Transformativ IP

Criminal and Civil Penalties For Healthcare Regulatory Non-Compliance

State and Federal Regulations on AI, Privacy, Healthcare, PBMs, FDXs for Hospital CEOs, CTOs, and CISOs,

Executive Summary

The compliance landscape has fundamentally changed. It is no longer just a financial risk, it is now also a personal criminal risk for healthcare executives

The U.S. regulatory environment drastically changed in 2025–2026, with new state laws governing **AI, data privacy, healthcare, PBM, and financial data.** Non-compliance now poses a personal criminal risk, including simultaneous prosecution, imprisonment, and multi-million dollar fines for both organizations and individual executives.

Three Critical Shifts:

1. **Criminalization:** States increasingly treat violations as criminal, with maximum prison terms up to 40 years (Arkansas/healthcare fraud) and 50 years (Nebraska/AI-related child exploitation).

2. **Cumulative Fines:** Per-violation structures can generate cumulative civil penalties in the hundreds of millions (e.g., Maine's CDPA: up to $30 million per repeated violation).

3. **Accelerated Enforcement:** States (NH, OR, RI) have eliminated or shortened "cure periods," shifting from compliance coaching to immediate enforcement.

There is a new strategic imperative for hospital executives to view compliance as an enterprise-level strategic priority due to the cumulative exposure risk when a single incident triggers violations across multiple regulatory domains.

This document reviews civil and criminal penalties across the AI, Privacy, Healthcare, PBMs, FDXs domains, identifying and ranking the states with the most severe combined penalties.

5 Tables for the Worst State Penalties for Regulatory Non Compliance (with Discussions)

Table 1 — AI Reg Violations: Discussion of Most Severe States Penalties

---

- ***AI Governance Failures Now Carry Felony Charges and Multi-Decade Prison Sentences***
- ***Emerging AI Laws Create Direct Criminal Exposure for Hospital Technology Leaders***

Artificial intelligence regulation has accelerated at a pace that many hospital technology leaders have not yet matched internally. As of early 2026, states are targeting deepfake creation and distribution, unauthorized AI use in healthcare decision-making, algorithmic discrimination in employment and insurance, and the exploitation of minors through AI-generated content.

The severity of these penalties should command immediate board-level attention.

Nebraska: authorizes up to 50 years imprisonment for AI-related Class 1D felonies.

Louisiana: extends sentences to 50 years when AI is used to generate child exploitation material.

Utah: penalty range of 3.5 to 25 years for AI-assisted fraud spans nearly every category of serious felony.

New York: RAISE Act introduces civil exposure of up to $30 million for frontier AI violations — and this applies to any organization deploying advanced AI systems in patient care, utilization review, or administrative functions.

For hospital CTOs and CISOs specifically: the deployment of AI in clinical decision support, prior authorization workflows, or patient-facing applications without documented governance

frameworks and human oversight protocols is no longer merely a quality-of-care concern. It is a criminal compliance risk.

Table 1 — AI Reg Violations: Table of States with the Most Severe Penalties

State	Max Civil Penalty	Max Criminal Fine	Max Imprisonment
New York	$10M–$30M (RAISE Act)	N/A (civil focus)	N/A (civil)
Utah	$3M (frontier models)	$10,000 (deepfake fraud)	3.5–25 years (CSAM)
New Hampshire	$200,000/violation	Class B Felony fine	Up to 7 years
Texas	$80,000–$200,000/violation	N/A (TRAIGA civil)	N/A (civil)
West Virginia	$100,000/day (orgs)	$10,000 (deepfakes)	1–5 years
Missouri	$5,000–$100,000/violation	$2,500 (Class A misd.)	Up to 1 year
Colorado	$20,000–$50,000/violation	N/A	N/A
Pennsylvania	$5,000–$500,000 (aggregate)	$15,000 (3rd-degree felony)	Up to 7 years
Michigan	TBD (proposed rules)	$50,000+ (felony fine)	4–8 years
Illinois	$16,000–$70,000 (employment)	N/A (civil focus)	N/A
Kansas	$50,000/violation (SB 405)	$100,000+ (genetic data felony)	5–20+ years
Rhode Island	$50,000/violation (healthcare AI)	N/A (civil)	N/A
Louisiana	$10,000/violation (healthcare)	$50,000 (minors deepfakes)	10–50 years (minors)
California	$1M (AG actions) / $5,000/day	$10,000–$250,000	Up to 3 years
Massachusetts	$500,000 (child safety)	$10,000–$50,000 (CSAM)	Up to 10 years
Nebraska	$7,500–$50,000/violation	$25,000 (Class III felony)	Up to 50 years (1D felony)
Georgia	$50,000 (computer crimes)	$50,000 (felony)	1–15 years
Hawaii	$15,000–$20,000/day	Deepfake fine	Up to 4 years
Florida	$50,000/violation (proposed)	$1,000 (misdemeanor)	Up to 1 year
Minnesota	$100,000 (sexual deepfakes)	$10,000 (felony)	Up to 5 years

