Transformativ IP

Regulations for Healthcare, AI, Privacy, and PMB and the Severe Penalties for Violations in 50 States

Failure to comply with the latest federal and state regulations regarding Healthcare, Privacy, AI, FDX, and PBMs carries severe penalties. These penalties can range from criminal charges and potential imprisonment to millions of dollars in fines and civil liability. A single regulatory lapse often triggers multiple regulatory violations. This applies to both individuals, such as CEOs, CTOs, Board members, and physicians, and organizations such as medical clinics and hospitals.

To quickly see the fines, civil or criminal penalties, and imprisonment for these regulatory violations in any of 50 states, consult either of the two resources below.

To verify this information, use the saved Google AI Search Results below by Either:

1. Selecting "Search Results" for any state listed below, or...
2. Clicking on the state's name, then clicking the yellow-highlighted hyperlink found immediately beneath that state's name on that state's dedicated page.

Quantum computing introduces a severe, new threat: "Harvest Now, Decrypt Later" (HNDL), which allows these advanced computers to bypass all existing data and cyber encryption. This has led to a significant escalation in state-sponsored hacking, particularly by China and Russia, according to intelligence from the FBI and NSA. We offer comprehensive educational materials and the best software solutions to help organizations effectively manage these critical quantum and regulatory risks. Our solution is 100% software-based, and free trialware is available.

Our PQC+® is 100% certified (FDA ATO) software and addresses all of this and:

1. **Proven & Certified:** We hold all required USA, Canada, and EU certifications including a FDA Authority to Operate. We have many client references, including a client with 1 million users.
2. **We help Hospitals / Clinics qualify for the** $50 billion Rural Health Transformation Program.
3. **We will be a Rural Health Transformation Program (RHT) software vendor in 50 states.**
4. **We exceed all 26 criteria for the CMS RHT** for privacy, cybersecurity and interoperability.
5. **Our PQC+ software provides unique and compelling profit increasing capabilities** such as chronic disease management, triage services, value-based care and the lowest cost PMB.

Summary of the State Regulations, Penalties, Fines and Imprisonment

This interactive Table of Contents hyperlinks to the specific criminal charges, imprisonment, fines and civil liability for each of the 50 states. This document is 99-pages.

Alabama

https://share.google/aimode/fWJe9Fxj5Nwd93iY2 Click on link to see the saved Google AI search result

Pharmacy Benefit Managers (PBMs)

The **Community Pharmacy Relief Act (SB 252)**, which took effect **October 1, 2025**, established a new PBM Compliance Division within the Alabama Department of Insurance (ALDOI) to enforce reimbursement and steering rules.

- **Civil Penalties:** A minimum of **$1,000 per violation**.
- **Administrative Actions:** The Insurance Commissioner may order claim reprocessing at compliant rates (e.g., ensuring the **$10.64 dispensing fee**) and cessation of prohibited practices.
- **Pharmacy Recoupment:** If a pharmacy's complaint is proven, the PBM must repay a filing fee (up to $100) to the pharmacy.

Data Privacy

Proposed 2026 legislation and existing 2024–2025 laws focus on civil enforcement by the Attorney General.

- **Alabama Personal Data Protection Act (HB 351/HB 283):** These 2026 bills grant the Attorney General exclusive authority to enforce consumer rights. Violations typically do not offer a private right of action but allow for structured civil fines.
- **App Store & Minor Privacy (HB 161):** Violations are classified as "deceptive trade practices."
    - **Civil Fines:** Up to **$7,500 per violation**.
    - **Punitive Damages:** Available for consistent patterns of knowing or reckless conduct.
- **Data Breach Notification Act:** Failure to notify residents of a breach can result in fines of up to **$5,000 per day**, capped at **$500,000 per breach**.
- **Genetic Data Privacy Act (AGDPA):** Carries civil penalties of up to **$3,000 per violation**.

AI and Healthcare

Regulations focusing on AI oversight in medical decisions primarily utilize civil remedies and administrative discipline.

- **Medical Necessity Oversight (SB 63/HB 515):**
    - **Civil Action:** Injured persons may bring a civil suit for compensatory or **punitive damages**, injunctive relief, and attorney fees.
    - **Administrative Discipline:** The Alabama Department of Insurance may take disciplinary action against licensed insurers.
- **Deepfake & AI Deception (Criminal):** Distributing "materially deceptive media" (deepfakes) with intent to harm a candidate's reputation is a **Class A Misdemeanor**, punishable by up to **one year in jail**. Subsequent violations are **Class D Felonies**.
- **Medicaid Interoperability:** Non-compliance with the **January 1, 2026**, prior authorization standards may result in monetary penalties of up to **$100,000 per act or omission**.

Summary of General Penalties in Alabama Code

When a specific act does not define its own penalty but falls under general criminal code for health or business records, the following standard ranges apply:

- **Class C Misdemeanor:** Up to **$500 fine** and/or **6 months imprisonment**.
- **Class B Felony:** (Used for serious fraud or interruption of public services exceeding $2,500) Punishable by **2 to 20 years imprisonment** and fines up to $30,000.
- **Wilful Regulatory Violations (Health):** Some older health codes allow for fines up to **$25,000 per day** or up to **one year imprisonment**.

Alaska

https://share.google/aimode/oRJ4FUVnnVX4rv9wX (click on link to see the saved Google AI search result)

Alaska's regulatory framework for **2026** emphasizes civil penalties and administrative sanctions rather than imprisonment for most corporate violations in AI, healthcare, and insurance.

Artificial Intelligence (AI)

Most AI-specific penalties are civil, as recent legislation focused on state agency accountability and transparency.

- **Civil Penalties:**
  - **State Agency Violations:** Under **SB 177**, individuals harmed by a state agency's misuse of AI or failure to perform impact assessments can sue for **actual damages**, **punitive damages**, and full attorney fees.
  - **Deepfake Disclosures:** Failure to disclose AI-generated "deepfakes" in election communications allows candidates or groups to sue for **damages suffered**, attorney fees, and injunctive relief.
- **Criminal Penalties:**
  - **AI-Generated Child Sexual Abuse Material:** Knowingly creating or exchanging AI depictions of minors is a **Class B or C felony** (up to **5–10 years** imprisonment and/or fines up to **$50,000–$100,000**).

Healthcare & Prior Authorization

Penalties for violating the new **SB 133** prior authorization standards (effective **January 1, 2026**) target insurance carriers.

- **Civil Penalties:**
  - **Per Instance:** Up to **$25,000** for each instance of non-compliance with prior authorization timelines (72 hours for routine, 24 hours for expedited).
  - **Administrative Actions:** The Director of Insurance may suspend or revoke an insurer's **certificate of authority** for persistent or severe violations.
- **Medical Misconduct:** Healthcare providers failing to follow prescribing or telehealth standards may face civil fines up to **$25,000** and license suspension.

Privacy & Data Security

Alaska relies on both the Alaska Personal Information Protection Act (APIPA) and the new **Insurance Data Security Law (SB 134)**.

- **APIPA (General Breach):**
  - **Civil:** Up to **$500 per consumer** not notified, capped at **$50,000** per breach.
  - **Trade Practices:** Violations are considered "unfair or deceptive acts," potentially triggering fines of **$1,000 to $25,000** per violation.
- **SB 134 (Insurers):**
  - **Civil:** The Alaska Division of Insurance can impose fines of up to **$2,500** for each violation of security program or notification requirements.
- **Criminal:**
  - **Govt Employees:** Intentional disclosure of personal info by a state employee is a **misdemeanor**, punishable by up to **1 year** in prison and/or a **$2,000** fine.

Pharmacy Benefit Managers (PBMs)

Under **SB 132/SB 134**, PBMs are now regulated similarly to insurance licensees.

- **Civil Penalties:**
  - **Unlicensed Activity:** Operating without the mandatory **$20,000** license is subject to substantial administrative fines determined by the Director of Insurance, typically up to **$2,500** per violation under standard insurance statutes.
  - **Audit Compliance:** PBMs failing to pay for mandated state examinations or audits face additional administrative sanctions.

Arizona

https://share.google/aimode/aIX0SIggrjGhUDd6G (click on link to see the saved Google AI search result)

In 2026, Arizona maintains a tiered system of civil and criminal penalties to enforce healthcare technology and privacy regulations. Penalties often combine state-specific fines with federal HIPAA mandates.

AI in Healthcare (Human Review Requirements)

Violations of the human-oversight requirements for AI in medical claim denials (HB 2175, effective July 1, 2026) are primarily handled through professional disciplinary actions.

- **Unprofessional Conduct:** Failure by a medical director or provider to conduct an individual review before an AI-recommended denial is legally classified as "unprofessional conduct".
- **Board Sanctions:** TheArizona Medical Board may impose:
  - **Civil Penalties:** Typically up to **$1,000 per violation**.
  - **Licensure Actions:** Reprimands, probation, or suspension/revocation of the medical license.

Privacy and Data Security

Arizona's data breach and privacy statutes carry heavy financial weight, enforced by the Attorney General.

- **Data Breach Notification (A.R.S. § 18-552):**
  - **Civil Penalties:** Up to **$10,000 per affected individual** or the total economic loss sustained, whichever is less.
  - **Maximum Cap:** Total penalties from a single breach or related series of breaches cannot exceed **$500,000**.
- **HIPAA/Medical Privacy (Federal & State Integration):**
  - **Civil:** $100 to $50,000 per violation, with an annual cap of **$1.5 million** for identical violations.
  - **Criminal (Federal DOJ):**
  - **Knowing violations:** Up to $50,000 fine and **1 year** in prison.
  - **False pretenses:** Up to $100,000 fine and **5 years** in prison.
  - **Malicious intent/commercial gain:** Up to $250,000 fine & **10 years** in prison.

Pharmacy Benefit Managers (PBMs)

Enforcement is managed by the Arizona Department of Insurance and Financial Institutions (DIFI) and the Board of Pharmacy.

- **General Non-Compliance:** If a PBM violates formulary or reimbursement statutes (e.g., SB 1102), the DIFI Director may impose civil penalties.
- **Licensing Violations:** Operating without a mandatory certificate of authority can lead to cease-and-desist orders and administrative fines.
- **Pharmacy Misconduct:** For PBM-affiliated pharmacy violations:
  - **Civil Penalties:** Up to **$1,000 per violation**.
  - **Criminal Class:** Many pharmacy statute violations (if not specifically assigned) fall under **Class 2 Misdemeanors**, punishable by up to 4 months in jail and **$10,000** for enterprises.

General Healthcare Sentencing (2025-2026) for statutory violations (misdemeanors)

Class	Max Imprisonment	Max Fine Individual	Max FIne Enterprise
Class 1 Misdemeanor	6 Months	$2,500	$20,000
Class 2 Misdemeanor	4 Months	$750	$10,000
Class 3 Misdemeanor	30 Days	$500	$2,000

Arkansas

https://share.google/aimode/sTjS82iBKH6cLgJoz (click on link to see the saved Google AI search result)

In Arkansas, penalties for regulatory violations vary significantly based on whether the offense falls under consumer protection, insurance law, or criminal code.

AI (Artificial Intelligence)

Insurance AI (Bulletin 13-2024): Violations are treated as "unfair methods of competition" or "deceptive acts" under the Trade Practices Act.

- **Civil:** The Commissioner may levy fines of up to **$1,000 per violation** (not to exceed an aggregate of **$10,000**) for unintentional acts, or up to **$5,000 per violation** (not to exceed **$50,000** aggregate) if the person knew or should have known they were in violation.
- **Administrative:** Failure to comply with AI information requests is grounds for **suspension or revocation of the insurer's license**.

- **Deepfakes & Likeness (Act 827):**
  - **Criminal:** Unlawful creation/distribution of sexually explicit deepfakes is a **Class A Misdemeanor** for first offenses (up to 1 year jail; $2,500 fine) and a **Class D Felony** for subsequent offenses (up to 6 years prison; $10,000 fine).
  - **Civil:** Individuals may seek **injunctive relief** and actual or punitive damages. Violating an injunction can result in a **$1,000 per day** fine.

Healthcare

Insurance Mandates: Non-compliance with mandates like lung cancer screenings or bariatric coverage typically triggers administrative penalties from the Arkansas Insurance Department.

- **Civil:** General insurance code violations carry fines of up to **$1,000 per violation** unless a specific statute provides otherwise.

- **Health Data (PIPA):** Organizations failing to protect healthcare data are subject to the Arkansas Personal Information Protection Act.
- **Civil:** The Attorney General can seek up to **$10,000 per violation** under the Deceptive Trade Practices Act.

Privacy

Children's Online Privacy (HB 1717):

- **Civil:** Exclusively enforced by the Attorney General. While the law focuses on **injunctive relief** and restitution, it integrates with the Deceptive Trade Practices Act, allowing for fines up to **$10,000 per violation**.

- **Social Media Safety (SB 611):**
  - **Civil:** Direct private right of action for parents. Social media platforms can be fined **$10,000 per violation**, with each day a minor has improper access counting as a separate violation.

PBMs (Pharmacy Benefit Managers)

Ownership Ban (Act 624):

- **Administrative:** The Arkansas Board of Pharmacy can **revoke the license** of any pharmacy found in violation of the ownership prohibition.
- **Civil:** Fines can reach up to **$1,000 per violation**, with each day of non-compliance potentially being treated as a separate offense.

FDX (Financial Data Exchange)

General Protections: Since there are no specific state FDX statutes, violations are prosecuted under general **fraud or data breach laws**.

- **Criminal:** Identity theft or unauthorized access can range from a **Class C Felony** (3–10 years prison) to a **Class Y Felony** (10–40 years) depending on the financial amount involved.

California -

(The 9 saved Google AI Search results are accessible within each section. Click on any link below to view)

1. **AB 3030 (AI in Healthcare Act):** Requires healthcare facilities and providers to notify patients when using Generative AI to communicate clinical information.
2. **SB 1120 (Physicians Make Decisions Act):** Prohibits insurers from using AI as the sole basis for denying care and mandates human physician review for medical necessity decisions.
3. **AB 489:** An "anti-impersonation" law effective January 1, 2026, that prohibits AI from mimicking licensed professionals or using titles like M.D. or R.N..
4. **SB 243:** Regulates human-like "companion" AI chatbots, requiring suicide prevention protocols and crisis referrals.
5. **AB 2013:** Requires AI developers to disclose training data sources for systems, including those used in clinical settings.
6. **SB 942:** (AI Transparency Act): Mandates that large providers offer tools to detect AI-generated content.
7. **AB 288**: (Algorithmic Accountability Act): Standardizes AI definitions and requires inventories of high-risk automated decision systems used by state agencies.
8. **Confidentiality of Medical Information Act (CMIA):** A long-standing statute regulating the disclosure of identifiable medical information.
9. **SB 40:** Caps insulin copayments at $35 per month for state-regulated health plans

1. AB 3030 (AI in Healthcare Act): Requires healthcare facilities and providers to **notify patients when using Generative AI** to communicate clinical information.

https://share.google/aimode/rTQQZtvvCyiVjbJDn (click on link to see the saved Google AI search result)

- **Civil Penalties/Fines:**
  - **Licensed Health Facilities:** Up to **$25,000 per violation**. Liability falls on the facility, enforced under Health and Safety Code Sections 1425–1429.
  - **General Civil Enforcement:** Potential liability of **$5,000 per violation, per day**, enforceable through civil action by the California Attorney General, city attorneys, or county counsel. Liability falls on covered providers.
  - **Licensed Clinics:** Subject to enforcement and fines under Article 3 of Chapter 1 of the Health and Safety Code. Liability falls on the clinic.
- **Disciplinary Action (Non-Monetary):**
  - **Physicians and Surgeons:** Formal disciplinary action against their license (e.g., suspension or revocation). Liability falls on the individual physician/surgeon, enforced by the Medical Board of California or the Osteopathic Medical Board of California.
- **Criminal Penalties:** AB 3030 **does not** establish independent criminal penalties. Liability is **None** under this specific law.

2. SB 1120 (Physicians Make Decisions Act): Prohibits insurers from using AI as the **sole basis for denying care** and mandates human physician review for medical necessity decisions.

https://share.google/aimode/k3ZCkdgD8NeKiTs35 (click on link to see the saved Google AI search result)

Penalties for Violation of California SB 1120 (Physicians Make Decisions Act)

- **Criminal Penalties (Misdemeanor):**
  - **Imprisonment:** Up to **one year** in a county jail.
  - **Fines:** Up to **$10,000** for each willful violation.
  - **Liability:** Individuals associated with the Health Care Service Plan (HCSP) or insurer found to have committed a **willful violation** of the health plan provisions.

- **Civil and Administrative Penalties (HCSPs - Department of Managed Health Care (DMHC)):**
  - **Standard Fines:** Utilizes existing regulatory authority (SB 1120 does not set unique new fine schedule).
  - **Willful Fines:** Up to **$10,000 per violation** if the non-compliance is found to be willful.
  - **Liability:** The **Health Care Service Plan (HCSP)**.
- **Civil and Administrative Penalties (Disability Insurers - Insurance Commissioner):**
  - **Standard Fines:** Up to **$5,000 per violation**.
  - **Willful Fines:** Up to **$10,000 per violation** if non-compliance is willful.
- **Liability:** The **Disability Insurer**.

3. AB 489: Summary of Penalties for California AB 489 (AI Anti-Impersonation Law

https://share.google/aimode/XWtHoUCseLW4QzH5t (click on link to see the saved Google AI search result)

Category	Liability / Responsible Party	Fines & Imprisonment	Key Details
Civil & Administrative	AI Systems / Entity responsible for AI advertising / functionality	**Fines:** Determined by the relevant licensing board; no specific minimum /maximum fine provided by AB 489 itself.	Enforcement through health care professional licensing boards (e.g. Medical Board of CA). Each individual use of a prohibited term is a **separate violation**.
Criminal (Misdemeanor)	Individual/Entity falling under existing Anti-impersonation statutes.	**Imprisonment:** Up to **one year** in county jail.	This is the general classification for violations under existing criminal statutes for falsely indicating professional licensure (amended AB 489).
		Fines (General): Often range **up to $1,000** for basic online impersonation.	
Related Criminal: Penal Code 528.5 (Online Impersonation)	Individual impersonating an *actual person* online with intent to harm or defraud.	**Imprisonment:** Up to **one year** in jail.	A specific misdemeanor statute used in conjunction with AB 489.
		Fines: $1,000 fine.	

Related Criminal: Penal Code 529 (False Personation)	Individuals involving acts that make the victim liable for a suit or penalty.	**Misdemeanor:** Up to **one year** in county jail and a **$10,000 fine**.	This is a "wobbler" offense (can be misdemeanor or felony). **Felony:** Up to **three years** in state prison and a **$10,000 fine**.

4. SB 243: Regulates human-like **"companion" AI chatbots**, requiring suicide prevention protocols and crisis referrals.
https://share.google/aimode/tkq8qYkqgsLRqhJAL (click on link to see the saved Google AI search result)
As of January 2026, California **SB 243**, also known as the first-in-the-nation AI chatbot safety measure, is in effect and primarily carries **civil penalties**. The law regulates "companion chatbots"—AI systems designed for human-like social interactions—specifically focusing on protecting minors and preventing self-harm.

- **Liability:** Primarily falls on **AI Chatbot Operators** (companies/entities operating the companion chatbots).
- **Civil Penalties (Fines):**
  - **Minimum Fine: $1,000 per violation** (or actual damages, whichever is greater).
  - **Maximum Fine:** Potential for fines up to **$5,000 per violation per day** under related AI transparency enforcement; major violations could reportedly reach up to **$1 million** in actions brought by the Attorney General.
  - **Other Remedies:** Injunctive relief (court orders to stop noncompliance) and recovery of the plaintiff's attorney's fees and costs.
  - **Enforcement:** Primarily through a **private right of action** by individuals who suffer an "injury in fact."
- **Criminal Penalties (Fines/Imprisonment):**
  - **Status:** SB 243 **does not currently include criminal penalties** or imprisonment terms for standard noncompliance.

5. AB 2013: Requires AI developers to **disclose training data sources** for systems, including those used in clinical settings.
https://share.google/aimode/KPQeKTFKt0j6NIAKt (click on link to see the saved Google AI search result)

Here is a summary of the civil and criminal penalties for California's **AB 2013** (Generative Artificial Intelligence Training Data Transparency Act):

Civil Penalties (Liability):

- **Basis:** Enforced under California's **Unfair Competition Law (UCL)**.
- **Maximum Fine:** Up to **$2,500 per violation**.
- **Enforcement Authority (Who has liability):** The California Attorney General, district attorneys, or county counsel may bring civil actions against AI developers for non-compliance.
- **Private Right of Action:** No broad private right of action, but individuals who can prove specific injury and financial loss may potentially bring a claim under the UCL.
- **Other Remedies:** Courts may issue injunctive relief, potentially suspending an AI model's commercial use until compliance is demonstrated.

- **Criminal Penalties (Fines and Imprisonment):**
  - **No Criminal Liability:** AB 2013 specifies **no criminal penalties** (no imprisonment or criminal fines) for violations.

6. SB 942 (AI Transparency Act): Mandates that large providers offer tools to **detect AI-generated content**.
https://share.google/aimode/xSuVm9balvGdy8bFZ (click on the link to see the saved Google AI search result)

Compliance Deadline: The provisions of SB 942 become operative and enforceable starting **January 1, 2026**. Certain amendments (AB 853) may extend specific latent disclosure deadlines to August 2, 2026.
Enforcement Authorities: Individual consumers cannot sue under this law; enforcement is limited to public officials : California Attorney General, City Attorneys and County Counsel
Civil Penalties (Liability for Covered Providers):

- **Monetary Fines:** $5,000 per violation.
- **Accumulation:** Fines accumulate daily ($5,000 per day) until compliance is achieved.
- **Attorney's Fees:** The prevailing plaintiff (enforcing authority) is entitled to recover reasonable costs and fees.
- **Injunctive Relief:** Available for third-party licensees (to force cessation of use).

Criminal Penalties/Imprisonment:

- None. SB 942 does not establish any criminal penalties or provisions for imprisonment.

Liability:

- Primary liability for falls upon **Covered Providers** (producing a GenAI system with over one million monthly visitors or users that are publicly accessible in California).

7. AB 2885 (Algorithmic Accountability Act): Standardizes AI definitions and mandates state agencies **inventory high-risk automated decision systems**.
https://share.google/aimode/na0CSve8gjWqXjxju (Click on the link to see the saved Google AI search result)

Effective **January 1, 2026**, California's AB 2885 (signed September 2024) standardizes the definition of "artificial intelligence" for existing state codes and mandates uniform agency reporting. The Act **does not create new civil or criminal penalties** for private entities or individuals.

California's AB 2885, known as the "Artificial Intelligence" bill, does not establish a new set of penalties for an "Algorithmic Accountability Act". Instead, its primary purpose is to create a uniform definition of "artificial intelligence" to be used across existing California laws, and it incorporates AI-related provisions into various existing regulatory frameworks.

As such, potential penalties for non-compliance with the specific provisions AB 2885 enables would depend on the *existing* enforcement mechanisms of the underlying laws it amends (e.g., Business and Professions Code, Education Code, Government Code). The bill itself does not specify new fines or imprisonment terms for the general use of AI.

Penalties for other, separate California AI laws vary widely:

1. California AI Transparency Act (SB 942, as amended by AB 853): Violations by covered providers can result in civil penalties of up to $5,000 per violation per day, enforceable by the California Attorney General, city attorneys, or county counsel.
2. Transparency in Frontier Artificial Intelligence Act (SB 53): Failure to comply with requirements, such as reporting critical safety incidents, is subject to a civil penalty of up to $1 million per violation, enforced by the state attorney general.
3. AI Call Disclosures Law (AB 2905): Violations related to using AI voices in robocalls without disclosure are subject to penalties of up to $500 per violation.
4. Amendment of California CSAM Laws: The bill expanding the scope of child pornography statutes to include AI-generated material is punishable by existing criminal penalties.

In summary, AB 2885 itself provides no specific civil or criminal penalties, instead relying on the enforcement mechanisms of other, related state laws it helps to standardize and define.

8. Confidentiality of Medical Information Act (CMIA): A long-standing statute regulating the **disclosure of identifiable medical information**.
https://share.google/aimode/6rNy3i0j0gR2uzDwi (Click on the link to see the saved Google AI search result)

The California Medical Information Act (CMIA) violations carry significant civil and criminal consequences, with liability generally falling on the violator, including licensed healthcare professionals and other individuals/entities. Enforcement is pursued by the California Attorney General or other government officials.-----**Administrative & Civil Penalties (Government Enforcement)**

Violation Type	Penalty
Negligent Disclosure	Up to **$2,500** per violation.
Knowing & Willful Violation (General)	Up to **$25,000** per violation.
Intentional/Willful (Financial Gain)	Up to **$250,000** per violation, plus disgorgement of profits.
Alternative Financial Gain Tiers	**$5,000** (1st offense), **$25,000** (2nd offense), **$250,000** (subsequent offenses).
Licensed Healthcare Professionals (Knowing & Willful)	1st offense: **$2,500**; 2nd offense: **$10,000**; Subsequent offenses: **$250,000**.

Criminal Penalties (Knowing & Willful Misconduct)
These violations are classified as **Misdemeanors**.

Violation Type	Imprisonment & Fines
Imprisonment	Up to 1 year in county jail.
Criminal Fines (Knowing violations)	Up to **$50,000**.
Criminal Fines (Intent to sell or profit)	Up to **$250,000**.

Civil Penalties (Private Right of Action)
Individuals affected by a breach can sue covered entities.
Proof of actual harm is not required for certain damages.

Type of Recovery	Amount/Context
Nominal Damages	**$1,000** per violation.
Actual Damages	Compensation for financial losses or emotional distress.
Punitive Damages	Up to **$3,000** in specific civil contexts.
Legal Costs	Recovery of attorney's fees (up to **$1,000**) and litigation costs.

9. SB 40: Caps **insulin copayments at $35** per month for state-regulated health plans
https://share.google/aimode/VZYKCc0iwrJzMB3Z1 (Click on the link to see the saved Google AI search result)

Criminal Penalties (Liability rests with the individual/entity responsible for the violation):

- **Action:** Willful violation of SB 40 is a crime under the California Knox-Keene Health Care Service Plan Act.
- **Classification:** Typically prosecuted as a misdemeanor.
- **Punishment:**
  - Imprisonment in a county jail for up to six months.
  - A fine not exceeding $1,000.
  - Or both.

