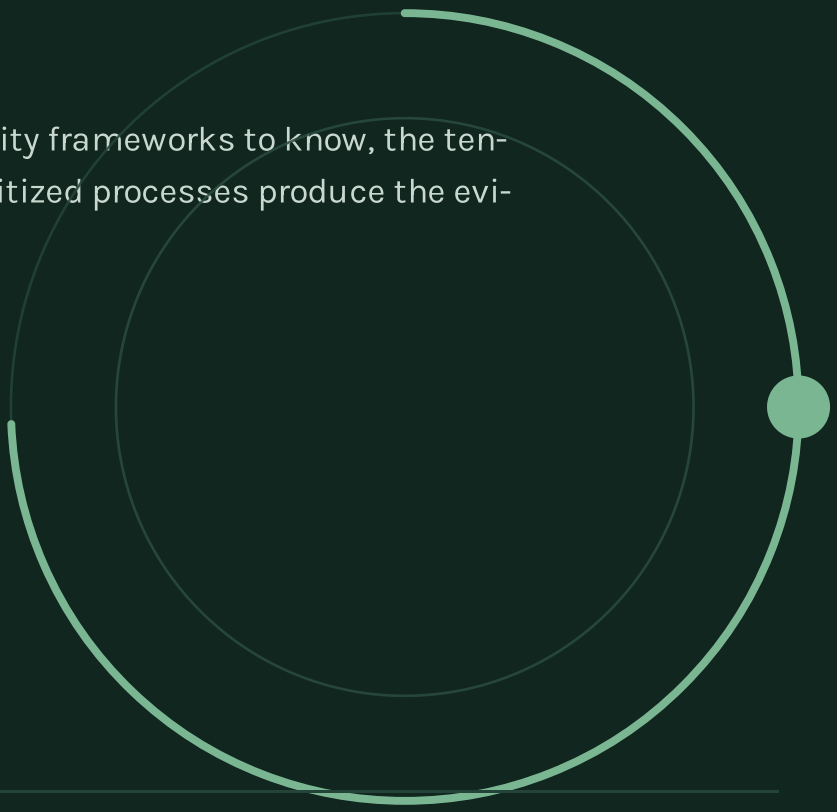
TERMINUS 2π

GUIDE

QUALITY & COMPLIANCE · LIFE SCIENCES AND HEALTHCARE

Regulatory compliance, built into your processes

The GxP, data, quality and security frameworks to know, the tensions to anticipate, and how digitized processes produce the evidence by design.



Terminus 2π

October 2026

Framework matrix after a synthesis published by Gencovery in 2025

About this guide

This guide is for leaders, quality, regulatory affairs and IT managers in life sciences and healthcare companies: biotech, pharma, medtech, laboratories, clinics, e-health. It presents the main regulatory frameworks that apply to their processes and data, the friction points between these frameworks, and how digitizing processes makes compliance simpler.

It does not replace advice from a qualified regulatory affairs consultant: it is a map to find your way, ask the right questions and set priorities.

Contents

1 · Compliance: a foundation, not a burden

2 · AI raises the bar

3 · Overview: 13 frameworks in 7 domains

4 · Four tensions to anticipate

5 · What digitized processes change

6 · Choosing hosting to fit your constraints

7 · Where to start

CHAPTER 1

Compliance: a foundation, not a burden

In life sciences and healthcare, regulatory compliance is not an administrative formality: it is the condition for market access. GxP, GDPR, HDS, ISO 13485: each framework translates a safety, traceability and quality requirement that protects patients and guarantees the integrity of scientific data.

The cost of compliance rarely comes from the requirements themselves. It comes from the way they are met: evidence rebuilt by hand before every audit, non-conformities tracked in spreadsheets, paper signatures, documents whose latest version nobody can find.

> Digitized processes are traceable by design. Compliance stops being a layer added afterwards: it becomes a property of the processes, and the evidence is already there on audit day.

CHAPTER 2

AI raises the bar

Adopting artificial intelligence in R&D and healthcare processes creates new regulatory challenges. An AI model used in a medical or regulatory decision must be transparent, auditable and validated: this is required by the EU AI Act (2024), but also by existing GxP rules on computerized system validation (GAMP 5, 21 CFR Part 11).

