GovSoft

AI GOVERNANCE TOOLKIT

Regulated Industry AI Compliance Checklist

Sector-Specific AI Governance for Healthcare (HIPAA), Financial Services & Insurance

Scan for governance consulting

www.govsoft.us/contact

AGT-004 Rev 06/2026

BEFORE YOU DEPLOY IN A REGULATED SECTOR

Every regulated industry has its own history of harm that explains why its rules exist. Healthcare regulations grew from experiments conducted without informed consent. Financial regulations followed crises where opaque instruments destroyed livelihoods. Insurance regulations emerged because actuarial decisions can exclude entire communities from protection. AI does not change these histories; it accelerates them.

govsoft.us/contact

00 RESPONSIBLE PARTIES

Complete this section first. Assign a unique ID (up to 4 characters, such as initials) to each party. These IDs are used throughout the checklist to record who is assigned, completes, and verifies each item.

ID	ROLE	NAME	DATE
	Compliance Officer		
	Sector-Specific Counsel		
	Regulatory Affairs Lead		
	Clinical/Business Owner		
	IT Security Officer		

01 HEALTHCARE / HIPAA

	ASSIGNED	DONE	VERIFIED
☐ AI system classified under FDA regulatory framework (SaMD, clinical decision support, or exempt).	ID / DATE	ID / DATE	ID / DATE
☐ Business Associate Agreement (BAA) executed with all AI vendors handling PHI.	ID / DATE	ID / DATE	ID / DATE
☐ HIPAA Security Rule requirements verified for AI system components.	ID / DATE	ID / DATE	ID / DATE
☐ Minimum necessary standard applied to PHI used in AI training and inference.	ID / DATE	ID / DATE	ID / DATE
☐ Patient notification procedures established for AI-assisted clinical decisions.	ID / DATE	ID / DATE	ID / DATE
☐ Clinical validation completed per intended use case and patient population.	ID / DATE	ID / DATE	ID / DATE
☐ AI system integrated into existing quality assurance and patient safety programs.	ID / DATE	ID / DATE	ID / DATE
☐ Clinician training completed on AI system capabilities and limitations.	ID / DATE	ID / DATE	ID / DATE

	ASSIGNED	DONE	VERIFIED
☐ Override and escalation procedures documented for AI-assisted clinical decisions.	ID / DATE	ID / DATE	ID / DATE
☐ Adverse event reporting procedures established for AI-related incidents.	ID / DATE	ID / DATE	ID / DATE
☐ PHI de-identification verified for any AI training data (Safe Harbor or Expert Determination).	ID / DATE	ID / DATE	ID / DATE

BAA Executed With: _____

Date: _____

02 FINANCIAL SERVICES

	ASSIGNED	DONE	VERIFIED
☐ AI model risk management framework established per OCC 2011-12 / SR 11-7.	ID / DATE	ID / DATE	ID / DATE
☐ Model validation completed by independent risk management function.	ID / DATE	ID / DATE	ID / DATE
☐ Fair lending analysis completed for AI-driven credit and lending decisions.	ID / DATE	ID / DATE	ID / DATE
☐ Adverse action notice procedures updated to explain AI-influenced decisions.	ID / DATE	ID / DATE	ID / DATE

	ASSIGNED	DONE	VERIFIED
☐ CFPB adverse action guidance compliance verified.	ID / DATE	ID / DATE	ID / DATE
☐ Anti-money laundering (AML) AI models validated against regulatory expectations.	ID / DATE	ID / DATE	ID / DATE
☐ Customer-facing AI disclosures drafted and reviewed by compliance.	ID / DATE	ID / DATE	ID / DATE
☐ Model inventory updated to include all AI/ML models with risk classifications.	ID / DATE	ID / DATE	ID / DATE
☐ Stress testing and scenario analysis completed for AI model performance.	ID / DATE	ID / DATE	ID / DATE
☐ Board and senior management reporting established for AI model risk.	ID / DATE	ID / DATE	ID / DATE

Model Risk Owner: _____

Model ID: _____

03 INSURANCE

	ASSIGNED	DONE	VERIFIED
☐ NAIC AI Principles reviewed and compliance mapped.	ID / DATE	ID / DATE	ID / DATE