Civil and Administrative Penalties (Liability rests with the non-compliant health plans/insurers):

- **Enforcement Agencies:** California Department of Managed Health Care (DMHC) and California Department of Insurance (CDI).
- **Administrative Fines (DMHC/CDI):** State regulators can levy "behavior-changing" fines.
  - **Maximum:** Historic fines for large-scale, severe violations can be substantial (e.g., DMHC has previously issued fines up to $35 million).

Civil Action Penalties (Can be triggered by violations):

- **Maximum:** Up to $1 million against companies for major regulatory failures under new 2026 enforcement standards.

COLORADO

https://share.google/aimode/98xxzWCOLHGXGxgxU Click on link to see the saved Google AI search result.

Violations of Colorado's AI, privacy, and PBM regulations primarily result in **civil penalties** enforced by the Colorado Attorney General, with potential for **criminal charges** only in specific healthcare and general public health scenarios. There are no explicit imprisonment penalties under the AI Act, the Colorado Privacy Act, or the PBM-specific legislation.

AI Act (Colorado AI Act)

Violations are classified as deceptive trade practices under the Colorado Consumer Protection Act (CCPA).

- **Civil Penalties**: Up to **$20,000 per violation**.
- **Enhanced Civil Penalties**: Up to **$50,000 per violation** if committed against an elderly person (over 60).
- **Criminal Penalties**: The Act does not provide for criminal penalties or imprisonment.
- **Private Right of Action**: None. Enforcement is exclusively by the Colorado Attorney General and District Attorneys.

Privacy (Colorado Privacy Act - CPA)

Similar to the AI Act, violations are treated as deceptive trade practices under the CCPA.

- **Civil Penalties**: Up to **$20,000 per violation**.
- **Maximum Aggregate Penalty**: Up to **$500,000** for related violations.
- **Criminal Penalties**: While some general consumer protection laws might allow for criminal charges, the CPA itself focuses on civil enforcement and does not specify imprisonment.
- **Private Right of Action**: None. Enforcement is exclusively by the Colorado Attorney General and District Attorneys.

Pharmacy Benefit Managers (PBMs)

Enforcement for PBM regulations involves administrative actions and civil penalties imposed by the Commissioner of Insurance.

- **Administrative Action**: The Commissioner can deny, suspend, revoke, or refuse to renew a PBM registration, or issue cease-and-desist orders for violations of an insurance law.
- **Civil Penalties**: Up to **$1,000 per violation per day**.
- **Criminal Penalties**: PBM-specific legislation does not outline criminal penalties or imprisonment.

Healthcare (General State Regulations)

Penalties vary widely depending on the specific statute violated and can include both civil and criminal components.

- **Unlicensed Operation**: Operating a healthcare entity without a license is a misdemeanor, punishable by a fine of **$50 to $500**. Each day of operation is a separate offense.
- **Facility Deficiencies**: Fines for deficiencies can range from **$100 to over $10,000**, with higher penalties for egregious violations or those resulting in serious harm or death.
- **Public Health Orders**: Violations of general public health orders can result in a penalty of up to **$50 per day** of violation.
- **HIPAA Violations (Federal Standard)**: Entities handling Protected Health Information (PHI) are also subject to federal HIPAA rules, which can impose:
    - **Civil Fines**: Ranging from **$137 to over $2 million annually**.
    - **Criminal Fines & Imprisonment**: Ranging up to **$250,000 and 10 years in prison** for the most severe cases, such as wrongful disclosure with intent to sell PHI.

Connecticut

https://share.google/aimode/KPbbvlEwib69EHYnd Click on link to see the saved Google AI search result.

Violations of Connecticut's rapidly evolving regulatory landscape for AI, privacy, and healthcare primarily result in substantial civil penalties and restitution, with criminal liability reserved for specific cases of fraudulent or intentional harm.

Artificial Intelligence (AI)

The 2026 mandates for "high-risk" AI systems introduce specific enforcement mechanisms focused on algorithmic discrimination.

- Civil Penalties (Discrimination): The Commission on Human Rights and Opportunities (CHRO) can impose fines between $3,000 and $7,000 if a developer or deployer fails to use reasonable care to prevent discriminatory practices.
- General Violations: Other violations of the AI act are treated as "unfair trade practices." Civil penalties for such violations can reach $100 per day, with an aggregate cap of $10,000 for certain procedural failures.
- Criminal Penalties: Knowingly distributing deceptive synthetic media (deepfakes) within 90 days of an election or primary is a crime. Disseminating synthetic intimate images is a Class A misdemeanor (up to 1 year in prison) for a single victim, or a Class D felony (1 to 5 years in prison) if sent to multiple people.

Privacy & Healthcare Data (CTDPA)

Healthcare data privacy is regulated under the umbrella of the Connecticut Data Privacy Act (CTDPA) as "sensitive data."

- Civil Penalties: The Attorney General can seek civil penalties of up to $5,000 per willful violation. Because each affected consumer can be considered a separate violation, total fines can be massive; for example, a settlement in 2025 reached $85,000 for a single company's failure to cure deficient privacy notices.
- Additional Remedies: Courts may also order restitution for affected consumers, disgorgement of profits, and permanent injunctive relief.
- Healthcare-Specific Caps: For individual healthcare providers, the Department of Public Health (DPH) can impose penalties up to $25,000, an increase from the previous $10,000 cap.

Pharmacy Benefit Managers (PBMs)

PBM regulations focus on transparency and fiduciary duties toward health carriers and patients.

- Civil Penalties: The Insurance Commissioner has the authority to levy fines of up to $100,000 per violation for non-compliance with network transparency and patient access mandates.
- Fiduciary Liability: The establishment of a fiduciary duty and a duty of good faith and fair dealing (effective October 1, 2025) exposes PBMs to civil litigation for breaches that harm health plan sponsors or covered individuals.

FDX & Financial Data Exchange

Regulatory enforcement for financial data exchange in Connecticut largely mirrors federal standards set by the CFPB.

- Federal Alignment: While there are no specific criminal "FDX" penalties in CT state law, violations of financial data rights are typically handled under the Connecticut Unfair Trade Practices Act (CUTPA), which carries the same $5,000 per violation civil penalty as general privacy breaches.

Delaware

https://share.google/aimode/pwfd6Zw1knzueT3sb Click on link to see the saved Google AI search result.

Delaware's enforcement of data, healthcare, and corporate regulations primarily relies on civil penalties and administrative actions, though specific criminal penalties exist for fraudulent or high-risk technology misuse.

1. Data Privacy (DPDPA)

The Delaware Personal Data Privacy Act is enforced exclusively by the Delaware Department of Justice (DOJ).

- **Civil Penalties:** Up to **$10,000 per willful violation**.
- **Administrative Remedies:** The DOJ may seek **injunctive relief**, **restitution**, or **disgorgement of profits** gained through non-compliant data practices.
- **Criminal Penalties:** None currently specified for standard privacy violations; however, identity theft or broad fraud remains punishable under general criminal code.
- **Note:** As of **January 1, 2026**, the mandatory 60-day "right to cure" has expired, meaning the DOJ can initiate enforcement immediately without prior notice.

2. Artificial Intelligence (AI)

While broad AI regulation is still developing, specific statutes target high-risk AI applications:

- **Deepfakes (HB 316):**
  - **Criminal:** Violations are generally **Class B misdemeanors**.
  - **Escalation:** If intended to cause violence or harm, it becomes a **Class A misdemeanor**. Repeat offenses within five years are elevated to a **Class E felony** (punishable by up to 2 years in prison).
- **AI Commission Oversight:** The Delaware AI Commission does not currently have independent fining authority but makes recommendations for agency-level enforcement and legislative penalties expected in late 2026.

3. Healthcare & PBMs

Enforcement is split between the Department of Health and Social Services (DHSS) and the Insurance Commissioner.

- **Pharmacy Benefit Managers (PBMs):**
  - **Civil Penalties:** The Insurance Commissioner can levy fines up to **$10,000 per violation**.
  - **Licensing:** Egregious or repetitive violations can result in the **revocation of a PBM's authority** to operate in Delaware.
- **Facility & Patient Rights:**
  - **Civil Money Penalties:** Range from **$1,000 to $10,000** for violations involving patient health, safety, or welfare.
  - **Continuing Violations:** For non-health and safety issues, penalties can reach **$2,500 per day** beyond the initial day.
  - **Criminal:** Fraudulent prescription orders by a pharmacist are a **Class F felony**, carrying fines between **$1,000 and $10,000**.

4. Financial Data (FDX)

Delaware does not have a standalone "FDX law." Instead, financial data is protected under the DPDPA and federal GLBA standards.

- **Civil Penalties:** Financial institutions that fail to meet DPDPA data portability requirements (if not exempt) face the same **$10,000 per violation** fine mentioned above.

Category	Max Civil Fine	Max Criminal Penalty	Enforcement Body
Privacy	$10,000 per violation	N/A	Department of Justice
AI (Deepfakes)	N/A	Class E Felony	Superior Court
PBMs	$10,000 per violation	Registration Revocation	Insurance Commissioner
Healthcare	$10,000 per instance	Class F Felony (Fraud)	DHSS / DOJ

Florida

https://share.google/aimode/H8SCSrei1ogAsvuAd Click on link to see the saved Google AI search result.

Penalties for Florida's regulations concerning AI, healthcare, privacy, and PBMs vary depending on the specific statute violated. Many of Florida's AI and healthcare AI regulations are part of bills proposed for the **2026 legislative session** and may not yet be enacted into law.

Artificial Intelligence (AI)

Penalties for AI-related violations often fall under existing laws or specific new statutes targeting harmful uses.

- **AI-Generated Political Ads (Undisclosed)**: A violation of the AI political ad disclosure requirement is a **first-degree misdemeanor**, punishable by up to a **$1,000 fine** and up to **one year imprisonment**.
- **AI for Firearm Detection**: Using AI to detect firearms in public areas is a **first-degree misdemeanor**, with penalties as provided by general Florida statutes (e.g., up to $1,000 fine and one year in jail).
- **AI Bill of Rights (Proposed)**: Proposed legislation (SB 482) includes a civil penalty of **$50,000 per violation** for entities engaging in unfair or deceptive trade practices, such as selling a user's personal data or using a person's image/likeness without consent, with potential trebling of damages for violations involving children. These are not yet fully enacted laws.
- **Sexual Deepfakes**: Creating, possessing, soliciting, or sharing AI-generated sexual images without consent is a felony, with significant penalties.

Healthcare

Most Florida healthcare privacy regulations fall under the federal Health Insurance Portability and Accountability Act (HIPAA) and state professional licensing rules.

Civil Penalties (HIPAA)

Civil penalties are tiered based on intent and knowledge:

- **Unknowing Violations**: **$100 to $50,000 per violation**, with an annual maximum of **$25,000**.
- **Reasonable Cause**: **$1,000 to $50,000 per violation**, with an annual maximum of **$100,000**.
- **Willful Neglect (Corrected in 30 days)**: **$10,000 to $50,000 per violation**, with an annual maximum of **$250,000**.
- **Willful Neglect (Not Corrected)**: **$50,000 per violation**, with an annual maximum of **$1.5 million**.

Criminal Penalties (HIPAA)

Criminal penalties are prosecuted by the Department of Justice and can include imprisonment:

- **Knowing Violation**: Up to **$50,000 fine** and up to **one year imprisonment**.
- **False Pretenses**: Up to **$100,000 fine** and up to **five years imprisonment**.
- **Intent to Sell/Harm/Advantage**: Up to **$250,000 fine** and up to **ten years imprisonment**.

State Professional Licensing Penalties

Healthcare professionals can face additional administrative fines (up to **$10,000 per offense**) and license suspension or revocation for a range of violations, including failure to maintain confidentiality.

Privacy (Florida Digital Bill of Rights - FLDBR)

The FLDBR focuses on large "Big Tech" companies, with enforcement handled exclusively by the Florida Department of Legal Affairs (no private right of action).

- **Civil Penalties**: Up to **$50,000 per violation**.
- **Trebled Penalties**: Fines can be tripled (up to **$150,000 per violation**) for violations involving children, or for noncompliance with consumer opt-out or deletion requests.

Pharmacy Benefit Managers (PBMs)

Florida's PBM reform laws, effective January 1, 2024, are enforced by the Florida Office of Insurance Regulation.

- **Operating Without a License**: Any PBM operating in Florida without a valid Certificate of Authority is subject to a fine of **$10,000 per violation per day**.
- **Prohibited Practices**: The law prohibits practices like spread pricing and forcing consumers to use mail-order pharmacies. Violations may result in administrative action, though specific fine amounts beyond the licensing requirement are tied to general insurance regulations and administrative enforcement mechanisms.

Georgia

https://share.google/aimode/VUNz4cQKuDFge1iXX Click on link to see the saved Google AI search result.

Georgia law provides for various civil and criminal penalties for violations related to privacy, PBMs, and healthcare as of 2026.

Privacy Regulations

Georgia's privacy laws distinguish between data privacy and traditional computer crimes.

- **Georgia Consumer Privacy Protection Act (SB 473)** (Effective July 1, 2026):
  - **Civil Penalties**: Up to **$7,500 per violation**.
  - **Criminal Penalties**: None; the Attorney General has exclusive civil enforcement authority.
  - **Cure Period**: Businesses are granted a **60-day period** to fix violations before the Attorney General initiates legal action.
- **Computer Data Privacy & Crimes (O.C.G.A. § 16-9-93)**:
  - **Civil Penalties**: Aggrieved parties may sue for any damages sustained, including the costs of the suit.
  - **Criminal Penalties**: Violations like computer theft, trespass, or invasion of privacy are felonies. Conviction carries fines up to **$50,000** and/or imprisonment for up to **15 years**.
  - **Password Disclosure**: Fines up to **$5,000** and/or imprisonment for up to **one year**.

Pharmacy Benefit Managers (PBMs)

PBMs are subject to oversight by the Commissioner of Insurance.

- **Civil Penalties**:
  - Fines of up to **$1,000 per violation** to be paid to the aggrieved party (insured or pharmacy).
  - Standard monetary penalties of up to **$2,000 per act** in violation.
  - For **willful violations**, the penalty can increase up to **$10,000 per act**.
- **Administrative Actions**: The Commissioner can issue cease and desist orders, suspend or revoke licenses, and order reimbursement for monetary losses.
- **Private Right of Action**: As of 2025/2026, HB 690 establishes a private right of action, allowing individuals to file civil lawsuits for damages against PBMs.

Healthcare Regulations

Penalties for healthcare-related violations vary by the specific act.

- **Consumer Access to Contracted Healthcare (CATCH) Act**:
  - **Civil Penalties**: Insurers may be fined up to **$2,000 per violation**. If the insurer "knew or reasonably should have known" they were in violation, the fine increases up to **$5,000 per act**.
- **Facility Licensing & Care**:
  - **General Violations**: Fines up to **$2,000 per day** per violation, capped at **$40,000** total.
  - **Serious Harm/Death**: For long-term care facilities, a mandatory minimum fine of **$5,000** applies if a violation causes serious physical harm or death.
  - **Criminal Misdemeanor**: Operating a home health agency without a license carries a fine of up to **$500** and/or imprisonment for up to **six months**.
- **Referral & Kickback Violations**:

- **Misdemeanor**: Violations involving fewer than 10 patients carry up to **12 months** imprisonment and a **$1,000 fine** per violation.
- **Felony**: Violations involving 20+ patients carry up to **10 years** imprisonment and a **$500,000 fine** per violation.

Artificial Intelligence (AI)

Specific penalties for AI usage in healthcare and governance are still evolving.

- **Criminal (Deepfakes/Exploitation)**: Under the **Ensuring Accountability for Illegal AI Activities Act** (Effective July 2025), creating or distributing AI-generated obscene material involving children is a felony punishable by **one to 15 years** in prison.
- **Healthcare Decision-Making**: While recent bills (like HB 887) prohibit relying solely on AI for clinical decisions, enforcement is primarily through the **Georgia Composite Medical Board**, which can discipline physicians through license suspension or revocation.

Hawaii

https://share.google/aimode/CV5QIAQgTOYG1a8sc Click on link to see the saved Google AI search result.

Penalties for violating Hawaii's regulations in these sectors vary significantly based on the specific act and the nature of the offense. Many of the newer regulations introduced for 2025 and 2026 rely on **civil penalties** enforced by the Attorney General or the Office of Consumer Protection.

Artificial Intelligence (AI)

- **Algorithmic Discrimination (SB 2524 / HB 1607):**
  - **Civil Penalties:** Up to **$10,000 per violation** for covered entities or service providers.
  - **Private Cause of Action:** Aggrieved individuals can sue for actual damages or statutory damages between **$100 and $10,000 per violation**.
- **Minors' Protection & AI Companion Systems (SB 2788):**
  - **Civil Penalties:** Up to **$15,000 per day** for violations such as failing to implement age assurance or encouraging dependency in minors.
- **Deepfakes & Deceptive Media:** Violation of laws regarding invasive or humiliating AI-generated images can result in fines up to **$20,000** or up to **4 years of imprisonment**.

Healthcare

- **Health Care Decision Guardrails:** While specific penal tiers for the 2026 AI utilization review rules (HB 820) are often tied to existing insurance code violations, general health facility violations in Hawaii carry:
  - **Administrative Penalties:** Up to **$10,000 per offense**.
  - **Criminal Penalties (HB 1961):** Intentionally or recklessly violating specific health parts is a **petty misdemeanor**.
    - **1st Offense:** Minimum **$250 fine** and **24 hours imprisonment**.
    - **2nd Offense:** Minimum **$750 fine** and **7 days imprisonment**.
    - **3rd+ Offense:** Minimum **$1,000 fine** and up to **30 days imprisonment**.
- **Federal HIPAA Overlay:** For data-related healthcare violations, federal fines range from **$137 to $68,928 per violation**, with criminal terms up to **10 years** for malicious intent.

Privacy

- **Geolocation & Browser Data (SB 3017 / SB 1163):**
  - **Civil Penalties:** The Attorney General can seek up to **$10,000 per violation, per day**.
  - **Consumer Redress:** Consumers may sue for the greater of **$1,000 or treble (triple) damages** per violation.
- **Data Broker Violations (HB 2463):** Non-compliance with deletion requests or registration typically triggers daily civil fines similar to general consumer protection laws (**$500 to $10,000 per violation**).

Pharmacy Benefit Managers (PBMs)

- **Pricing & Transparency (HB 2225):** Violations related to non-disclosure or discriminatory reimbursement are generally treated as unfair or deceptive acts.
  - **General Fines:** Civil penalties typically range from **$500 to $10,000 per violation**, enforced by the Director of the Office of Consumer Protection.

Financial Data Exchange (FDX)

- Because FDX compliance in Hawaii currently relies on **federal standards** (like the CFPB 1033 rule), state-specific criminal penalties are rare. Civil enforcement for data security failures falls under Hawaii's **Data Breach Notification law**, where failure to notify can result in a civil penalty of up to **$2,500 for each violation**.

Idaho

https://share.google/aimode/00KZxlRtLEbCRzOzM Click on link to see the saved Google AI search result.

Violations of Idaho's specific regulations for AI, healthcare, privacy, and PBMs carry a wide range of penalties, from administrative fines to significant criminal prison time.

Artificial Intelligence (AI)

Idaho's AI laws focus on protecting its development as free speech while regulating specific consumer interactions.

- **Consumer Deception (HB 127):** Using an AI agent or chatbot without disclosing it is AI is an "unfair and deceptive trade practice."
  - **Civil Penalties:** A minimum of **$10,000** plus **$1,000 per violation**.
  - **Private Right of Action:** Consumers can sue for actual damages or **$1,000 statutory damages**, whichever is greater. Class action damages are capped at **$10,000**.
- **Explicit Synthetic Media:** Disclosing "explicit synthetic media" (deepfakes) without consent is a crime.
  - **Criminal Penalties:** Typically prosecuted as a misdemeanor or felony depending on the severity and intent to harm.

Healthcare & Medicaid

Idaho enforces strict anti-fraud and anti-kickback statutes for healthcare providers and Medicaid services.

- **Medicaid Fraud and Abuse (ID Code § 56-209h):**
  - **Civil Penalties:** Up to **$1,000 per violation** plus recovery of all improper payments.
  - **Administrative:** Immediate suspension of payments or termination of provider agreements.
- **Insurance Fraud (ID Code § 41-293):** Intentionally deceiving an insurer for money or benefits.
  - **Criminal Penalties:** A **felony** punishable by up to **15 years in prison**.
  - **Criminal Fine:** Up to **$15,000** per instance.
- **Anti-Kickback Violations (ID Code § 41-348):**
  - **Civil Penalties:** Monetary penalties of up to **$5,000 per referral**.

Privacy & Data Security

Penalties for privacy violations in Idaho distinguish between commercial entities and government employees.

- **Data Breach Notification (ID Code § 28-51-105):** Intentional failure to notify residents of a data breach.
  - **Civil Fine:** Up to **$25,000 per breach**.
- **Government Employee Disclosure:** A government employee who intentionally discloses personal information not allowed by law is guilty of a **misdemeanor**.
  - **Criminal Penalties:** Up to **1 year in jail**.
  - **Fine:** Up to **$2,000**.
- **HIPAA Violations (Federal/State Enforced):**
  - **Civil:** Tiers ranging from **$137** to **$2,067,813** annually depending on the level of neglect.

- **Criminal:** Up to **10 years in prison** and fines of **$250,000** for malicious intent to sell data.

Pharmacy Benefit Managers (PBMs)

The **Idaho Department of Insurance (DOI)** oversees PBM compliance under the new 2025 transparency laws.

- **Regulatory Violations (ID Code § 41-349):**
  - **Administrative Action:** Includes significant **fines** and the potential **loss of license** to operate in Idaho.
  - **Specific Bans:** Violating the ban on "spread pricing" or failing to pass through 100% of rebates can trigger DOI enforcement actions and fines.

Financial Data Exchange (FDX)

There are currently **no specific Idaho state-level criminal or civil fines** for FDX standards, as they are market-led. However, once the federal **Section 1033** rule is fully implemented, violations would fall under the **Consumer Financial Protection Bureau (CFPB)** enforcement authority, which can levy civil penalties of over **$1 million per day** for "knowing" violations of federal consumer financial laws.

Illinois

https://share.google/aimode/lU6OSMSRD3xNIF2oa Click on link to see the saved Google AI search result.

Penalties for violating Illinois regulations in these sectors vary by the specific act violated, ranging from civil fines per incident to felony criminal charges for serious healthcare-related offenses.

Artificial Intelligence (AI)

- **Healthcare (Mental Health):** Under the **Wellness and Oversight for Psychological Resources Act** (effective August 2025), use of AI to make independent therapeutic decisions or interact with patients without licensed human oversight carries civil penalties of up to **$10,000 per violation**.
- **Employment Discrimination:** Violations of the **Illinois Human Rights Act** (as amended by HB 3773, effective January 1, 2026) regarding discriminatory AI hiring practices or failure to provide notice can result in:
  - **Civil Penalties:** Up to **$16,000** for a first offense, **$42,500** for a second within five years, and up to **$70,000** for three or more within seven years.
  - **Remedies:** Back pay, reinstatement, and attorney's fees.
- **AI Likeness:** Violations involving unauthorized digital replicas (Digital Voice and Likeness Protection Act) can result in statutory damages of **$1,000** or actual damages plus profits.

Healthcare & Pharmacy Benefit Managers (PBMs)

- **Healthcare Fraud:** Generally a **Class 4 felony**, punishable by:
  - **Imprisonment:** Up to **3 years**.
  - **Fines:** Up to **$25,000** for individuals and **$50,000** for corporations.
  - **Serious Violations:** If a violation results in death, penalties can increase up to **life imprisonment** under certain statutes.
- **PBM Regulations:** PBMs failing to provide required certifications or violating insurance code provisions may face "appropriate regulatory action" by the Director of Insurance, though specific statutory fine amounts for PBM-specific codes are typically assessed per violation under general insurance code authority.

Privacy

- **Biometric Privacy (BIPA):** Aggrieved individuals can sue for:
  - **Negligent Violations: $1,000** per violation.
  - **Intentional/Reckless Violations: $5,000** per violation.
  - **2026 Limit:** Following 2024 amendments, "per violation" is now limited to **one recovery per person** for repeated collections of the same biometric data, preventing the "annihilative" damages seen in earlier years.
- **Healthcare Privacy (HIPAA State Enforcement):** The Illinois Attorney General may issue fines up to **$25,000 per violation category, per year**.
- **Workplace Privacy:** Violations of the Right to Privacy Workplace Act carry fines **$100 to $1,000** per violation, increasing to **$1,000–$5,000** for repeat offenses within three years.

Indiana

https://share.google/aimode/3qyjwmiU5uXRWtzPd Click on link to see the saved Google AI search result.

As of 2026, Indiana has established specific civil penalties for violations of privacy, pharmacy benefit management (PBM), and healthcare-related regulations. Criminal penalties generally apply to broader categories like "invasion of privacy" or unauthorized medical practices.

1. Privacy (Indiana Consumer Data Protection Act - ICDPA)

Effective **January 1, 2026**, the ICDPA is enforced solely by the Indiana Attorney General.

- **Civil Penalties**: Up to **$7,500 per violation**.
- **Cure Period**: Businesses have a **30-day "right to cure"** notice. If they rectify the violation within this period, the Attorney General may not proceed with an enforcement action.
- **Additional Costs**: The Attorney General may also recover reasonable investigative and litigation costs, including attorney's fees.
- **Private Right of Action**: There is **no private right of action** for individuals to sue under the ICDPA.
- **Criminal Penalties**: While the ICDPA is civil, general Indiana law classifies "Invasion of Privacy" as a **Class A Misdemeanor** (up to 1 year in jail and $5,000 fine), which can be elevated to a **Level 6 Felony** (6 months to 2.5 years in prison) for repeat offenders.

2. Pharmacy Benefit Managers (PBMs)

New reforms including **SB 140** and **HB 1606** (effective 2025/2026) regulate PBM practices.

- **Civil Penalties**:
  - **$1,000** for the first violation.
  - **$2,500** for the second violation.
  - **$10,000** for each additional violation.
- **Administrative Sanctions**: The Insurance Commissioner may suspend or revoke a PBM's license for noncompliance.
- **Reimbursement**: The commissioner may order a PBM to reimburse persons who incurred monetary loss due to violations.

3. Healthcare and AI Disclosure

Regulations governing AI use in healthcare (IC 16-51-2.5 and IC 27-8-44) take effect **July 1, 2025**.