Poorly traced input data can invalidate every conclusion of a study. Conversely, a traceable, well-governed data infrastructure makes AI usable in high-stakes regulatory contexts, including submissions to the FDA or the EMA.

AI Act (EU, 2024) · GAMP 5 · 21 CFR Part 11 · FDA · EMA

That is why, at Terminus 2π, AI agents embedded in processes work with human approval, and every action is traced: who proposed what, who approved it, on which data.

CHAPTER 3

Overview: 13 frameworks in 7 domains

Thirteen frameworks shape the compliance of biotech, pharma and medtech operations. They cover seven domains: quality systems, data integrity, privacy / gdpr, health data, it systems, security / gxp, environment. The table gives the overview; each framework is then detailed.

FRAMEWORK	DOMAIN	REGION
GAMP 5	IT / Quality	Global (ISPE)
GLP	GxP / Safety	OECD / Global
21 CFR Part 11	Data integrity	USA (FDA)
RGPD / GDPR	Privacy	EU (applies globally)
HDS	Health data	France (ANS/ANSSI)
ISO 13485	Quality	Global (ISO)
ICH Q10	Quality	Global (ICH)
GMP / EudraLex Vol.4	GxP / Safety	EU (EMA)
GCP / ICH E6(R3)	GxP / Clinical	Global (ICH)
ISO 27001	IT security	Global (ISO)
ICH Q9 (R1)	Risk management	Global (ICH)
REACH / CLP	Environment / Safety	EU (ECHA)
HIAPP	eHealth / Apps	France (ANS / HAS)

GAMP 5

IT / QUALITY · GLOBAL (ISPE)

Scope	Validation of computerised systems in regulated life sciences
Key requirements	Risk-based software categorisation (Cat 1–5), validation plans, IQ/OQ/PQ, change control, audit trails
Applies to	Pharma, biotech, medtech manufacturers
Overlaps	Overlaps with 21 CFR Part 11 & Annex 11 on electronic records and audit trails
What sets it apart	Risk-based categorisation of software; the only framework specifically guiding how to validate GxP systems

GLP

GXP / SAFETY · OECD / GLOBAL

Scope	Non-clinical safety studies (toxicology, ecotoxicology)
Key requirements	Study director accountability, SOPs, raw data archiving, test facility inspection, specimen retention
Applies to	CROs, labs conducting non-clinical studies for regulatory submission
Overlaps	Shares data integrity & audit trail goals with 21 CFR Part 11 / GAMP 5
What sets it apart	Covers the physical conduct of studies (animals, reagents, notebooks), not just electronic systems

21 CFR Part 11

DATA INTEGRITY · USA (FDA)

Scope	Electronic records & electronic signatures in FDA-regulated industries
Key requirements	ALCOA+ data principles, audit trails, e-signature controls, system validation, access controls, record retention
Applies to	Any US FDA-regulated entity (pharma, biotech, device, food)
Overlaps	Mirrors EU Annex 11 (EudraLex); both enforced alongside GAMP 5 guidance
What sets it apart	Legally binding US regulation; specifically governs e-signatures as legally equivalent to handwritten ones

RGPD / GDPR

PRIVACY · EU (APPLIES GLOBALLY)

Scope	Personal data processing of EU residents
Key requirements	Lawful basis, data subject rights, DPO appointment, DPIA, data minimisation, breach notification ≤72h, cross-border transfer rules
Applies to	Any entity processing EU personal data, including patient data in trials
Overlaps	Overlaps with HDS on health data; pairs with ICH E6 on clinical trial data governance
What sets it apart	Broadest personal data law; unique right-to-erasure tension with GxP data retention requirements

HDS

HEALTH DATA · FRANCE (ANS/ANSSI)

Scope	Hosting of personal health data on behalf of third parties in France
Key requirements	Mandatory HDS certification, ISO 27001 base, data localisation (FR/EU), sub-contractor control, reversibility plan
Applies to	Cloud providers, SaaS vendors, CROs hosting French patient data
Overlaps	Built on GDPR + ISO 27001; stronger than GDPR alone for health data hosted in France
What sets it apart	Requires certified host — cannot self-certify; contractual chain must be fully certified end-to-end