Table 2 — Privacy Regulatory Violations: States with the Most Severe Penalties

- ***Data Breaches Are No Longer Financial Events Alone — They Are Criminal Exposures***
- ***State Privacy Laws Now Subject CISOs and Senior Leadership to Personal Prosecution***

State	Max Civil Penalty	Max Criminal Fine	Max Imprisonment
Maine	$10M–$30M (LD 1088)	N/A (civil only)	N/A
New York	$250,000 (SHIELD Act cap)	$250,000 (HIPAA criminal)	Up to 10 years (HIPAA)
California	$250,000/violation (CMIA)	$250,000 (intent to sell)	Up to 1 year
New Hampshire	$10,000–$100,000/violation	Felony for entities	Misdemeanor/Felony
Florida	$50,000–$150,000/violation	N/A (civil focus)	N/A
Colorado	$20,000/violation ($500K agg.)	N/A	N/A
Oklahoma	$150,000/breach	N/A (AG exclusive)	N/A
Nebraska	$7,500–$50,000/violation	N/A (civil)	N/A
Georgia	$7,500/violation (SB 473)	$50,000 (computer crimes)	Up to 15 years
Vermont	$10,000–$25,000/violation	N/A (civil)	N/A
Maryland	$10,000–$25,000/violation	$1,000 (misdemeanor)	Up to 1 year
Hawaii	$10,000/violation/day	$2,000 (govt employees)	Up to 1 year
South Dakota	$10,000/day/violation	$250,000 (HIPAA)	Up to 10 years (HIPAA)
Illinois	$5,000/violation (BIPA)	$25,000/category/year	N/A
Rhode Island	$10,000/violation	$500 (knowing disclosure)	Up to 1 year (HIPAA)
Oregon	$7,500/violation (OCPA)	Class C felony possible	Varies
Texas	$7,500/violation (TDPSA)	Computer Crimes Act	Misdemeanor to 1st-degree felony
Virginia	$7,500/violation ($2.5M cap)	$250,000 (HIPAA)	1–10 years (HIPAA)
Tennessee	$7,500–$22,500/violation	N/A (civil)	N/A
North Carolina	$2,500–$1.5M/year	Class 2 misdemeanor	Up to 60 days

Table 2 — Privacy Reg Violations: Discussion of States with Worst Penalties

The state privacy landscape has matured dramatically since California's initial CCPA framework. By 2026, over 20 states have enacted comprehensive consumer data protection laws, most modeled after Virginia's VCDPA or Connecticut's approach — but with increasingly aggressive penalty structures that go well beyond the original California model.

Maine: stands apart with its Consumer Data Privacy Act, which authorizes civil fines of up to $30 million for repeated violations.

Georgia: computer crimes statute carries up to 15 years of imprisonment for data-related offenses.

Oklahoma: authorizes breach-specific civil penalties of up to $150,000 per incident, with no cure period available.

Texas: extends potential criminal exposure to first-degree felony charges under its Computer Crimes Act for knowing violations.

Critically, HIPAA federal penalties overlay every one of these state regimes, adding criminal exposure of up to 10 years imprisonment and $250,000 in fines specifically for malicious disclosure of protected health information.

For hospital CISOs, this means a ransomware incident or insider data theft event triggers parallel enforcement tracks at both the state and federal levels — simultaneously.

The elimination of mandatory cure periods in **New Hampshire, Oregon, and Rhode Island** signals that the days of self-reporting a breach and receiving an opportunity to remediate before penalty assessment are ending.

