COMPLIANCE ASSESSMENT

01

# Healthcare & Hospitals Compliance Assessment

A structured checklist for evaluating your AI and software vendor's readiness across HIPAA, HITECH, FDA 21 CFR Part 11, and SOC 2 Type II obligations.

# Contents

## 01 — REGULATORY FRAMEWORKS COVERED

- ☐ HIPAA / HITECH
- ☐ FDA 21 CFR Part 11
- ☐ SOC 2 Type II
- ☐ HL7 FHIR R4
- ☐ ONC Cures Act

This assessment covers the primary regulatory and compliance frameworks your technology vendor must address. Each section below maps directly to one or more of these frameworks.

## 02 — DATA HANDLING & PHI CONTROLS

- [ ] BAA executed with all data processors
- [ ] PHI encrypted at rest (AES-256) and in transit (TLS 1.2+)
- [ ] Access controls limited to minimum-necessary principle
- [ ] Audit logs retained for minimum 6 years
- [ ] De-identification procedures documented per Safe Harbor or Expert Determination
- [ ] Breach notification procedures defined and tested annually
- [ ] Employee HIPAA training completed within last 12 months

## 03 — TECHNICAL SAFEGUARDS

- [ ] Automatic logoff after session inactivity
- [ ] Unique user identification for all system access
- [ ] Emergency access procedures documented
- [ ] Encryption and decryption mechanisms in place
- [ ] Multi-factor authentication on all PHI systems
- [ ] Vulnerability scanning conducted quarterly
- [ ] Penetration test within last 12 months

## 04 — FDA 21 CFR PART 11 (SAMD)

- [ ] System validation documentation complete
- [ ] Audit trails enabled and tamper-evident
- [ ] Electronic signatures linked to records
- [ ] Access controls by role with documented authority
- [ ] Computer-generated records reviewed for accuracy
- [ ] Training records maintained for all users

## 05 — VENDOR DUE DILIGENCE

- [ ] SOC 2 Type II report reviewed within last 12 months
- [ ] Subprocessor list reviewed and approved
- [ ] Data Processing Agreement (DPA) executed
- [ ] Incident response SLA defined (target: <72 hours)
- [ ] Business continuity plan tested within last 12 months
- [ ] Right-to-audit clause in vendor contract

## SCORING GUIDE

Score 1 point for each confirmed item. 25–28: Compliant. 18–24: Needs remediation. Below 18: Urgent review required.

## NEXT STEPS

If your score falls below the compliant threshold, The Algorithm offers a structured gap remediation programme:

1. Technical gap audit (2 weeks)
2. Remediation roadmap with prioritised backlog
3. Engineering sprint to close critical gaps
4. Evidence package for regulatory review

Contact us at contact@the-algo.com or visit the-algo.com/contact

# Ready to talk?

We audit your current vendor, map the gaps, and present a structured migration plan — no commitment required.

**the-algo.com/contact**