- **Disciplinary Action**: Healthcare practitioners who violate AI disclosure or telehealth regulations are subject to disciplinary action by their respective licensing boards under **IC 25-1-9**.
- **Fines for Practitioners**: Licensing boards may assess fines up to **$1,000 per violation**.
- **Infractions for Employers**: An employer or contractor of a practitioner who violates these standards commits a **Class B Infraction**, which typically carries a civil fine but no imprisonment.
- **Reporting Violations**: Hospitals or entities failing to meet expanded ownership disclosure requirements can face fines of **$1,000 per day** for late reports.

4. Artificial Intelligence (State Agency Policy)

For state employees and partners, AI regulations are largely administrative and contractual.

- **Employee Discipline**: Violations by state employees may constitute **misconduct**, potentially leading to termination or removal from AI activities.
- **Contractual Penalties**: External partners (contractors) violating AI policies may face contract termination and removal of access to state systems.
- **Deepfake Penalties**: Under 2026 legislation (HB 1183), creating or distributing certain nonconsensual AI-generated images can range from a **Class A Misdemeanor** to a **Level 5 Felony** (up to 6 years imprisonment and $10,000 fine).

Iowa

https://share.google/aimode/uxxo6uPU9xjLaGevG Click on link to see the saved Google AI search result.

In Iowa, penalties for regulatory violations in 2026 range from administrative civil fines to criminal felony charges, depending on the specific sector and the severity of the offense.

1. AI and Synthetic Media

Iowa's regulation of AI primarily targets deceptive content and election integrity (e.g., **SF 2166** as of early 2026).

- **Civil Penalties:** Violators are subject to a fine of up to **$1,000** for a first offense and up to **$5,000** for each subsequent offense.
- **Criminal Penalties:** Knowing violations committed with the **intent to defraud** are classified as a **serious misdemeanor**.
    - **Imprisonment:** Up to **one year** in jail.
    - **Fines:** Between **$430** and **$2,560**.
- **Private Right of Action:** Injured parties may also bring civil suits for injunctive relief and damages, including reasonable attorney fees.

2. Privacy (ICDPA)

The **Iowa Consumer Data Protection Act (ICDPA)** is enforced exclusively by the Iowa Attorney General; there is no private right of action for consumers.

- **Civil Penalties:** Up to **$7,500 per violation**.
- **Mandatory Cure Period:** The Attorney General must provide a **90-day** written notice and opportunity to cure before initiating any legal action or imposing fines.
- **Criminal Penalties:** There are currently **no criminal penalties** for standard consumer data privacy violations under the ICDPA.

3. Healthcare (General and AI Utilization)

Penalties for healthcare entities vary based on the type of facility and the nature of the violation.

- **Health Facility Citations:** Under **Iowa Code 135C.36**, a "Class I" violation (direct threat to life/safety) carries a penalty of **$2,000 to $10,000** per citation.
- **Medical Assistance/Fraud:** Violations involving medical assistance funds can result in suspension from programs or criminal charges. Convictions for crimes punishable by **over one year** of imprisonment can lead to permanent exclusion from state health programs.
- **AI in Utilization Review:** Complaints regarding non-compliance with AI-driven medical reviews (SF 562) are directed to the **Iowa Insurance Division**, which may issue administrative orders and penalties.

4. Pharmacy Benefit Managers (PBMs)

PBM regulation in Iowa (SF 383) is currently facing significant legal challenges in federal court, which has temporarily stayed some enforcement.

- **Administrative Penalties:** The Iowa Insurance Commissioner has the authority to impose monetary penalties and risk the **PBM's licensure** in the state for non-compliance.
- **Civil Actions:** The Attorney General can seek **restitution and reimbursement** for impacted Iowans, as seen in ongoing litigation against PBMs for alleged pricing schemes.
- **Criminal Penalties:** While standard PBM violations are civil/administrative, they may trigger criminal investigations if they involve broader fraud or "deceptive trade practices".

5. FDX (Financial Data Exchange)

As FDX is a technical standard rather than a specific Iowa state law, its "penalties" are largely tied to broader financial consumer protection laws.

- **Federal Authority:** Primary enforcement of financial data rights falls under the **CFPB Section 1033**. While a judicial stay exists as of early 2026, future violations could trigger federal civil penalties of up to **$5,000 to $1,000,000+ per day**, depending on the level of "knowing" non-compliance.
- **State Level:** Failure to provide consumer-permissioned data could be pursued as an "unfair or deceptive act or practice" under the **Iowa Consumer Fraud Act**, carrying civil penalties of up to **$40,000** per violation.

Standard Iowa Criminal Penalty Framework (2026)

If a regulatory violation is escalated to a criminal charge, the following statutory maximums apply:

Charge Level	Max Imprisonment	Fine Range
Serious Misdemeanor	1 Year	$430 – $2,560
Aggravated Misdemeanor	2 Years	$855 – $8,540
Class D Felony	5 Years	$1,025 – $10,245
Class C Felony	10 Years	$1,370 – $13,660

Kansas

https://share.google/aimode/U1pbsSD0t8Lv7xVmi Click on link to see the saved Google AI search result.

In Kansas, penalties for violating regulations in AI, healthcare, privacy, and PBM sectors vary based on whether the violation is civil or criminal. As of early 2026, the specific penalties for the regulations mentioned are as follows:

Artificial Intelligence (AI) & Healthcare

Regulatory oversight for AI in Kansas recently introduced civil fines and professional sanctions for specific harms.

- **Healthcare AI Misconduct (SB 405, 2026)**:
  - **Civil Fine**: Up to **$50,000 per violation**.
  - **Injunctive Relief**: Courts may order a temporary or permanent cease of the AI's operation until the conduct is corrected, or mandate new training for the AI model.
- **Government AI Ban (HB 2313, 2025)**:
  - This law primarily mandates administrative action (deactivating and deleting accounts) rather than direct criminal fines for state employees. However, genetic data violations linked to these platforms carry significant criminal weights:
    - **Class C Felony**: Selling or transferring genetic data to a third party without consent.
    - **Class D Felony**: Disclosing another individual's genetic data to a third party.
    - **Class A Misdemeanor**: Collecting/retaining DNA with intent to perform unauthorized analysis.
- **Judicial Sanctions (Standing Order 26-01)**:
  - Attorneys using AI to generate "hallucinated" citations in court filings may face **Rule 11 sanctions**, including monetary penalties, attorney fees, and disciplinary referrals to licensing authorities.

Pharmacy Benefit Managers (PBMs)

The **Kansas Consumer Prescription Protection and Accountability Act (SB 360, 2026)** enforces strict licensing and operational standards.

- **Unlicensed Operation**: A fine of **$5,000 to $100,000** for the period in which the PBM operated without a license.
- **Administrative Orders**: The Insurance Commissioner may issue cease and desist orders or modify existing orders to protect public interest.

Privacy & Cybersecurity

While Kansas lacks a singular comprehensive privacy law, sector-specific privacy violations (like genetic data or consumer funding) have established tiers.

- **Consumer Legal Funding (SB 426, 2026)**:
  - **Statutory Damages**: A company violating the transparency act is liable to the consumer for up to **$10,000 per violation** or **three times actual damages**, whichever is greater.
  - **Contract Termination**: Violations result in the **automatic termination** of the legal funding contract.
- **Cybersecurity & Consumer Protection (KCPA)**:
  - **Civil Penalties**: Generally up to **$10,000 per violation** for acts declared unlawful.
  - **Willful Court Order Violations**: Civil penalties of up to **$20,000 per violation**.
- **Deepfakes & Sexual Privacy**:

- **Civil Recovery**: Plaintiffs can recover actual damages, **punitive damages** (equal to all revenue the defendant received from the content), and attorney fees.
- **Criminal Class A Misdemeanor**: Punishable by up to **one year in jail** and a **$2,000 fine** if there is harmful intent.

Summary of Penalty Ranges

Category	Civil Fine (Max)	Criminal Fine (Max)	Imprisonment (Max)
Healthcare AI (SB 405)	$50,000 / violation	N/A (Bill focus is civil)	N/A
Genetic Data (HB 2313)	Varies by KCPA	$100,000+ (as part of Felony)	5-20+ years (Class C/D Felony)
PBM (SB 360)	$100,000	Administrative/Fine based	N/A
Deepfakes (NCII)	Unlimited Punitive	$2,000	1 year (Misdemeanor)
Consumer Privacy	$10,000 / violation	N/A	N/A

Note: FDX (Financial Data Exchange) regulations in Kansas are currently market-led; specific state-level statutory penalties have not yet been codified as federal rules (Section 1033) remain under judicial stay.

Kentucky

https://share.google/aimode/WFT8Chp1GeQ6IN7qe Click on link to see the saved Google AI search result.

Violations of Kentucky's 2026 regulations carry substantial civil penalties, though criminal imprisonment is generally reserved for egregious data breaches or fraud within specific sectors.

Privacy (KCDPA)

The Kentucky Consumer Data Protection Act (KCDPA) is enforced exclusively by the Kentucky Attorney General.

- **Civil Penalty:** Up to **$7,500 per violation**.
- **Cure Period:** Businesses have a **30-day "cure period"** to fix a violation before any fines are assessed.
- **Multipliers:** Because fines are per violation, large-scale data mishandling affecting thousands of residents can result in millions in cumulative penalties.
- **Criminal:** The KCDPA itself does not establish criminal prison sentences, but extreme cases (e.g., identity theft) may still fall under broader state criminal codes.

Artificial Intelligence (AI)

- **State Use (HB 672):** There are currently no direct criminal penalties for government agencies. Instead, oversight is handled via the AI Governance Committee, and citizens have a **right to appeal** AI-driven decisions.
- **Consumer AI (Lawsuits):** Companies like Character.AI are currently facing **civil lawsuits** by the Attorney General for violating existing consumer protection and KCDPA laws, with the state seeking injunctions and maximum civil fines.
- **Election Deepfakes:** Candidates may bring **civil actions** for damages if their likeness is manipulated within 45 days of an election.

Healthcare & Medical Data

Healthcare violations often involve both Kentucky-specific rules and federal HIPAA standards.

- **Medical Privacy (KRS 223.991):** Violating general public health certification rules is a **misdemeanor**, with fines of **$100–$500** and up to **30 days in jail** per day the violation continues.
- **HIPAA/Data Misuse:**
  - **Knowing Disclosure:** Up to **$50,000** fine and **1 year in prison**.
  - **False Pretenses:** Up to **$100,000** fine and **5 years in prison**.
  - **Malicious Intent (Selling Data):** Up to **$250,000** fine and **10 years in prison**.
- **Organ Brokering:** Knowingly failing to report illegal organ sales carries a fine of **$10,000–$50,000**.

Pharmacy Benefit Managers (PBMs) & FDX

- **License Penalties:** PBMs pay a **$500 penalty** for late license renewals. New regulations (201 KAR 2:416) also introduced a **$10,000 registration fee** for increased oversight.
- **Reimbursement Violations:** Under SB 188, the Department of Insurance (DOI) can order PBMs to reimburse pharmacies for the difference in mandatory fees (e.g., the **$10.64** floor), though many contract disputes are referred to the courts.
- **FDX:** Penalties for financial data misuse align with the Kentucky Consumer Protection Act, which allows for civil penalties of up to **$2,000 per violation** (or $10,000 if the victim is over 60) for unfair or deceptive practices.

Louisiana

https://share.google/aimode/vaaMmZy36UcRTL9m8 (click on link to see the saved Google AI search result)

Louisiana has established significant civil and criminal penalties for violations related to AI-generated content, healthcare AI usage, data privacy, and Pharmacy Benefit Managers (PBMs).

Artificial Intelligence (AI)

Penalties for AI focus heavily on the nonconsensual creation and distribution of deepfakes.

- **Sexually Explicit Deepfakes (Adults):** Violations are classified as a **misdemeanor**, punishable by up to **6 months** in jail, a fine of up to **$750**, or both.
- **Deepfakes Involving Minors:**
  - **Creation/Possession: 5 to 20 years** at hard labor and a fine of up to **$10,000**.
  - **Sale/Promotion: 10 to 50 years** at hard labor and a fine of **$50,000**.
- **Legal Evidence:** Use of AI-generated evidence in court without disclosure can result in **sanctions** authorized by the court.

Healthcare

The focus is on the authorized vs. prohibited use of AI tools by providers.

- **Independent Diagnosis/Treatment by AI:** Proposed legislation (HB114, 2025) establishes a civil penalty of **$10,000 per violation** if AI is used to treat or diagnose patients without professional human review.
- **Standard Healthcare Violations:** Civil fines for general regulatory violations range from **$50 to $100** for minor administrative issues to **$20,000 per month** for repeated serious violations.

Privacy

Penalties for privacy revolve primarily around data breach notifications and unauthorized access to health information.

- **Data Breach Notification:**
  - **Civil Fines:** Failure to notify the Attorney General within 10 days of a breach can result in a fine of up to **$5,000 per violation per day**.
  - **Civil Action:** Individuals may file a private right of action to recover **actual damages**.
- **Wrongful Disclosure of Health Info (Criminal):**
  - **Knowing Violation:** Up to **1 year** in prison and a **$50,000** fine.
  - **False Pretenses:** Up to **5 years** in prison and a **$100,000** fine.
  - **Intent to Sell/Malicious Harm:** Up to **10 years** in prison and a **$250,000** fine.

Pharmacy Benefit Managers (PBMs)

The **PBM Reform Act of 2025** provides robust enforcement powers to state officials.

- **Civil Monetary Penalties:** Violations of PBM regulations can result in fines of up to **$1,000 per claim**.
- **Unfair Trade Practices:** Many violations are categorized as unfair trade practices, allowing the Attorney General to seek **restitution**, **treble (triple) damages**, and attorney fees.
- **Enforcement Fund:** Penalties collected are deposited into a dedicated PBM Enforcement Fund to cover investigation costs.

Maine

https://share.google/aimode/1nmVFbEBDsPsRgn8d Click on link to see the saved Google AI search result.

Maine's 2026 regulatory landscape includes civil and criminal penalties for non-compliance, primarily enforced through the Maine Attorney General and the Bureau of Insurance.

Artificial Intelligence (AI)

- Consumer AI Transparency (LD 1154): Violations are treated as breaches of the Maine Unfair Trade Practices Act (UTPA).
  - Civil Penalty: Up to $1,000 per violation.
  - Private Right of Action: Consumers can sue for actual damages if they suffer financial loss due to a violation.
- AI Healthcare Denials (LD 1301): Failure to involve a clinical peer in an AI-driven denial is a regulatory violation.
  - Civil Penalty: General insurance violations are punishable by fines up to $1,000 per instance, potentially up to $25,000 per day for repeat offenders within 5 years.

Privacy

- Consumer Data Privacy Act (LD 1088): Enforced by the Attorney General under the UTPA framework.
  - Civil Penalty: Up to $10 million for initial violations and up to $30 million for subsequent or persistent violations.
  - Cure Period: The Attorney General must provide 30 days' notice to allow a business to correct a violation before initiating an action.
- Employee Surveillance (LD 61):
  - Civil Penalty: Fines ranging from $100 to $500 for each violation.
- Data Breach Notification:
  - Civil Penalty: Fines of up to $500 per violation, capped at $2,500 per day.

Pharmacy Benefit Managers (PBMs)

- Spread Pricing & Rebate Compliance (LD 1580):
  - Civil Penalty: Failure to obtain a proper PBM license results in a fine of $5,000 per day.
  - Certification Violations: PBMs must certify compliance with the spread pricing ban annually. Non-compliance is generally subject to insurance regulatory penalties, which include fines of up to $1,000 or imprisonment for less than one year for willful violations.
- Withdrawal from State Market: Manufacturers who withdraw drugs to avoid price regulations face a massive civil penalty of $500,000 assessed by the Attorney General.

Healthcare & PFML

- Paid Family and Medical Leave (PFML):
  - Civil Penalty: Employers failing to pay required premiums or provide notice are subject to a $100 fine per employee per violation.
- Medical Privacy (LD 1088/Existing Statues):
  - Civil Penalty: Intentional disclosures of health data can result in penalties of up to $5,000 per disclosure. If deemed a general business practice, fines can reach $50,000 for a facility.

FDX & Financial Data

- Maine follows federal standards for financial data exchange. Violations of data security laws (e.g., identity theft or unauthorized access) are categorized as:
  - Criminal Penalty: Class D crimes (Identity Theft), which carry sentences of less than one year of imprisonment and a maximum $2,000 fine.

Maryland

https://share.google/aimode/NczSNAioenbQo2qyp (click on link to see the saved Google AI search result)

Maryland's enforcement landscape for AI, privacy, and PBMs includes substantial civil fines, administrative sanctions, and potential criminal misdemeanor charges for specific violations.

AI & Healthcare Penalties (HB0820/HB1240)

- **Civil Penalties**: The Insurance Commissioner or relevant department can impose fines of **up to $10,000 per offense**.
- **Criminal Penalties**: Violations regarding the use of AI in healthcare utilization management may result in **misdemeanor charges**.
- **Administrative Actions**: Non-compliance can lead to the **suspension or revocation of certificates**, cease-and-desist orders, and requirements to provide **restitution to harmed patients**.

Privacy Penalties (MODPA)

Maryland's privacy law (MODPA) is enforced under the **Maryland Consumer Protection Act (MCPA)**.

- **Civil Fines**:
  - **First Violation**: Up to **$10,000** per violation.
  - **Repeated Violations**: Up to **$25,000** per violation.
- **Criminal Penalties**: Violations of the MCPA are considered a **misdemeanor**, punishable by a fine of up to **$1,000** and/or **imprisonment for up to one year**.
- **Grace Period**: Until **April 1, 2027**, a **60-day cure period** may be granted at the Attorney General's discretion before penalties are imposed.

PBM Penalties (SB896)

- **Civil Fines**: The Insurance Commissioner may impose a penalty of **up to $10,000 for each violation**.
- **Administrative Orders**: PBMs can be ordered to:
  - **Cease and desist** the illegal activity.
  - Take specific **affirmative actions** to correct the violation.
  - Provide **restitution** of money or assets.
- **Daily Penalties (for Carriers/MCOs)**: For certain related health mandates, additional penalties of up to **$1,000 per day** can apply until compliance is reached after notification.

Summary of Health Data Penalties (HIPAA-Related)

While MODPA excludes some HIPAA data, separate Maryland health-general laws apply to identifiable health info:

- **Knowing Violations**: Liable for **actual damages**.
- **Intent to Sell/Personal Gain**: If health information is wrongfully disclosed for commercial advantage or malicious harm, criminal penalties can reach up to **$250,000** in fines and/or **10 years of imprisonment**.

Massachusetts

https://share.google/aimode/HNjG6SzTewHS1b3y5 (click on link to see the saved Google AI search result)

Massachusetts enforcement for AI, healthcare, privacy, and PBMs involves a tiered system of civil penalties and criminal sanctions. Many of these regulations were established or expanded through legislation effective in **2025** and **2026**.

Artificial Intelligence (AI)

Penalties are primarily enforced through the **Massachusetts Consumer Protection Act** (Chapter 93A) and specific new statutes.

- **Civil Penalties**: Attorney General enforcement can result in fines of up to **$5,000 per violation**. For specific platforms violating child safety or mental health outcomes, civil penalties can reach **$500,000**.
- **Criminal Penalties**: Specialized offenses, such as the creation of AI-generated child sexual abuse material, carry severe criminal penalties:
    - **Imprisonment**: Up to **10 years** in state prison or 2.5 years in a house of correction.
    - **Criminal Fines**: **$10,000 to $50,000**.

Healthcare

Breaches of patient confidentiality and reporting requirements incur both state and federal (HIPAA) penalties.

- **Civil Penalties**:
    - **Reporting Violations**: Failure to make timely reports (e.g., by Registered Provider Organizations) can result in fines of **$25,000 per week**.
    - **HIPAA/State Privacy**: Civil fines range from **$100 to $50,000** per violation, with a calendar-year cap of approximately **$2.06 million** for willful neglect.
- **Criminal Penalties**:
    - **Licensing**: Operating a long-term care facility without a license is punishable by a fine of up to **$1,000** or imprisonment for up to **two years**.
    - **Patient Data Misuse**: Intentional misuse of health information for personal gain or malicious harm can lead to up to **10 years** in prison and a fine of **$250,000**.

Privacy

The **Massachusetts Data Privacy Act (MDPA)**, effective **July 1, 2026**, is enforced exclusively by the Attorney General.

- **Civil Penalties**: Violations are treated as unfair trade practices under Chapter 93A, with penalties of up to **$5,000 per violation**.
- **Cure Period**: Businesses have a **60-day period** to fix violations between July 2026 and December 2027 before facing penalties.
- **Private Right of Action**: While the MDPA largely bars private suits, some versions (H. 4746) propose a private right of action for "large data holders" under Chapter 93A, allowing for **double or treble (triple) damages** for willful violations.

Pharmacy Benefit Managers (PBMs)

New regulations effective **January 1, 2026**, empower the DOI to enforce compliance.

- **Unlicensed Operation**: Fines of **$5,000 per day** for operating without a license.
- **Statutory Violations**: General violations of PBM laws carry a minimum fine of **$5,000**.
- **False Reporting**: Knowingly submitting false or misleading information in required reports can lead to civil penalties of up to **$25,000 per violation**.
- **Prohibited Practices**: Engaging in banned "spread pricing" or retroactive fees may result in a **10% surcharge**.
- **License Sanctions**: The DOI may also suspend, revoke, or refuse to renew a PBM's license for fraudulent activity or failure to comply with reporting.

Michigan

https://share.google/aimode/WB8Ej8E9zBzTaygRD **Click on link to see the saved Google AI search result**

In Michigan, penalties for violating regulations in healthcare, AI, privacy, and Pharmacy Benefit Management (PBM) range from administrative fines to significant criminal imprisonment, depending on the severity of the violation and intent.

1. Pharmacy Benefit Managers (PBMs)

Under the **Pharmacy Benefit Manager Licensure and Regulation Act** (PA 11 of 2022), the Department of Insurance and Financial Services (DIFS) oversees enforcement.

- **Civil/Administrative Penalties:**
  - **Suspension/Restriction Fines:** A PBM with a suspended or restricted license may be fined up to **$20,000 per month** until the issue is remedied.
  - **Transparency Violations:** Failure to submit annual transparency reports by the April 1 deadline can lead to license suspension or revocation.
  - **General Non-Compliance:** DIFS has the authority to issue rules establishing specific fines, restrictions, or the complete revocation of a PBM's license for act violations.

2. Artificial Intelligence (AI)

As of 2026, Michigan has introduced aggressive legislation (HB 4667 and HB 4668) targeting the misuse of AI.

- **Criminal Penalties (Proposed/Active 2026):**
  - **Felony AI Misuse:** It is a felony to possess, develop, or deploy an AI system with the intent to commit a crime.
  - **Imprisonment:** Penalties range from **4 to 8 years** in prison, with mandatory consecutive sentencing for certain AI-related crimes.
  - **Mandatory Restitution:** Convicted individuals must pay restitution to victims of AI-facilitated crimes.
- **Civil/Regulatory Penalties:**
  - Proposed rules in 2025–2026 would require AI developers to implement safety protocols and risk assessments; failure to do so could result in significant administrative fines.

3. Healthcare Privacy (HIPAA & State Law)

Michigan healthcare privacy is enforced through both state statutes and federal HIPAA/HITECH standards.

- **Civil Monetary Penalties (Per Violation):**
  - **Unknowing Violation:** $100 – $50,000; annual cap of $1.5 million (inflation-adjusted for 2026).
  - **Reasonable Cause:** $1,000 – $50,000; annual cap of $1.5 million.
  - **Willful Neglect (Corrected within 30 days):** $10,000 – $50,000.
  - **Willful Neglect (Uncorrected):** Minimum **$50,000 per violation**; annual cap of $1.5 million.
- **Criminal Penalties (Federal/State Prosecution):**
  - **Knowing Disclosure:** Up to **$50,000** fine and up to **1 year** in prison.
  - **False Pretenses:** Up to **$100,000** fine and up to **5 years** in prison.
  - **Personal Gain/Malicious Harm:** Up to **$250,000** fine & **10 years** in prison.

4. General Healthcare Violations

- **Misdemeanor Violations:** General violations of Michigan's Public Health Code (Act 368 of 1978) are typically classified as misdemeanors, punishable by up to **6 months** in jail, a fine of up to **$200**, or both.
- **Corporate Violations:** Health care corporations that violate specific sections of the Michigan Insurance Code (such as improper use of Social Security numbers) face fines of up to **$1,000 per violation**.
- **Private Right of Action:** For certain privacy or insurance code violations, individuals can sue for actual damages or a statutory minimum of **$200**, whichever is greater, plus attorney fees.

Minnesota

https://share.google/aimode/8pDWDZbvu5G39p2RK Click on link to see the saved Google AI search result.

In Minnesota, penalties for violating regulations in AI, healthcare, privacy, and PBMs vary significantly by sector, ranging from civil fines to felony imprisonment.

1. Artificial Intelligence (AI)

Penalties primarily target deepfakes and automated decision-making in healthcare.

- **Election Deepfakes:**
  - **90-day First Offense:** Imprisonment up to **90 days** and/or a fine up to **$1,000**.
  - **Violence/Bodily Harm Intent:** Imprisonment up to **1 year** and/or a fine up to **$3,000**.
  - **Repeat Offense (within 5 years):** Felony imprisonment up to **5 years** and/or a fine up to **$10,000**.
- **Sexual Deepfakes:**
  - **Criminal:** Felony imprisonment up to **3 years** and/or a fine of **$5,000**.
  - **Civil:** Victims may seek a civil penalty of up to **$100,000**, plus general/special damages and attorney fees.
- **Healthcare AI (Prior Authorization):** While specific statutory fines for the new 2026 ban are often handled via administrative insurance licensing, standard health carrier violations can lead to fines under the Commissioner of Commerce's general authority (typically up to **$10,000 per violation**).

2. Privacy (MCDPA)

The Minnesota Consumer Data Privacy Act is enforced exclusively by the Attorney General.

- **Civil Penalties:** Up to **$7,500 per violation**.
- **Other Relief:** The court may order injunctive relief and recovery of reasonable attorney fees and litigation expenses.
- **Private Right of Action:** Explicitly **prohibited**; consumers cannot sue for statutory damages under this act.