Table 3 — Healthcare Regulatory Violations: States w/ Most Severe Penalties

---

- ***Healthcare Penalties Now Include Life Imprisonment and 40-Year Felony Sentences***
- ***Clinical Operations, Revenue Cycle, and AI-Driven Utilization Review All Carry Escalating Criminal Risk***

Healthcare regulatory penalties remain the most severe of all five domains analyzed, a reflection of the life-and-safety stakes that legislators associate with healthcare fraud, data misuse, and patient harm. The numbers documented in the table below represent an existential risk profile that hospital CEOs and their boards must engage with directly.

State	Max Civil Penalty	Max Criminal Fine	Max Imprisonment
New York	$50,000/violation (AI mental health)	$250,000 + 2x gain (fraud)	1–25 years (fraud)
Montana	$50,000 (felony fine)	$50,000 (health code felony)	Up to 20 years
Illinois	$25,000–$50,000 (corp.)	$250,000 (data misuse)	Up to life (death results)
Georgia	$500,000/violation (kickbacks)	$500,000 (felony)	Up to 10 years
Idaho	$25,000/breach (civil)	$15,000 (insurance fraud)	Up to 15 years
New Hampshire	$5,500–$11,000/claim + 3x damages	Medicaid fraud fine	3.5–7 years
Pennsylvania	$50,000/violation (HIPAA)	$250,000 (HIPAA criminal)	Up to 10 years
West Virginia	$50,000/violation (HIPAA)	$250,000 (intent to sell)	Up to 10 years
Oklahoma	$500,000/year (aggregate)	$100,000/violation	Felony (varies)
Louisiana	$20,000/month (repeat)	$250,000 (intent to sell)	Up to 10 years
Kentucky	$50,000 (organ brokering)	$250,000 (HIPAA malicious)	Up to 10 years
Florida	$50,000/violation (HIPAA)	$250,000 (intent to sell)	Up to 10 years
California	$250,000/violation (CMIA)	$250,000 (criminal)	Up to 1 year
New Jersey	$5,000–$25,000 (records)	$50,000 (kickbacks)	3–5 years
Michigan	$50,000/violation (HIPAA)	$250,000 (malicious)	Up to 10 years
Massachusetts	$25,000/week (reporting)	$250,000 (data misuse)	Up to 10 years
Alabama	$100,000/act (Medicaid)	$30,000 (Class B felony)	2–20 years
Minnesota	$7,500/violation	$250,000 (HIPAA)	Up to 10 years
Wisconsin	$10,000/claim + 3x damages	Up to $100,000	10–20 years (fraud)
Arkansas	$10,000/violation	Class Y felony fine	Up to 40 years (fraud)

Table 3 — Healthcare Reg Violations: Discussion of Worst State Penalties

New York: imposes some of the nation's most severe healthcare fraud penalties, with first-degree fraud exceeding $1 million classified as a Class B felony carrying up to 25 years in

prison. Illinois allows potential life imprisonment when a healthcare violation results in patient death.

Arkansas: applies its Class Y felony framework — the highest criminal classification in that state — to certain healthcare fraud scenarios, authorizing up to 40 years of imprisonment.

Montana: authorizes up to 20 years for healthcare code felonies. Alabama imposes 2 to 20 years for Medicaid fraud offenses.

Multiple states have specifically expanded healthcare penalty regimes to cover AI-driven utilization review violations — a development with immediate and direct implications for any hospital using algorithmic tools in coverage or care approval decisions.

Oklahoma: caps aggregate insurer fines at $500,000 per year for AI coverage denial violations;

Rhode Island: authorizes $50,000 per violation when AI is used to deny insurance coverage without review by a qualified clinical professional.

Federal HIPAA penalties compound these state exposures further, with civil fines of up to $2 million annually and criminal penalties of up to 10 years for intentional misuse of protected health information.

Table 4 — PBM Regulatory Violations: States with the Most Severe Penalties

- ***PBM Regulation Is one of the most active legislative areas in 2025–2026***
- ***Driven by legislative concern over drug pricing opacity, spread pricing practices, and pharmacy reimbursement disputes.***
- ***Hospitals operating specialty pharmacies or managing PBM contracts face escalating state enforcement***

Vermont and Pennsylvania: lead the severity rankings, each authorizing civil penalties of $100,000 per violation.

