

PharmacoLearn

MRA101T Good Regulatory Practices, M.Pharm Semester 1

Unit 3: Good Automated Laboratory Practices

Free notes at pharmacolearn.fyi

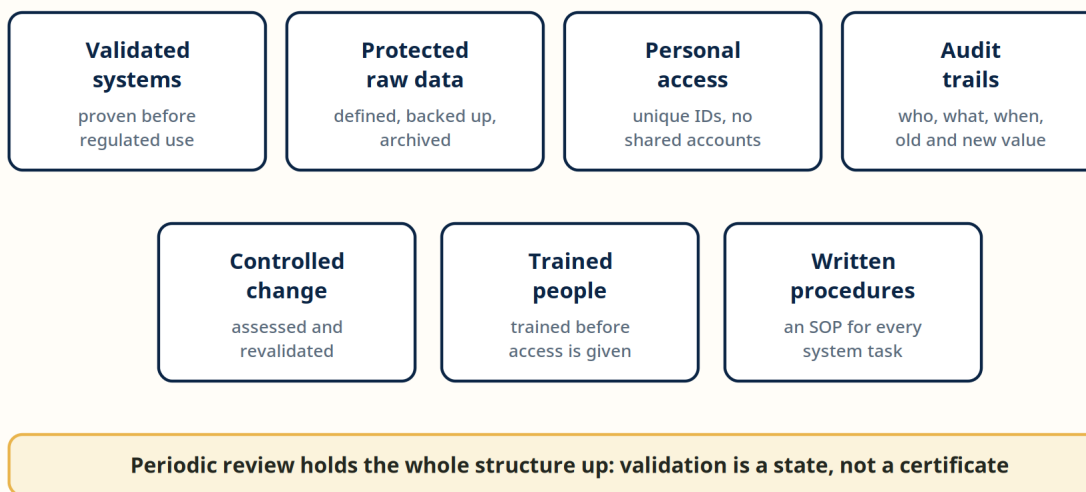
3.1 Why automation needed a practice of its own

By the 1980s the analytical laboratory was filling with computers: chromatographs with integrators, balances printing to systems, laboratory information management systems (LIMS) holding results. Each removed a human transcription step and added an invisible one: data could be altered, reprocessed or deleted without the strike through and initials that paper GLP made visible. **Good Automated Laboratory Practices (GALP)** arose to extend GLP's guarantees into that world. The US Environmental Protection Agency, whose laboratories faced the problem first at scale, issued GALP guidance for its own automated laboratories, and the framework was taken up across regulated industry as the working statement of how a computerized laboratory system stays trustworthy: documented, validated, secure, and operated by trained people under SOPs. GALP is best understood as GLP translated for systems: wherever GLP says a record, GALP asks what the record is when it is a database entry; wherever GLP says a signature, GALP asks what proves identity on a screen.

3.2 Principles of GALP

The GALP principles can be stated as a short creed, and examiners accept them in this form. **Data are the raw material and must be protected as such:** electronic raw data are defined, backed up and archived with the same seriousness as paper notebooks. **Systems are validated before use:** a computerized system must be shown to do what it purports to do, consistently, before regulated work depends on it. **Changes are controlled:** hardware, software and configuration changes pass through documented change control with revalidation proportionate to the change. **Access is personal and limited:** users have unique identities, authority matched to role, and no shared accounts behind which an action could hide. **Everything is attributable:** audit trails record who did what, when, and what the value was before and after. **People are trained and procedures are written:** automation removes no responsibility; it relocates it to those who configure, operate and review the system. And **the system is periodically reviewed:** validation is a state to be maintained, not a certificate to be framed.

The Pillars of GALP



© 2026 PharmacoLearn, pharmacolearn.fyi

Figure: The GALP pillars: validated systems, protected raw data, personal access, audit trails, controlled change, trained people, written procedures.

The validation life cycle of a laboratory system

User requirements written (what the lab needs the system to do)

- > Vendor and software evaluation against the requirements
- > Installation Qualification: installed as specified
- > Operational Qualification: operates to specification
- > Performance Qualification: performs in real laboratory use
- > Release for regulated use, under change control
- > Periodic review, revalidation after significant change

3.3 GALP requirements in practice

Translated into requirements, the principles produce the working list a laboratory is audited against.