ISO 13485

QUALITY · GLOBAL (ISO)

Scope	Quality management system for medical devices
Key requirements	Design controls, risk management, CAPA, post-market surveillance, supplier qualification, traceability
Applies to	Medical device manufacturers & supply chain
Overlaps	Overlaps ISO 9001 (QMS base); aligns with EU MDR / IVDR and 21 CFR 820
What sets it apart	Device-specific QMS; mandatory for CE marking under MDR — not applicable to pure pharma/biotech

ICH Q10

QUALITY · GLOBAL (ICH)

Scope	Pharmaceutical quality system across product lifecycle
Key requirements	Management responsibility, continuous improvement, CAPA, knowledge management, lifecycle approach (dev → discontinuation)
Applies to	Pharmaceutical & biotech companies globally
Overlaps	Complements ICH Q8 (design) & Q9 (risk); implemented via EU GMP Part III / FDA guidance
What sets it apart	Lifecycle view — explicit coverage from early development to market withdrawal, unlike site-focused GMP

GMP / EudraLex Vol.4

GXP / SAFETY · EU (EMA)

Scope	Manufacturing of medicinal products for human & veterinary use
Key requirements	Premises & equipment, personnel, documentation, production, QC, QA, out-sourced activities, complaints, recalls; Annex 11 (computerised systems)
Applies to	EU pharmaceutical & biotech manufacturers, importers
Overlaps	Mirror of US cGMP (21 CFR 210/211); Annex 11 ≈ 21 CFR Part 11
What sets it apart	Legally enforceable EU manufacturing law; Annex 11 is the authoritative EU counterpart to GAMP 5 recommendations

GCP / ICH E6(R3)

GXP / CLINICAL · GLOBAL (ICH)

Scope	Design, conduct, recording and reporting of clinical trials
Key requirements	Protocol, IRB/IEC approval, informed consent, investigator responsibilities, data management, monitoring, adverse event reporting, TMF
Applies to	Sponsors, CROs, investigators running clinical trials
Overlaps	Requires GAMP 5-compliant CTMS/EDC; patient data governance intersects with GDPR
What sets it apart	Solely governs the clinical trial process; E6(R3) adds risk-based monitoring and data governance modernisation

ISO 27001

IT SECURITY · GLOBAL (ISO)

Scope	Information security management system (ISMS)
Key requirements	Risk assessment, 93 controls (Annex A), ISMS scope, incident management, business continuity, supplier security, access management
Applies to	Any organisation handling sensitive data — prerequisite for HDS
Overlaps	Foundation for HDS; supports GDPR Article 32 (technical measures); under-pins GAMP 5 infrastructure controls
What sets it apart	Horizontal security standard — not industry-specific; must be combined with sector regulations (GMP, HDS, GDPR)

ICH Q9 (R1)

RISK MANAGEMENT · GLOBAL (ICH)

Scope	Quality risk management across pharmaceutical operations
Key requirements	Risk assessment tools (FMEA, HAZOP, FTA), risk review, risk communication, integration into QMS and regulatory decision-making
Applies to	Pharma, biotech — any GxP operation
Overlaps	Provides the risk methodology used by GAMP 5 for software categorisation and by GMP for process validation
What sets it apart	Pure methodology standard — defines how to do risk management; referenced by virtually every other GxP framework

REACH / CLP

ENVIRONMENT / SAFETY · EU (ECHA)

Scope	Registration, evaluation, authorisation of chemicals; hazard communication
Key requirements	Substance registration (REACH), SVHC authorisation, safety data sheets (SDS), hazard labelling & packaging (CLP/GHS)
Applies to	Biotech companies manufacturing, importing or using chemical substances
Overlaps	Intersects with GLP (ecotoxicology data feeds REACH dossiers); links to GMP for excipient safety
What sets it apart	Covers the chemical substance itself (not the product/drug) — distinct regulatory pathway from medicinal product authorisation

HIAPP

EHEALTH / APPS · FRANCE (ANS / HAS)