Pennsylvania: further caps aggregate annual penalties at $1 million for knowing violations — a ceiling that can be reached quickly when violations are calculated per claim or per affected beneficiary.

Tennessee: 2025 enforcement reform eliminated the previous $250,000 aggregate cap on PBM penalties entirely, giving the Tennessee Department of Commerce and Insurance open-ended authority to levy fines based on the number of impacted claims.

Connecticut: also authorizes $100,000 per violation for PBMs that fail to meet network transparency and patient access standards.

North Dakota: stands alone among the most aggressive states in classifying unlicensed PBM operation as a Class C felony carrying up to 5 years imprisonment — a criminal exposure that

extends to individual executives responsible for compliance oversight.

Across all states analyzed, the most common enforcement tools include license suspension or revocation, mandatory restitution to affected pharmacies, and escalating daily fines for ongoing non-compliance. For hospital leadership, the strategic imperative is to ensure PBM contracts include robust compliance warranties and audit rights, and that specialty pharmacy operations are licensed in every state where services are rendered.

State	Max Civil Penalty	Max Criminal Fine	Max Imprisonment
Vermont	$100,000/violation	License revocation	N/A
Pennsylvania	$100,000/violation ($1M/year)	N/A (administrative)	N/A
Connecticut	$100,000/violation	N/A (civil)	N/A
Kansas	$5,000–$100,000 (unlicensed)	Administrative/fine	N/A
Tennessee	$25,000/violation (no cap)	N/A (civil)	N/A
Minnesota	$25,000/violation + $10,000/day	N/A (administrative)	N/A
Mississippi	$25,000 (admin) + $1,000/day	N/A	N/A
West Virginia	$10,000–$20,000/violation	N/A (civil)	N/A
Michigan	$20,000/month (suspended)	N/A (administrative)	N/A
Massachusetts	$5,000/day + $25,000 (false rpt)	N/A	N/A
New Jersey	$250–$10,000/day	N/A (administrative)	N/A
North Dakota	$10,000–$50,000/violation	Class C Felony	Up to 5 years
Oregon	$10,000/violation + $10,000/day	N/A	N/A
Florida	$10,000/violation/day	N/A (administrative)	N/A
Rhode Island	$10,000/violation	N/A (civil only)	N/A
Oklahoma	$100–$10,000/violation	License revocation	N/A
Delaware	$10,000/violation	Registration revocation	N/A
Maine	$5,000/day (unlicensed)	$1,000 (willful)	Up to 1 year
New York	$1,000–$5,000/violation	Perjury penalties possible	Varies
South Carolina	$10,000/violation	License revocation	N/A

Table 5 — FDX (Financial Data Exchange) Violations: States w/ Most Severe Penalties

- ***Federal and State Financial Data Enforcement Is Converging at $1 Million Per Day***
- ***Open Banking Rules / State Criminal Statutes Create a Dual-Track Enforcement Environment***

Financial Data Exchange regulation is the least developed of the five domains at the state level, as FDX itself is primarily an industry-led technical standard rather than a statutory framework.

However, states enforce financial data protections through a combination of computer crimes statutes, consumer protection acts, securities laws, and the overlay of federal CFPB enforcement under Section 1033 of the Dodd-Frank Act — and that federal overlay is where the most severe penalties reside.

The Consumer Financial Protection Bureau can impose civil fines of up to $1 million per day for knowing violations of consumer financial data rights.

These penalties apply to state-chartered financial institutions in every state, and as federal open banking rules take full effect, states are actively layering additional enforcement mechanisms on top of the CFPB framework.

For hospital systems with affiliated financial products, patient financing programs, or health savings account partnerships, this regulatory intersection creates exposure that may not yet appear on the compliance team's radar.

Georgia and West Virginia: impose the stiffest criminal penalties, with Georgia's computer crimes statute authorizing up to 15 years imprisonment and $50,000 in fines for unauthorized access to financial data.

Wyoming: has established minimum mandatory sentences of 3 years imprisonment and $10,000 in fines for operating unlicensed virtual currency kiosks — a risk relevant to any health system exploring cryptocurrency payment options or digital asset programs.

Oklahoma classifies fraudulent financial statements filed with insurance regulators as felonies carrying up to 5 years imprisonment.