3. Healthcare (Health Records Act)

- **Civil Penalties:** Patients can sue for **compensatory damages**, plus costs and reasonable attorney fees.
- **Administrative:** Disciplinary action by licensing boards, including civil penalties up to **$7,500 per separate violation** and potential license suspension or revocation.
- **Government Data (MGDPA):** For violations by government entities, civil penalties are up to **$1,000**, while willful violations by employees can result in **criminal prosecution** and dismissal.

4. Pharmacy Benefit Managers (PBMs)

Enforcement is managed by the Minnesota Department of Commerce.

- **General Violations:** Administrative fines of up to **$25,000 per violation** (each occurrence is a separate violation).
- **Unlicensed Activity:** A fine of **$5,000**, with a minimum of **$10,000 per day** for the duration of the violation.
- **Fiduciary Duty Breach:** Can lead to broader civil liability and mandatory reimbursement of overpayments or illicit "spread" profits.

5. Financial Data Exchange (FDX)

- **Regulatory Basis:** Primarily governed by federal CFPB Section 1033 and Minnesota's general consumer protection laws.
- **Penalties:** Administrative penalties for non-compliance with secure data sharing can reach **thousands of dollars per day** under federal authority, while Minnesota's AG can apply general deceptive trade practice penalties (typically up to **$10,000 per violation**).

Mississippi

https://share.google/aimode/Gv9E6ZF90H5ssqZPu Click on the link to see the saved Google AI search result.

Violations of Mississippi's recent regulations on AI, healthcare, privacy, and PBMs carry significant civil and administrative penalties, with specific criminal consequences for malicious use of AI.

1. AI & Healthcare (HB 1717)

The **Mississippi Medical Judgment Protection Act** focuses on ensuring human oversight in medical AI applications.

- **Administrative Fines**: Payers (insurers) who violate the act by using AI to automate the denial of medical services may be fined up to **$5,000 per violation**.
- **Licensing Sanctions**: For clinicians and healthcare facilities, a violation constitutes "unprofessional conduct" or failure to meet the minimum standard of care. This can lead to **license suspension or revocation** by the respective state licensing board.
- **Criminal Penalties (Malicious AI Use)**: Under separate legislation (SB 2577), using AI to create digital content with the intent to cause harm, incite violence, or deter voting is a felony punishable by up to **5 years in prison** and/or a fine of up to **$50,000**.

2. Privacy (HB 1051)

The **Mississippi Consumer Privacy Protection Act** provides for enforcement primarily through the state's Attorney General.

- **Civil Penalties**: Businesses ("controllers") found in violation of consumer data rights can face civil penalties of up to **$7,500 per violation**.
- **Private Right of Action**: In the event of a data breach, consumers may sue for statutory damages ranging from **$100 to $750 per consumer** per incident, or actual damages, whichever is greater.
- **Injunctions**: The Attorney General has the authority to issue cease-and-desist orders and seek court-ordered injunctions to stop unlawful data processing.

3. Pharmacy Benefit Managers (PBMs) (HB 1672)

PBM regulations are enforced by the **Mississippi Board of Pharmacy**.

- **Administrative Penalties**: PBMs or PSAOs that fail to pay 95% of "clean claims" within a calendar quarter are subject to an administrative penalty of up to **$25,000**.
- **Daily Fines**: General violations of market conduct rules or failure to respond to information requests can carry a fine of up to **$1,000 per day**, up to a maximum of **$50,000**.
- **Licensing Actions**: The Board may also issue cease-and-desist orders or suspend/revoke a PBM's license for repeated failure to comply with prompt pay or anti-steering laws.

4. Financial Data Exchange (FDX)

As there is no standalone Mississippi "FDX Act," enforcement generally falls under broader state and federal financial statutes.

- **Civil Disciplinary Penalties**: Under the **Mississippi Securities Act**, registered financial entities can be fined up to **$25,000 per violation**.
- **Criminal Penalties**: Willful violations of state securities laws involving financial data can result in a fine of up to **$25,000** and potentially criminal prosecution for fraud.
- **Elder Protection**: Fines may be increased by up to **$15,000** if the violation is committed against a disabled person or an elder.

Missouri

https://share.google/aimode/EsPhlOux8To6GZ3Mu (click on link to see the saved Google AI search result)

Missouri's legal landscape for 2026 includes established federal penalties and new state-specific AI and PBM regulations.

Artificial Intelligence (AI)

- Transparency and Labeling (SB 1324): Creators failing to label AI content or disclaim deepfakes depicting real individuals face civil penalties ranging from $5,000 to $100,000 per violation.
- Elections and Deepfakes (SB 1012/SB 509): Failure to include a required AI disclaimer on political ads is a Class A misdemeanor (up to 1 year in jail and fines up to $2,500). Distributing fraudulent deepfakes of candidates within 90 days of an election can range from a Class B misdemeanor to a Class E felony.
- Mental Health Representation (SB 1444): Representing AI as a mental health professional carries civil penalties of $10,000 for a first violation and $20,000 for subsequent violations.
- Intimate Deepfakes: Unauthorized disclosure of intimate digital depictions is a Class D, E, or C felony, depending on circumstances such as intent to facilitate violence.

Healthcare and Privacy

Missouri adheres to HIPAA for enforcement, which uses a tiered penalty structure based on culpability:

- Civil Penalties:
  - Unknowing Violations: $100 to $50,000 per violation; annual cap of approximately $25,000 to $2.1 million (adjusted for inflation).
  - Willful Neglect (Not Corrected): Minimum $50,000 per violation, up to an annual maximum of $1.5 million (or higher with 2026 inflation adjustments).
- Criminal Penalties:
  - Knowingly Obtaining/Disclosing PHI: Up to $50,000 fine and 1 year in prison.
  - False Pretenses: Up to $100,000 fine and 5 years in prison.
  - Malicious Intent/Commercial Gain: Up to $250,000 fine and 10 years in prison.

Pharmacy Benefit Managers (PBMs)

- Civil Fines (SB 846/SB 363): The Director of the Department of Commerce and Insurance can impose civil penalties not to exceed $5,000 per violation, per day for specific prohibited practices, such as discriminatory 340B drug pricing.
- Disciplinary Action: The state may censure a PBM, place them on probation for up to five years, or suspend/revoke their license for up to three years.
- Fraudulent Activity: Under the Missouri False Claims Act, entities found liable for false representations regarding material facts may be liable for double the amount of payments received plus prosecution costs.

Montana

https://share.google/aimode/xlfSfZVsAYk9Mewep Click on link to see the saved Google AI search result

Montana has established a robust regulatory framework for AI, healthcare data, and privacy as of **February 2026**. Notably, the state legislature is biennial and remains closed for regular sessions during 2026, meaning the regulations currently in effect are primarily those enacted or amended in 2025.

Artificial Intelligence (AI)

Montana regulates AI through sector-specific laws focusing on government use, critical infrastructure, and digital likeness.

- **Government AI Use (HB 178):** Effective **October 1, 2025**, this law prohibits state and local government entities from using AI for cognitive behavioral manipulation, discriminatory profiling, or malicious purposes.
    - **Human Oversight:** Decisions impacting a person's rights or privileges made by AI must be reviewed and can be rejected by a trained human.
    - **Disclosure:** Public-facing interfaces and AI-generated materials must be clearly disclosed as such.
- **Critical Infrastructure (SB 212):** Known as the **"Right to Compute Act,"** it requires deployers of "critical AI systems" used in infrastructure to develop risk management policies based on standards like the **NIST AI Risk Management Framework**.
- **Digital Likeness & Deepfakes:** As of **January 1, 2026**, new protections under **MCA Title 30** (HB 513) grant individuals property rights over their names, voices, and visual likenesses against unauthorized AI fabrication.
- **Education:** Guidelines issued in **late 2025** emphasize that K-12 AI use must comply with FERPA and COPPA, ensuring human engagement remains at the center of learning and grading.

Healthcare

Regulatory updates in healthcare focus on electronic interoperability and patient data transparency.

- **Electronic Health Records (HB 590):** Set to become effective **July 1, 2026**, this bill requires health insurance carriers to maintain standard APIs (Application Programming Interfaces) for patient access, provider directories, and payer-to-payer exchanges.
- **Patient Notification:** This same law mandates that sensitive medical results (such as malignancy or HIV tests) must be disclosed to patients within **72 hours** of finalization.
- **Confidentiality:** Health information remains governed by the **Uniform Health Care Information Act** (MCA 50-16-530), which restricts the release of records without authorization except for specific public health needs.

Data Privacy

Montana's privacy landscape is governed by the **Montana Consumer Data Privacy Act (MTCDPA)**, which was significantly amended in 2025.

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in Montana?

Penalties for violating Montana’s regulations in these sectors range from civil fines of up to

$7,500 per violation for privacy breaches to criminal felony charges with up to **20 years of imprisonment** for certain healthcare violations.

1. Artificial Intelligence (AI)

Montana regulates specific AI applications with varying penalties based on the context of use:

- **Election Deepfakes (SB 25):** Violating prohibitions on unlabelled AI deepfakes in political ads within 60 days of an election carries a **$5,000 maximum fine** and up to **6 months imprisonment** for a second violation, increasing to **2 years** for a third.
- **Explicit Synthetic Media (SB 413):** Knowingly disclosing explicit AI-generated media without consent is punishable by fines up to **$1,000** and up to **1 year imprisonment**. For second offenses or those involving minors, penalties increase to **$10,000** and up to **10 years** in prison.
- **AI Likeness (HB 513):** Effective **January 1, 2026**, unauthorized commercial use of an individual's digital voice or visual likeness makes the violator liable for **actual damages** plus any profits gained from the unauthorized use.

2. Healthcare

Healthcare regulations carry some of the state's most severe criminal penalties:

- **General Health Violations:** Many healthcare-related violations are subject to civil penalties not exceeding **$1,000 per day** of the violation.
- **Specific Medical Acts:** Certain violations of the Health and Safety Code (e.g., chemical abortions or infant safety acts) are classified as felonies. Penalties can reach a maximum fine of **$50,000** and imprisonment for up to **20 years**.
- **Professional Sanctions:** Licensed providers may face a minimum **1-year license suspension** in addition to a civil fine of at least **$5,000 per violation**.

3. Privacy

Enforcement of the **Montana Consumer Data Privacy Act (MCDPA)** is handled exclusively by the Attorney General:

- **Civil Penalties:** Violations are subject to civil penalties of up to **$7,500 per violation**.
- **Cure Period:** A 60-day "right to cure" period allows businesses to fix violations before penalties are imposed; however, this provision is set to **sunset on April 1, 2026**.
- **Privacy in Communications:** Purposely intercepting electronic communications can lead to a **$10,000 fine** and up to **5 years in state prison** for third or subsequent offenses.

4. Pharmacy Benefit Managers (PBMs)

Montana's PBM regulations (e.g., HB 740) focus on transparency and reimbursement rates:

- **Enforcement:** The **Montana Insurance Department** serves as the lead regulatory agency.
- **Scope:** Regulations prohibit practices like "spread pricing" and retroactive claim denials. While specific state-level penalty amounts for newer PBM transparency laws are often tied to broader insurance code violations, proposed federal counterparts suggest fines of up to **$100,000 per violation** for reporting failures.

5. FDX (Financial Data Exchange) & Financial Trade

Violations involving financial data or deceptive trade practices are often prosecuted under the **Montana Unfair Trade Practices and Consumer Protection Act**:

- **Civil Liability:** Violators are liable for **actual and consequential damages** or **$500**, whichever is greater, plus attorney fees.
- **Specific Fines:** Entities like unlicensed credit counselors can be fined up to **$5,000 per violation**.

Nebraska

https://share.google/aimode/Q2jJEHj0NTwf6xj7h Click on the link to see the saved Google AI search result

As of February 2026, Nebraska has recently implemented or finalized several significant regulatory frameworks across these domains, particularly focusing on data privacy and the protection of minors.

Artificial Intelligence (AI)

Nebraska has established comprehensive rules for high-risk AI systems, with major enforcement milestones in early 2026.

- Artificial Intelligence Consumer Protection Act (LB 642)**:** Effective **February 1, 2026**, this law regulates high-risk AI systems.
  - **Developers** must use "reasonable care" to avoid algorithmic discrimination and provide technical documentation to deployers.
  - **Deployers** must implement risk management policies, conduct impact assessments, and notify consumers when AI is used for "consequential decisions" (e.g., employment, lending, or healthcare).
- **Transparency Requirements:** Any AI system intended to interact with consumers must disclose that it is an AI, unless it is obvious to a reasonable person.
- **Enforcement:** The Attorney General has exclusive enforcement authority; there is no private right of action.

Healthcare

The primary regulatory shift in Nebraska healthcare for 2026 involves AI in insurance and new Medicaid work requirements.

- **AI in Utilization Review (LB 77):** Nebraska law prohibits AI-based algorithms from being the **sole basis** for denying or modifying healthcare services. Human review is required for adverse determinations.
- **Medicaid Work Requirements:** Nebraska is the first state to implement federal Medicaid work requirements early, with enforcement beginning **May 1, 2026**.
  - **Applicability:** Able-bodied adults aged 19–64 in the Medicaid expansion group.
  - **Requirement:** 80 hours per month of qualifying activities (work, school, volunteering, or job training).

Privacy

Nebraska's privacy landscape is governed by two major acts, one broad and one specifically targeting minors.

- **Nebraska Data Privacy Act (NDPA):** Effective **January 1, 2025**, this law grants residents rights to access, correct, delete, and port their personal data. It requires companies to obtain **opt-in consent** for processing "sensitive data," which includes health, biometric, and precise geolocation data.
- **Age-Appropriate Online Design Code Act (LB 504):** Effective **January 1, 2026**, this law requires online services to prioritize "privacy by design" for minors under 18.
  - **Restrictions:** Banning targeted advertising to minors and restricting push notifications during school hours (8 a.m. – 4 p.m.) and nighttime (10 p.m. – 6 a.m.).
  - **Default Settings:** Highest privacy protections must be enabled by default for users under 18.
- **Parental Rights in Social Media Act (PRISMA):** Effective **July 1, 2026**, this requires social media companies to verify parental consent before allowing a minor to create an account.

Financial Data Exchange (FDX)

Nebraska follows federal standards for financial data portability, which were significantly updated in 2025.

- **CFPB Section 1033 Compliance:** Under federal "Open Banking" rules, Nebraska financial institutions must allow consumers to transfer their data to third-party providers for free.
- **FDX Standards:** The Financial Data Exchange (FDX) was officially recognized as the standard-setting body in **January 2025**. Nebraska-based banks and fintechs are expected to adopt these technical standards to ensure interoperability and security in consumer-permissioned data sharing.

Pharmacy Benefit Managers (PBMs)

Significant reforms to PBM practices in Nebraska became operative at the start of 2026.

- **PBM Licensure and Regulation Act (LB 198):** Operative **January 1, 2026**, this law introduces several protections for local pharmacies and patients:
  - **Spread Pricing Ban:** Prohibits PBMs from using "spread pricing" (charging a health plan more than they pay the pharmacy) in new contracts.
  - **Specialty Pharmacy Rights:** PBMs cannot exclude Nebraska pharmacies from specialty networks if they meet standard criteria.
  - **Patient Choice:** Prevents PBMs from requiring patients to use exclusively mail-order or PBM-affiliated pharmacies.
- **Cost-Sharing Transparency (LB 158):** Effective **January 1, 2026**, PBMs must include any amount paid by an enrollee (or on their behalf by a third party) when calculating out-of-pocket maximums.

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in Nebraska?

In Nebraska, penalties for violating these regulations primarily consist of **civil fines** and administrative actions rather than criminal imprisonment, with the exception of specific AI-related crimes involving minors or intimate images.

Artificial Intelligence (AI)

- **Civil Penalties (LB 642):** The Attorney General has exclusive authority to enforce the Artificial Intelligence Consumer Protection Act. Violations of requirements for high-risk systems can lead to civil penalties, with similar frameworks often capping such fines at **$7,500 per violation**.
- **Criminal Penalties (AI Misuse):**
  - **Child Pornography:** Using AI to generate or share child pornography is a **Class III felony** (up to 4 years imprisonment and/or $25,000 fine).
  - **Adult Violations:** Adults sharing AI-generated child pornography may face a **Class 1D felony** (minimum 3 years, maximum 50 years imprisonment).

Healthcare

- **Medicaid Work Requirements:** There are no criminal penalties for failing to meet work requirements; instead, the penalty is **loss of coverage** or benefits after a failure to comply for a set period [1.1].

- **Reporting Violations:** Healthcare facilities or professional associations that fail to report required data are subject to a civil penalty of **$500 for a first offense** and up to **$1,000 for subsequent offenses**.

Privacy

- **Data Privacy Act (NDPA):** Effective January 1, 2025.
  - **Civil Fine:** Up to **$7,500 per violation** after a 30-day cure period.
  - **Cure Period:** Businesses have 30 days to resolve violations once notified before fines are levied.
- **Age-Appropriate Online Design Code (LB 504):** Operative January 1, 2026.
  - **Civil Fine:** Up to **$50,000 per violation**.
  - **Enforcement:** Begins July 1, 2026, giving companies a six-month grace period to comply.

Financial Data Exchange (FDX)

- **Civil Penalties:** Violations of federal data access rules (CFPB Section 1033) are enforced through the Consumer Financial Protection Act.
  - **Tier 1:** Up to **$5,000 per day** for simple violations.
  - **Tier 2 (Reckless):** Up to **$25,000 per day**.
  - **Tier 3 (Knowing):** Up to **$1,000,000 per day**.

Pharmacy Benefit Managers (PBMs)

- **Administrative Fines (LB 198):** The Director of Insurance can impose a monetary penalty of up to **$1,000 per entity, per violation** for non-compliance with the PBM Licensure and Regulation Act.
- **License Action:** The Director may also **suspend or revoke** the PBM's license for severe or repeated violations.
- **General Insurance Violations:** Under broader insurance laws, administrative fines can reach up to **$1,000 per violation** or more if the person "knew or should have known" they were in violation.

Nevada

https://share.google/aimode/Q2jJEHj0NTwf6xj7h Click on link to see the saved Google AI search result.

Nevada has implemented several new regulations effective in **2026** particularly concerning **Artificial Intelligence (AI)** in elections and healthcare, as well as significant reforms for **Pharmacy Benefit Managers (PBMs)**.

Artificial Intelligence (AI)

Nevada has enacted strict transparency and usage laws for AI, with major provisions taking effect **January 1, 2026**.

- **Election Transparency (AB 73 / AB 271):** Starting **January 1, 2026**, all political advertisements must clearly disclose if they use AI-generated or digitally manipulated images, video, or audio.
- **Deepfake Prohibitions:** Legislation effective in **2026** prohibits the distribution of deceptive "deepfakes" of candidates within 90 days of an election.
- **Voting System Ban:** AI is strictly prohibited from being used in any equipment for voting, ballot processing, or ballot counting.
- **Mental Healthcare (AB 406):** AI providers are prohibited from claiming their systems can provide professional mental or behavioral health care. Licensed professionals are banned from using AI to deliver therapy directly to patients, though administrative use is permitted.

Healthcare

New healthcare regulations for **2026** focus on access, licensing, and consumer protections.

- **Battle Born State Plans (BBSP):** For the **2026 plan year**, Nevada is launching new state-approved health plans designed to control premium growth and expand coverage statewide.
- **Market Stabilization:** A new market-wide reinsurance program begins in **2026** to lower individual market premiums.
- **Streamlined Licensing:** New laws make it easier for doctors from countries with similar standards (e.g., UK, Australia) to get licensed in Nevada and create a specific telemedicine license for out-of-state providers.
- **Right to Contraception:** Protections are strengthened to ensure access to family planning without government interference.

Privacy

Nevada's privacy framework is primarily governed by **NRS 603A**, with specific updates regarding sensitive data.

- **Opt-Out Rights:** Consumers have the right to opt out of the "sale" of their personal information for monetary consideration.
- **Privacy Notices:** Businesses must provide a clear notice detailing categories of information collected, third parties shared with, and a designated request address for opt-outs.
- **Exemptions:** Notably, financial institutions (subject to GLBA) and healthcare entities (subject to HIPAA) are generally exempt from these specific state-level online privacy requirements.

Pharmacy Benefit Managers (PBMs)

Significant PBM reforms go into effect on **January 1, 2026**, to increase transparency and lower costs.

- **Single State PBM:** Nevada is moving toward a single state PBM to manage prescription drug services for Medicaid and the Children's Health Insurance Program.
- **Spread Pricing Ban:** The new system prohibits "spread pricing" (where PBMs charge payers more than they pay pharmacies) and discriminatory reimbursement practices.
- **Reporting Requirements:** PBMs must submit annual reports detailing business practices, pricing, and rebates to the State Commissioner.
- **Licensing:** PBMs are increasingly required to register or obtain licensure through the state to conduct business.

FDX (Financial Data Exchange)

While not a Nevada-specific state statute, the **FDX API** serves as the industry technical standard for financial data sharing in the U.S.

- **Current Standard:** As of **January 2026**, **v6** of the FDX API is the stable release, incorporating enhanced data clusters

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in Nevada?

Penalties in Nevada for these sectors vary significantly, with new regulations taking effect in **2026** focusing on civil fines and professional disciplinary action rather than widespread imprisonment.

Artificial Intelligence (AI)

- **Healthcare (AB 406):**
  - **Civil:** Violations by AI providers (such as claiming a system can provide professional mental health care) are subject to a civil penalty not to exceed **$15,000 per violation**.
  - **Criminal:** Under existing law, providing professional services without a license can be a criminal offense, though specific "AI therapist" criminal sentencing remains largely under existing unlicensed practice statutes.
  - **Professional:** Licensed providers who use AI in direct patient care (prohibited except for administrative tasks) face **disciplinary action** and potential loss of license.
- **Elections (AB 271 / AB 73):**
  - **Criminal:** Distributing deceptive deepfakes or failing to disclose AI use in political ads is generally classified as a **misdemeanor**.
  - **Civil:** Affected candidates may seek **injunctive relief** and general or special damages in district court.

Healthcare (BBSP & General)

- **Market Compliance:** Insurers failing to meet premium reduction targets (3% by 2026) for **Battle Born State Plans (BBSP)** face administrative remedies. The Division of Insurance can **suspend or revoke** a carrier's certificate of authority for repeat non-compliance.
- **Fraud:** Under **NRS 686A.2815**, healthcare fraud is a **Category D felony**, punishable by **1 to 4 years** in state prison and a fine of up to **$5,000**.
- **Federal Interplay (2026):** IRS "pay-or-play" penalties for employers failing to offer minimum coverage rise to **$3,420 per full-time employee** in 2026.

Privacy (NRS 603A)

- **Civil:** The Nevada Attorney General has sole enforcement authority. Violations of privacy notice or opt-out requirements carry a civil penalty of up to **$5,000 per violation**.

- **Criminal:** There is generally **no criminal penalty** for standard violations of Nevada's online privacy statutes.
- **Private Right of Action:** Nevada law explicitly **does not** allow individual consumers to sue businesses for privacy violations; only the Attorney General can initiate legal proceedings.

Pharmacy Benefit Managers (PBMs)

- **Regulatory:** PBMs operating without a license or violating the 2026 "spread pricing" ban are subject to **administrative fines** and potential **revocation of registration** by the Commissioner of Insurance.
- **Reporting:** Failure to submit mandatory annual transparency reports can lead to daily fines until the report is filed.

FDX (Financial Data Exchange)

- **Status:** As FDX is a market-led technical standard rather than a state statute, there are **no state-level civil or criminal penalties** specifically for failing to use FDX.
- **Federal Context:** Enforcement would primarily fall under the **Consumer Financial Protection Bureau (CFPB)** if the Section 1033 rule is fully implemented.

New Hampshire

https://share.google/aimode/VCeKJ4yZx6QwbedNc Click on the link to see the saved Google AI search result.

As of 2026, New Hampshire has significantly expanded its regulatory framework, particularly through the implementation of a comprehensive privacy act and new legislative sessions focusing on artificial intelligence (AI) and healthcare reform.

Artificial Intelligence (AI)

New Hampshire regulates AI through a mix of internal state policies and new legislative proposals aimed at broader commercial oversight.

- **State Agency Use (HB 1688):** Enacted in 2024, this law mandates that AI used by state agencies must be transparent and non-discriminatory. It prohibits real-time biometric surveillance without a warrant and requires human review for AI-generated decisions.
- **Proposed Comprehensive Framework (HB 1725):** A 2026 bill proposes a new **NH AI Council** to oversee AI development. If passed, it would require clear disclosures when consumers interact with AI and set an effective date for many provisions on **January 1, 2027**.
- **Deepfake Protections:** Regulations criminalize the creation of deceptive deepfakes for malicious purposes, though exceptions exist for satire or news reporting.

Privacy

The **New Hampshire Privacy Act (NHPA)**, originally signed as SB 255, is the primary regulatory standard for data protection.

- **Effective Dates:** The law took effect on **January 1, 2025**. A significant change occurred on **January 1, 2026**, when the mandatory 60-day "cure period" for businesses to fix violations became discretionary at the Attorney General's level.
- **Consumer Rights:** Residents have the right to access, correct, and delete personal data, as well as the right to opt-out of data sales, targeted advertising, and profiling.
- **Business Thresholds:** The law applies to entities doing business in NH that process the data of at least **35,000 unique consumers** (or 10,000 if they derive 25%+ of revenue from data sales).
- **Sensitive Data:** Controllers are prohibited from processing sensitive data (health info, biometrics, geolocation) without **explicit consent**.

Healthcare

Current 2026 legislative activity focuses on protecting clinical judgment and ensuring telehealth parity.

- **AI in Healthcare (HB 1406):** This 2026 bill prohibits health carriers from using AI to overrule or alter a provider's clinical judgment. It allows AI for internal fraud detection but requires full documentation for state audits.
- **Telehealth Parity (HB 1232):** Proposed legislation requires insurers to reimburse telemedicine at the same rate as in-person visits to prevent financial disincentives for rural care.

FDX (Financial Data Exchange) & Open Finance

Regulatory oversight for financial data sharing remains primarily at the federal level, though it impacts NH institutions.

- **Standards Adoption:** By 2026, the **FDX API v6** and **FAPI 1.0** have become industry benchmarks for secure, consumer-permissioned financial data sharing.

- **Legal Status:** While the CFPB's Section 1033 rule (mandating open banking) faced a judicial stay in early 2026, NH financial institutions continue to adopt FDX standards voluntarily to ensure interoperability and security.

Pharmacy Benefit Managers (PBMs)

The 2026 legislative session introduced major PBM reforms to increase drug cost transparency.

