Transformativ IP

C-suite Regulatory Crisis and our Proactive Software Solutions

We Mitigate C-suite State and Federal Criminal Penalties in 50 States

Today, a C-suite executive can be imprisoned in 39 states for violating an AI regulation, and 37 states for violating a healthcare regulation, as shown in the table below. Over 15 new state regulations will begin enforcement later in 2026, further complicating your regulatory burden. It is highly probable your organization must comply with all 50 states regulations since jurisdiction is based on the state of your client's/patient's driver's license or your vendor's/business associate's head office state. Only 5 states still provide a regulatory grace period, and that is expected to come to an end by 2027.

Your 2026 Regulatory Reality

- **Criminal Fines/Imprisonment:** DOJ-DSP willful violation is up to 20 years in prison and a $1M fine per violation. By 2027, 85% of states will mandate prison for AI and healthcare regulatory breaches. Pages 3-7 of this PDF show states where the potential state prison sentence is 50 years for a violation.
- **90%+ Conviction Rate:** DOJ regulatory conviction rate is >90%. Total defense resolution costs typically exceed $3M. Losing a trial averages a 15-yr sentence, plea deals average a 2-yr. sentence.
- **D&O Insurance Limitations:** D&O insurance never covers penalties, restitution or disgorgement. If you are found guilty or accept a plea you must refund the DO insurance firm all of the funds that were spent on your defense and it cannot be discharged in a bankruptcy. Download our 5-pg DO article

How Many of the 50 States have Civil or Criminal Penalties or Imprisonment

Regulation	Civil Penalties	Criminal Penalties	Imprisonment	Page # in this PDF
AI	48	31	39	3
Healthcare	50	31	37	4
Privacy	50	20	21	5
PBM	50	9	6	6
Federal	Many	Many	Many	7

The Four Sections of this PDF

(Section 2 uses Saved Google Search Hyperlinks so you can Instantly Verify Levied Penalties)

1. **Civil, Criminal, and Imprisonment Penalties:** (*pgs.3-7)* Summaries of the civil and criminal penalties, including imprisonment, in all 50 states for Ai, privacy, healthcare and PBM regulations.
2. **Google Search Results Verifying Levied Penalties:** *(pgs.8-9)* Lists saved Google search links for all 50 states to instantly verify federal and each state's levied regulatory penalties (civil and criminal). Know who, how much they paid in fines and how long their prison sentence is.
3. **PQC+ & Drone software:** (*pgs.10-12)* Our certified 100% software proactively mitigates and future proofs regulatory and other risks across all 50 states. No-risk free trialware available. Our drone command and control system fully enables FAA Part 108 and other US regulations.
4. **Teaching Resources:** (*pgs.13-16)* Videos, slide decks, FAQs, articles, and podcasts—provide the real insight your team needs to make informed decisions. Having critical insights such as the three key legal doctrines: "Willful Violation," "Responsible Corporate Officer", and the "Learned Hand" rule is most wise. Your future freedom and wealth may depend on this insight.

Why Your Biggest Regulatory Nightmare is HNDL and How We Uniquely Solve It

Google, Microsoft, and IBM have publicly predicted "Q-Day" for 2029—the moment quantum computers will break current encryption, which secures 95% of the global economy. This is not just a technological forecast; it's **a *regulatory notice based on the three legal doctrines at the bottom of page one*.** China, Russia, Iran and cybercriminals have been executing "Harvest Now, Decrypt Later" (HNDL) attacks for several years, stealing encrypted data waiting to decrypt it when quantum computing arrives in 2029. Armies of AI software bots scout networks like yours for vulnerabilities 24/7. The FBI and NSA have stated China's theft of US IP has accelerated, and is probably over $500 billion annually. **The critical takeaway:** Today's stolen data can destroy your company's value in three years. Once you engage with our education available on pages 12-16 you will understand why failing to prepare for Q-Day exposes your C-suite to personal criminal liability and potential imprisonment in multiple states and federally as well.

Liability for regulatory non-compliance and "Q-Day" risks defaults to the CTO or CISO. However, this liability shifts directly to the CEO and Board of Directors if they deny funding for the resources requested by the CTO/CISO to proactively mitigate these real present risks. Decisions—or the failure to make them—by leadership in 2026 will have direct implications: a data breach disclosed in 2029 will be considered a regulatory violation stemming directly from those 2026 decisions by the CEO and BOD.

PQC+ is Our Unique Solution: Navigating the constantly shifting federal and state regulations governing data handling and communication presents an overwhelming challenge, further complicated by the impending arrival of Q-Day. Our software, "**PQC+**," is a unique and comprehensive solution that proactively ensures both regulatory compliance and HNDL protection. PQC+ is the fastest and easiest post-quantum cryptographic (PQC) solution to implement. While most PQC solutions take years, PQC+ is fully operational in just 90 days. It boasts the lowest latency and simplifies the transition without costly "rip and replace" of existing software or hardware. Download our 14-pg. article/videos on Q-Day

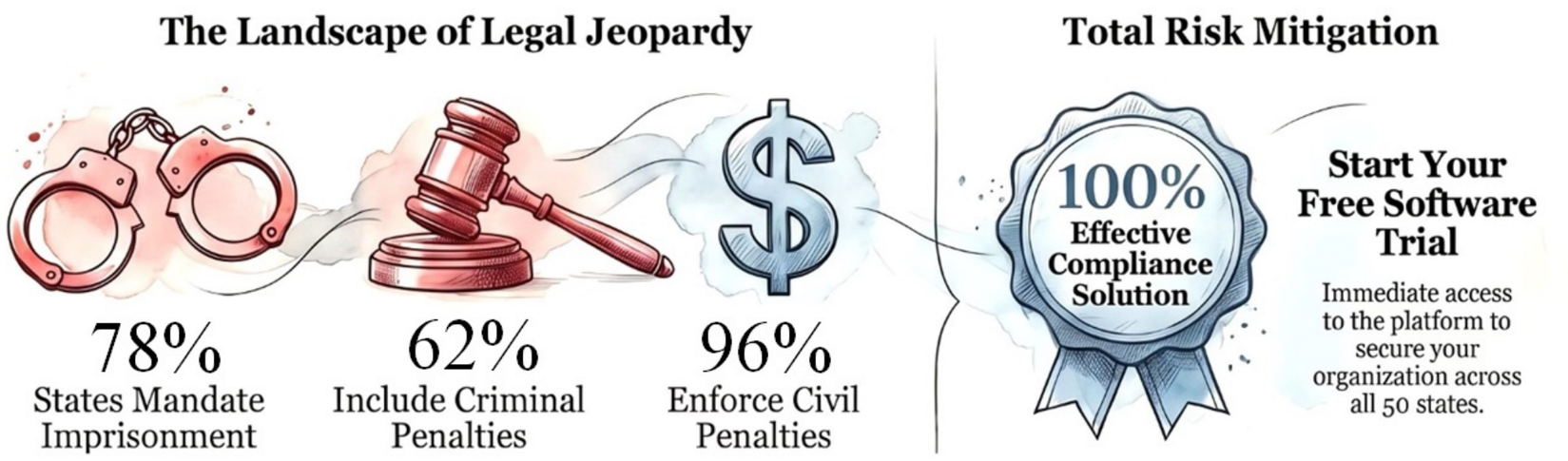
Saved Google Search Verification of State and Federal Regulatory Criminal Sentences

PDF	Pages	Download here
1) AI, Privacy, Healthcare, and PBMs Regulations by State Text summaries of regulations for each state, and links to the Google search result.	100	**Download PDF**
2) State Civil and Criminal Convictions List of actual Individual convictions with levied fines and prison sentences, for violations of both state regulations.	235	**Download PDF**
3) Federal Criminal Convictions List of actual individual convictions, and levied fines and prison sentences, concerning violations of federal criminal regulations.	82	**Download PDF**

About Us: Our tech team has decades of software development expertise working with US federal agencies (Veterans Affairs, Dept. of War) and state/city governments. We are experts in both IT and OT cybersecurity, dedicated to securing businesses and governments across the US, Canada, and Europe.

