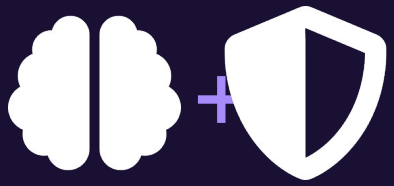


AI & HIPAA Compliance

What Healthcare & Health Tech Companies Must Know in 2026

46% of US healthcare organizations are already implementing GenAI

An Infinitra Innovations Initiative

healthtechcompliance.com

HIPAA Wasn't Written for AI

But every existing HIPAA rule still applies to AI systems that touch PHI.

1st

major update in 20 years

The 2025 proposed HIPAA Security Rule now explicitly names AI systems

Expected to be finalized May 2026

AI = Business Associate

Any AI vendor processing PHI must be under a BAA

AI = Risk Analysis Required

AI tools must be included in your HIPAA risk assessment

AI Training = PHI Rules Apply

PHI used in training data must be de-identified or fully compliant

Business Associate Agreements for AI

If an AI vendor touches PHI on your behalf, a BAA is legally required.

Safeguard PHI

Vendor must implement Security Rule protections

Minimum Necessary

Access only the PHI essential for the function

AI Training Limits

Address if and how PHI can be used for model training

Subcontractor Flow

Requirements must flow down to sub-processors

Breach Reporting

Vendor must report security incidents promptly

Data Return/Destroy

PHI handling upon contract termination

PHI in AI Training Data

The FTC has ordered companies to destroy AI models built with improperly collected health data.

Path 1: De-Identify the Data

Safe Harbor Method

Remove all 18 identifiers listed in 45 CFR §164.514(b)(2): Names, dates, ZIP codes, phone numbers, SSN, etc.

Expert Determination

A qualified statistical expert certifies re-identification risk is "very small"

Path 2: Full HIPAA Compliance

- BAA with AI vendor in place
- Encryption at rest and in transit
- Role-based access controls
- Audit logging for all PHI access
- Minimum necessary standard enforced
- Breach notification procedures
- Risk analysis covering AI workflows

AI-Specific Risk Analysis

The 2025 proposed HIPAA Security Rule update requires AI in your technology asset inventory.

1	**Inventory All AI Tools**	Document every AI system that creates, receives, maintains, or transmits ePHI
2	**Map Data Flows**	Trace how PHI moves into, through, and out of each AI system
3	**Assess Threats**	Evaluate data leakage, model bias, unintended PHI exposure during training
4	**Evaluate Controls**	Use NIST AI Risk Management Framework to assess privacy, fairness, security
5	**Document & Monitor**	Written risk analysis with regular updates as AI capabilities change

Reference: NIST AI Risk Management Framework | 45 CFR §164.308(a)(1)

State AI Laws Layering on HIPAA

No federal AI law yet — states are setting the rules. These take effect in 2026.

TEXAS
Patient Disclosure Required
Effective Jan 1, 2026

- Written disclosure before AI is used in diagnosis or treatment
- Must be provided before or at time of interaction
- Applies to all AI-assisted clinical decisions

COLORADO
Toughest AI Act in the US
Effective Jun 30, 2026

- Disclosure when AI is used in high-risk decisions
- Annual impact assessments required
- Anti-bias controls and 3-year record-keeping

CALIFORNIA
No Fake Credentials
Effective Jan 1, 2026

- AI systems cannot imply they hold a healthcare license
- Prohibits misleading terms or design elements
- Applies to both developers and deployers

More states expected to follow — Indiana, Kentucky, Rhode Island privacy laws also effective Jan 2026

AI Workforce Training Gaps

Your staff is probably using AI tools right now. Do they know the rules?

What Staff Get Wrong

- Entering PHI into ChatGPT or similar tools without a BAA
- Using AI-generated content without clinical verification
- Sharing ePHI with AI tools via copy-paste
- Assuming "anonymized" data is truly de-identified

What Training Must Cover

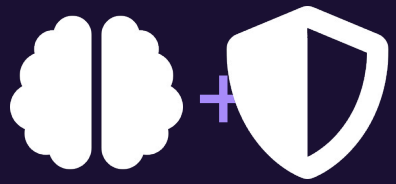
- Which AI tools have BAAs and are approved for use
- Risks of AI confabulation combining unrelated data
- Proper de-identification before using AI tools
- Reporting procedures for AI-related PHI incidents

Penalties: Up to $50,000 per violation | Criminal penalties up to $250K and 10 years

Your AI + HIPAA Compliance Checklist

- [ ] Inventory all AI systems that interact with ePHI — CRITICAL
- [ ] Execute BAAs with every AI vendor processing PHI — CRITICAL
- [ ] Include AI tools in your HIPAA risk analysis — CRITICAL
- [ ] Verify PHI de-identification in AI training data — CRITICAL
- [ ] Update workforce training to cover AI-specific risks — HIGH
- [ ] Review state AI disclosure laws (TX, CO, CA) — HIGH
- [ ] Implement audit logging for AI system access — HIGH
- [ ] Update BAA templates with AI-specific language — HIGH
- [ ] Establish AI governance and oversight committee — MEDIUM
- [ ] Prepare for Joint Commission AI certification (2026) — MEDIUM

Assess your full HIPAA compliance posture at navigator.healthtechcompliance.com



Is Your AI Strategy HIPAA Compliant?

Take the free HIPAA Compliance Assessment

navigator.healthtechcompliance.com

50 questions | 15 minutes | Free | No email required

An Infinitra Innovations Initiative

Built by Ex-AWS Leaders: Saida Babu Chanda & Yogananda Karra