- **Comprehensive Reform (SB 478 / SB 547):** These bills aim to **ban spread pricing** (where PBMs charge plans more than they pay pharmacies) and **rebate retention**.
- **Fiduciary Duty:** Proposed laws establish a fiduciary duty for PBMs to act in the best interests of their health carrier clients.
- **Transparency Requirements:** PBMs must file annual reports with the New Hampshire Insurance Department detailing all rebates and administrative fees received from manufacturers.
- **Consumer Protections:** New rules prohibit "gag clauses" that prevent pharmacists from telling patients about cheaper drug options at the point of sale.

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in New Hampshire?

In 2026, New Hampshire enforcement mechanisms prioritize Attorney General (AG) oversight, with many regulations tied to the state's
Consumer Protection Act.

Artificial Intelligence (AI)

- **Civil Penalties:**
  - **Proposed Framework (HB 1725):** The AG has exclusive authority to impose fines up to **$200,000 per violation** for commercial AI non-compliance.
  - **Deepfakes (HB 1432):** Violations involving deceptive deepfakes (e.g., in elections) carry a civil penalty of **$5,000 per violation**.
- **Criminal Penalties:** Misuse of deepfakes to provoke violence or by repeat offenders (within 5 years) is a **Class B Felony**. Otherwise, it is typically a **Class A Misdemeanor**.
- **Private Right of Action:** Generally prohibited for broader AI framework violations, but allowed for individuals injured by deepfakes, who can recover actual damages or **$1,000** (whichever is greater), or up to **3x damages** for willful violations.

Privacy (NHPA / SB 255)

- **Civil Penalties:** Fines up to **$10,000 per violation** under the New Hampshire Consumer Protection Act (RSA 358-A).
- **Criminal Penalties:**
  - **Natural Persons:** A misdemeanor conviction for purposeful non-compliance.
  - **Entities:** A **felony conviction** if the business purposely fails to comply, with potential fines reaching **$100,000 per violation**.
- **Enforcement Detail:** As of **January 1, 2026**, the 60-day "right to cure" is no longer mandatory and is granted only at the AG's discretion.

Healthcare & False Claims

- **Civil Penalties:**

    - **NH False Claims Act (NHFCA):** Violators are liable for a civil penalty between **$5,500 and $11,000 per claim**, plus **3x the damages** sustained by the state.
    - **Administrative Remedies (PFCRA):** Maximum of **$5,000 per claim** plus assessment of up to twice the false claim amount.
- **Criminal Penalties:** Medicaid fraud is a **Class B Felony**, punishable by **3.5 to 7 years** in state prison.

Pharmacy Benefit Managers (PBMs)

- **Civil Penalties:**
    - **Transparency Violations:** Insurers or PBMs violating rebate or transparency rules face civil fines up to **$10,000 per violation** at the Insurance Commissioner's discretion.
    - **Unfair Practices (SB 478):** Proposed 2026 legislation includes civil monetary penalties not to exceed **$1,000 per claim** for specific prohibited practices.
- **Criminal Penalties:** Certain 2026 bills (e.g., SB 247) classify failure to comply with provider contract standards as a violation of the Consumer Protection Act, which can trigger criminal misdemeanor or felony charges for "unfair or deceptive" acts.

FDX (Financial Data Exchange)

- **Penalties:** New Hampshire does not currently have specific state-level criminal or civil statutes for FDX. Enforcement typically falls under **federal CFPB authority** or state consumer protection laws (up to **$10,000 per civil violation**) if data sharing involves deceptive practices or unauthorized access.

New Jersey

https://share.google/aimode/B7amGsNwlQAf6Xnkh Click on the link to see the saved Google AI search result.

Penalties for violating New Jersey's regulations in AI, healthcare, privacy, and PBMs primarily involve significant civil fines, though certain actions (like deceptive deepfakes) can lead to criminal imprisonment.

Artificial Intelligence (AI) & Deepfakes

Penalties vary by the specific use case, ranging from consumer fraud violations to third-degree crimes.

- **Mental Health AI (Bill A5603):** Advertising an AI system as a licensed mental health professional is a violation of the Consumer Fraud Act.
  - **First Offense:** Up to **$10,000**.
  - **Subsequent Offenses:** Up to **$20,000**.
- **Deepfakes (Bill S2544 / A3540):** Creating or spreading deceptive AI-generated media for criminal purposes (e.g., harassment, extortion) is a **third-degree crime**.
  - **Criminal Imprisonment: 3 to 5 years**.
  - **Criminal Fine:** Up to **$30,000** (exceeding the standard $15,000 for third-degree crimes).
  - **Civil Remedies:** Victims can sue for actual damages (minimum **$1,000** per violation) plus punitive damages and attorney fees.
- **Algorithmic Discrimination:** Enforcement falls under the **New Jersey Law Against Discrimination (LAD)**. While specific fine amounts for AI vary by context (housing vs. employment), the AG can seek injunctive relief, victim compensation, and civil penalties.

Privacy (NJDPA)

Violations of the **New Jersey Data Protection Act** (effective 2025) are enforced by the Attorney General under the Consumer Fraud Act.

- **Civil Penalties:**
  - **Initial Violation:** Up to **$10,000**.
  - **Subsequent Violations:** Up to **$20,000** per violation.
- **Cure Period:** Businesses have a **30-day "right to cure"** (fix) violations until **July 15, 2026**. After this date, the cure period is at the Attorney General's discretion.
- **No Private Right of Action:** Individual citizens cannot sue businesses directly for NJDPA violations.

Healthcare

New Jersey imposes penalties for data breaches and improper financial practices like kickbacks.

- **Confidentiality & Record Violations:** Failure to disclose "serious preventable adverse events" or general medical record violations can result in:
  - **Adverse Events: $1,000 to $5,000** per failure to disclose.
  - **General Record Violations:** Up to **$2,500 per day** for most facilities, capped at **$25,000 per event**.
- **Healthcare Kickbacks (Bill A3973):** Elevated to a **third-degree crime**.
  - **Criminal Imprisonment: 3 to 5 years**.
  - **Criminal Fine:** Up to **$50,000**.
  - **Civil Fine:** Up to **$20,000** per violation.

Pharmacy Benefit Managers (PBMs)

The **PBM Licensure and Regulation Act** (S1300) imposes strict financial penalties for operating without a license or violating transparency rules.

- **Licensing Violations:**
  - **First Violation: $5,000**.
  - **Subsequent Violations: $10,000** each.
  - **Alternative Fine:** The aggregate gross receipts from the violations, if that amount is greater than the standard fines.
- **General Non-Compliance:** Not less than **$250** and not more than **$10,000 for each day** the PBM remains in violation.
- **Confidentiality Breach:** Employees who willfully disclose PBM-submitted information face civil penalties of up to **$500**.
- **Administrative Actions:** The state can suspend, revoke, or place a PBM license on probation for fraudulent activity.

New Mexico

https://share.google/aimode/IXFsuW4dLbV8bEbTi Click on the link to see the saved Google AI search result.

New Mexico has introduced several significant regulations and legislative updates for **2026** focusing on transparency, consumer protection, and increased oversight of emerging technologies.

Artificial Intelligence (AI)

The **Artificial Intelligence Transparency Act (HB 28)** and the **Artificial Intelligence Act (HB 60)** are central to the state's 2026 regulatory framework.

- **Effective Dates:** Primary provisions of these acts take effect on **July 1, 2026**.
- **High-Risk Systems:** Developers and deployers of "high-risk" AI systems—those making "consequential decisions" in areas like healthcare, employment, or housing—must conduct annual impact assessments and implement risk management policies.
- **Consumer Rights:** New Mexicans have the right to be notified when AI is used in consequential decisions, the right to an explanation of that decision, and the right to appeal to a human reviewer.
- **Synthetic Media:** The **Artificial Intelligence Accountability Act** requires mandatory disclosure (digital markers) for AI-generated images, audio, and video to prevent deceptive "deepfakes".
- **Government Use:** The **Artificial Intelligence Government Use Act (SB 68)** mandates that state and local agencies establish policies for employee AI use, ensuring a human always makes the final decision on consequential matters.

Healthcare

Healthcare regulations for 2026 focus on addressing staffing shortages and responding to federal changes.

- **Interstate Medical Licensure Compact (SB 1):** Signed into law in **February 2026**, this allows New Mexico to join a national compact, simplifying the process for out-of-state physicians to be licensed and practice in the state to address doctor shortages.
- **AI in Medical Practice:** The **New Mexico Medical Board** now requires practitioners to inform patients when AI is used in their care. Failure to properly oversee AI use can be considered "unprofessional conduct".
- **Staffing Standards:** As of **February 2026**, the New Mexico Attorney General is actively challenging proposed federal repeals of minimum staffing standards in long-term care facilities to maintain resident safety.
- **Program Eligibility:** New SNAP eligibility rules for certain non-citizens took effect **January 1, 2026**, and Medicaid eligibility reviews for many adults will increase to every six months starting **December 31, 2026**.

Privacy

New Mexico is strengthening data protections through several proposed and enacted measures in the 2026 session.

- **CHISPA (SB 53):** The **Community and Health Information Safety and Privacy Act** introduces a strict "opt-in" standard, requiring for-profit companies to obtain explicit consent before collecting or sharing non-essential personal data.
- **Health Data Privacy Act:** This act specifically regulates the processing of health information by non-HIPAA-covered entities (such as health apps and retailers), prohibiting the sale of health data and restricting geolocation tracking near reproductive or mental health facilities.

- **Driver Privacy (SB 40):** The **Driver Privacy and Safety Act** limits the sharing of data collected by automatic license plate readers with out-of-state or federal authorities to prevent unauthorized surveillance of residents.

Pharmacy Benefit Managers (PBMs)

Recent updates to the **Pharmacy Benefits Manager Regulation Act** aim to increase pricing transparency and protect independent pharmacies.

- **Spread Pricing & Steering:** New regulations prohibit "spread pricing" (where PBMs bill insurers more than they pay pharmacies) and "patient steering" (forcing patients to use PBM-affiliated pharmacies).
- **Prior Authorization (SB 20):** PBMs must now establish electronic appeal processes for denied prior authorization requests and conduct annual reviews of their authorization practices.
- **Audit Protections:** PBMs are prohibited from using minor clerical errors in audits as a basis for recouping payments from pharmacies.

FDX (Financial Data Exchange) & Trade

- **Note:** In the context of New Mexico, "FDX" often refers to regional trade and customs updates impacting the border.
- **Electronic Value Declaration:** Effective **April 1, 2026**, new rules require mandatory electronic value declarations for cross-border trade, digitizing customs valuation and increasing penalties for errors.
- **Import Duties:** Temporary duty increases on certain textile and apparel products are in effect through **April 2026**.

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in New Mexico?

Violations of New Mexico's 2026 regulations carry a range of civil and criminal penalties, from significant administrative fines for corporate entities to enhanced prison sentences for individuals who use emerging technology to commit crimes.

Artificial Intelligence (AI)

The **Artificial Intelligence Accountability Act (AI2A)** and **House Bill 60** introduce both civil and criminal enforcement mechanisms.

- **Civil Penalties (Corporate):** The Attorney General (AG) can investigate tech companies and social media platforms for failing to include mandatory digital markers on synthetic media. Violations can result in fines of up to **$15,000 per violation**. Each day of non-compliance may be treated as a separate violation.
- **Civil Remedies (Individuals):** Victims of "deceptive synthetic content" have a private right of action to sue for actual damages or **$1,000 per view/event**, whichever is greater.
- **Criminal Penalties:** While the use of AI itself may not always be a separate crime, the AI2A introduces a **one-year sentence enhancement** if generative AI is used in the commission of any non-capital felony.
- **Invasive Imagery:** For those who use AI to create invasive or degrading images resembling real people, penalties can reach up to **$20,000 in fines** and/or **four years of imprisonment**.

Healthcare

Penalties in healthcare are often tied to administrative oversight and existing protective statutes.

- **Provider Misconduct:** Under the New Mexico Medical Board, improper use of AI can lead to disciplinary actions including fines, **mandatory retraining**, and **license suspension or revocation**.
- **Facility Violations:** Failure to report abuse or neglect, or interfering with adult protective investigations, can result in civil penalties not exceeding **$10,000**.
- **Administrative Deficiencies:** General facility deficiencies are tiered
    - **Class A (Most Severe):** $500 – $5,000 fine.
    - **Class B:** $300 – $3,000 fine.
    - **Class C:** $100 – $500 fine.
- **False Claims:** Entities submitting fraudulent claims for state/federal funds face civil penalties between **$14,308 and $28,619 per claim**, plus up to three times the total damages.

Privacy

- **General Health Data:** Wilful violations of the **Health Information Act** can lead to a state-recovered civil penalty not exceeding **$1,000**.
- **Sensitive Images:** Unauthorized distribution of sensitive images (including digital forgeries) is a **misdemeanor** for a first offense. A second conviction is elevated to a **fourth-degree felony**, which typically carries a basic sentence of 18 months in prison.
- **Government Data:** State employees or contractors violating government AI or data policies face disciplinary action up to **termination** and related criminal penalties.

Pharmacy Benefit Managers (PBMs)

- **Administrative Fines:** Under the Pharmacy Benefits Manager Regulation Act, the Superintendent of Insurance may impose fines for non-compliance with transparency or audit rules. While specific caps vary by violation type, typical administrative penalties for insurance-related violations in NM can range from **$1,000 to $10,000 per incident**.

FDX (Financial Data Exchange) & Trade

- **Customs Valuation:** Effective April 2026, errors in mandatory electronic value declarations for trade can trigger increased administrative penalties. While specific minimums are set by individual trade agreements, typical customs fraud or misdeclaration penalties can reach **multiple times the value** of the goods involved.

New York

https://share.google/aimode/2Yt3LysKKhGontzvI Click on the link to see the saved Google AI search result.

Penalties for violating New York's regulations on AI, healthcare, privacy, and Pharmacy Benefit Managers (PBMs) primarily involve substantial civil fines and injunctive relief. Criminal penalties are typically reserved for cases involving fraud, perjury, or specific intent to cause harm.

Artificial Intelligence (AI)

New York has established some of the highest civil penalties in the country for AI-related violations.

- RAISE Act (Frontier AI): Enforced by the Attorney General, violations carry civil penalties of up to $10 million for the first offense. Subsequent violations can result in fines up to $30 million. There is no private right of action for individuals.
- AI Companion Safeguard Law: Operators of AI "companions" that fail to implement suicide detection protocols or clear user notifications face civil penalties of up to $15,000 per day. Fines collected are dedicated to the state's suicide prevention fund.
- Synthetic Media in Ads: Proposed amendments to the General Business Law would penalize the failure to disclose AI-generated "synthetic performers" with $1,000 for the first violation and $5,000 for subsequent ones.

Healthcare

Penalties in healthcare range from civil fines for regulatory non-compliance to severe criminal sentences for fraud.

- AI in Mental Health (S8484): Using AI for autonomous therapy without human oversight can result in a civil penalty of up to $50,000 per violation.
- Healthcare Fraud:
    - First-Degree (Class B Felony): For fraud exceeding $1,000,000; carries 1 to 25 years in prison and fines of up to twice the illegal gain.
    - Second-Degree (Class C Felony): For fraud between $50,000 and $1,000,000; carries a maximum of 5 to 15 years in prison.
    - Third-Degree (Class D Felony): For fraud between $10,000 and $50,000; carries up to 7 years in prison.
- HIPAA Violations (Civil): Range from $137 to $68,928 per violation depending on culpability (Unknowing vs. Willful Neglect), with a calendar-year cap of approximately $2.07 million.
- HIPAA Violations (Criminal): "Knowingly" obtaining or disclosing health information can result in a $50,000 fine and 1 year in prison. Offenses with intent to sell or use information for malicious harm carry fines of $250,000 and up to 10 years in prison.

Privacy

New York's privacy laws are enforced mainly through civil actions brought by the Attorney General.

- SHIELD Act:
    - Security Failures: Up to $5,000 per violation for failing to maintain reasonable safeguards.
    - Breach Notification Failures: For "knowing or reckless" violations, a court can award up to $20 per failed notification, capped at $250,000.

- Child Data Protection Act: Violations carry civil penalties of up to $5,000 per violation.
- LLC Transparency Act (2026): Failing to file required reports can result in daily fines of up to $500 once past due or delinquent.

Pharmacy Benefit Managers (PBMs)

PBM oversight is managed by the Department of Financial Services (DFS).

- Regulatory Violations: The DFS can impose fines for failure to disclose financial records or for prohibited practices like "patient steering." While general DFS fines often cap at $1,000 to $5,000 per violation, specific PBM non-compliance can lead to the suspension or revocation of their state license.
- Perjury: Statements made in required affirmations to state agencies are subject to perjury penalties, which may include both fines and imprisonment.

North Carolina

https://share.google/aimode/mn86B2SLdij4Ah0V7 Click on link to see the saved Google AI search result.

Penalties for violations of North Carolina's regulations vary significantly depending on the specific law and the nature of the offense, ranging from civil fines to potential imprisonment for criminal charges

.

Artificial Intelligence (AI)

Penalties for AI-related violations primarily concern the misuse of AI for harmful or criminal activities.

- **Unlawful Deepfakes**: Creating deepfake content without consent is a **Class 1 misdemeanor**, punishable by up to **120 days in jail**. Victims can also bring a civil lawsuit for actual damages or not less than **$1,000 per day** the violation continues, or **$10,000**, whichever is higher, plus attorney's fees.
- **Sexual Extortion**: Using AI-generated images for sexual extortion is a felony:
  - **Adult offender**: **Class F felony**.
  - **Minor first offense**: **Class 1 misdemeanor**.
  - **Minor subsequent offense**: **Class F felony**.
- **Aggravated Sexual Extortion (Victim Minor/Disabled)**: A violation is a **Class E felony**.
- **Licensed Chatbots (Effective Jan 1, 2026)**: A person injured by a violation of the AI Chatbots law can bring a civil action to recover the greater of actual damages or **$1,000 per violation**, plus attorney's fees. The Attorney General can also bring a civil action for injunctive relief and damages.

Healthcare

Violations in healthcare are largely governed by professional licensing boards and federal law, with associated disciplinary actions.

- **Physician Responsibility**: While no specific AI healthcare legislation currently exists at the state level, the NC Medical Board can impose disciplinary actions, including license suspension or revocation, for professional negligence or malpractice resulting from a physician's use of AI.
- **HIPAA Violations (Federal Law)**: The federal Health Insurance Portability and Accountability Act (HIPAA) applies, with civil fines ranging from **$137 to $68,928 per violation** (up to a calendar year maximum of over **$2 million**). Criminal penalties for knowingly misusing protected health information can include fines up to **$250,000** and imprisonment for up to **10 years** for offenses involving personal gain or malicious harm.

Privacy

Penalties for privacy violations are detailed in new legislation effective in **2026**.

- **NC Personal Data Privacy Act (Effective Jan 1, 2026)**: Businesses violating the act face significant penalties, including criminal misdemeanor charges and civil liability of up to **$2,500 per violation**.
- **Personal Privacy Protection Act**: Knowingly violating this act (effective **December 1, 2025**) is a **Class 2 misdemeanor**, punishable by up to **60 days in jail** and a fine. Civil actions can also be brought for at least **$2,500** per violation, with intentional violations up to **three times that sum**.
- **Security Breaches**: Businesses that fail to provide timely notice of a security breach are subject to civil penalties from **$100 to $50,000** or more per violation, with an annual cap of

$1,500,000.

Pharmacy Benefit Managers (PBMs)

Penalties for PBMs focus on regulatory compliance and transparency.

- **PBM Licensing Violations**: The NC Department of Insurance can impose civil penalties for non-compliance with licensing and reporting requirements.
- **Prohibited Practices**: The law prohibits practices such as spread pricing and requires rebate pass-through, with violations subject to various penalties to be recovered by the Commissioner of Insurance. Specific minimum and maximum fines are not a standard schedule but are based on the nature and severity of the violation (e.g., penalties not less than **$500** nor more than **$10,000** for certain types of violations, up to **$50,000** for other specific violations). The Attorney General or an injured party may also bring a civil suit.

North Dakota

https://share.google/aimode/XolkJkuuu16SWv3N7 Click on link to see the saved Google AI search result.

As of 2026, North Dakota has implemented several new regulations and legislative frameworks governing AI, healthcare, data privacy, and pharmacy operations.

Artificial Intelligence (AI)

North Dakota utilizes a pragmatic approach, applying existing legal frameworks to AI rather than a single comprehensive statute.

- **Healthcare Decision Limits:** A law effective **January 1, 2026**, mandates that licensed physicians—not AI systems—must make final prior authorization decisions for medical treatments involving medical judgment.
- **Criminalized Misuse:** New laws prohibit the use of AI-powered robots or systems to stalk or harass individuals, expanding existing harassment statutes.
- **Political Transparency: House Bill 1167** requires disclosure statements for any political campaign content created using AI.
- **Operational Guidelines:** The North Dakota Information Technology (NDIT) department enforces guidelines requiring accuracy evaluations for AI/ML outputs and periodic quality assurance checks for approved vendors.

Healthcare

Recent reforms focus on increasing transparency and reducing administrative delays in patient care.

- **Prior Authorization Reform:** Effective **January 1, 2026**, insurers must provide timely decisions (within **72 hours** for urgent requests and **7 days** for non-urgent ones).
- **Default Authorization:** If a request remains unanswered by the insurer within the mandated timeframe, it is automatically considered "authorized" by default.
- **Medicaid Coding Updates:** Starting **February 1, 2026**, new modifier requirements (e.g., -52 and -22) apply to claims based on face-to-face time spent with patients.
- **Discarded Drug Waste:** Beginning **January 1, 2026**, ND Medicaid only applies EAPG payments to non-waste drug lines; drug waste reported with the JW modifier is paid at $0.00.

Privacy & Data Security

Privacy in North Dakota is governed by sector-specific laws and general data breach notification requirements.

- **Financial Data Security: HB 1127**, signed in 2025, requires financial institutions to securely dispose of customer information within **two years** of its use, unless necessary for legitimate business purposes.
- **Breach Notification:** Entities must notify the Attorney General of any data breach affecting more than **250 individuals**. For financial corporations, notification to the Department of Financial Institutions is required within **45 days** if the breach affects **500 or more** consumers.
- **Consumer Opt-In (Proposed):** Legislative efforts in 2025/2026 have explored requiring explicit "opt-in" consent before a covered entity can sell a user's protected data, including health and location information.

Financial Data Exchange (FDX) & Financial Services

While North Dakota does not have a standalone "FDX" statute, it has expanded its financial data security framework significantly.

- **Cybersecurity Standards:** Financial entities are now required to conduct annual penetration testing, use multifactor authentication, and provide written annual reports to their boards on the status of their security programs.
- **Money Broker Expansion:** The Department of Financial Institutions now has the authority to classify "alternative financing products" as loans, effectively expanding money broker licensing requirements.

Pharmacy Benefit Managers (PBMs)

HB 1584 established a new regulatory framework for PBMs to increase accountability.

- **Licensing Requirements:** PBMs must obtain an annual license from the insurance commissioner, with fees up to **$10,000**, and maintain at least **$1 million** in financial responsibility.
- **Contractual Protections:** PBMs are prohibited from forcing pharmacies to participate in multiple contracts; pharmacies now have the right to opt in or out of specific contracts with proper notice.
- **Enforcement Fund:** The state established a dedicated PBM enforcement fund, allowing the commissioner to impose penalties of up to **$10,000 per violation**.

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in North Dakota?

In 2026, North Dakota enforces a range of civil and criminal penalties for violations of regulations concerning AI, healthcare, privacy, and pharmacy management.

Civil and Criminal Penalties by Sector

Category	Civil Penalties	Criminal Penalties	Imprisonment Potential
Artificial Intelligence (AI)	Variable; election violations align with campaign finance laws.	**Class A Misdemeanor** for unconsented deepfakes. **Class C Felony** for repeat stalking via AI/robotics.	Up to **360 days** (Class A Misdemeanor) or **5 years** (Class C Felony).
Healthcare (Prior Auth)	Up to **$500 per day** for failure to respond to data requests.	Typically administrative; professional licensing board sanctions may apply.	Not applicable for standard administrative delays.
Privacy (General)	Up to **$5,000 per offense** for data breach notice violations.	Violation of open records laws (knowing) results in **$1,000** or actual damages.	Dependent on underlying fraud or theft charges.

Financial Data (HB 1127)	Up to **$100,000 per violation**; additional **$1,000 daily fine** after order.	Removal of executives/employees found individually responsible.	Generally civil/administrative, but can trigger criminal fraud.
Pharmacy Benefit (PBMs)	Up to **$10,000 per violation**; **$50,000** for subsequent violations.	**Class C Felony** for operating without a mandatory PBM license.	Up to **5 years** for felony licensing violations.

Specific Regulatory Details

- **Artificial Intelligence:** The fraudulent use of "deepfake" images or videos is a **Class A Misdemeanor**, punishable by a maximum fine of **$3,000** and up to **360 days** in jail. Using AI-powered robots for stalking can escalate to a **Class C Felony** if it violates a protective order, carrying a fine up to **$10,000** and **5 years** in prison.
- **Privacy & Data Breach:** The Attorney General can seek civil damages of up to **$5,000** per offense for failure to notify residents of a security breach. For financial corporations, failing to implement security measures under **HB 1127** allows the Department of Financial Institutions to levy fines up to **$100,000** and suspend or revoke business licenses.
- **Pharmacy Benefit Managers (PBMs):** Beyond monetary fines of **$10,000** per violation, the Insurance Commissioner can order restitution to affected pharmacies or individuals for losses incurred due to the violation. Operating as a PBM without the required license is a **Class C Felony**.
- **Healthcare Malpractice:** While not a penalty, North Dakota has implemented new caps on noneconomic damages in healthcare malpractice. As of **July 1, 2026**, this limit will increase to **$1.5 million**.

Standard North Dakota Statutory Limits

For any regulation classified as a felony or misdemeanor, the following standard maximums apply under North Dakota Century Code:

- **Class C Felony:** 5 years imprisonment and/or **$10,000** fine (up to **$50,000** for organizations).
- **Class A Misdemeanor:** 360 days imprisonment and/or **$3,000** fine (up to **$30,000** for organizations).
- **Class B Misdemeanor:** 30 days imprisonment and/or **$1,500** fine (up to **$20,000** for organizations).

