AI Governance Compliance Checklist

Compliancy Group | Healthicity — A COMPLIANCY GROUP COMPANY

A companion to the *An AI Compliance Framework for Healthcare* webinar.

1. AI Policies and Governance Structures

RUAIH 1 · OIG 1, 2 · NIST GOVERN

- [ ] Establish a multidisciplinary AI governance committee spanning legal, IT and security, compliance, clinical, and business stakeholders.
- [ ] Assign a single accountable owner for AI risk, and designate an individual responsible for AI quality and safety issues.
- [ ] Extend existing HIPAA security, quality, and patient safety structures to cover AI rather than building a parallel one.
- [ ] Adopt written AI policies and procedures tied to the code of conduct, and align them with related internal policies and external regulatory and ethical frameworks.
- [ ] Document the committee charter, meeting cadence, and escalation path; review and update policies as strategy and regulations shift.
- [ ] Update the fiduciary board regularly on AI use and its outcomes.

2. AI Inventory and Risk Classification

OIG 6 · NIST MAP

- [ ] Maintain a living inventory of every AI tool in use: clinical, care support, administrative, and vendor-embedded.
- [ ] Classify each tool by proximity to patient care decisions, PHI exposure, and degree of autonomy.
- [ ] Complete a pre-deployment impact assessment for new tools (data touched, decisions affected, bias testing, human oversight, accountable owner).
- [ ] Use a recognized framework such as the NIST AI Risk Management Framework to structure the assessment.
- [ ] Reassess at least annually, and more often for tools close to clinical or coverage decisions.

RUAIH: Joint Commission and CHAI Guidance on the Responsible Use of AI in Healthcare (September 2025). OIG: seven elements of an effective compliance program, HHS OIG General Compliance Program Guidance (2023). NIST: AI Risk Management Framework 1.0, NIST AI 100-1 (January 2023). Informational only. **Not legal advice.**

3. Patient Privacy and Transparency

RUAIH 2 · OIG 1 · NIST MEASURE 2.8

- [ ] Adopt policies on data access, use, and protection under applicable state and federal law.
- [ ] Build a mechanism to disclose and educate patients and families on how AI tools are used and the benefit they provide.
- [ ] Address transparency for staff as well as patients: where AI sits in the workflow and what it does.
- [ ] Notify patients when AI directly impacts their care and how their data may be used; obtain consent where relevant.
- [ ] Ensure public-facing disclosures about AI activity match actual system capabilities.

4. Data Security and Data Use Protections

RUAIH 3 · OIG 1 · NIST GOVERN 6

- [ ] Map PHI flow through each AI system: training data, prompts and inputs, outputs, logging, and vendor retention.
- [ ] Confirm HIPAA Privacy, Security, and Breach Notification compliance; execute BAAs and apply the minimum necessary standard.
- [ ] Encrypt patient data in transit and at rest; enforce strict access controls and audit access logs regularly.
- [ ] Run regular security assessments and vulnerability scans on AI systems and their integrations.
- [ ] De-identify under Safe Harbor or Expert Determination where feasible, and keep watching for re-identification risk.
- [ ] In data use agreements: define permitted uses (including model outputs, local performance data, and monetization), require data minimization, prohibit re-identification, bind third parties to the same controls, and reserve audit rights with penalties.

5. Ongoing Quality Monitoring

RUAIH 4 · OIG 6 · NIST MEASURE

- [ ] At procurement, ask how the tool was validated for its intended use, whether the vendor will tune or validate on a representative local sample, and how biases were evaluated.
- [ ] Name the parties responsible for local monitoring, and settle monitoring responsibility in the contract.
- [ ] Validate and test performance and reliability on a schedule; compare outputs to known parameters.
- [ ] Scale monitoring frequency to risk: tools that inform clinical decisions get checked more often than documentation tools.
- [ ] Build an AI dashboard and confirm tools rely on up-to-date data.
- [ ] Set feedback channels so vendor model changes trigger an unplanned performance check.

RUAIH: Joint Commission and CHAI Guidance on the Responsible Use of AI in Healthcare (September 2025). OIG: seven elements of an effective compliance program, HHS OIG General Compliance Program Guidance (2023). NIST: AI Risk Management Framework 1.0, NIST AI 100-1 (January 2023). Informational only. **Not legal advice.**

6. Voluntary, Blinded Reporting of AI Safety Events

RUAIH 5 · OIG 4, 7 · NIST MANAGE 4.3

- [ ] Capture AI-related near misses and harm in internal incident systems: unsafe recommendations, degradation after an update, biased outputs.
- [ ] Submit de-identified details through a Patient Safety Organization or other confidential channel; use FDA pathways for regulated devices.
- [ ] Update the categories of incident you track so AI events are captured rather than filed as user error.
- [ ] Open a confidential, non-retaliatory channel for staff to raise AI concerns, and route it to the compliance officer.
- [ ] Add AI-specific scenarios to the incident response plan (PHI surfaced in output, vendor or subprocessor mishandling, model drift).
- [ ] Define escalation, correction, and refund procedures for AI-driven errors.