Our mission: is to empower you to thrive securely in the emerging AI and Quantum computing era. We offer best-in-class, proactive software solutions—available for free trial (trial ware)—to address critical challenges such as 50 state regulatory compliance, HNDL, post-quantum cryptography, 'Striker-like' MDM attacks, Anthropic AI MCP server compliance, and the tracking and control of third-party drones.

AI Regulatory Compliance Penalties in 50 States

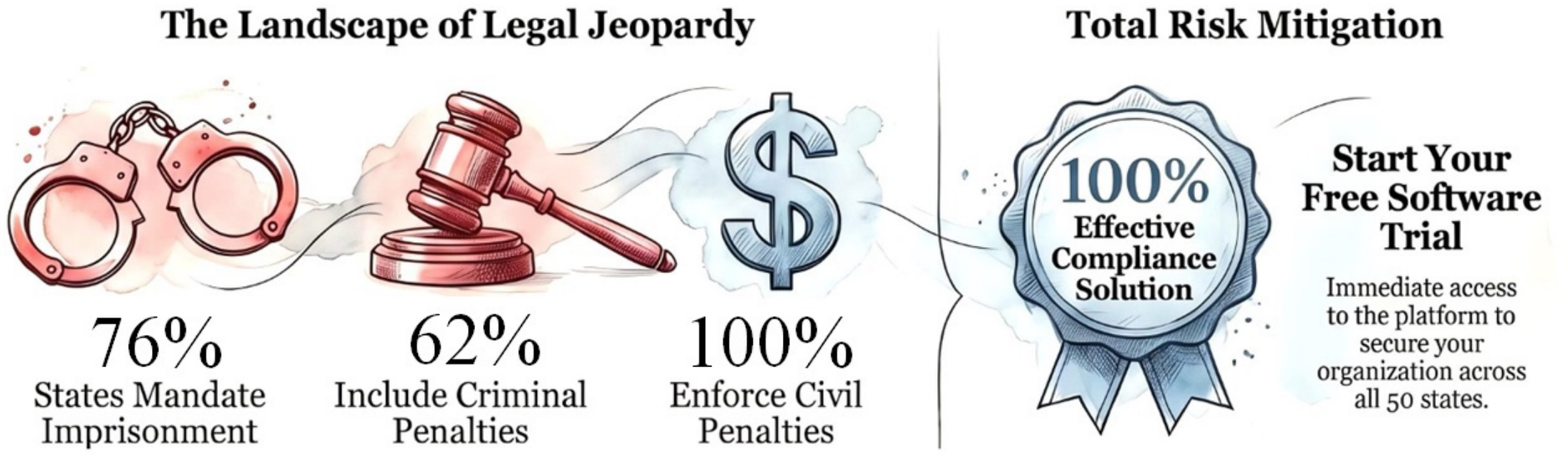


The Table shows the 50-state regulatory Penalties for violating AI regulations.
Similar info for Healthcare, Privacy, PBM and Federal regulations is on the following pages.

Download: Federal Criminal convictions State Civil and Criminal convictions Summary of 50 States AI, privacy, healthcare, PBM regulations

State	Key AI Law / Focus	Max Civil Fine	Max Criminal Fine	Max Imprisonment	Key Details
Alabama	Deepfake / SB 63	Punitive damages	N/A	**1 year (Class A Misd.)**	Medicaid AI non-compliance: $100K/act
Alaska	SB 177 / Deepfakes	Actual + punitive damages	**$100,000**	**10 years (CSAM)**	State agency AI accountability
Arizona	HB 2175 (AI healthcare)	$1,000/violation	**$10,000 (enterprise)**	**6 months (Class 1 Misd.)**	Board sanctions for AI denial failures
Arkansas	Bulletin 13-2024 / Act 827	$5,000/violation ($50K agg.)	**$10,000**	**6 years (Class D Felony)**	Deepfake NCII penalties
California	AB 3030 / SB 1120 / SB 243	$25,000 (facility); $1M (AG)	**$10,000**	**1 year (misdemeanor)**	9 separate AI laws; transparency focus
Colorado	Colorado AI Act	$20,000 ($50K elderly)	N/A	N/A	Deceptive trade practice classification
Connecticut	AI high-risk mandates	$7,000 (discrimination)	N/A	**5 years (deepfake felony)**	CHRO discrimination enforcement
Delaware	HB 316 (Deepfakes)	N/A	N/A	**2 years (Class E Felony)**	AI Commission recommendations pending
Florida	AI political ads / SB 482	$50,000	N/A	**1 year (1st degree misd.)**	Trebled for children's violations
Georgia	AI Activities Act	N/A	**$50,000 (PC crimes)**	**15 years (felony)**	Medical Board AI oversight
Hawaii	SB 2524 / SB 2788	$15,000/day (minors)	N/A	**4 years (deepfakes)**	Private cause of action
Idaho	HB 127 (Consumer AI)	$10,000 + $1K/violation	N/A	N/A	Disclosure required for AI agents
Illinois	HB 3773 / IHRA	$70,000 (3+ offenses)	N/A	N/A	AI hiring discrimination focus
Indiana	HB 1183 (Deepfakes)	$1,000/violation	**$10,000**	**6 years (Level 5 Felony)**	Licensing board enforcement
Iowa	SF 2166	$5,000 (subsequent)	**$2,560**	**1 year (serious misd.)**	Election integrity focus
Kansas	SB 405 / HB 2313	$50,000/violation	**$100,000+ (felony)**	**20+ years (Class C Felony)**	Genetic data AI violations severe
Kentucky	HB 672 / Consumer AI	$7,500 (KCDPA)	N/A	N/A	Right to appeal AI decisions
Louisiana	Deepfake laws	$10,000 (healthcare AI)	**$50,000**	**50 years (minor deepfakes)**	Harshest deepfake-minor penalties
Maine	LD 1154 / LD 1301	$25,000/day (repeat)	N/A	N/A	UTPA enforcement framework
Maryland	HB0820 / HB1240	$10,000/offense	**Misdemeanor**	**1 year**	Certificate suspension possible
Massachusetts	Chapter 93A	$500,000 (child safety)	**$50,000**	**10 years (CSAM)**	Broad consumer protection enforcement
Michigan	HB 4667 / HB 4668	Significant admin fines	N/A	**8 years (felony)**	Mandatory restitution; consecutive sentences
Minnesota	Deepfake laws	$100,000 (sexual civil)	**$10,000**	**5 years (repeat felony)**	Healthcare AI via insurance licensing
Mississippi	HB 1717 / SB 2577	$5,000/violation	**$50,000**	**5 years (felony)**	Medical Judgment Protection Act
Missouri	SB 1324 / SB 1012	$100,000/violation	**$2,500**	**Class E Felony possible**	Mental health AI: $20K subsequent
Montana	SB 25 / SB 413 / HB 513	Actual damages + profits	**$10,000**	**10 years (2nd offense minors)**	Right to Compute Act requirements
Nebraska	LB 642 (eff. Feb 2026)	$7,500 (est.)	**$25,000**	**50 years (Class 1D Felony CSAM)**	High-risk AI system regulation
Nevada	AB 406 / AB 271	$15,000/violation	**Misdemeanor**	**Misdemeanor terms**	AI mental health prohibition
New Hampshire	HB 1725 (proposed)	$200,000/violation	**Class B Felony**	**7 years (Class B Felony)**	Most aggressive proposed AI penalties
New Jersey	A5603 / S2544	$20,000 (subsequent)	**$30,000**	**5 years (3rd degree crime)**	Consumer Fraud Act enforcement
New Mexico	AI2A / HB 60	$15,000/violation/day	**$20,000**	**4 years + 1yr enhancement**	Sentence enhancement for AI crimes
New York	RAISE Act	$10 million (1st); $30M (sub.)	N/A	N/A	Highest civil penalties nationwide
North Carolina	Deepfake / Chatbot laws	$10,000/day	N/A	**Class E/F Felony (extortion)**	$1K/day or $10K per violation
North Dakota	HB 1167 / Deepfakes	$10,000	**$10,000**	**5 years (Class C Felony)**	AI stalking via robotics covered
Ohio	SB 217 / HB 524	$50,000 (AG action)	**$10,000**	**36 months (3rd degree felony)**	AI child obscenity proposed
Oklahoma	SB 746 / HB 3544	Injunctive relief + damages	**$1,000**	**30 months (minor deepfakes)**	AI personhood prohibited Nov 2026
Oregon	HB 2299 / UTPA	UTPA penalties	N/A	**Felony possible (repeat)**	Workplace violence AI tracking
Pennsylvania	SB 649 (Digital Forgery)	$15,000	**$15,000**	**7 years (3rd degree felony)**	Healthcare AI: $500K org cap
Rhode Island	S0627 / S0013	$50,000 (healthcare AI)	N/A	N/A	60-day cure; AG exclusive
South Carolina	State agency guidelines	Court sanctions	N/A	N/A	No comprehensive AI law yet
South Dakota	SB 169 / SB 168 / HB 1144	$10,000/violation	**$2,000**	**1 year (Class 1 misd.)**	Minors AI companion regulation
Tennessee	ELVIS Act	Actual damages + profits	**$2,500**	**11 months 29 days**	Voice as property right
Texas	TRAIGA (eff. Jan 2026)	$200,000 (uncurable)	N/A	N/A	$2K–$40K/day ongoing; AG exclusive
Utah	AIPA / HB 286	$3 million (frontier models)	**$10,000**	**3.5 years (Class I Felony)**	AI Learning Lab sandbox
Vermont	Consumer Protection Act	$10,000/violation	N/A	N/A	Developer liability for dangerous AI
Virginia	VA AI Act (eff. July 2026)	$10,000 (willful)	N/A	N/A	45-day cure period
Washington	CPA / Deepfakes	$7,500/violation	**$5,000**	**364 days (gross misd.)**	AI transparency $5K/violation/day
West Virginia	HB 4496 / SB 484	$100,000/day (orgs)	**$10,000**	**5 years (deepfake minors)**	Mental health AI: $10K eff. 2027
Wisconsin	AB 965 / Deepfakes	$25,000 (child safety)	**$10,000**	**3.5 years (Class I Felony)**	Healthcare AI restrictions active
Wyoming	Deepfake / Election laws	$4,000	**Felony possible**	**3 years (intimate media)**	Insurance AI human-review required