Ohio

https://share.google/aimode/ybDVTpG9ThScmwKkE Click on link to see the saved Google AI search result

Ohio state laws for 2026 carry various civil and criminal penalties for violations concerning AI, healthcare, privacy, and PBMs.

Artificial Intelligence (AI)

- **Education Policy (HB 96):** Public school districts and STEM schools must adopt an AI policy by **July 1, 2026**. While the law mandates this action, it does not currently specify a direct criminal or civil fine for a district's failure to meet the deadline.
- **Child Obscenity (Proposed SB 217):** Creating AI-generated child obscenity is proposed as a **third-degree felony** (9–36 months in prison; fine up to **$10,000**), while possession would be a **fourth-degree felony** (6–18 months in prison; fine up to **$5,000**).
- **AI Model Harm (Proposed HB 524):** Developers of AI models that encourage self-harm or violence could face civil penalties of up to **$50,000 per violation** brought by the Attorney General.

Healthcare

- Healthcare Privacy (ORC 3701.244): Unauthorized disclosure of certain health information (like HIV status) can lead to a civil action where victims may recover actual damages and attorney fees.
- General Health Order Violations: Disobeying health department orders can be a second-degree misdemeanor (up to 90 days in jail; fine up to $750).
- Medical Professional Discipline: Violations of privacy or practice standards by licensed professionals (e.g., nurses or doctors) can result in board-imposed civil penalties of up to $20,000 per violation and license suspension or revocation.

Privacy

- Data Breach Notification (ORC 1349.19): Failure to notify residents of a data breach is subject to tiered civil penalties enforced by the Attorney General:
    - First 60 days: Up to $1,000 per day.
    - 61 to 90 days: Up to $5,000 per day.
    - After 90 days: Up to $10,000 per day.
- Social Media Parental Notification (ORC 1349.09): Although this act was permanently struck down by a federal court in April 2025 as unconstitutional, it originally proposed civil penalties identical to the data breach notification tiers (up to $10,000 per day).
- Tampering with Computer Records (ORC 2913.42): Depending on the value of data involved, this can range from a first-degree misdemeanor (180 days jail) to a third-degree felony (up to 5 years in prison).

Pharmacy Benefit Managers (PBMs)

- Licensing Violations (ORC 3959): Operating without the required license or violating PBM conduct rules can lead to:
    - Administrative Penalty: $1,000 per violation, with each day considered a separate violation.
    - Criminal Penalty: Violating license requirements is a fourth-degree misdemeanor (up to 30 days in jail; fine up to $250).
- Regulatory Sanctions: The Superintendent of Insurance can also suspend or revoke a PBM's license and impose additional monetary forfeitures for non-compliance with transparency or reimbursement rules.

Oklahoma

https://share.google/aimode/fo8YVyQDcjZSDmrDm Click on the link to see the saved Google AI search result.

As of **2026**, Oklahoma has significantly updated its regulatory landscape across artificial intelligence, healthcare, and privacy, following several key legislative enactments and a landmark U.S. Supreme Court decision affecting Pharmacy Benefit Managers (PBMs).

Artificial Intelligence (AI)

Oklahoma's AI regulations are focused on state government accountability, political transparency, and professional oversight.

- **State Government Standards:** All AI systems used by state agencies must undergo a third-party security review and obtain "Authority to Operate" (ATO) approval from the Chief Information Security Officer. State agencies are prohibited from transmitting sensitive data (PII, HIPAA, CJIS) through public, unsecure AI instances.
- **Political Transparency:** As of **November 1, 2025**, SB 746 requires prominent disclosure on all political advertisements using generative AI to depict real people in fabricated situations.
- **AI Personhood Prohibition:** Effective **November 1, 2026**, HB 3546 codifies that AI systems and algorithms cannot be granted legal "personhood" status under state law.
- **Minors Protection:** Proposed 2026 legislation (HB 3544) seeks to prohibit the deployment of "social AI companions" or human-like chatbots to minors, requiring age-verification measures.

Healthcare

Healthcare regulations have expanded to include strict mandates on AI-driven clinical decisions and medical freedom protections.

- **AI Clinical Oversight:** HB 1915 mandates that AI devices in healthcare must be deployed according to FDA regulations and used exclusively by qualified end-users (licensed physicians) who have the authority to overrule AI outputs.
- **Utilization Review Restrictions:** Effective **November 1, 2026**, SB 1967 prohibits insurers from using AI to deny, delay, or modify healthcare services based on medical necessity; such determinations must be made by a licensed physician.
- **Oklahoma Medical Freedom Act:** This **2026** legislation (SB 2029) establishes an individual's right to refuse medical procedures, devices, or vaccines without interference.
- **Medical Ethics Defense Act:** SB 1798 protects the right of healthcare providers and payers to decline participation in services that violate their conscience.

Pharmacy Benefit Managers (PBMs)

Recent legal rulings have significantly reshaped the state's authority to regulate PBMs.

- Supreme Court Ruling (PCMA v. Mulready): On June 30, 2025, the U.S. Supreme Court declined to review a lower court ruling that invalidated parts of Oklahoma's 2019 "Patient's Right to Pharmacy Choice Act." As a result, federal ERISA law now preempts state attempts to regulate PBM networks for self-insured employer plans.
- Ownership Restrictions: HB 4457, introduced for the 2026 session, aims to prohibit PBMs from holding ownership interests in retail or mail-order pharmacies within Oklahoma, though the bill faces ongoing legal challenges.
- Surety Bond Requirements: Oklahoma requires PBMs to maintain surety bonds ranging from $50,000 to $500,000 based on the number of covered lives in the state.

Financial Data Exchange (FDX)

While Oklahoma does not have a standalone "FDX" statute, it regulates the security of financial data through its Privacy laws.

- Data Breach Inclusion: Financial account numbers in combination with access codes or passwords are treated as personal information under the 2026 breach notification amendments.
- Federal Compliance Exemption: Financial institutions that are already compliant with federal GLBA (Gramm-Leach-Bliley Act) or similar primary federal regulators are generally deemed compliant with Oklahoma's state-level notification requirements.

In Oklahoma, penalties for violating regulations in AI, healthcare, privacy, and PBMs range from administrative fines and license revocation to felony imprisonment, depending on the specific statute and the severity of the violation?

Artificial Intelligence (AI)

Oklahoma's AI regulations primarily focus on transparency and specific criminal misuse, with penalties varying by the nature of the act.

- **Political Transparency (SB 746):** Effective **November 1, 2025**, failure to disclose AI-generated content in political ads allows misrepresented candidates to seek **injunctive relief and civil damages**.
- **Intimate Images & Deepfakes:** Nonconsensual dissemination of artificially generated sexual depictions is a **misdemeanor** punishable by up to a **$1,000 fine**. Specific deepfake threats may carry up to **18 months imprisonment** for depictions of adults and **30 months** for minors.
- **Minor Protection (HB 3544/SB 2085):** Violations regarding social AI companions for minors are treated as **deceptive or unfair trade practices**, subject to civil penalties and Attorney General enforcement.

Healthcare

Penalties in healthcare often involve professional licensure actions alongside financial sanctions.

- **Clinical AI Oversight (HB 1915):** The State Department of Health enforces compliance; penalties for non-compliance include administrative actions against the healthcare facility's operating license.
- **Utilization Review (SB 1967/HB 3577):**
  - **Insurers:** Subject to a maximum aggregate fine of **$500,000 per calendar year**.
  - **Clinical Reviewers:** Subject to a maximum aggregate fine of **$100,000 per calendar year**.
  - **Specific Fines:** Up to **$5,000 per violation** or **$10,000 for willful violations**, plus license suspension or revocation.
- **Medical Ethics & Freedom (SB 1798/SB 2029):** Intentional or reckless violations of certain healthcare acts (e.g., related to Title 63) can be classified as a **felony**. Civil penalties may reach **$100,000 per violation**, with each day constituting a separate offense.

Privacy and Data Security

The **2026** updates to the Security Breach Notification Act (SB 626) establish a tiered penalty structure based on an entity's security posture.

- **Civil Penalties:**
  - **Failure to Notify & No Safeguards:** Up to **$150,000 per breach**.

    - **Failure to Use Safeguards (but provided notice):** Capped at **$75,000** plus actual damages.
- **Affirmative Defense:** Entities implementing "reasonable safeguards" may be exempt from these civil fines.
- **Consumer Protection Act:** Violations resulting in injury to residents are treated as violations of the Oklahoma Consumer Protection Act, with the Attorney General holding exclusive enforcement authority.

Pharmacy Benefit Managers (PBMs)

PBMs are subject to strict oversight by both the Insurance Commissioner and the Attorney General.

- **Administrative Fines:** Between **$100 and $10,000 per violation** of the Patient's Right to Pharmacy Choice Act or the Pharmacy Audit Integrity Act.
- **Licensing Penalties:** Censure, suspension, or **revocation of the PBM license**.
- **Operational Violations:** Each day a PBM operates without a license is deemed a separate violation of the Act.
- **Ownership Violations (HB 4457):** Effective **November 1, 2026**, PBMs violating ownership prohibitions face **license nonrenewal or revocation** by the State Board of Pharmacy.

Financial Data Exchange (FDX)

Oklahoma does not have a separate FDX penalty statute; instead, financial data is protected under the broader privacy and insurance codes.

- **Fraudulent Statements:** Insurers filing fraudulent statements with the Insurance Commissioner commit a **felony** punishable by a fine up to **$50,000**.
- **Individual Liability:** Employees causing such filings face a **felony**, a fine up to **$25,000**, and **1 to 5 years imprisonment**.
- **Late Reporting:** Willful reporting failures may result in a civil penalty of **$100 to $10,000 per occurrence**.

Oregon

https://share.google/aimode/WS1LWGeytzamLmpii Click on the link to see the saved Google AI search result.

In Oregon, penalties for violations in AI, healthcare, privacy, and PBM sectors range from administrative fines to felony imprisonment, depending on the severity and nature of the offense. As of 2026, many of these regulations have new or expanded enforcement mechanisms.

Artificial Intelligence (AI)

Penalties for AI-related violations often fall under broader consumer protection or criminal laws.

- **Civil Penalties (UTPA):** Violations involving deceptive AI use (e.g., misleading chatbots or deepfakes in advertising) can face civil penalties under the **Unlawful Trade Practices Act**.
- **Criminal Penalties (AI Deepfakes):** Under **House Bill 2299** (effective 2026), the non-consensual distribution of AI-generated intimate images (deepfakes) is a criminal offense.
  - **First and Second Degree Offenses:** Repeated violations can be elevated to a **felony**.
- **Workplace Violence (AI Tracking):** New laws in 2026 regarding healthcare violence, which include AI-supported tracking, carry fines up to **$125,000** and up to **5 years** in prison for certain repeated assault offenses related to the performance of duties.

Privacy (Oregon Consumer Privacy Act - OCPA)

The OCPA is exclusively enforced by the Oregon Attorney General; there is no private right of action for consumers.

- **Civil Penalties:** Up to **$7,500 per violation**.
  - *Note:* Starting **January 1, 2026**, the 30-day "cure period" for businesses to fix violations without penalty has expired, allowing for immediate enforcement.
- **Criminal Penalties (Privacy Invasions):** Knowing disclosure of private information (e.g., social security numbers or child photos) with intent to stalk or injure is a crime under **SB 1121** as of 2026.
  - **Invasion of Personal Privacy:** Can be classified as a **Class C felony**.

Healthcare

Penalties vary by facility type and the nature of the violation.

- **General Health Authority Penalties:** The Oregon Health Authority can impose civil penalties not to exceed **$500 per day** per violation.
- **Pharmacy Violations:** The State Board of Pharmacy may impose civil penalties up to **$1,000** for individuals and **$10,000** for drug outlets per violation.
- **Medical Imaging:** Specific violations (e.g., practicing without a license) carry fines ranging from **$500 to $1,000**.
- **Long-Term Care Facilities:** Aggregated penalties for violations within a 90-day period are capped at **$20,000** for a single facility.

Pharmacy Benefit Managers (PBMs)

Oregon has recently increased the stringency of PBM oversight, particularly regarding licensing and transparency.

- **Civil Penalties:** Violations of the insurance code by PBMs can result in civil penalties of up to **$10,000 per violation**.
- **Daily Fines:** Failure to comply with drug price transparency reporting requirements can lead to daily fines of up to **$10,000**.
- **Licensing Fines:** PBMs must now obtain an annual license (rather than just registration); operating without one or failing to update information within 30 days can trigger administrative sanctions.
- **Cost Growth Penalties:** Starting **January 1, 2026**, the Oregon Health Authority may impose financial penalties on payers or providers that exceed cost growth targets without reasonable cause.

Pennsylvania

https://share.google/aimode/WS1LWGeytzamLmpii Click on the link to see the saved Google AI search result.

Penalties for violating Pennsylvania's regulations in these sectors range from significant civil fines to multi-year prison sentences for felony-level offenses.

AI Regulations

Under the Digital Forgery Law (SB 649) signed in July 2025, penalties depend on the intent and severity of the harm caused.

- First-Degree Misdemeanor: For creating or disseminating deepfakes with fraudulent or injurious intent.
  - Imprisonment: Up to 5 years.
  - Fines: $1,500 to $10,000.
- Third-Degree Felony: For use in schemes to defraud, coerce, or steal monetary assets/property.
  - Imprisonment: Up to 7 years.
  - Fines: Up to $15,000.
- Proposed Healthcare AI (HB 1925): Non-compliance with proposed transparency and human-oversight rules could face civil penalties up to $5,000 per violation, with an annual aggregate cap of $500,000 for organizations and $100,000 for individuals.

Pharmacy Benefit Managers (PBMs)

The Pharmacy Benefit Reform Act (Act 77 of 2024) grants the Insurance Commissioner authority to impose the following:

- Known Violations: Fines of up to $100,000 per violation, capped at $1,000,000 per calendar year.
- Unknown Violations: Fines of up to $50,000 per violation, capped at $500,000 per calendar year.
- Administrative Sanctions: Suspension or revocation of operating licenses, cease and desist orders, and mandatory reimbursement to harmed pharmacies or patients.

Privacy (Data Breach)

Violations of the Breach of Personal Information Notification Act (BPINA) are treated as unfair or deceptive acts under the Unfair Trade Practices and Consumer Protection Law (UTPCPL).

- Civil Penalties: The Attorney General can seek up to $1,000 per willful violation.
- Senior Victims: Penalties increase to up to $3,000 per violation if the victim is 60 years or older.
- Other Remedies: Injunctions, restitution, and additional fines of up to $5,000 for violating court-ordered injunctions.

Healthcare (General)

Specific state regulations for facilities and professional conduct carry varied penalties:

- Summary Offenses: Fines not exceeding $300 per violation, with each day of a continuing violation counting as a separate offense.
- Falsifying Records: Willfully disclosing false information to health departments is a first-degree misdemeanor (up to 5 years prison) and leads to mandatory license suspension (6 months for first offense; revocation for third).
- HIPAA (Federal/State Hybrid): In PA, state officials can enforce HIPAA-equivalent standards with civil fines of $100 to $50,000 per violation. Criminal penalties for "knowingly" disclosing info can reach 10 years imprisonment and $250,000 in fines.

Rhode Island

https://share.google/aimode/0AFRucanaQgrPJqlZ Click on link to see the saved Google AI search result
As of February 2026, Rhode Island has enacted several comprehensive regulations and legislative acts covering artificial intelligence, healthcare, privacy, and pharmacy benefit managers (PBMs).

Artificial Intelligence (AI)

Rhode Island has transitioned from guidance to formal regulation of high-risk AI systems, particularly in "consequential decision" sectors like insurance and employment.

- **High-Risk AI Systems (RI S0627):** Developers and deployers of high-risk AI must use "reasonable care" to protect consumers from algorithmic discrimination. They are required to maintain risk management policies and conduct regular impact assessments.
- **AI Companion Safety (HB 7350):** Effective in early **2026**, providers of AI "companion" technology must implement protocols to address user expressions of suicidal ideation, self-harm, or financial harm.
- **Disclosure Requirements:** Deployers must notify consumers when AI is used in decision-making and provide opportunities to appeal adverse decisions.
- **Enforcement:** The Rhode Island Attorney General has exclusive enforcement authority; there is no private right of action for individuals.

Privacy

The **Rhode Island Data Transparency and Privacy Protection Act (RIDTPPA)** became fully effective on **January 1, 2026**.

- **Applicability:** Applies to businesses processing personal data of at least **35,000** Rhode Island consumers annually, or **10,000** consumers if they derive more than **20%** of revenue from data sales.
- **Consumer Rights:** Residents can now access, correct, delete, and port their personal data. They also have the right to opt out of targeted advertising, data sales, and profiling.
- **Sensitive Data:** Businesses must obtain explicit **opt-in consent** before processing sensitive information, such as precise geolocation, racial/ethnic origin, or biometric data.
- **Penalties:** Violations can lead to fines of up to **$10,000** per violation, with no mandatory cure period for businesses to fix issues before enforcement.

Healthcare

New regulations in 2026 focus on corporate transparency and the intersection of AI with medical insurance.

- Medical Group Transactions: Effective January 28, 2026, medical practice groups must provide pre-merger notification for material corporate transactions, including those involving private equity firms.
- AI in Healthcare Claims (RI S0013): Effective June 30, 2026, health insurers must disclose AI models used for coverage decisions. Any adverse determination made by AI must be reviewed and approved by a qualified healthcare professional.
- AI Licensing Restrictions: AI systems are prohibited from using terms or designs that imply they possess a healthcare license.

Pharmacy Benefit Managers (PBMs)

State regulations have tightened to protect local pharmacies and ensure reimbursement transparency.

- Reimbursement Standards (RI S0222): PBMs are required to reimburse pharmacists at a rate no less than the National Average Drug Acquisition Cost (NADAC) plus a professional dispensing fee.
- Audit Restrictions: PBMs are restricted from conducting unannounced audits of pharmacies; recent enforcement actions in early 2026 have targeted PBMs violating these state-specific audit laws.
- Enforcement: The Office of Health Insurance Commissioner (OHIC) can impose fines up to $10,000 per PBM violation.

Financial Data Exchange (FDX)

While Rhode Island does not have a standalone "FDX Act," financial data exchange is primarily regulated through the RIDTPPA and federal standards.

- Data Portability: Under the privacy act effective January 1, 2026, consumers have the right to obtain their financial data in a "portable and readily usable format".
- Exemptions: Entities already complying with federal standards like the Gramm-Leach-Bliley Act (GLBA) are generally exempt from the state's specific consumer privacy act requirements, as they are governed by federal financial data sharing rules

The civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in Rhode Island are:

In Rhode Island, penalties for violating the recently enacted regulations (as of early 2026) are primarily civil and focused on financial restitution. Criminal penalties, including imprisonment, are generally reserved for extreme cases of fraud or intentional disclosure of sensitive health data under overarching laws like HIPAA or the state False Claims Act.

1. Artificial Intelligence (AI)

Penalties for AI-related violations vary by the specific sector (e.g., insurance vs. general high-risk systems).

- General High-Risk AI (S0627):
  - Civil Penalty: Up to $10,000 per violation.
  - Cure Period: Features a 60-day period for businesses to remedy violations before the Attorney General pursues legal action.
  - Enforcement: Exclusively handled by the Attorney General; there is no private right of action for individuals.
- AI in Healthcare Insurance (S0013 / H5172):
  - Civil Penalty: Up to $50,000 per violation for insurers who fail to disclose AI models or who use AI to deny coverage without qualified professional review.
  - Additional Sanctions: Potential license revocation for the insurer.
  - Private Right of Action: Unlike general AI laws, this allows patients to sue insurance companies directly for AI-driven decisions.

2. Privacy (RIDTPPA)

The Rhode Island Data Transparency and Privacy Protection Act treats violations as deceptive trade practices under Title 6 of Rhode Island's Commercial Law.

- Civil Penalty: Up to $10,000 per violation.
- Intentional Disclosure: A specific additional fine of $100 to $500 per disclosure applies to individuals or entities that knowingly release personal data.
- No Cure Period: Businesses are immediately liable for non-compliance as of January 1, 2026.
- Criminal Penalty: While the Act itself is civil, "knowing" disclosure of health-related data can trigger federal criminal penalties under HIPAA, including up to $50,000 in fines and 1 year

of imprisonment.

3. Healthcare Transactions

New rules for medical group mergers and acquisitions carry significant "per day" penalties to ensure compliance.

- Pre-Merger Notification Failure:
  - Daily Penalty: Up to $200 per day starting from the 59th day prior to the transaction.
  - Maximum Civil Fine: Up to $100,000 if notice is not provided before the transaction closes.
  - Hospital-Specific Fines: Larger hospital conversions can face fines up to $2 million and license revocation.
- Injunctive Relief: The Attorney General may legally pause a transaction until compliance is met.

4. Pharmacy Benefit Managers (PBMs)

Civil Penalty: The Office of the Health Insurance Commissioner (OHIC) can assess fines up to $10,000 per violation for PBMs that fail to meet reimbursement standards or violate audit laws.

- Licensing: Continued violations may lead to the suspension or revocation of the PBM's license to operate within the state.

5. Financial Data Exchange (FDX)

Rhode Island does not currently have a standalone criminal or civil penalty specific to FDX. Instead, enforcement falls under the RIDTPPA (see Privacy above) or federal laws like the Gramm-Leach-Bliley Act (GLBA) for financial institutions.

Regulation Category	Max Civil Penalty	Criminal/Imprisonment	Enforcement Body
Privacy (RIDTPPA)	$10,000 / violation	No (Civil only)	Attorney General
High-Risk AI	$10,000 / violation	No (Civil only)	Attorney General
Healthcare AI	$50,000 / violation	No (Civil only)	OHIC / EOHHS
Medical Mergers	$100,000 total	No (Civil only)	Attorney General
PBMs	$10,000 / violation	No (Civil only)	OHIC

South Carolina

https://share.google/aimode/7NQCAFf8UbEYLedz2 Click on the link to see the saved Google AI search result.

As of February 2026, South Carolina has implemented several new and updated regulations across these sectors, with a notable shift toward protecting youth online and increasing transparency for pharmacy services.

Artificial Intelligence (AI)

South Carolina primarily manages AI through strategic state agency guidelines and targeted sector-specific policies rather than a single comprehensive state law.

- State Agency Strategy: The South Carolina State Agencies Artificial Intelligence Strategy guides agencies on adopting AI while protecting citizen privacy and ensuring human oversight.
- Judicial Branch Policy: An interim policy issued by the Chief Justice provides guidance for the legal community on the ethical use of Generative AI in the judicial system.
- Campaign Restrictions: As of early 2026, South Carolina remains among the states without specific restrictions on the use of AI in political campaigns.
- Proposed Open-Source Support: Recent legislative resolutions (e.g., Bill 225) express support for open-source AI development to avoid monopolistic bias and censorship.

Healthcare

Regulatory updates in 2026 focus on Medicaid eligibility, facility standards, and parental rights.

- Medicaid Expansion: Effective January 1, 2026, eligibility for Medicaid expanded to include adults aged 65 and younger with incomes at or below 133% of the federal poverty level.
- Parental Rights in Healthcare: A 2026 bill (advanced in February) gives parents increased control over the medical decisions of 16- and 17-year-olds, raising the age for independent medical consent for non-emergency care.
- Hospital Licensing: The Department of Public Health (DPH) has updated minimum standards for licensing hospitals (Regulation 61-16) to align with current state safety and disaster management laws.

Privacy

Privacy regulations have significantly strengthened in 2026, particularly for minors and law enforcement professionals.

- Age-Appropriate Design Code (HB 3431): Passed in January 2026, this act (also known as the Social Media Regulation Act) mandates high default privacy settings for users under 18 and prohibits targeted advertising to minors.
- Judicial & Law Enforcement Privacy: Effective January 1, 2026, active or former judges and law enforcement officers can request the removal of their personal contact information (home addresses, cell numbers) from publicly available government websites.
- General Data Protection: While no comprehensive consumer privacy law like California's CCPA exists, South Carolina adheres to sectoral federal laws like HIPAA and GLBA for specialized data.

Pharmacy Benefit Managers (PBMs)

Significant reforms effective January 1, 2026, aim to increase transparency and protect local pharmacies.

- Reimbursement Minimums: PBMs must now reimburse pharmacies at least 104% of the National Average Drug Acquisition Cost (NADAC) plus a dispensing fee.

- Anti-Steering Rules: PBMs are prohibited from steering patients toward their own affiliated pharmacies without written disclosure.
- Licensure & Audits: PBMs must be licensed through the SC Department of Insurance ($1,000 fee) and are subject to audits at least every five years.
- Medicaid Direct Management: The state can now directly manage Medicaid pharmacy services to limit PBM "spread pricing".

Financial Data Exchange (FDX)

Regulation of financial data exchange in South Carolina largely follows federal standards and industry-led consensus.

- Open Banking Standards: South Carolina financial institutions increasingly align with the FDX API standards, which were recognized by the CFPB in early 2025 as the industry benchmark for secure, consumer-controlled data sharing.
- CFPB Section 1033 Compliance: State-chartered institutions must comply with the federal Section 1033 rule, which bans fees for data transfers and limits third-party data use to what is "reasonably necessary" for the service requested

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in South Carolina?

Violations of South Carolina's current and newly implemented 2026 regulations carry a range of severe financial and custodial penalties.

Artificial Intelligence (AI)

Because South Carolina manages AI through sector-specific policies rather than a single omnibus law, penalties are derived from existing frameworks:

- **Judicial Ethics:** Attorneys who improperly use Generative AI in court filings may face **court sanctions**, including dismissal of motions, fines, or disciplinary action by the State Bar.
- **Proposed Product Liability:** Under pending federal and state frameworks (e.g., AI LEAD Act), developers could face **civil liability** for harm caused by AI systems, with damages determined by the extent of the harm.

Healthcare (Medicaid & Pharmacy Monitoring)

Penalties for medical assistance fraud and prescription monitoring violations are specifically codified:

- **Medicaid Provider Fraud:**
  - **Criminal:** Guilty of a **Class A misdemeanor**; up to **3 years** in prison and a fine of up to **$1,000**.
  - **Civil:** The Attorney General can recover up to **treble damages** (3x the overpayment) plus a **$2,000 penalty per false claim**.
- **Prescription Monitoring (PMP):**
  - **Submission Violations:** Knowingly failing to submit or submitting incorrect info is a misdemeanor; up to **2 years** in prison and/or a fine of up to **$2,000**.
  - **Unauthorized Disclosure:** Disclosing or using PMP info illegally is a **felony**; up to **10 years** in prison and/or a fine of up to **$10,000**.