7. Risk and Bias Assessment

RUAIH 6 · OIG 6 · NIST MEASURE 2.11

- [ ] Categorize and document the potential risks and biases of each tool across relevant domains.
- [ ] Request vendor information on known risks, biases, limitations, and which populations bias was evaluated for. A model card collects it well.
- [ ] Confirm the tool used fit-for-purpose, representative training data and underwent bias detection in development.
- [ ] Verify the algorithm is tested and tuned for the populations you serve, using local data where possible.
- [ ] Test before deployment and keep auditing after, then record the results.
- [ ] Document human oversight and override for any output influencing a clinical or coverage decision.

8. Education and Training

RUAIH 7 · OIG 3, 5 · NIST GOVERN 2.2

- [ ] Define and document how users receive tool documentation and role-specific training.
- [ ] Train clinicians and staff on proper use, limitations, and guidelines for use, and collect a signed attestation.
- [ ] Decide which tools require training before implementation and which require recurring training.
- [ ] Run broader AI literacy and change management education, with common terminology across the organization.
- [ ] Make it clear where staff can find tool information and the organization's AI policies.
- [ ] Define consequences for unauthorized AI use and incentives that reinforce compliant use.

RUAIH: Joint Commission and CHAI Guidance on the Responsible Use of AI in Healthcare (September 2025). OIG: seven elements of an effective compliance program, HHS OIG General Compliance Program Guidance (2023). NIST: AI Risk Management Framework 1.0, NIST AI 100-1 (January 2023). Informational only. **Not legal advice.**

9. Vendor Management and Legal Review

OIG 1, 6 · NIST MAP 4

- [ ] Update BAAs to explicitly cover AI training use, model inputs, and downstream data use.
- [ ] Confirm BAAs clearly delineate breach notification procedures.
- [ ] Involve in-house counsel as an active AI governance stakeholder, not only as a technology matter.
- [ ] Assess litigation exposure created by AI tools (malpractice, False Claims Act, discrimination claims).
- [ ] Verify subcontractor and subprocessor AI use is disclosed and contractually covered.

10. Billing, Coding, and Program Oversight

OIG 6, 7 · NIST MANAGE

- [ ] Audit AI-assisted billing and coding output with the same rigor applied to manually coded claims.
- [ ] Keep AI-generated claims inside the audit sample rather than exempt from it.
- [ ] Report AI status to the board on a set cadence: inventory, incidents, regulatory developments.
- [ ] Prepare transparency documentation for AI-generated claim review or coverage decisions.
- [ ] Disclose generative AI use in compliance program work if you are operating under a Corporate Integrity Agreement.
- [ ] Document a corrective action plan with root cause for every substantiated AI-driven error, and verify the fix held.

QUICK-REFERENCE REGULATORY WATCHLIST

- **Joint Commission and CHAI** Responsible Use of AI in Healthcare guidance, playbooks, and voluntary certification
- **OIG** CIA template now requires generative AI use disclosure
- **OCR** proposed HIPAA Security Rule update reaching AI systems
- **CMS** guidance against AI-only coverage denials
- **FDA** SaMD and Clinical Decision Support classification
- **HHS Section 1557** nondiscrimination in AI-enabled tools
- **State AI laws** transparency and bias-prevention requirements
- **State attorneys general** consumer protection enforcement on AI accuracy claims

RUAIH: Joint Commission and CHAI Guidance on the Responsible Use of AI in Healthcare (September 2025). OIG: seven elements of an effective compliance program, HHS OIG General Compliance Program Guidance (2023). NIST: AI Risk Management Framework 1.0, NIST AI 100-1 (January 2023). Informational only. **Not legal advice.**

Three-Framework Crosswalk

Every checklist section maps to all three frameworks. One program satisfies the Joint Commission and CHAI guidance, the OIG seven elements, and the NIST AI Risk Management Framework at once.

CHECKLIST SECTION	RUAIH	OIG	NIST AI RMF
1. AI Policies and Governance	1	1, 2	Govern 1 to 4
2. AI Inventory and Risk Classification	–	6	Govern 1.6, Map 1 to 3
3. Patient Privacy and Transparency	2	1	Measure 2.8, 2.10
4. Data Security and Data Use	3	1	Govern 6, Measure 2.7
5. Ongoing Quality Monitoring	4	6	Measure 2.3, 2.4
6. Voluntary, Blinded Reporting	5	4, 7	Manage 4.3, Govern 4.3
7. Risk and Bias Assessment	6	6	Measure 2.11, Map 5
8. Education and Training	7	3, 5	Govern 2.2, Map 3.4
9. Vendor Management and Legal	3, 4	1, 6	Govern 6, Map 4, Manage 3
10. Billing, Coding, Program Oversight	–	6, 7	Manage 1, 4

RUAIH: Joint Commission and CHAI Guidance on the Responsible Use of AI in Healthcare (September 2025). OIG: seven elements of an effective compliance program, HHS OIG General Compliance Program Guidance (2023). NIST: AI Risk Management Framework 1.0, NIST AI 100-1 (January 2023). Informational only. **Not legal advice.**