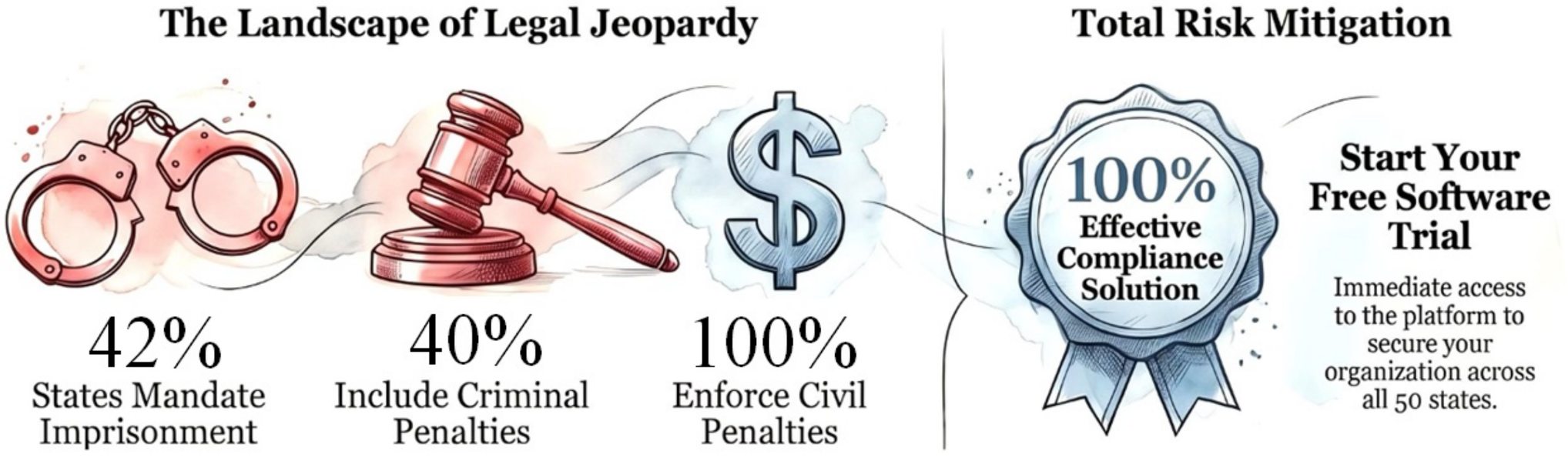
Healthcare Regulatory Compliance Penalties in 50 States



Download: Federal Criminal convictions State Civil and Criminal convictions Summary of 50 States AI, privacy, healthcare, PBM regulations