Arkansas: applies Class C through Class Y felony structures to financial fraud, with imprisonment ranging from 3 to 40 years depending on the severity of the offense.

Vermont: authorizes up to 10 years imprisonment for repeat financial data access violations.

Table 5 — FDX Reg Violations: Discussion of the Worst State Penalties

State	Max Civil Penalty	Max Criminal Fine	Max Imprisonment
Nebraska	$1M/day (knowing, federal)	$25,000/day (reckless)	N/A (civil)
South Dakota	$1M/day (knowing, federal)	N/A (federal civil)	N/A
Iowa	$40,000/violation (state CFA)	$1M+/day (federal)	N/A
North Dakota	$100,000/violation (HB 1127)	$1,000 daily after order	Criminal fraud possible
Oklahoma	$50,000 (fraudulent statements)	$25,000 (individual)	1–5 years
Wyoming	$10,000+ (kiosk violations)	$10,000 (false certification)	3+ years (minimum)
Connecticut	$5,000/violation (CUTPA)	N/A	N/A
Mississippi	$25,000/violation (securities)	$25,000 (willful)	Criminal prosecution
Vermont	$10,000 (identity misappropriation.)	$5,000 (unauthorized access)	Up to 10 years (repeat)
Georgia	Damages + costs (civil)	$50,000 (computer crimes)	Up to 15 years
West Virginia	$50,000/violation (HIPAA)	$10,000 (felony access)	Up to 10 years
Wisconsin	$10,000 (Class H felony)	$10,000	Up to 6 years
New Mexico	Multiple times goods value	Customs fraud penalties	Varies
Montana	$500+ or actual damages	$5,000 (unlicensed)	N/A
Kentucky	$2,000–$10,000/violation	N/A	N/A
Hawaii	$2,500/violation (breach)	N/A	N/A
Maine	$2,000 (Class D crime)	$2,000	Up to 1 year
New Hampshire	$10,000/violation (CPL)	N/A	N/A
Arkansas	Class C–Y felony fines	Varies	3–40 years (fraud)

Conclusion: From Warning to Action

The Compliance Investment Decision Has Already Been Made — By Regulators

The data across these five tables tells an unambiguous story: the regulatory cost of non-compliance in AI, privacy, healthcare, PBM operations, and financial data exchange has escalated to a level that poses existential risk for individuals and organizations alike. States are no longer treating violations as minor administrative matters deserving of modest fines and cure periods. The trajectory is unmistakably toward criminal prosecution, multi-million-dollar civil penalties, and immediate enforcement — without the safety net of grace periods.

Multi-State Exposure: The Compounding Effect That Changes Every Risk Calculation

For healthcare organizations, technology companies, pharmacy benefit managers, and financial institutions operating across multiple states, the compliance challenge is particularly acute. A single data breach, an improperly deployed AI system, or a PBM reimbursement violation can trigger simultaneous enforcement actions in dozens of jurisdictions — each with its own penalty schedule, enforcement timeline, and criminal threshold. The cumulative exposure from a single incident is not additive; in many cases, it is multiplicative.

Three Strategic Imperatives for Hospital Executive Teams

1. Compliance infrastructure must be treated as a board-level capital investment priority, not a departmental expense. The penalty ceilings documented in this analysis dwarf the cost of proactive compliance programs by orders of magnitude.
2. Rapidly evolving legislative landscape across all 50 states requires dedicated regulatory monitoring — not annual reviews, but continuous tracking of enacted and proposed legislation in every state where your organization operates or serves patients.
3. Treatment of regulatory adherence as a fundamental business imperative — not a cost center — must be embedded in executive performance frameworks, incentive structures, and organizational culture from the top down.

The Question Is No Longer Whether You Can Afford Compliance

The penalties documented in this analysis serve as both a warning and a call to action. The question for regulated entities is no longer whether they can afford to invest in compliance — it is whether they can afford not to. The executives who internalize this shift earliest will be the ones still in their roles when the next enforcement wave arrives.

Source: Regulations for Healthcare, AI, Privacy, PBM, and FDX — Severe Penalties for Violations in 50 States (February 2026). Data compiled from enacted and pending state legislation, administrative rules, and regulatory guidance effective through early 2026.