System documentation: an inventory of hardware and software with versions and configurations, network and interface maps, and the validation dossier for each regulated system. **Security administration:** user account management, password rules, role based permissions, and prompt removal of leavers' access.

Data management: defined raw data for each system, backup schedules with tested restoration, time synchronization across systems so audit trails can be correlated, and archives from which electronic records remain readable for the full retention period, including after software upgrades. **Operational**

discipline: SOPs for use, administration, incident handling and disaster recovery; a change log; and vendor management for hosted and cloud systems, in which the laboratory keeps responsibility for data even where a supplier keeps the servers. None of this is ornament: every item answers a failure that has actually been found in inspections, from shared logins to backups that had never once been restored.

3.4 SOPs of GALP, and training documentation

GALP requires its own SOP family, distinct from the analytical SOPs of the laboratory: SOPs for system use (per system), for user account and access management, for backup and restore, for change control of computerized systems, for audit trail review, for incident and problem management, for periodic review, and for archiving and retirement of systems. Behind them sits **training documentation:** a training matrix mapping each role to the systems and SOPs it requires, records showing each user was trained before being given access, and evidence of effectiveness where the task is critical. The audit question that exposes weak laboratories is simple: show me who may reprocess a chromatogram in this system, and

show me where each of them was trained and authorised to do so. If the answer lives in a person's memory rather than in records, the GALP requirement is unmet however good the software is.

3.5 21 CFR Part 11: electronic records and electronic signatures

The regulation that gives GALP its legal teeth in the United States is **21 CFR Part 11**, "Electronic Records; Electronic Signatures", issued by the FDA in 1997. Its premise is equivalence under conditions: electronic records and signatures are acceptable in place of paper records and handwritten signatures required by the predicate rules (such as Parts 58 and 211) when the systems holding them meet Part 11's controls. For **electronic records** the core controls are: system **validation**; the ability to generate accurate and complete copies for inspection; record protection throughout the retention period; **computer generated, time stamped audit trails** that record operator entries and actions creating, modifying or deleting records, with prior values never obscured; **authority checks** limiting system access to authorised individuals and functions; operational and device checks; and documentation control. For **electronic signatures**, Part 11 requires that a signature be unique to one individual, that identity be verified before an account is issued, that a signed record display the signer's name, the date and time, and the meaning of the signing (review, approval, authorship), and that signatures be linked to their records so they cannot be copied to another document. The FDA's 2003 guidance on the **scope and application** of Part 11 narrowed enforcement to these core elements while keeping the regulation itself in force, a distinction worth one line in any examination answer: the rule stands; the guidance sets enforcement priorities.