State	Key Healthcare Focus	Max Civil Fine	Max Criminal Fine	Max Imprisonment	HIPAA Criminal Overlay
Alabama	SB 63/HB 515 medical necessity	$100,000/act	**$30,000**	**20 years (Class B Felony)**	Yes
Alaska	SB 133 prior auth	$25,000/instance	**N/A**	**License suspension**	Yes
Arizona	HB 2175 AI oversight	$1,000/violation	**$10,000 enterprise**	**6 months**	Yes — up to $250K/10 years
Arkansas	Insurance mandates	$1,000/violation	**N/A**	**N/A**	Yes
California	SB 1120 / AB 3030	$25,000 (facility)	**$10,000**	**1 year**	Yes
Colorado	General facility/HIPAA	$10,000+	**$250,000**	**10 years**	Yes — up to $250K/10 years
Connecticut	DPH enforcement	$25,000	**N/A**	**N/A**	Yes
Delaware	DHSS/Insurance Commissioner	$10,000/instance	**$10,000 (Class F Felony)**	**Felony terms**	Yes
Florida	HIPAA + state licensing	$50,000/violation	**$250,000**	**10 years**	Yes — full HIPAA tiers
Georgia	CATCH Act / Facility licensing	$5,000 (serious harm min.)	**$500,000 (kickback felony)**	**10 years**	Yes
Hawaii	HB 820 AI review	$10,000/offense	**N/A**	**30 days (petty misd.)**	Yes — up to $68,928/violation
Idaho	Medicaid fraud / Anti-kickback	$5,000/referral	**$15,000**	**15 years (insurance fraud)**	Yes
Illinois	Healthcare fraud	$50,000 (corp.)	**$25,000**	**Life (if death results)**	Yes
Indiana	IC 16-51-2.5 AI disclosure	$1,000/violation	**N/A**	**N/A**	Yes
Iowa	Iowa Code 135C.36	$10,000/citation (Class I)	**N/A**	**Program exclusion**	Yes
Kansas	SB 405 Healthcare AI	$50,000/violation	**N/A**	**N/A**	Yes
Kentucky	KRS 223.991	$500	**$250,000 (HIPAA)**	**10 years (HIPAA)**	Yes
Louisiana	HB 114 AI diagnosis	$10,000/violation	**$250,000**	**10 years**	Yes
Maine	LD 1301 AI denials	$25,000/day (repeat)	**N/A**	**N/A**	Yes
Maryland	HB0820 AI healthcare	$10,000/offense	**$250,000 (health data)**	**10 years**	Yes
Massachusetts	RPO reporting	$25,000/week	**$250,000**	**10 years**	Yes
Michigan	Public Health Code	$50,000 (willful neglect)	**$250,000**	**10 years**	Yes — full HIPAA tiers
Minnesota	Health Records Act	$7,500/violation	**Criminal prosecution**	**License revocation**	Yes
Mississippi	HB 1717 Medical Judgment	$5,000/violation	**N/A**	**License suspension**	Yes
Missouri	HIPAA enforcement	$50,000	**$250,000**	**10 years**	Yes — full HIPAA tiers
Montana	HCA / Facility violations	$50,000	**N/A**	**20 years (felony)**	Yes
Nebraska	LB 77 AI review	$1,000 (subsequent)	**N/A**	**N/A**	Yes
Nevada	AB 406 / BBSP	$15,000/violation	**$5,000 (Category D Felony)**	**4 years**	Yes
New Hampshire	HB 1406 / NHFCA	$11,000/claim + 3x damages	**Class B Felony**	**7 years (Medicaid fraud)**	Yes
New Jersey	A3973 kickbacks	$20,000/violation	**$50,000**	**5 years**	Yes
New Mexico	Medical Board / False Claims	$28,619/claim + 3x damages	**N/A**	**License revocation**	Yes
New York	Healthcare fraud	Up to $2.07M/year (HIPAA)	**$250,000**	**25 years (1st degree)**	Yes
North Carolina	Medical Board	$68,928/violation (HIPAA)	**$250,000**	**10 years**	Yes
North Dakota	Prior auth reform	$500/day	**Board sanctions**	**N/A**	Yes
Ohio	ORC 3701.244	$20,000/violation	**$750 (health order)**	**90 days (2nd degree misd.)**	Yes
Oklahoma	SB 1967 / HB 1915	$500,000/year (aggregate)	**$100,000/violation**	**Felony possible**	Yes
Oregon	OHA / Board of Pharmacy	$10,000 (pharmacy)	**N/A**	**N/A**	Yes
Pennsylvania	Facility licensing / HIPAA	$50,000/violation	**$250,000**	**10 years (HIPAA)**	Yes
Rhode Island	S0013 healthcare AI	$50,000/violation (insurer)	**N/A**	**N/A**	Yes
South Carolina	Medicaid fraud / PMP	Treble damages + $2K/claim	**$10,000**	**10 years (PMP felony)**	Yes
South Dakota	SB 169 AI review	Cease-and-desist	**$250,000 (HIPAA)**	**10 years (HIPAA)**	Yes
Tennessee	SB 1261 AI utilization	Punitive damages	**N/A**	**N/A**	Yes
Texas	SB 1188 / TRAIGA	$250,000 (financial gain)	**N/A**	**License revocation**	Yes
Utah	HB 452 mental health chatbots	Admin fines	**N/A**	**N/A**	Yes
Vermont	Green Mountain Care Board	$10,000 (drug pricing)	**$1,000/claim**	**10 years (Medicaid fraud)**	Yes
Virginia	SB 754 reproductive data	$5,000 (subsequent willful)	**N/A**	**N/A**	Yes — up to $250K/10 years
Washington	Mental health parity	$300,000 (admin)	**N/A**	**364 days (gross misd.)**	Yes
West Virginia	WV Code §9-7	$50,000/violation (HIPAA)	**$10,000**	**10 years (record destruction)**	Yes
Wisconsin	Provider AI restrictions	$25,000 (willful)	**$100,000 (for profit)**	**3.5 years**	Yes
Wyoming	SF0057 Price Transparency	$1,000/day	**$250,000 (HIPAA)**	**10 years (HIPAA)**	Yes

Privacy Regulatory Compliance Penalties in 50 States

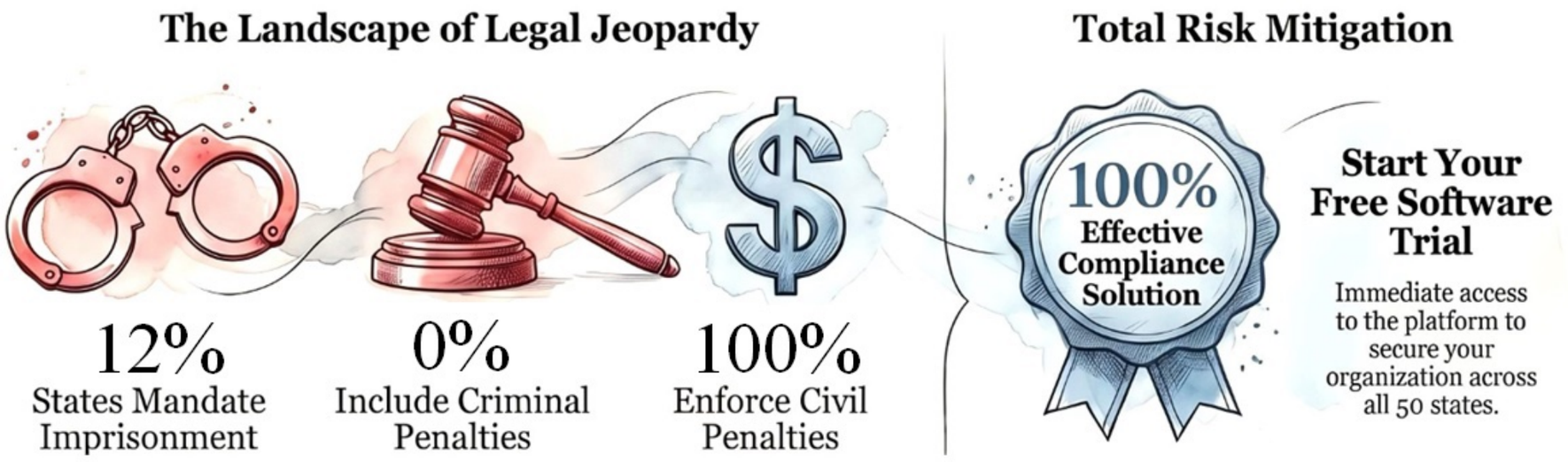


Download: Federal Criminal convictions | State Civil and Criminal convictions | Summary of 50 States AI, privacy, healthcare, PBM regulations