Privacy (Social Media Regulation Act - HB 3431)

Effective March 1, 2026, this act introduces robust enforcement measures:

- **Treble Damages:** Violators are liable for **3x the financial damages** incurred.
- **Personal Liability:** Officers and employees of online services can be held **personally liable** for "willful and wanton" violations.
- **Enforcement:** The Attorney General is authorized to investigate and bring civil actions for non-compliance.

Pharmacy Benefit Managers (PBMs)

The SC Department of Insurance oversees PBM compliance:

- **Licensing Violations:** Operating without a license in South Carolina carries a fine of up to **$10,000 per violation**.
- **General Non-Compliance:** PBMs are subject to periodic examinations and audits. Failure to adhere to transparency and reimbursement rules can result in additional administrative fines and potential **revocation of licensure**.

Financial Data Exchange (FDX)

Since FDX standards in South Carolina are governed by the federal CFPB Section 1033 rule:

- **Civil Penalties:** The CFPB can impose tiered civil money penalties. For "knowing" violations, fines can reach **$1 million per day**.
- **Data Restrictions:** Violators may be banned from processing further consumer data and required to provide restitution to affected consumers.

South Dakota

https://share.google/aimode/CVgQA35pPOVKJSIC9 Click on the link to see the saved Google AI search result.

Artificial Intelligence (AI)

South Dakota does not have a single comprehensive AI law, but the 2026 Legislative Session has introduced several sector-specific regulations:

- Utilization Review (SB 169): This 2026 bill mandates that AI systems used by health carriers for "utilization review" (deciding if healthcare services will be paid for) cannot be the sole basis for a denial. Decisions must be based on individual patient circumstances, and any adverse determination must be made by a licensed healthcare professional.
- Chatbots and Minors (SB 168): Regulates the use of AI chatbots by minors, requiring age verification for any AI marketed as a "companion" or possessing human-like features.
- Mental Health Services (HB 1144): Sets strict requirements for licensed professionals using AI in therapy. It limits AI use to administrative tasks (scheduling, billing, record-keeping) and requires explicit written consent from clients for any session recording or transcription.
- Deepfakes & Elections: Existing laws prohibit the use of deepfakes to influence elections or the distribution of non-consensual AI-generated pornographic material.
- Taskforce (HB 1125): A 2026 bill to create a task force to study AI's impact on the state, with a report due by 2028.

Healthcare

Healthcare regulations are detailed in Title 34 and Title 58 of the South Dakota Codified Laws:

- Telehealth (SDCL 34-52): Regulates patient treatment through telehealth, requiring a provider-patient relationship and informed consent for services.
- Utilization Review oversight: In addition to the new AI-specific rules, insurers must implement programs ensuring trade practices are not unfairly discriminatory.
- Reporting Requirements: Physicians and laboratories are required by law (SDCL 34-22-12) to report communicable diseases to the Department of Health.

Privacy

South Dakota recently strengthened digital privacy protections through the South Dakota Attorney General's Office:

- Genetic Privacy (SB 49): A 2026 bill designed to safeguard genetic data, requiring genetic testing companies to have clear privacy policies and obtain express consent before sharing data.
- Criminal Invasion of Privacy (SB 41): Revises laws to include prohibitions against unauthorized digital recordings and the creation of harmful "digitally fabricated material".
- HIPAA-Confidentiality: The state Department of Health maintains strict confidentiality policies (Statement No. **25) for infectious disease surveillance data, aligning with federal HIPAA standards.**

Financial Data Exchange (FDX)

FDX is an industry-led standard rather than a state-specific regulation. However, it intersects with South Dakota via federal and market-wide rules:

- CFPB Rule 1033: South Dakota financial institutions are subject to the federal Consumer Financial Protection Bureau's "Final 1033 Rule," which mandates secure, permissioned data sharing, often using the FDX API Standard.

- Five Core Principles: These include Control, Access, Transparency, Traceability, and Security for consumer financial data.

Pharmacy Benefit Managers (PBMs)

PBMs are strictly regulated under SDCL Chapter 58-29E:

- Licensing: PBMs must be licensed as third-party administrators (TPAs) by the South Dakota Division of Insurance.
- Fee Prohibitions: PBMs are prohibited from charging pharmacies certain fees, including accreditation, credentialing, or "performance-based" fees.
- Pricing Transparency: They must update their "maximum allowable cost" (MAC) lists within seven days of a 10% increase in drug prices from wholesale distributors.
- Clawback Bans: State law prohibits PBMs from requiring pharmacies to charge patients more than the actual cost of the drug (anti-clawback).

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in South Dakota?

Penalties in South Dakota range from administrative fines for business non-compliance to criminal prosecution for individual or intentional misconduct.

Artificial Intelligence (AI)

- Healthcare (SB 169): Violations regarding AI-driven medical denials are primarily handled through administrative enforcement. The Division of Insurance may issue cease and desist orders.
- Mental Health (HB 1144): Professionals using AI for prohibited therapeutic decisions or unauthorized recording face civil penalties of up to $10,000 per violation, enforced by the Secretary of Health.
- Election Deepfakes: Distributing intentionally harmful, unlabeled deepfakes of politicians is a Class 1 misdemeanor.
    - Criminal: Up to 1 year in county jail and/or a $2,000 fine.
- AI Companions (SB 168): Targeted at minors, violations can lead to civil penalties up to $5,000 per incident per minor.

Healthcare

- General Fraud: Knowingly submitting false healthcare claims is a Class 1 misdemeanor (up to 1 year jail / $2,000 fine).
- False Claims Act: Civil penalties for fraudulent billing (e.g., Medicare/Medicaid) include treble damages (3x the loss) plus fines typically ranging from ~$11,000 to ~$22,000 per false claim.
- HIPAA Violations (Federal/State Hybrid):
    - Civil: Tiered fines from $137 to over $2 million per year for willful neglect.
    - Criminal: Up to $250,000 in fines and 10 years in prison for malicious intent or commercial gain.

Privacy

- **Genetic Data (SB 49):** Sharing DNA data without express consent triggers civil penalties up to **$5,000 per violation**, recoverable by the Attorney General.
- **Data Breaches:** Failure to notify residents of a breach within 60 days can result in civil penalties of up to **$10,000 per day per violation** under the Deceptive Trade Practices Act.
- **Digital Privacy (SB 41):** Criminal "invasion of privacy" involving unauthorized digital recordings can range from misdemeanors to felonies depending on the victim's age and the

nature of the recording.

FDX & PMBs

- **Financial Data (FDX/1033):** Enforcement is largely federal via the CFPB. Violations of consumer data rights can result in civil penalties of up to **$1,000,000 per day** for "knowing" violations of federal consumer financial laws.
- **Pharmacy Benefit Managers (PBMs):**
    - **Licensure:** Failure to comply with fee bans (SDCL 58-29E-16) can lead to the **revocation or suspension** of their Third-Party Administrator license.
    - **Discriminatory Acts:** PBMs are liable for **actual and consequential damages**, plus reasonable attorney fees.
    - **Clawbacks:** Overcharging patients can be flagged as a violation by the Division of Insurance, leading to administrative settlements and restitution.

Tennessee

https://share.google/aimode/PtguNzEMRO0asHlMu Click on the link to see the saved Google AI search result.

Enforces strict civil and criminal penalties for violations across AI, healthcare, privacy, and PBM sectors. As of 2026, recent legislative changes have increased the financial stakes for non-compliance.

Artificial Intelligence (AI) - ELVIS Act

The Ensuring Likeness, Image, and Voice Security (ELVIS) Act protects an individual's "voice" as a property right.

- Criminal Penalties: Violations are a Class A Misdemeanor.
  - Imprisonment: Up to 11 months and 29 days.
  - Fine: Up to $2,500.
- Civil Penalties: Individuals or rights holders can file lawsuits for actual damages and any profits derived from the unauthorized use of their voice or likeness.

Healthcare (AI in Utilization Review)

Under 2025 regulations (SB 1261/HB 1382), health insurance issuers using AI for medical necessity determinations face specific liabilities.

- Civil Penalties: Violations are classified as Unfair Claims Practices.
  - Private Right of Action: Aggrieved individuals can sue for actual damages, punitive damages, and reasonable attorney fees.
  - Regulatory Fines: The Department of Commerce and Insurance may impose sanctions pursuant to state insurance laws.

Privacy - Tennessee Information Protection Act (TIPA)

Effective July 1, 2025, TIPA is enforced exclusively by the Tennessee Attorney General.

- Civil Penalties: After a 60-day cure period, the court may impose:
  - Standard Violation: Up to $7,500 per violation.
  - Willful Violation: Treble damages (up to $22,500 per violation).
- Safe Harbor: Companies compliant with the NIST Privacy Framework may be protected against monetary fines.
- Note: There is no private right of action for consumers under TIPA.

Pharmacy Benefit Managers (PBMs)

Tennessee significantly bolstered PBM enforcement in 2025 through SB 881/HB 1244.

- Civil Penalties:
  - Cap Removal: As of May 2025, the previous $250,000 aggregate cap on penalties has been eliminated.
  - Per-Violation Fines: While standard penalties were previously $25,000 per violation (often capped at $250k), the TDCI now has the authority to issue significantly steeper fines based on the number of claims impacted.
- Recent Enforcement Examples: In 2025, the TDCI issued consent orders against major PBMs (e.g., Express Scripts and Caremark) totaling hundreds of thousands of dollars for reimbursement and audit violations.

Texas

https://share.google/aimode/FmcFGkWJqpQ6QK4Kf Click on link to see the saved Google AI search result

As of 2026, Texas has implemented several landmark regulations governing artificial intelligence (AI), healthcare data, privacy, and Pharmacy Benefit Managers (PBMs). Notably, the **Texas Responsible AI Governance Act (TRAIGA)**, which took effect **January 1, 2026**, serves as the state's comprehensive framework for AI regulation.

Artificial Intelligence (AI)

The **Texas Responsible AI Governance Act (TRAIGA)**, effective **January 1, 2026**, imposes significant duties on both government and private entities.

- **Prohibited Practices**: Prohibits developing or deploying AI intended to incite self-harm, commit crimes, or unlawfully discriminate against protected classes.
- **Government Disclosures**: State agencies (except hospital districts and higher education) must disclose when consumers are interacting with an AI system.
- **Regulatory Sandbox**: Establishes a 36-month program allowing companies to test AI systems with relaxed regulatory constraints in exchange for data sharing with the state.
- **Enforcement**: The Texas Attorney General holds exclusive enforcement power, with civil penalties ranging from **$10,000 to $200,000** per violation.

Healthcare

Regulations focus on AI transparency and strict data localization for medical records.

- **AI Disclosure (SB 1188 & TRAIGA)**: Effective **September 1, 2025**, and reinforced **January 1, 2026**, healthcare providers must clearly disclose the use of AI in diagnostic or treatment services to patients.
- **Practitioner Oversight**: Providers must personally review all AI-generated records and recommendations before making clinical decisions.
- **Data Localization**: A strict mandate effective **January 1, 2026**, prohibits the physical offshoring of electronic medical records; all such records must be stored within the U.S. or its territories.
- **Biological Sex Fields**: New standards for electronic health records require "observed biological sex at birth" to be recorded separately.

Privacy

Privacy is governed by the **Texas Data Privacy and Security Act (TDPSA)** and sector-specific laws for minors.

- **General Data Rights**: Residents have the right to access, correct, delete, and opt out of the sale or processing of their personal data for targeted advertising.
- **Small Business Exemptions**: Most small businesses are exempt unless they sell sensitive personal data, which requires prior consumer consent.
- **App Store Accountability Act (TASAA)**: Effective **January 1, 2026**, app stores must verify user age, obtain parental consent for minors, and allow parents to restrict their child's interactions.
- **Sensitive Data**: Processing sensitive data (biometrics, precise geolocation, child data) requires informed and unambiguous consent.

Pharmacy Benefit Managers (PBMs)

New laws standardise PBM conduct and reimbursement transparency.

- **Standardized Compliance (SB 1122)**: Effective **January 1, 2026**, PBMs must comply with state insurance code provisions for every health plan they administer, even if those plans are issued outside of Texas.
- **Reimbursement Protections (SB 1354)**: PBMs must reimburse pharmacies at least their actual cost for drugs and devices and pay a dispensing fee equal to or higher than the Medicaid fee-for-service rate.
- **Appeal Rights**: Creates a formal process for pharmacies to challenge inadequate reimbursement rates.

Financial Data Exchange (FDX)

While "FDX" refers to an industry standard rather than a specific Texas state law, state regulations intersect with these standards via broader privacy mandates.

- **Interoperability**: FDX standards for secure, permissioned data sharing are increasingly referenced by regulators like the CFPB to prevent market fragmentation.
- **Texas TDPSA Alignment**: Financial institutions governed by the GLB Act are exempt from the TDPSA, but entities using FDX standards to handle non-exempt data must still follow Texas's "privacy by design" requirements, including clear disclosure and secure data practices.

What are the civil and criminal penalties, including minimum and maximum fines and imprisonment, for violating the above regulation for AI, healthcare, Privacy, FDX, and PMBs in TEXAS?

Texas has established a tiered enforcement system for its new regulations, primarily utilizing civil penalties and professional sanctions rather than criminal imprisonment, except in specific cases of data theft or unauthorized access.

1. Artificial Intelligence (AI)

The Texas Responsible AI Governance Act (TRAIGA) is enforced exclusively by the **Texas Attorney General**.

- **Civil Penalties (Per Violation)**:
  - **Curable Violations**: **$10,000 to $12,000** if the entity fails to address the issue within a 60-day cure period.
  - **Uncurable Violations**: **$80,000 to $200,000** for practices such as deploying AI for prohibited criminal or discriminatory purposes.
  - **Ongoing Violations**: Daily fines between **$2,000 and $40,000** for each day a violation continues.
- **Professional Sanctions**: State agencies may impose additional fines up to **$100,000** or suspend/revoke professional licenses for practitioners using AI improperly.
- **Criminal Penalties**: TRAIGA itself does not establish specific criminal terms.

2. Healthcare (EHR & AI Disclosure)

Violations of **SB 1188** (AI disclosure and data localization) carry penalties based on the violator's intent.

- **Civil Penalties**:
  - **Negligent Violations**: Up to **$5,000** per violation per year.
  - **Knowing/Intentional Violations**: Up to **$25,000** per violation per year.
  - **Intentional for Financial Gain**: Up to **$250,000** per violation.
- **Administrative Actions**: Regulatory boards (e.g., Texas Medical Board) may **suspend or revoke licenses** for entities with three or more violations.

3. Privacy (TDPSA)

The Texas Data Privacy and Security Act (TDPSA) follows a single-tier civil penalty structure.

- **Civil Penalties**: Up to **$7,500 per violation**.
- **Cure Period**: Businesses have **30 days** to resolve alleged violations before being subject to fines.
- **Criminal Penalties**: While the TDPSA is civil, unauthorized access to "sensitive personal information" can trigger criminal charges under the Texas Computer Crimes Act, which may range from a Class B misdemeanor to a first-degree felony depending on the amount of data and intent.

4. Pharmacy Benefit Managers (PBMs)

PBM compliance is monitored by the Texas Department of Insurance (TDI).

- **Administrative Fines**:
  - **Unauthorized Substitutions**: **$1,000**.
  - **Fraudulent Reimbursement Claims**: Up to **$5,000**.
  - **Confidentiality Breaches**: **$1,000 to $5,000**.
- **Reimbursement Appeals**: PBMs that fail to adjust rates after a successful appeal for below-cost reimbursement may face broader enforcement actions for violating the Texas Insurance Code.

5. Financial Data Exchange (FDX)

There is currently no standalone Texas statute titled "FDX Act." However, entities using FDX standards that fail to secure financial data may face:

- **TDPSA Penalties**: Up to **$7,500** per record for non-exempt data.
- **Data Breach Fines**: Up to **$100 per individual per day** for failure to notify the Attorney General of a breach, capped at **$250,000** per breach.

Utah

https://share.google/aimode/YFRtelQ0cQjmeRgUX Click on link to see the saved Google AI search result

Utah's regulatory landscape for 2026 features significant updates to AI transparency, healthcare privacy, and consumer data rights. Key regulations for each category are listed below:

Artificial Intelligence (AI)

Utah governs AI primarily through the **Artificial Intelligence Policy Act (AIPA)**, which was expanded in 2025 and 2026.

- **Transparency Disclosures**: General businesses must disclose AI use if a consumer makes a "clear and unambiguous" request. However, "regulated occupations" (e.g., healthcare, law) must provide **proactive, prominent disclosure** at the start of any interaction.
- **High-Risk Interactions**: As of **2026**, stricter disclosure mandates apply to "high-risk" AI interactions, including those involving medical, legal, or financial advice.
- **AI Learning Laboratory**: The state established an **Office of Artificial Intelligence Policy (OAIP)** and a "Learning Lab" where companies can receive temporary regulatory mitigation (waived fines) while testing AI applications under state oversight.
- **Frontier Model Requirements**: Proposed 2026 legislation (**HB286**) requires developers of advanced "frontier models" to publish child protection plans and provide whistleblower protections, with potential civil penalties of up to **$3 million** for violations.

Healthcare

Healthcare-specific AI and data regulations focus on mental health and prescription management.

- **Mental Health Chatbots (HB 452)**: Chatbots must disclose they are non-human before access, at the start of interactions if more than **7 days** have passed since last use, and any time the user asks.
- **Health Data Privacy**: Suppliers of mental health chatbots are prohibited from selling or sharing individually identifiable health information or user inputs without explicit consent.
- **Prescription Refills**: The OAIP recently approved regulatory mitigation for AI systems to assist in medical decision-making for prescription renewals, aiming to streamline care for chronic conditions.

Privacy

The **Utah Consumer Privacy Act (UCPA)** is the primary framework, with major updates taking effect in **2026**.

- **Right to Correct**: Effective **July 1, 2026**, Utah residents gain a new right to request that businesses correct inaccuracies in their personal data.
- **Data Portability**: Also starting **July 1, 2026**, social media services must allow users to port their personal data to other platforms in a usable format.
- **Existing Rights**: Consumers retain the right to access, delete, and opt out of the sale of personal data or its use for targeted advertising.
- **Public Sector Privacy**: **HB 491** (Data Privacy Amendments) establishes standardized privacy requirements for government entities, including the creation of a **Data Privacy Ombudsperson**.

Financial Data Exchange (FDX)

Utah does not have a standalone state statute for FDX, but state-regulated entities must align with federal standards currently in flux.

- **Open Banking Standards**: The **Consumer Financial Protection Bureau (CFPB)** officially recognized **Financial Data Exchange (FDX)** as a standard-setting body in early 2025.
- **Regulatory Status**: As of **2026**, the federal **Personal Financial Data Rights** rule is subject to a judicial stay, leaving the transition to FDX-based APIs largely voluntary for market participants.

Pharmacy Benefit Managers (PBMs)

Recent legislation aims to increase transparency and lower consumer costs.

- **HB 257 (Effective May 7, 2025)**: Prohibits "spread pricing" in self-funded health plans and requires that manufacturer rebates be used to lower enrollee out-of-pocket costs or premiums.
- **Transparency**: PBMs must provide a Maximum Allowable Cost list for generic drugs and are prohibited from requiring pharmacies to join multiple networks.
- **Drug Synchronization**: Health plans must allow patients to align medication refill dates without additional fees.

💡 Artificial Intelligence (AI)

Penalties primarily target deepfakes and automated scams, with significant legislative activity in **early 2026**.

- **AI Scams & Fraud**: Under **SB 815** (introduced Jan 2026), using deepfakes to defraud individuals of money is a **Class I Felony**, punishable by up to **$10,000** in fines and/or **3.5 years** in prison.
- **Harassment via AI**: Creating synthetic digital representations to harass or intimidate is a **Class A Misdemeanor** (up to **$10,000** fine and/or **9 months** in jail).
- **Political Deepfakes**: Intentionally violating disclosure requirements for AI-generated political ads carries a **$1,000** civil forfeiture per offense.
- **AI Child Exploitation**: Generating AI sexual abuse material (CSAM) is a **Class D Felony**, recently enforced in **January 2026**, carrying significant prison time (typically up to **25 years** for Class D, though specific AI-related convictions have seen **3-year** sentences).

⚕️ Healthcare & Privacy

Wisconsin applies tiered penalties for medical records and general privacy violations.

Violation Type	Civil Penalty	Criminal Penalty
Negligent Disclosure	Up to **$1,000** per violation	Up to **$1,000** fine
Knowing/Willful Breach	Up to **$25,000** + attorney fees	Up to **$25,000** fine and **9 months** jail
Disclosure for Profit	Actual damages + fees	Up to **$100,000** fine and **3.5 years** prison
Healthcare Fraud	**$5,000–$10,000** per claim + triple damages	Up to **10–20 years** imprisonment

🔎 Consumer Data & Privacy

Wisconsin is currently considering the **Consumer Data Protection Act** (slated for **2027**), but existing identity theft and invasion of privacy laws apply.

- **Identity Theft**: Unauthorized use of identifying information is a **Class H Felony** (up to **$10,000** fine and **6 years** in prison).
- **Consumer Data Protection (Proposed)**: Pending legislation grants the Department of Justice authority to seek penalties of up to **$10,000** per violation starting in **July 2027**.
- **Invasion of Privacy**: Surveillance in private places is typically a **Class A Misdemeanor** (up to **9 months** jail), but can escalate to a **Class I Felony** if it involves minors or specific aggravating factors.

📊 FDX & PMBs

Regulation in these areas is largely administrative or focuses on unfair trade practices.

- **Pharmacy Benefit Managers (PBMs)**: Violations of transparency or reimbursement rules (e.g., prohibited network penalties) are often subject to civil forfeitures under general insurance or trade statutes. Violations of **SB 50** (pharmaceutical marketing) can lead to **license suspension** or revocation.
- **Financial Data Exchange (FDX)**: As in Utah, no specific state criminal statute exists for FDX standards. Instead, violations are prosecuted under **Offenses Against Computers** (**Wis. Stat. § 943.70**), where unauthorized modification or destruction of data ranges from a **Class A Misdemeanor** to a **Class H Felony** if damages exceed **$2,500**.

Vermont

https://share.google/aimode/CreOnb8Lz2qlriYOp Click on link to see the saved Google AI search result)

As of 2026, Vermont has implemented or is in the final stages of adopting major regulations across artificial intelligence, healthcare, data privacy, and pharmacy benefit management.

Artificial Intelligence (AI)

Vermont has focused on creating oversight bodies and sector-specific rules, particularly in healthcare and education.

- Oversight Bodies: The Council on Artificial Intelligence and the Division of Artificial Intelligence within the Agency of Digital Services provide ongoing oversight and ethical guidance for AI use in state government.
- Healthcare Decision Mandates: As of July 1, 2026, health plans using AI for utilization reviews must ensure decisions are based on individual medical history rather than group data sets. Denials or modifications of services must be reviewed by a licensed human provider.
- Mental Health Services: New regulations prohibit representing AI as providing therapeutic judgment or diagnosis. Professionals may use AI for administrative support but must retain clinical responsibility.
- Education Guidance: On January 27, 2026, the Agency of Education released a framework for schools to use AI while maintaining human agency and student well-being.

Healthcare

Significant reforms targeting transparency and cost-sharing are active or pending in 2026.

- Outpatient Drug Pricing: Starting in January 2026, most Vermont hospitals face a cap on charges for prescription drugs administered in outpatient settings, limited to 120% of the Average Sales Price (ASP).
- 340B Program Protections: Manufacturers are prohibited from interfering with 340B drug delivery to contract pharmacies and must provide pricing as an upfront discount.
- Health Insurance Changes: For the 2026 plan year, enhanced premium tax credits have expired, leading to higher premiums for many enrollees. Advanced Premium Tax Credit (APTC) repayment caps have also been removed.
- Global Budgets: By February 15, 2026, the Green Mountain Care Board must report on the feasibility of implementing global hospital budgets.

Privacy

Vermont's privacy landscape is defined by the Vermont Data Privacy Act (VDPA), which has a phased implementation.

- Applicability Thresholds: On July 1, 2026, the "middle applicability threshold" takes effect, lowering the compliance requirement to businesses that process data for at least 12,500 consumers.
- Sensitive Data: The law strictly prohibits the sale of sensitive data and requires prior consumer consent for processing.
- Consumer Rights: Vermonters have the right to access, delete, and correct their data, as well as opt out of targeted advertising.
- Consumer Health Data: Special provisions prohibit using geofencing within 1,850 feet of healthcare facilities for tracking health data.

Pharmacy Benefit Managers (PBMs)

Oversight of PBMs has transitioned from simple registration to mandatory licensure.

- Mandatory Licensure: PBMs operating in Vermont must be licensed by the Department of Financial Regulation (DFR) by January 1, 2026.
- Prohibited Practices: State law prohibits "spread pricing" (where PBMs charge insurers more than they pay pharmacies) and "gag clauses" that prevent pharmacists from sharing cheaper drug options with patients.
- Financial Disclosures: PBMs must report annually (by July 1) the aggregate amount they retained on all claims charged to health insurers.

FDX (Financial Data Exchange)

While Vermont does not have a unique state-level "FDX law," it falls under federal open banking standards.

- Open Banking Standards: The federal CFPB Section 1033 rule (finalized late 2024) mandates that financial institutions allow consumers to share their data securely with third parties.
- Standard-Setting: The Financial Data Exchange (FDX) was officially recognized as a standard-setting body in early 2025 to help institutions comply with these federal data-sharing requirements.

In Vermont, penalties for violating regulations in these sectors vary from administrative fines to significant criminal imprisonment, depending on whether the act is classified as a consumer protection violation or a criminal offense.

💡 Penalty Overview

The Vermont Consumer Protection Act serves as a backstop for many regulatory violations (like AI and Privacy), while healthcare and PBM-specific laws carry targeted administrative or criminal consequences.

✅ Artificial Intelligence (AI)

Vermont's 2026 AI regulations primarily trigger civil penalties through consumer protection frameworks.

- Civil Penalties: Violations—such as misrepresenting AI as human therapeutic judgment or failing to have human oversight in healthcare decisions—carry a penalty of $10,000 per violation.
- Developer Liability: New 2025/2026 rules clarify that developers are liable for harm caused by "inherently dangerous" AI systems, including private right of action for consumers to seek actual damages and legal costs.