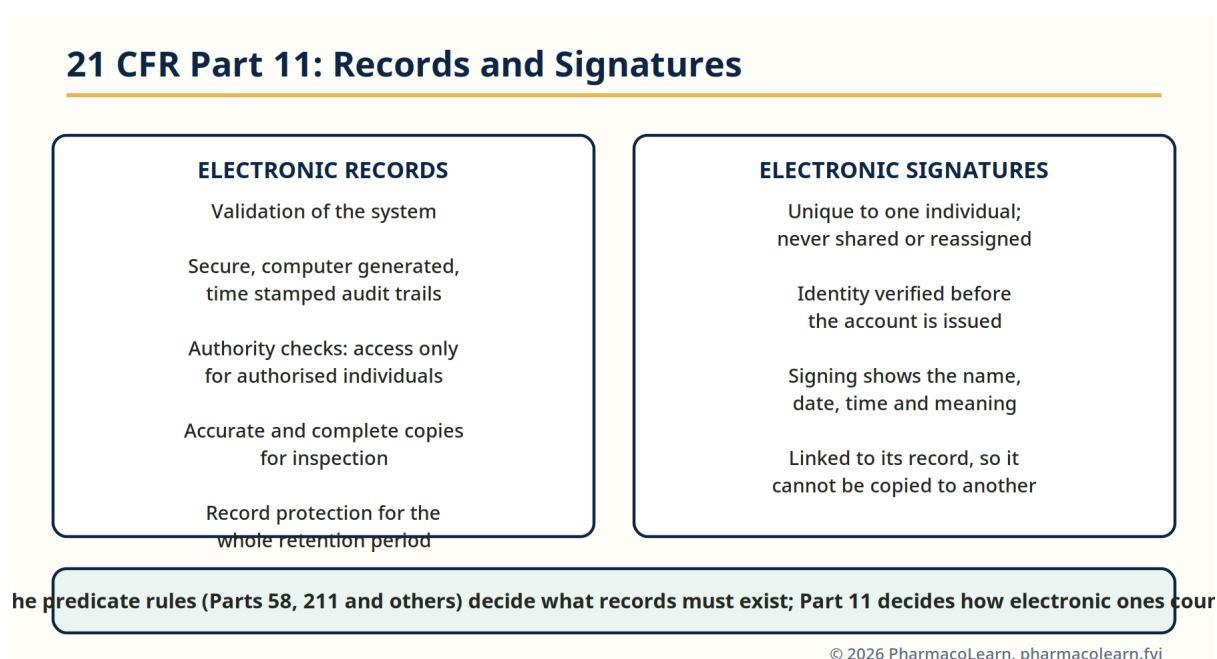


Figure: 21 CFR Part 11 in one view: the record controls on the left, the signature controls on the right, validation beneath both.

3.6 The general checklist of 21 CFR Part 11

The syllabus asks for the **general checklist** by which a system is judged Part 11 compliant, and it is best learned as questions an auditor asks, in order. Is the system validated, with documented evidence, for its intended regulated use? Are access controls enforced, with unique user IDs, password complexity and expiry, and automatic logoff or screen locking? Is a secure, computer generated audit trail active, recording creation, modification and deletion with user, date, time and old and new values, retained at least as long as the records, and protected from the users it watches? Are electronic signatures unique, identity verified, displayed with name, date, time and meaning, and cryptographically or logically linked to their records? Can the system produce accurate and complete copies of records, in human readable and electronic form, for

inspection? Are records retrievable throughout their retention period, with backup and archive procedures proven by test restoration? Are operational sequence checks and device checks in place where the process needs them? Is there documentation control over system documentation itself, and training records for every user? A system for which any answer is "no, but" is a system carrying a Part 11 finding in waiting.

3.7 The software evaluation checklist

Before validation comes selection, and GALP formalises it in the **software evaluation checklist** used when a laboratory buys or builds a system. Its heads: **functional fit** (does the software perform the laboratory's required functions, tested against the written user requirements, not the vendor's brochure?); **regulatory capability** (audit trail design, access control model, electronic signature support, data export and archiving features, in short native Part 11 capability); **vendor quality** (the supplier's development and testing practices, established by questionnaire or audit, its installed base in regulated laboratories, its support and patch discipline); **technical fit** (platform, interfaces to instruments and other systems, performance, backup architecture); **validation cost** (the effort the product's design will demand: configurable products with vendor validation documentation cost less to validate than custom code, the GAMP 5 category logic of Unit 1); and **life cycle terms** (licensing, upgrade policy, data migration on retirement). The checklist's purpose is economic as much as scientific: the cheapest software to buy is often the dearest to make compliant, and the evaluation is where that truth is cheapest to learn.

3.8 ISO and QCI standards in the automated laboratory

The standards layer of Unit 2 returns here with an automation accent. **ISO/IEC 17025** accreditation of a testing laboratory now examines its information management directly: the standard requires that laboratory information management systems be validated, protected from unauthorised access and tampering, and operated with data integrity safeguards, so an accredited laboratory cannot treat its LIMS as outside its quality system. **ISO 9001** supplies the general management system frame (documented information, control of changes, corrective action) within which many laboratories house their system procedures. In India, **NABL** accreditation assessments under QCI test these points on site, and CDSCO and NGCMA inspections of GLP and GMP facilities apply the same expectations to the systems they find. The examination answer to hold is one of convergence: GALP stated the principles, Part 11 made them law for FDA regulated records, and the ISO family absorbed the same expectations into accreditation, so a laboratory that builds to GALP is rarely surprised by any of its judges.

*More free M.Pharm notes and unit wise PDFs at pharmacolearn.fyi
Free video lectures on the PharmacoLearn YouTube channel*