State	Key Privacy Law	Max Civil Fine (per violation)	Max Criminal Fine	Max Imprisonment	Notes
Alabama	Data Breach Notification Act /	$7,500	**$500,000 cap/breach**	**N/A**	AG exclusive enforcement; $5K/day breach
Alaska	APIPA / SB 134	$25,000	**$2,000**	**1 year**	Govt employee disclosure = misdemeanor
Arizona	A.R.S. § 18-552	$10,000/individual	**N/A**	**N/A**	$500K cap per breach
Arkansas	PIPA / Deceptive Trade	$10,000	**N/A**	**N/A**	AG enforcement under DTPA
California	CMIA / CCPA / AB 2013	$25,000 (willful)	**$250,000**	**1 year**	Private right of action; $1K nominal damages
Colorado	CPA	$20,000	**N/A**	**N/A**	$500K aggregate cap; AG exclusive
Connecticut	CTDPA	$5,000 (willful)	**N/A**	**N/A**	Per-consumer violations can be massive
Delaware	DPDPA	$10,000 (willful)	**N/A**	**N/A**	No cure period as of Jan 2026
Florida	FLDBR	$50,000	**N/A**	**N/A**	Trebled to $150K for children
Georgia	SB 473 (eff. July 2026)	$7,500	**$50,000 (computer)**	**15 years (felony)**	60-day cure period
Hawaii	SB 3017 / SB 1163	$10,000/day	**N/A**	**N/A**	Treble damages for consumers
Idaho	ID Code § 28-51-105	$25,000/breach	**$2,000**	**1 year**	Govt employee disclosure = misdemeanor
Illinois	BIPA	$5,000 (intentional)	**N/A**	**N/A**	One recovery per person per biometric type
Indiana	ICDPA (eff. Jan 2026)	$7,500	**$5,000 (privacy invasion)**	**2.5 years (Level 6 Felony)**	30-day cure; no private right of action
Iowa	ICDPA	$7,500	**N/A**	**N/A**	90-day mandatory cure; AG exclusive
Kansas	KCPA	$10,000	**N/A**	**N/A**	$20K for willful court order violations
Kentucky	KCDPA	$7,500	**N/A**	**N/A**	30-day cure period
Louisiana	Data Breach Notification	$5,000/day	**$250,000**	**10 years**	Criminal for wrongful health info disclosure
Maine	LD 1088	$10 million (initial)	**N/A**	**N/A**	$30M for subsequent; 30-day cure
Maryland	MODPA / MCPA	$25,000 (repeat)	**$1,000**	**1 year**	60-day cure until April 2027
Massachusetts	MDPA (eff. July 2026)	$5,000	**$250,000 (health data)**	**10 years**	60-day cure July 2026–Dec 2027
Michigan	HIPAA/State	$50,000/violation	**$250,000**	**10 years**	Federal HIPAA tiers apply
Minnesota	MCDPA	$7,500	**N/A**	**N/A**	AG exclusive; no private right of action
Mississippi	HB 1051	$7,500	**N/A**	**N/A**	$100–$750 per consumer for breaches
Missouri	HIPAA (federal)	$50,000	**$250,000**	**10 years**	Federal HIPAA enforcement
Montana	MTCDPA	$7,500	**$10,000**	**5 years**	Cure period sunsets April 2026
Nebraska	NDPA / LB 504	$50,000 (minors)	**N/A**	**N/A**	$7,500 general; 30-day cure
Nevada	NRS 603A	$5,000	**N/A**	**N/A**	AG sole enforcement; no private right
New Hampshire	NHPA / SB 255	$10,000	**$100,000 (entity felony)**	**Felony possible**	Cure discretionary as of Jan 2026
New Jersey	NJDPA	$20,000 (subsequent)	**N/A**	**N/A**	30-day cure until July 2026
New Mexico	CHISPA / SB 53	$1,000 (health data)	**N/A**	**18 months (2nd offense)**	Opt-in standard for data collection
New York	SHIELD Act	$20,000 (notification)	**N/A**	**N/A**	$5K/violation security failures
North Carolina	NC Personal Data Privacy Act	$2,500	**Misdemeanor**	**60 days (Class 2)**	$50K cap for breach notification
North Dakota	HB 1127	$100,000	**$10,000 (financial)**	**5 years (Class C Felony)**	$5K/offense breach notice
Ohio	ORC 1349.19	$10,000/day (after 90 days)	**N/A**	**5 years (tampering)**	Tiered daily fines for breach notice
Oklahoma	SB 626 (2026)	$150,000/breach	**N/A**	**N/A**	Affirmative defense for safeguards
Oregon	OCPA	$7,500	**Class C felony possible**	**Felony possible**	No cure period as of Jan 2026
Pennsylvania	BPINA / UTPCPL	$5,000 (injunction)	**N/A**	**N/A**	$3K/violation for senior victims
Rhode Island	RIDTPPA	$10,000	**N/A**	**N/A**	No cure period; no private right of action
South Carolina	HB 3431 (Social Media)	Treble damages	**N/A**	**N/A**	Personal liability for officers
South Dakota	SB 49 (Genetic) / DTPA	$10,000/day	**N/A**	**N/A**	$5K/violation genetic data
Tennessee	TIPA	$7,500 ($22,500 willful)	**N/A**	**N/A**	60-day cure; NIST safe harbor
Texas	TDPSA	$7,500	**N/A**	**N/A**	30-day cure; AG exclusive
Utah	UCPA	N/A (AG enforcement)	**N/A**	**N/A**	Right to correct eff. July 2026
Vermont	VDPA	$10,000 ($25K filings)	**N/A**	**N/A**	Private right of action 2026–2028
Virginia	VCDPA	$7,500 ($2.5M cap	**N/A**	**N/A**	30-day cure; no private right of action
Washington	MHMDA / CPA	$7,500 (AG) / $25K treble	**$250,000 (HIPAA)**	**10 years (HIPAA)**	Private right of action under MHMDA
West Virginia	HB 4868 (proposed 2026)	$10,000/violation	**$10,000**	**10 years (felony)**	AG exclusive enforcement
Wisconsin	AB-172 (proposed)	$10,000/infraction	**$100,000 (for profit)**	**3.5 years**	Pending legislation for 2027
Wyoming	SF0065 / HIPAA	$250,000 (malicious)	**$250,000**	**10 years**	Govt data restrictions eff. July 2026

PBM Regulatory Compliance Penalties in 50 States

PBM is a Pharmacy Benefit Manager



Download: Federal Criminal convictions State Civil and Criminal convictions Summary of 50 States AI, privacy, healthcare, PBM regulations