	ASSIGNED	DONE	VERIFIED
☐ Actuarial AI models reviewed for unfair discrimination.	ID / DATE	ID / DATE	ID / DATE
☐ Rate-setting AI models filed with applicable state insurance departments.	ID / DATE	ID / DATE	ID / DATE
☐ Consumer notification procedures established for AI-driven underwriting decisions.	ID / DATE	ID / DATE	ID / DATE
☐ Adverse underwriting decision explanations updated to address AI involvement.	ID / DATE	ID / DATE	ID / DATE
☐ Claims processing AI reviewed for consistency and fairness.	ID / DATE	ID / DATE	ID / DATE
☐ Third-party AI vendor governance requirements established per NAIC guidance.	ID / DATE	ID / DATE	ID / DATE
☐ Proxy discrimination testing completed (race, gender, disability, other protected classes).	ID / DATE	ID / DATE	ID / DATE
☐ State-specific AI insurance regulations reviewed (Colorado, Connecticut, other).	ID / DATE	ID / DATE	ID / DATE
☐ Complaints process updated to handle AI-related consumer concerns.	ID / DATE	ID / DATE	ID / DATE

	ASSIGNED	DONE	VERIFIED
☐ Annual AI fairness review schedule established with actuarial sign-off.	ID / DATE	ID / DATE	ID / DATE

State(s) Filing Required: _____

04 CROSS-SECTOR REQUIREMENTS

	ASSIGNED	DONE	VERIFIED
☐ NIST AI RMF sector profile completed for applicable industry.	ID / DATE	ID / DATE	ID / DATE
☐ Anti-discrimination testing completed across all protected classes.	ID / DATE	ID / DATE	ID / DATE
☐ Vendor AI governance requirements included in all relevant contracts.	ID / DATE	ID / DATE	ID / DATE
☐ Incident response plan updated to cover AI-specific failure modes.	ID / DATE	ID / DATE	ID / DATE
☐ Regulatory change monitoring established for AI-related guidance.	ID / DATE	ID / DATE	ID / DATE
☐ Third-party AI audit scheduled with qualified auditor.	ID / DATE	ID / DATE	ID / DATE

	ASSIGNED	DONE	VERIFIED
☐ Consumer/patient/customer complaint mechanism established for AI concerns.	ID DATE	ID DATE	ID DATE
☐ Cross-sector regulatory mapping completed (identify overlapping requirements).	ID DATE	ID DATE	ID DATE

Third-Party Audit Scheduled: _____

Date: _____

05 SIMPLE STEPS

1. Identify regulated sector(s)
2. Verify sector compliance covers AI
3. Update vendor agreements
4. Complete anti-discrimination testing
5. Establish monitoring and complaints
6. Schedule regulatory review

06 DECISION POINT

SECTOR RULES

Sector regulations impose stricter requirements
Sector rules take precedence over general AI governance

CONSULT COUNSEL

General AI governance and sector regulations conflict
Regulator issues new AI-specific guidance
Novel use case without regulatory precedent

DO NOT DEPLOY

Sector-specific compliance not confirmed
General AI governance alone is insufficient
Regulated industry requires explicit sector approval

⚠ COMMON PITFALLS

PITFALL	WHY IT MATTERS
Treating AI governance as purely an IT function	In regulated industries, AI governance is a compliance function. IT implements; compliance, legal, and clinical/business leadership must govern.
Ignoring sector regulators who reference NIST AI RMF	The FTC, CFPB, FDA, SEC, and EEOC all reference NIST AI RMF principles in enforcement guidance. "We did not know" is not viable.
Assuming vendor HIPAA or SOC 2 compliance covers AI	A vendor's general security compliance does not address AI-specific risks like model bias, training data provenance, or clinical validation.

FRAMEWORKS REFERENCED

- HIPAA Security Rule
- Treasury Financial Services AI RMF (February 2026)
- OCC Bulletin 2011-12
- Federal Reserve SR 11-7
- NIST AI RMF Sector Profiles
- NAIC AI Principles
- CFPB Adverse Action Guidance

For planning purposes only. This checklist is a compliance planning aid for regulated industries. Sector-specific regulations are subject to change. Verify current requirements with legal counsel, regulatory affairs, and applicable regulatory bodies before deployment.