✅ Healthcare & Medicaid

Penalties in healthcare are often tied to fraud or illegal drug pricing practices.

- Medicaid Fraud:
  - Civil: Up to $500 per false claim or three times the amount of wrongfully obtained benefits, whichever is greater.
  - Criminal: Fines up to $1,000 per claim and/or imprisonment for up to 10 years.
- False Claims Act: Civil penalties of $5,000 to $11,000 per violation, plus treble damages (three times the state's loss).
- Drug Price Transparency: Failure to justify drug price increases can result in a $10,000 civil penalty.

✅ Data Privacy (VDPA)

The Vermont Data Privacy Act (VDPA), largely taking effect in 2025 and 2026, treats non-compliance as an "unfair and deceptive act".

- Civil Fines:
  - General Violations: Up to $10,000 per violation under the Consumer Protection Act.
  - Data Broker Non-Registration: $125 per day.
  - Incorrect Filings: Up to $25,000 for materially incorrect information.
- Private Right of Action: Consumers can sue for violations between 2026 and 2028, though this right is currently scheduled to sunset.

✅ Pharmacy Benefit Managers (PBMs)

With the transition to mandatory licensure by January 1, 2026, the Department of Financial Regulation (DFR) has expanded enforcement power.

- Administrative Fines: The Insurance Commissioner may levy penalties up to $100,000 per violation for practices like "ghost networks" or prohibited spread pricing.
- License Revocation: Failure to meet fiduciary responsibilities or transparency mandates can result in the loss of the PBM's license to operate in Vermont.

✅ FDX & Financial Data

Violations of computer and data access laws in Vermont carry specific criminal weights.

- Unauthorized Access: Knowingly accessing a computer system or data without authority is a misdemeanor punishable by 6 months imprisonment and/or a $500 fine.
- Identity Misappropriation: Obtaining personal identifying information illegally carries a maximum of 3 years in prison and/or a $5,000 fine for a first offense. Second offenses can reach 10 years and $10,000.

Penalty Summary Table (2026)

Sector	Max Civil Fine (Per Violation)	Max Imprisonment
AI	$10,000	N/A (Civil primarily)
Medicaid Fraud	$500 (or 3x damages)	10 Years
Data Privacy	$10,000 (up to $25k for filings)	N/A
PBMs	$100,000	License Revocation
Data Access	$10,000	10 Years (Subsequent)

Virginia

https://share.google/aimode/6sALHPfZQXkyengMw Click on the link to see the saved Google AI search result.

Virginia's regulatory landscape for AI, healthcare, privacy, and Pharmacy Benefit Managers (PBMs) primarily involves civil penalties enforced by the Attorney General, with significant new laws taking effect in 2026.

Artificial Intelligence (AI)

The **Virginia Artificial Intelligence Act** (HB 2094/HB 747), effective **July 1, 2026**, imposes the following for high-risk AI system violations:

- **Civil Penalties:**
  - **Standard Violation:** Up to **$1,000** per occurrence, plus attorney fees and costs.
  - **Willful Violation:** Between **$1,000 and $10,000** per occurrence.
- **Enforcement Details:** The Attorney General has exclusive authority. There is a **45-day cure period** to fix violations before penalties are assessed.
- **Criminal Penalties:** None specified for AI regulation itself; however, certain fraudulent uses of AI (e.g., mail theft or intimidation) may fall under broader criminal codes.

Data Privacy

The **Virginia Consumer Data Protection Act (VCDPA)** regulates how businesses handle personal data.

- **Civil Penalties:**
  - **Standard Violation:** Up to **$7,500** per violation.
  - **Continuing Violation:** Up to **$750** per day, capped at **$2.5 million**.
- **Enforcement Details:** The Attorney General provides a **30-day notice** and cure period. There is **no private right of action** (individuals cannot sue directly under VCDPA).

Healthcare & Reproductive Data

For reproductive and sexual health data, Virginia enacted **SB 754** (effective 2025), which integrates with the **Virginia Consumer Protection Act (VCPA)**.

- **Civil Penalties:**
  - **Willful Violation:** Up to **$2,500** per violation.
  - **Subsequent Willful Violation:** Between **$2,000 and $5,000**.
- **Private Right of Action:** Unlike general privacy laws, individuals **can sue** for the greater of **$500** or actual damages. If the violation is willful, damages can be tripled (treble) or increased to **$1,000**.
- **Criminal Penalties:** While state privacy laws are civil, HIPAA violations (federal) can lead to **1–10 years imprisonment** and fines up to **$250,000** for malicious intent.

Pharmacy Benefit Managers (PBMs)

PBMs are regulated by the **State Corporation Commission (SCC)** under Title 38.2 of the Code of Virginia.

- **Civil Penalties:**
  - **Daily Fine:** Up to **$5,000** for each day a violation occurs.
- **Administrative Actions:** The Commission may **revoke, suspend, or refuse to renew** a PBM's license for non-compliance.
- **Private Right of Action:** Aggrieved parties (e.g., pharmacies or enrollees) may bring an action in court for breach of duty by a PBM.

Washington

https://share.google/aimode/WS1LWGeytzamLmpii Click on the link to see the saved Google AI search result.

Washington state enforcement for AI, healthcare, privacy, and PBM regulations primarily involves civil penalties and consumer protection actions, though certain specific violations can trigger criminal charges.

Privacy (My Health My Data Act)

Violations of the **My Health My Data Act (MHMDA)** are considered *per se* violations of the Washington **Consumer Protection Act (CPA)**.

- **Civil Penalties**:
  - **State Action**: The Attorney General may seek up to **$7,500 per violation**.
  - **Private Right of Action**: Consumers can sue for actual damages, including mental pain and suffering.
  - **Treble Damages**: Courts may award up to three times the actual damages, capped at **$25,000** for CPA violations.
- **Criminal Penalties**:
  - There are no general criminal penalties for MHMDA violations. However, federal HIPAA violations (often overlapping) can lead to **1–10 years in prison** and fines up to **$250,000** for willful or malicious disclosure.

Artificial Intelligence (AI) in Healthcare

Washington began implementing transparency and oversight requirements for AI in 2025 and 2026.

- **Civil Penalties**:
  - **Transparency Violations**: Developers failing to document and disclose AI training datasets may face civil penalties of **$5,000 per violation/day**.
  - **Unfair Practices**: Deceptive use of AI (e.g., misleading a consumer into believing they are talking to a human) is an unlawful trade practice subject to CPA penalties of up to **$7,500 per violation**.
- **Criminal Penalties**:
  - Specific criminal penalties for AI in healthcare are limited, but "deepfake" violations (if applicable to health communication) can be prosecuted as a **gross misdemeanor**, punishable by up to **364 days in jail** and/or a **$5,000 fine**.

Pharmacy Benefit Managers (PBMs)

Under **RCW 48.200**, the Office of the Insurance Commissioner (OIC) oversees PBM conduct.

- **Civil Penalties**:
  - **Standard Violation**: **$1,000** for each act in violation of the chapter.
  - **Knowing/Willful Violation**: **$5,000** for each act.
- **Criminal Penalties**:
  - The PBM statutes (RCW 48.200) do not currently specify criminal imprisonment terms for business practice violations.

General Healthcare Regulation

Failure to comply with state health orders or parity requirements can lead to severe sanctions.

- **Civil Penalties**: The state frequently imposes high-value administrative fines for non-compliance, such as a **$300,000 fine** (with $100,000 suspended) issued in January 2026 for mental health parity violations.
- **Criminal Penalties**: Violating a state health order is a **gross misdemeanor**, punishable by up to **364 days in jail** until the order is complied with.

West Virginia

https://share.google/aimode/kcLWSnXns0zKbmhZK Click on link to see the saved Google AI search result

As of February 2026, West Virginia's regulatory landscape features significant new activity, particularly in artificial intelligence and consumer privacy.

Artificial Intelligence (AI)

- Mental Health AI Regulation: House Bill 4770, introduced in January 2026, establishes strict limitations on using AI for mental health care.
    - AI may only be used to flag or triage high-risk communications (e.g., self-harm).
    - Direct therapeutic decisions must be made by a licensed professional who retains sole clinical authority.
    - Disclosures: Operators must notify users when they are interacting with AI.
    - Effective Date: Regulations take effect January 1, 2027, with civil penalties up to $10,000 per violation.
- State Governance: The West Virginia Task Force on Artificial Intelligence (established under §5A-6-9) continues to develop strategic policies for AI adoption within state agencies.

Healthcare & Privacy

- Consumer Privacy Act of 2026: House Bill 4868 was introduced in January 2026 to create a comprehensive consumer data protection framework.
    - It grants residents rights to access, correct, delete, and opt out of the sale of personal data.
    - Enforcement: Handled exclusively by the State Attorney General, with no private right of action.
- Health Information Exchange (HIE): The West Virginia Health Information Network (WVHIN) allows providers to share patient data unless the patient explicitly opts out.
- HIPAA/42 CFR Part 2 Updates: By the February 16, 2026 federal deadline, healthcare providers in West Virginia must update their Notice of Privacy Practices (NPP) to reflect new substance use disorder (SUD) data protections.

Pharmacy Benefit Managers (PBMs)

- Transparency & Rebates: HB 2263 (2021) requires PBMs to pass 100% of manufacturer rebates to plan sponsors.
- Reimbursement Caps: Senate Bill 852 (2025) prohibits PBMs from collecting cost-sharing from patients that exceeds the total charges submitted by the pharmacy.
- Licensing: All PBMs must be licensed by the West Virginia Office of the Insurance Commissioner (OIC) and renew their licenses every two years.
- 340B Protections: PBMs are prohibited from discriminating against 340B entities (discounted outpatient drug programs) regarding reimbursement rates.

Financial Data Exchange (FDX)

- Open Banking Standards: While not a specific West Virginia statute, the federal Consumer Financial Protection Bureau (CFPB) approved the Financial Data Exchange (FDX) in early 2025 as the official standard-setter for "open banking" under Dodd-Frank Section 1033.
- Impact: West Virginia financial institutions are increasingly adopting these FDX standards to ensure secure, consumer-authorized data sharing with third-party apps.

As of February 2026, West Virginia has established various civil and criminal penalties for regulations involving Artificial Intelligence (AI), healthcare, privacy, and Pharmacy Benefit Managers (PBMs). While "FDX" (Financial Data Exchange) often refers to industry standards rather than a specific state-level penal code, general privacy and financial data laws apply.

Artificial Intelligence (AI)

Current 2026 legislation focuses heavily on undisclosed AI-generated media and its use in elections or for criminal exploitation.

- **AI-Generated Media Disclosure (HB 4496):**
  - **Civil Penalties (Organizations):** Up to **$100,000 per day** for each separate violation involving the distribution of undisclosed AI media.
  - **Civil Penalties (Individuals):** Up to **$1,000 per day** per violation.
  - **Enhanced Penalties:** Additional daily fines of up to **$100,000** for violations involving political deception, identity manipulation, or public safety risks.
- **AI in Elections (SB 484):**
  - **Criminal Penalty:** Violations are a **misdemeanor** punishable by a fine of up to **$1,000** per violation.
  - **Civil Penalty:** Courts may impose a civil penalty not to exceed **$1,000** per violation.
- **Deepfake Criminal Exploitation:**
  - **Criminal Penalty:** Creating AI-generated deepfakes of minors engaged in sexually explicit conduct carries a penalty of **$10,000** in fines and/or **1 to 5 years** in a state correctional facility.

Healthcare & Data Privacy

Penalties often align with federal HIPAA standards while incorporating specific state-level misdemeanor and felony charges for localized violations.

- **General Healthcare Privacy (HIPAA/State Law):**
  - **Civil Penalties:** Fines range from **$100** to **$50,000** per violation, with an annual cap of **$1.5 million** for severe cases.
  - **Criminal Penalties:** Intentional misuse of health information can lead to fines up to **$250,000** and imprisonment for up to **10 years**.
- **Medical Program Records (WV Code §9-7):**
  - **Misdemeanor:** Knowingly failing to maintain proper records for five years can lead to **up to 1 year** of imprisonment and/or a fine of up to **$1,000**.
  - **Felony:** Knowingly destroying records within five years is a felony, punishable by **1 to 10 years** in a state correctional facility and/or a fine of up to **$10,000**.

General Privacy & Computer Crimes (WV Code §61-3C)

- **Unauthorized Computer Access:**
  - **Misdemeanor:** Accessing a computer to obtain services without authorization can result in a fine of **$200 to $1,000** and/or up to **1 year** in jail.
  - **Felony (High Value):** Possession of unauthorized computer data valued at **$5,000 or more** is a felony punishable by up to **10 years** in the penitentiary and/or a fine of up to **$10,000**.
- **Criminal Invasion of Privacy:**
  - **First Offense:** Misdemeanor with a fine of up to **$5,000** and/or **up to 1 year** in jail.
  - **Subsequent Offenses:** Felony punishable by **1 to 5 years** in a state correctional facility and/or a fine of up to **$10,000**.

Pharmacy Benefit Managers (PBMs)

West Virginia has significantly enhanced oversight of PBMs through the West Virginia Offices of the Insurance Commissioner (WVOIC).

- **Licensure & Compliance Violations:**
  - **Civil Penalty:** The Insurance Commissioner may order a PBM to pay a penalty not to exceed **$10,000 per violation**.
  - **Unlicensed Operation:** For entities operating without a license, the fine can reach up to **$20,000 per unauthorized act**, plus potential restitution for affected persons.
- **Cost-Sharing and Transparency (HB 3092):**
  - **Civil Penalty:** Violations of cost-sharing requirements (effective January 1, 2026) are subject to civil penalties of up to **$10,000 per violation**.

Wisconsin

https://share.google/aimode/W9c9TiGxO5Hazmdf0 Click on link to see the saved Google AI search result)

Wisconsin's regulatory landscape in 2026 features a mix of established statutes and significant legislative activity across AI, healthcare, and privacy.

Artificial Intelligence (AI)

As of February 2026, Wisconsin does not have a single comprehensive AI law, but several targeted regulations are in the legislative process:

- Data Center Regulation: On January 20, 2026, the Wisconsin Assembly passed a bill to regulate the state's expanding AI data center industry, focusing on balancing economic benefits with energy rate protections.
- Child Safety: Introduced in late January 2026, a proposed bill targets AI chatbots that encourage self-harm or illegal activities in minors under 18, with fines of $25,000 per violation.
- Healthcare Utilization Review: 2025 legislation restricts utilization review agents from using AI to make adverse health benefit determinations and requires insurers to submit algorithms to the Department of Insurance to minimize bias.
- Study Committee: The Study Committee on the Regulation of AI continues to monitor high-risk AI uses, including disinformation and artificial imagery, to recommend further legislation.

Healthcare

Regulations for 2026 focus on benefit changes and provider standards:

- Provider AI Restrictions: Effective January 1, 2026, updated provider manuals include specific restrictions on the use of AI in performing health plan functions.
- Pharmacy Benefit Shifts: Beginning January 1, 2026, continuous glucose monitors (CGMs) are covered solely under the pharmacy benefit for state health plans.
- Catastrophic Plan Eligibility: A new 2026 hardship exemption expands eligibility for catastrophic plans to individuals who do not qualify for Marketplace savings due to income.

Privacy

Wisconsin is currently debating a major comprehensive privacy bill:

- Wisconsin Data Privacy Act (AB-172): This bill advanced in the Assembly in January 2026. It would grant consumers the right to access, copy, and request the deletion of their personally identifiable information (PII) held by data collectors.
- Health Data Protections: Proposed amendments to privacy law broadly define "health data" and require "separate and distinct" authorization before an entity can sell sensitive data.
- Record Disposal: Under Wis. Stat. § 134.97, businesses must shred or destroy records containing personal information before disposal.
- Constitutional Amendment: As of February 1, 2026, Democratic lawmakers are advancing a constitutional amendment to establish a fundamental right to privacy for all residents.

Pharmacy Benefit Managers (PBMs)

Wisconsin has implemented several "crackdown" measures to increase transparency:

- Licensure Requirements: All PBMs must be licensed by the Office of the Commissioner of Insurance (OCI).
- Transparency Reporting: PBMs are required to file annual reports by June 1 detailing

aggregate rebates received from manufacturers and the amount retained versus returned to plan sponsors.
- Cole's Act / SB 203: Significant 2025-2026 legislation (often referred to as Cole's Act) requires PBMs to:
    - Pay a professional dispensing fee at least equal to the state's Medicaid rate.
    - Allow patients to use any licensed pharmacy in the state without penalty.
    - Reimburse pharmacies within 30 days.
    - Prohibit "gag clauses" that prevent pharmacists from discussing lower-cost drug options with patients.

Financial Data Exchange (FDX)

Regulation of FDX and "Open Banking" in Wisconsin primarily follows federal direction:

- Standard Setting: The CFPB recognized FDX as an official standard-setting body in early 2025 to facilitate the sharing of financial data.
- Regulatory Uncertainty: As of early 2026, the federal Personal Financial Data Rights (PFDR) rule is subject to a judicial stay, meaning mandatory compliance deadlines are currently paused while the FDX API remains the voluntary industry technical foundation.

Wisconsin's regulatory landscape in 2026 includes a mix of recently enacted laws and active legislation, each with specific penalty structures.

💡 Artificial Intelligence (AI)

Penalties for AI-related violations vary significantly by the specific harm or application:

- Companion Chatbots (AB 965): For violations involving AI systems simulating relationships with children, operators face civil penalties up to $25,000 per violation.
- Deepfake Scams: Legislation introduced in early 2026 distinguishes between harassment and fraud:
    - Harassment: Classified as a Class A misdemeanor (fine up to $10,000, up to 9 months imprisonment, or both).
    - Monetary Fraud: Classified as a Class I felony (fine up to $10,000, up to 3.5 years in prison, or both).
- Healthcare AI Misrepresentation: Under 2025 legislation, AI developers implying an AI has a healthcare license face enforcement by professional licensing boards, including injunctive relief.

🏥 Healthcare & Privacy

Privacy protections for healthcare and personal data carry some of the state's strictest penalties.

- Healthcare Record Violations (Wis. Stat. § 146.84):
    - Negligent Disclosure: Forfeiture of up to $1,000 for each violation.
    - Intentional Disclosure: Fines up to $25,000 and/or 9 months in jail.
    - Disclosure for Profit: If done for pecuniary gain, fines increase to $100,000 and up to 3.5 years imprisonment.
- Data Privacy Act (AB-172): Current 2026 legislation proposes fines of up to $10,000 per infraction.
- Record Disposal (§ 134.97): Entities that fail to properly destroy records face forfeitures up to $1,000. Possessing discarded records with intent to use the data can lead to a $1,000 fine and 90 days in jail.

💊 Pharmacy Benefit Managers (PBMs)

Penalties for PBMs are generally administrative and financial, managed by the Office of the Commissioner of Insurance (OCI).

- Reporting Failures: Under Wis. Stat. § 632.865, PBMs failing to submit mandatory transparency reports can face administrative fines and potential license revocation by the OCI.
- Prohibited Practices: Under the 2025-2026 "Cole's Act", PBMs are barred from imposing penalties on pharmacies for informing patients of lower drug costs. Violations may trigger civil damages and professional discipline.

📊 Financial Data Exchange (FDX)

Because FDX in Wisconsin is largely governed by federal CFPB standards, penalties are currently tied to federal enforcement:

- CFPB Enforcement: Under the Consumer Financial Protection Act, the CFPB can seek civil penalties ranging from roughly $5,000 per day for simple violations to over $1,000,000 per day for "knowing" violations of financial data rights.

⚠️ Penalty Summary Table

Regulation Category	Civil Fine (Max)	Criminal Penalty (Max)	Prison/Jail Time
AI Child Safety	$25,000 / violation	N/A	None
AI Fraud (Deepfake)	Varies	$10,000	3.5 Years
Healthcare Privacy	$25,000 (willful)	$100,000 (for profit)	3.5 Years
Data Disposal	$1,000	$1,000	90 Days
Privacy Act (Proposed)	$10,000 / infraction	N/A	None

Wyoming

https://share.google/aimode/xTrJ4B3KiCWXno56Q Click on link to see the saved Google AI search result)

As of February 2026, Wyoming's regulatory landscape for these sectors is defined by a mix of recent 2025-2026 legislative sessions and existing state statutes.

Artificial Intelligence (AI)

Wyoming does not have a single comprehensive AI law but regulates it through specific applications and sector-based rules:

- **Insurance Claims:** Wyoming law requires that a human physician make final decisions on insurance claims, effectively prohibiting AI from making autonomous denial decisions.
- **Deepfakes and Elections:** As of **January 9, 2026**, Wyoming is one of 46 states with laws prohibiting the creation or distribution of nonconsensual AI-generated "deepfake" intimate images and is among 28 states regulating AI-generated deepfakes in political communications.
- **Hiring and Employment:** There are ongoing legislative discussions regarding the use of automated tools in hiring to minimize discrimination and tracking job losses due to automation.

Healthcare

- **Right to Health Care Decisions:** In a landmark **January 6, 2026** ruling, the Wyoming Supreme Court affirmed that the state constitution protects a competent adult's right to make their own health care decisions, which currently includes access to abortion and abortion pills.
- **Price Transparency:** The **Hospital Price Transparency Act** (SF0057), effective **July 1, 2026**, requires hospitals to list standard charges for medical items and services, including at least 300 "shoppable" services.
- **Prior Authorization:** New rules taking effect **January 1, 2026**, expand exemptions from prior authorization for healthcare providers to reduce delays in patient care.

Privacy

- **Government Data Privacy: SF0065**, effective **July 1, 2026**, prohibits state government entities from purchasing, selling, or trading personal data without express written consent. Residents have the right to request copies of their data and must receive responses within **60 days**.
- **Health Information Exchange:** Wyoming requires a framework for the electronic exchange of health information, mandating that providers and insurers maintain and transmit data electronically or risk license suspension.
- **Genetic Testing:** Specific protections exist for genetic testing data under **W.S. § 35-32-102**.

Pharmacy Benefit Managers (PBMs)

- **Licensure Requirements:** PBMs operating in Wyoming must be licensed by the Wyoming Department of Insurance, regardless of whether they serve federal programs or ERISA plans.
- **Audit Standards:** The **Wyoming PBM Act** limits audit lookback periods to two years and requires PBMs to deliver preliminary audit reports within **120 days** of an audit's conclusion.
- **Patient Choice:** State laws prohibit PBMs from restricting a covered person's ability to use in-network retail pharmacies.

|

Financial Data Exchange (FDX) & Digital Assets

Wyoming is a leader in digital asset regulation, though it does not yet have a specific "FDX" named statute:

- **Virtual Currency Kiosks:** Effective **July 1, 2026**, operators of virtual currency kiosks (crypto ATMs) must be licensed money transmitters or chartered financial institutions.
- **Special Purpose Depository Institutions (SPDIs):** Wyoming has established a regulatory framework for SPDIs to handle digital assets and provide banking services for blockchain-based businesses.
- **Stable Tokens:** The **Wyoming Stable Token Commission** is authorized to issue state-backed stablecoins, with new amendments considered for the **2026** session.

Penalties for violating Wyoming regulations vary significantly by the specific act. Many recent **2025-2026** laws rely on **civil daily fines**, while older criminal statutes carry **misdemeanor** classifications.

🔎 Artificial Intelligence (AI)

Wyoming primarily targets specific harms like deepfakes and election interference rather than general AI use.

- **Deepfakes (Sexual Conduct):** Knowingly creating or exchanging AI-generated sexual images of minors is a **felony** or **misdemeanor** depending on intent and severity.
- **Election Deception:** Distributing deceptive AI media within **30 days** of an election is often classified as a **Class A misdemeanor**, punishable by up to **1 year** in jail and fines up to **$4,000**.
- **Intimate Media:** Non-consensual distribution can lead to up to **3 years** imprisonment.

🏥 Healthcare

Recent **2026** transparency laws use a tiered daily penalty system to ensure hospital compliance.

- **Hospital Price Transparency (SF0057):** Effective **July 1, 2026**, daily civil penalties are applied if a hospital fails to follow a corrective action plan:
  - **Critical Access Hospitals: $100/day** (1st offense); **$500/day** (2nd); **$1,000/day** (3rd+).
  - **Prospective Payment Hospitals: $1,000/day** for each day of violation.
- **License Revocation:** The Department of Health can also suspend or revoke a hospital's license for transparency violations.
- **Prior Authorization:** Failure to respond to urgent requests within **24 hours** results in an **automatic authorization** by default.

🛡️ Privacy

Regulations focus on government data handling and medical privacy.

- **Government Data (SF0065):** While this **2025** act focuses on resident rights (like data access within **60 days**), specific financial penalties for state agencies are not currently codified as fixed fines.
- **Medical Privacy (HIPAA/State):** Knowingly disclosing protected health information can lead to **$50,000** fines and **1 year** in prison.
- **Malicious Intent:** If data is sold for gain, fines can reach **$250,000** with up to **10 years** in prison.

💊 Pharmacy Benefit Managers (PBM)

PBMs are governed by the Wyoming Insurance Code and specific auditing standards.

- **Audit Violations:** PBMs cannot assess chargebacks or penalties until the internal appeal process is exhausted.
- **General Insurance Code Violations:** Willful violations of the PBM Act can be treated as **misdemeanors**, typically carrying up to **1 year** in jail and/or fines up to **$1,000**.

📊 Virtual Currency & FDX

Wyoming has established strict criminal penalties for unlicensed financial operations.

- **Virtual Currency Kiosks (HB0075):** Operating without a license after **July 1, 2026**, is a **misdemeanor**:
  - **Imprisonment:** Not less than **3 years**.
  - **Fine:** Not less than **$10,000**.
- **False Certification:** Making false entries in required financial records is a **felony** punishable by at least **3 years** in prison and a **$10,000** minimum fine.

Detailed Penalty Comparison Table

Regulation	Violation Type	Minimum Fine/Time	Maximum Fine/Time
AI (Election)	Class A Misdemeanor	N/A	$4,000 / 1 Year
Health Transparency	Critical Access Daily	$100 / Day	$1,000 / Day
Health Transparency	Standard Hospital	$1,000 / Day	$1,000 / Day
Privacy (Malicious)	Felony	N/A	$250,000 / 10 Years
Crypto Kiosks	Unlicensed (Misd.)	$10,000 / 3 Years	$10,000 / 3 Years
PBM Audit	Misdemeanor	N/A	$1,000 / 1 Year

The End

Transformativ IP

Software Development & Implementation for
Regulatory Compliance & Quantum Security

Info@TransformativIP.com