State	Key PBM Law	Max Civil Fine	Key Provisions	Max Imprisonment
Maine	LD 1580	$5,000/day (unlicensed)	Spread pricing ban; $500K market withdrawal	$1,000 + <1 year
California	SB 40 (Insulin cap)	$35M historic (DMHC)	$35/month insulin copay cap	$1,000 + 6 months
Ohio	ORC 3959	$1,000/violation/day	Superintendent license revocation	30 days (4th degree misd.)
Arizona	SB 1102 / DIFI	$1,000/violation	Cease-and-desist authority	4 months (Class 2 Misd.)
North Dakota	HB 1584	$10,000/violation ($50K subsequent)	Enforcement fund; $1M financial responsibility	5 years (Class C Felony unlicensed)
Vermont	DFR Licensure	$100,000/violation	Spread pricing ban; gag clause ban	License revocation
Wyoming	WY PBM Act	$1,000 + 1 year (willful)	2-year audit lookback; patient choice	Misdemeanor
New Hampshire	SB 478/SB 547 (proposed)	$10,000/violation	Fiduciary duty; gag clause ban	Misdemeanor/Felony possible
New York	DFS oversight	$1,000–$5,000/violation	License suspension/revocation	Perjury possible
Alabama	SB 252 (Community Pharmacy Relief)	$1,000/violation	$10.64 dispensing fee; ALDOI enforcement	
Alaska	SB 132/SB 134	$2,500/violation	$20K license required	
Arkansas	Act 624 (Ownership Ban)	$1,000/violation/day	License revocation for ownership violations	
Colorado	Insurance Commissioner	$1,000/violation/day	Registration denial/revocation	
Connecticut	Insurance Commissioner	$100,000/violation	Fiduciary duty established Oct 2025	
Delaware	Insurance Commissioner	$10,000/violation	Authority revocation possible	
Florida	FL Office of Insurance Reg.	$10,000/violation/day	Spread pricing prohibited	
Georgia	HB 690	$10,000/act (willful)	Private right of action established	
Hawaii	HB 2225	$10,000/violation	Unfair/deceptive acts enforcement	
Idaho	ID Code § 41-349	Admin fines + license loss	Spread pricing ban; 100% rebate pass-through	
Illinois	Insurance Code	Regulatory action	Director of Insurance enforcement	
Indiana	SB 140 / HB 1606	$10,000 (3rd+ violation)	$1K first; $2.5K second; license suspension	
Iowa	SF 383	Admin penalties + license	Federal legal challenges ongoing	
Kansas	SB 360	$100,000 (unlicensed)	Strict licensing; cease-and-desist	
Kentucky	SB 188 / 201 KAR 2:416	$500 (late renewal)	$10K registration fee; DOI enforcement	
Louisiana	PBM Reform Act 2025	$1,000/claim	Treble damages; enforcement fund	
Maryland	SB 896	$10,000/violation	$1K/day carrier penalties; restitution	
Massachusetts	Eff. Jan 2026	$25,000 (false reporting)	$5K/day unlicensed; 10% surcharge	
Michigan	PA 11 of 2022	$20,000/month (suspended)	License revocation; DIFS oversight	
Minnesota	Dept. of Commerce	$25,000/violation	$10K/day unlicensed; fiduciary duty	
Mississippi	HB 1672	$25,000 (admin)	$1K/day general; Board of Pharmacy	
Missouri	SB 846/SB 363	$5,000/violation/day	Probation up to 5 years; license revocation	
Montana	HB 740	Insurance code violations	Spread pricing ban; retroactive denial ban	
Nebraska	LB 198 (eff. Jan 2026)	$1,000/entity/violation	Spread pricing ban; specialty pharmacy rights	
Nevada	Single State PBM	Admin fines + registration revocation	Spread pricing ban; transparency reports	
New Jersey	S1300	$10,000/day (non-compliance)	$5K first; $10K subsequent; gross receipts	
New Mexico	PBM Regulation Act	$1,000–$10,000/incident	Spread pricing ban; audit protections	
North Carolina	Dept. of Insurance	$500–$50,000/violation	Spread pricing ban; rebate pass-through	
Oklahoma	Patient's Right to Pharmacy Choice	$100–$10,000/violation	License revocation; $50K–$500K surety bonds	
Oregon	Insurance Code	$10,000/violation	$10K/day transparency reporting; cost growth	
Pennsylvania	Act 77 of 2024	$100,000/violation ($1M/year cap)	$50K unknown violations; $500K/year cap	
Rhode Island	S0222 / OHIC	$10,000/violation	NADAC + dispensing fee minimum	
South Carolina	SC Dept. of Insurance	$10,000/violation	104% NADAC + dispensing fee; anti-steering	
South Dakota	SDCL 58-29E	License revocation + damages	Fee ban; anti-clawback; MAC list updates	
Tennessee	SB 881/HB 1244	$250K cap removed	TDCI consent orders; aggressive enforcement	
Texas	SB 1122/SB 1354	$1,000–$5,000	Pharmacy appeal rights; cost + dispensing fee	
Utah	HB 257	Admin fines	Spread pricing ban; drug synchronization	
Virginia	SCC Title 38.2	$5,000/day	License revocation; private right of action	
Washington	RCW 48.200	$5,000 (willful)	$1K standard; OIC oversight	
West Virginia	HB 3092 / OIC	$20,000 (unlicensed)	$10K/violation; 100% rebate pass-through	
Wisconsin	Cole's Act / SB 203	Admin fines + license revocation	Medicaid dispensing fee; gag clause ban	

Federal Regulatory Compliance Penalties in 50 States

Regulation	Civil	Criminal	Imprisonment Penalties	Liability Trigger or Standard
CEO	CEO	CEO	CEO	CEO
HIPAA/HITECH ACT				**Organizational Oversight Failure**
Tier 1 - Unknowing	$141 - $71,162 /violation; $2,134,831/year cap			Failure of foundational compliance
Tier 2 - Reasonable Cause	$1,424 - $71,162 per violation; $2,134,831/year cap			"Should have known" standard
Tier 3 - Willful Neglect	$14,232 -$71,162 /violation; $2,134,831/year cap			Direct executive accountability
Tier 4 - Willful Neglect	Min. $71,162 per violation; $2,134,831/year cap			Personal liability attaches
HIPAA CRIMINAL				
Knowingly Obtaining/Disclosing PHI		$50,000	Up to 1 year	Knowledge of violation
False Pretenses		$100,000	Up to 5 years	Deceptive conduct
Commercial Gain/Malicious Harm		$250,000	Up to 10 years	Intent to profit or harm
21ST CENTURY CURES ACT				**Strategic & Operational Decisions**
Information Blocking	Up to $1,000,000; CMS discretion for max cap			Decisions impeding data flow
Medicare PI Program	75% market basket loss; Compounds annually			Revenue impact on CEO's watch
CURES ACT (via HIPAA/Civil Rights)				
Malicious Intent / Commercial Gain		$250,000	Up to 10 years	Commercial motivation
CLIA (1888)				**Ongoing Operational Risk**
Immediate Jeopardy	$3,050 - $10,000/day; No Max cap		Up to 3 years	Failure to address critical lab issues
Certificate Revocation	Complete revenue loss; Min. 1 year			Existential operational failure
DOJ DATA SECURITY PROGRAM				
Civil Penalty	$368,136 OR 2x value; No statutory cap			Direct personal liability as a 'U.S. Person'
Willful National Security Data Transfer		$1,000,000	Up to 20 years	"Reasonably should have known"
Medicare / FCA	**Treble Damages = $27K Claim**			
FDA MEDICAL DEVICE REGS	Up to $15,000; $1,000,000/proceeding	**$250,000**	**3 years**	**Responsible, corporate officer doctrine**
FD&C Act Sec. 524B	**$1,000,000 per proceeding**	**>$1 million**	**10-20 years**	**FDA guides**
FDA/FD&C ACT CRIMINAL				
Misdemeanor (First Offense)		$100,000	Up to 1 year	Strict liability
Felony (Intent to Defraud/Repeat)		$250,000	Up to 3 years	Intent or prior violation
FTC HBNR	$53,000 per violation			
MEDICARE / FALSE CLAIMS ACT				
Civil Penalty	$11,000 - $27,894/claim; PLUS treble damages			Billing/attestation oversight
False Statements (18 USC § 1001)		$250,000	Up to 5 years	Knowing false statement
Healthcare Fraud / Anti-Kickback		Substantial	Up to 10 years	Scheme to defraud

