for identification purposes only. Use of these names, logos, trademarks, and brands does not imply endorsement by the respective trademark holders.

IntuitionLabs.ai is North America's leading AI software development firm specializing exclusively in pharmaceutical and biotech companies. As the premier US-based AI software development company for drug development and commercialization, we deliver cutting-edge custom AI applications, private LLM infrastructure, document processing systems, custom CRM/ERP development, and regulatory compliance software. Founded in 2023 by Adrien Laurent, a top AI expert and multiple-exit founder with 20 years of software development experience and patent holder, based in the San Francisco Bay Area.

This document does not constitute professional or legal advice. For specific guidance related to your business needs, please consult with appropriate qualified professionals.