REGHELM | FREE RESOURCE

The Regulated Company's AI Governance Checklist

A practical, inspection-minded checklist for adopting AI in pharma, biotech & medtech - safely.

Use this before you let any AI tool touch regulated work. If you can tick most boxes, you're audit-ready. If you can't, those gaps are exactly where risk - and rework - hide.

Aligned in spirit to FDA/EMA expectations, ICH guidance, 21 CFR Part 11 and GxP principles. This is a readiness aid, not legal or regulatory advice.

1. Strategy & Use-Case Selection

- ☐ Each AI use-case has a clear business purpose and defined success measure.
- ☐ Use-cases are risk-ranked (patient safety / data integrity / decision impact).
- ☐ A human owner is accountable for every AI-assisted output.
- ☐ "Do not use AI" zones are defined (where risk is too high).

2. Data Readiness, Privacy & Security

- ☐ Training/input data sources are documented, lawful and fit for purpose.
- ☐ Personal / patient data handling complies with applicable privacy law (e.g. GDPR, HIPAA).
- ☐ Data quality, completeness and bias risks have been assessed.
- ☐ Access controls, encryption and data residency requirements are met.
- ☐ No confidential or regulated data is sent to ungoverned public AI tools.

3. Model / Vendor Selection & Validation

- ☐ AI vendors are assessed for security, compliance posture and data use terms.
- ☐ Model purpose, limitations and intended use are documented.
- ☐ The system is validated for intended use (GxP / computer system validation).
- ☐ Electronic records & signatures meet 21 CFR Part 11 where applicable (audit trails, access control, record integrity).
- ☐ Model versions and changes are controlled and traceable.

4. Human-in-the-Loop & Accountability

- ☐ A qualified human reviews and approves AI output before regulated use.
- ☐ The level of human oversight matches the risk of the use-case.

- ☐ Staff know AI is assistive - not a replacement for professional judgment.
- ☐ Escalation paths exist when AI output is wrong, uncertain or out of scope.

5. Documentation & Inspection Readiness

- ☐ AI use is documented: purpose, data, model, controls, validation, owners.
- ☐ Decisions influenced by AI are traceable and reconstructable.
- ☐ You could explain to an inspector how the AI works and how it's controlled.
- ☐ Records are retained per your retention and GxP requirements.

6. Risk, Monitoring & Lifecycle

- ☐ AI outputs are monitored for drift, errors and degradation over time.
- ☐ Performance and incidents are logged and periodically reviewed.
- ☐ A defined process handles model updates, retraining and retirement.
- ☐ A rollback / contingency plan exists if the AI must be switched off.

7. Governance Structure & Policy

- ☐ A written AI policy defines acceptable use, roles and approval gates.
- ☐ An AI governance owner or committee is accountable across functions.
- ☐ Staff are trained on safe, compliant AI use.
- ☐ Governance keeps pace with evolving FDA/EMA and ICH guidance.

How did you score?

Mostly ticked? You're in strong shape - keep governance current as guidance evolves.

Several blanks? Those gaps are where audit findings and stalled pilots come from. They're fixable - usually faster than teams expect.

Want help closing the gaps - or a governance framework built for your team? I build inspection-ready AI governance and validation for regulated life-sciences companies, and rescue stalled AI pilots. Fahad Syeed | fahad@reghelm.com | +91 97404 66633