Regulation	Civil	Criminal	Imprisonment Penalties	Liability Trigger or Standard
CTO	CTO	CTO	CTO	CTO
HIPAA SECURITY RULE				
1. Encryption / Access Control Failure	$141 - $71,162; $2,134,831/year cap			System configuration decisions
2. Audit Log / Risk Assessment Failure	Up to $71,162; $2,134,831/year cap			Monitoring & analysis deployment
HIPAA CRIMINAL				
Wrongful Disclosure (System Config)		$50,000	Up to 1 year	Access control failures
False Pretenses (Security Capabilities)		$100,000	Up to 5 years	Attestation fraud
Commercial Gain (Data Access)		$250,000	Up to 10 years	Data monetization schemes
CURES ACT - TECHNICAL				
3. EHR Configuration / API Non-Compliar	Up to $1,000,000; 25% Medicare reduction			Non-standard blocking mechanisms
CLIA - TECHNICAL				
4. Quality Control / Equipment Validation	Up to $10,000/day; No cap			QC system implementation/maintenance
CLIA CRIMINAL				
Intentional Violation		Per Title 18 USC	Up to 3 years	Direct oversight of lab systems
DOJ DSP - TECHNICAL				
5. CISA Security / Vendor Due Diligence	$368,136 OR 2x value; No statutory cap			System controls & technology oversight
DOJ DSP CRIMINAL				
Willful Violation / Gross Negligence		$1,000,000	Up to 20 years	Control person' over failed systems
Inadequate Vendor Due Diligence		$1,000,000	Up to 20 years	Direct authority over vendor systems
FDA SEC. 524B - DEVICE CYBERSECURITY				
6. SBOM / Patch Management Failure	Up to $15,000; $1,000,000/proceeding			30/60-day response windows
FDA/FD&C ACT CRIMINAL				
Misdemeanor (Device Cybersecurity)		$100,000	Up to 1 year	Failure of technical implementation
Felony (Knowingly Allowing Violations)		$250,000	Up to 3 years	Responsible Corporate Officer standard
FTC HEALTH BREACH NOTIFICATION				
Breach Detection System Deployment	Up to $53,088; $50M+ potential			Breach detection system deployment

Regulation / Liability Type	Organizational Penalty	Maximum Exposure	Board Fiduciary Impact
BOD - Board of Directors	BOD - Board of Directors	BOD - Board of Directors	BOD - Board of Directors
HIPAA / HITECH act	$1M - $16M+ Settlement	$115M+ Class Action	Governance oversight failure
CURES ACT	Up to $1,000,000/violation	25% Medicare revenue reduction	Failure of strategic compliance oversight
CLIA	Certificate Revocation	Complete lab revenue loss	Existential governance failure
DOJ DSP	$368,136 OR 2x value per violation	Can exceed $100M	Failure to ensure nat'l security compliance
Medicare/ False Claims Act	Treble damages + fines	Can exceed $100M	Failure of billing compliance oversight
Corporate Integrity Agreements	$2M - $20M implementation cost	3-5 year duration	Intensive, direct Board reporting required
Breach of Fiduciary Duty	Liability for damages	Personal liability for damages	Failure to ensure adequate compliance
Shareholder Derivative Suits	Liability for damages	Personal financial liability	Regulatory violations results in financial harm
State AG Actions	Liability for penalties	State-level penalties, injunctions	Consumer protection violations
Qui Tam Whistleblower Risk	15-30% of recovery to whistleblower	Personal financial liability	Internal whistleblowers filing FCA suits

VERIFY USING SAVED GOOGLE SEARCHES

Regulatory Convictions Matrix

Transformativ IP

State Civil & Criminal Penalties and Federal Criminal Penalties

Including Imprisonment — Covering AI, Healthcare, Privacy, and PBM Regulations

All 50 U.S. States | With Third-Party Verification via Saved Google Searches

HOW TO USE THIS DOCUMENT

Every hyperlink in this document is designed for rapid, independent verification. The legend below explains what you will see when clicking each link type throughout the 100-page matrix.

HYPERLINK LEGEND

HYPERLINK	WHAT YOU WILL SEE WHEN CLICKED
1) Search Results	Saved Google search of each state's Penalties for AI, privacy, healthcare and PBM regs.
2) CRIMINAL or CIVIL	Under *State Penalties Paid* — opens a saved Google search listing people convicted, amounts paid, restitution, and prison sentences. Results appear for criminal or civil track.
3) State Name (Federal Criminal column)	Under *Federal Criminal Penalties Paid* — opens a saved Google search for each state of people convicted of federal criminal violations, fines, restitution, and prison sentences.

CONSOLIDATED CONVICTION RECORDS

The two PDFs below combine every saved Google search referenced above into single, downloadable documents.

RESOURCE 1 100-page PDF

All 50 states penalties for Ai, privacy, healthcare and PBM Regulations

Aggregation of all 50 States penalties for Ai, privacy, healthcare and PBM Regulations

RESOURCE 2 235-page PDF

50 State's Civil and Criminal Convictions

Aggregation of all 50 state's convictions with fines, restitution, and prison sentences.

A Google Search conducted on April 26th (results on the next page) uncovered a significantly greater number of State (Criminal and Civil) convictions compared to the earlier search on April 18th (documented in the 235-page PDF). This sharp rise in searchable convictions, apparent in just eight days, underscores the rapidly evolving availability of information as regulators continue to prosecute regulations that began enforcement after January 1, 2026.

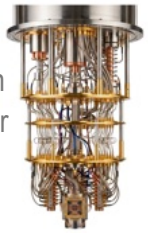
RESOURCE 3 82-page PDF

Federal Criminal Convictions in All 50 States

Aggregation of all 50 state's federal criminal convictions with fines, restitution, and prison sentences.

State	Page	Saved Google AI Searches	State Penalties Paid	Federal Criminal Penalties Paid
Alabama	Search Results		Criminal, Civil	Alabama
Alaska	Search Results		Criminal Civil	Alaska
Arizona	Search Results		Criminal Civil	Arizona
Arkansas	Search Results		Criminal Civil	Arkansas
California	9 Search Results		Criminal, Civil	California
Colorado	Search Results		Criminal, Civil	Colorado
Connecticut	Search Results		Criminal, Civil	Connecticut
Delaware	Search Results		Criminal, Civil	Delaware
Florida	Search Results		Criminal, Civil	Florida
Georgia	Search Results		Criminal, Civil	Georgia
Hawaii	Search Results		Criminal, Civil	Hawaii
Idaho	Search Results		Criminal, Civil	Idaho
Illinois	Search Results		Criminal, Civil	Illinois
Indiana	Search Results		Criminal, Civil	Indiana
Iowa	Search Results		Criminal, Civil	Iowa
Kansas	Search Results		Criminal, Civil	Kansas
Kentucky	Search Results		Criminal, Civil	Kentucky
Louisiana	Search Results		Criminal, Civil	Louisiana
Maine	Search Results		Criminal, Civil	Maine
Maryland	Search Results		Criminal, Civil	Maryland
Massachusetts	Search Results		Criminal, Civil	Massachusetts
Michigan	Search Results		Criminal, Civil	Michigan
Minnesota	Search Results		Criminal, Civil	Minnesota
Mississippi	Search Results		Criminal, Civil	Mississippi
Missouri	Search Results		Criminal, Civil	Missouri
Montana	Search Results		Criminal, Civil	Montana
Nebraska	Search Results		Criminal, Civil	Nebraska
Nevada	Search Results		Criminal, Civil	Nevada
New Hampshire	Search Results		Criminal, Civil	New Hampshire
New Jersey	Search Results		Criminal, Civil	New Jersey
New Mexico	Search Results		Criminal, Civil	New Mexico
New York	Search Results		Criminal, Civil	New York
North Carolina	Search Results		Criminal, Civil	North Carolina
North Dakota	Search Results		Criminal, Civil	North Dakota
Ohio	Search Results		Criminal, Civil	Ohio
Oklahoma	Search Results		Criminal, Civil	Oklahoma
Oregon	Search Results		Criminal, Civil	Oregon
Pennsylvania	Search Results		Criminal, Civil	Pennsylvania
Rhode Island	Search Results		Criminal, Civil	Rhode Island
South Carolina	Search Results		Criminal, Civil	South Carolina
South Dakota	Search Results		Criminal, Civil	South Dakota
Tennessee	Search Results		Criminal, Civil	Tennessee
Texas	Search Results		Criminal, Civil	Texas
Utah	Search Results		Criminal, Civil	Utah
Vermont	Search Results		Criminal, Civil	Vermont
Virginia	Search Results		Criminal, Civil	Virginia
Washington	Search Results		Criminal, Civil	Washington
West Virginia	Search Results		Criminal, Civil	West Virginia
Wisconsin	Search Results		Criminal, Civil	Wisconsin
Wyoming	Search Results		Criminal, Civil	Wyoming

PQC+™



A 90-Day Path to Post-Quantum Resilience

> Google, IBM, and Microsoft project that quantum capability will break the public-key encryption protecting roughly 95% of the global economy by 2029. The question is no longer *whether* to move to post-quantum cryptography. It is whether you move in time to withstand legal and regulatory scrutiny — and to keep the C-suite out of personal liability. Every encrypted record you hold today — patient or client files, financial data, IP, communications — is now being harvested by adversaries who plan to decrypt it in 2029.