Scope	Referencing and certification of digital health applications integrating the national ecosystem (Mon Espace Santé, ENS)
Key requirements	GDPR compliance, HDS hosting if personal health data, FHIR/HL7 interoperability, CE marking if SaMD, clinical or usage validation, consent management, accessibility (RGAA)
Applies to	Digital health app publishers, mHealth and DTC solutions targeting the French market or the national digital health bouquet
Overlaps	Built on GDPR, HDS and ISO 27001 as a foundation; aligns with ISO 13485 for apps with a medical claim (SaMD)
What sets it apart	National framework specific to Mon Espace Santé; jointly evaluates security, interoperability, clinical validity and user experience

CHAPTER 4

Four tensions to anticipate

Frameworks overlap, and sometimes contradict each other. Four friction points come up often; they are best handled when processes are designed.

1. Right to erasure (GDPR) versus retention (GxP)

The GDPR gives people the right to have their data erased; GxP rules require some records to be kept for up to 15 to 30 years. These two obligations are in direct tension. They call for case-by-case legal analysis and pseudonymization strategies that separate a person's identity from the data that must be kept.

2. GAMP 5 validation of SaaS and cloud tools

Validation obligations (GAMP 5, Annex 11) also apply to SaaS tools: EDC, LIMS, MES. Choosing a cloud provider means checking that it can supply the required validation documentation.

3. An HDS-certified hosting chain

Even if your own systems comply, the host of personal health data must hold HDS certification (French health data hosting). The obligation extends to every subcontractor in the chain: self-certification is not allowed.

4. Two pathways: REACH and medicines regulation

REACH covers the chemical substance itself; the authorization of the medicine or biologic (EMA, FDA) covers the product. A biotech may need to run both procedures in parallel for the same molecule.

CHAPTER 5

What digitized processes change

Most of the requirements listed in chapter 3 come down to a few questions: who did what, when, on which data, with what approval, and can it be proven? A process digitized end to end answers them natively.

- **Audit trail**: every entry, change and approval is recorded with its author and date (ALCOA+, 21 CFR Part 11, Annex 11).
- **Access management**: everyone sees and changes what their role allows (ISO 27001, GDPR).
- **Information entered once**: no more re-keying between tools, so fewer errors and consistent data.
- **Versions and signatures**: documents have a reference version and traced electronic approvals.
- **Retention and reversibility**: retention periods are enforced by the system, not by people's memory.
- **Evidence ready**: audit files are prepared in hours, from the processes' own data.

AI agents fit into this framework: they prepare, check and follow up, but their proposals go through human approval, and their actions leave the same trail as the teams'.

> Terminus 2π helps you bring your processes into compliance; certifications are still issued by accredited bodies.

CHAPTER 6

Choosing hosting to fit your constraints

There is no compliant hosting in the absolute, only hosting suited to your data and your obligations. Health data of French patients requires an HDS-certified host; clinical trial data adds GCP requirements; some organizations require their data to stay on-premises.

Liquid instances are deployed with global hosting providers (Google Cloud, AWS, Scaleway, OVH) or on-premises for organizations that prefer it. In our engagements, we help you choose the hosting that meets your compliance constraints: data location, certifications of the host and its subcontractors, reversibility, validation documentation.

CHAPTER 7

Where to start

Three steps are enough to turn compliance into an advantage:

1. **Map** your processes and identify the frameworks that apply to each.
2. **Prioritize** the processes where compliance costs the most: re-keying, manual evidence, audits prepared in a rush.
3. **Digitize** these processes end to end, so traceability becomes automatic.

The Express Process Diagnostic does exactly that in ten days: a map of your key processes, a measure of your time, quality and cost losses, and a costed action plan.

Let's talk about your constraints

Terminus 2π · Digital process first. AI at the core.

Website: terminus2pi.com · E-mail: contact@terminus2pi.com

LinkedIn: linkedin.com/company/terminus-2pi

This guide is provided for reference and is not legal or regulatory advice: check your situation with a qualified regulatory affairs consultant. Framework matrix and tensions after a synthesis published by Gencovery in 2025, reviewed and extended by Terminus 2π.