Why Your Status Quo Fails

- **Two-front attack chain.** The swarm of AI bots is already a force multiplying harvester, scanning for weak implementations and quickly exfiltrating data. Quantum is the decryptor — Shor's algorithm collapses RSA/ECC from "lifetime of the universe" to minutes. Google's self-correcting Willow chip suggests that physics has been solved and that the problem is now engineering.
- **"Harvest Now, Decrypt Later" is active.** Long-lifespan data (health, financial, IP, defense) has a defined expiration date on its confidentiality. The clock started years ago.
- **An algorithm swap is not a strategy.** Replacing RSA or ECC with a NIST-approved PQC algorithm leaves the underlying architecture exposed: centralized key vaults remain a single point of failure, static long-lived keys turn one breach into years of stockpiled exposure, and external ACLs don't travel with the data once it leaves the perimeter.
- **Lattice-based PQC strains legacy systems.** Many schemes introduce data bloat and latency that OT, ICS, and mainframe environments cannot absorb without re-engineering. That is time-consuming, error-prone, and a massive time waster. Most CTOs and CISOs are overworked.
- **The personal-liability math has changed.** Under the Learned Hand standard, a leader is negligent when the burden of prevention is less than probability × magnitude of harm. B < (P * L). With prevention now a ~90-day software deployment, rising HNDL probability, regulatory compliance complexity, and effectively infinite loss magnitude, the math has flipped against inaction. Once a CTO or CISO flags the risk, the legal clock on the CEO starts running.

Why PQC+™ Is the Recommended Solution

PQC+ moves security out of the perimeter and into the data itself. It is 100% software, deploys in roughly 90 days with no rip-and-replace, and ships with two integration paths so brownfield and greenfield estates are covered without downtime:

- **SDK integration (greenfield):** embed libraries directly for field-level encryption and microservice ACLs — core operations in two lines of code.
- **Transport-layer protection (brownfield):** drop-in gateway transparently PQC-encrypts the data stream before it touches the network. Legacy OT, ICS, mainframes, and edge devices are protected with zero application changes.

PQC+ is built on NIST-standardized ML-KEM (FIPS 203) for key encryption and ML-DSA (FIPS 204) for digital identity signature encryption. PQC+ has the ability to manage encryption bit sizes of 1024 for commercial clients, 2048 for the US military, 5012 for the CIA, and 10240 for the NSA, with just software configuration, using the data encryption standard AES-256 for transport. Throughput runs near wire-line speed (~106 MB/s, 11 µs per packet) and operates

inside relational databases in real time. PQC+ is the only post-quantum-strength software carrying DoD Impact Level 5, alongside FIPS 140-3, FDA, and DHS approvals.

PQC+'s Two Components and Why They Matter

Q-SecurKey™ — eliminates the static key target

- **No keys are ever stored.** Decryption keys are derived on demand from verified attributes (identity, clearance, location, time, zero-trust token) plus secret seeds and public parameters.
- **Session-only existence.** Each key lives for a single transaction and ceases to exist after — there is no vault to breach and no long-term secret for an HNDL attacker to wait on.
- **Removes the highest-value target in your stack.** Centralized KMS/HSM compromises become structurally impossible because there is nothing centralized to compromise.

Q-InfoSecur™ — embeds authorization inside the data

- **Self-enforcing data.** The access-control list is cryptographically bound to the encrypted payload. The data enforces its own rules wherever it travels — inside the perimeter or far outside it.
- **Instant revocation, no re-encryption.** Update policy and access changes immediately. No bulk re-encryption project, no downtime.
- **Multi-classification on a single system.** Top Secret through Unclassified can coexist on the same infrastructure, with the embedded ACL acting as a gatekeeper.

Combined effect: *even if attackers obtain the ciphertext, they cannot decrypt it (PQC), cannot find keys (none stored), cannot brute-force it (AI-resistant), and cannot reach what they are not authorized for (embedded ACLs).*

PQC+ vs. Typical PQC Vendors

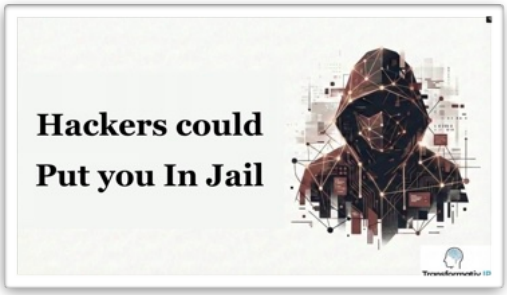
What Leadership Needs	Typical PQC Vendor	PQC+™
Time to deploy	Multi-year migration	~90 days, two lines of code
Hardware required	Yes — rip and replace	None — 100% software
Government certifications	Partial or none at PQ strength	FIPS 140-3, DoD IL5, FDA, DHS
Performance impact	Noticeable latency	Near wire-speed (~106 MB/s)
Free trial available?	Rare	Yes — fully functional trialware

The Decision in Front of You

Your mother told you to shop around — so do. When you do, the comparison is short: PQC+ deploys in ~90 days, fully installed, with no rip-and-replace, the strongest certification stack on the market, and a fully functional free trial. Doing nothing means guaranteed exposure to HNDL and personal liability under federal and state regulations. Running the trial costs nothing, requires no hardware, deploys against your real environment, and produces a documented record that leadership acted on a known, foreseeable risk — exactly the evidence that satisfies the Learned Hand test.

The threat is real. The legal exposure is personal. The remedy is unusually cheap. The only question is whether you start the trial this quarter or explain later why you didn't.

Our Educational Videos and their Detailed Article (highlighted in blue)



IP Theft: Chinese IP theft costs the US economy $225–$600 billion annually, affecting 20% of US companies, including Cisco, Apple, and AMSC (which lost over $1 billion). China is also the most active in targeting critical infrastructure. HNDL attacks in preparation for Q-Day are greatly increasing the stealing of data.
Healthcare: Avg healthcare data breaches cost nearly $10 million , with major HIPAA breaches exceeding $100 million (e.g., Anthem's $16 million settlement). CEOs often face shortened tenure after preventable breaches. How we Protect your from China's IP Theft

Modern executive accountability emphasizes personal liability for compliance failures across over a dozen federal regulations, shifting from reactive to documented, proactive compliance. Non-compliance creates "domino effect liability," risking operational shutdowns.

- **CEO:** Potential criminal liability under the "responsible corporate officer doctrine" for oversight failures.
- **CTO:** Gross negligence in cybersecurity is treated as a criminal violation.
- **BOD:** Personally liable in civil suits for compliance governance and resource allocation failures.

D&O Insurance has many Limitations that few Understand:
A guilty verdict converts millions in defense funds into personal, non-dischargeable debt. Insurance will not cover criminal fines, statutory penalties, or restitution.

Legal Doctrine of Willful Violation used by Regulatory Prosecutors
For executive liability, prosecutors need only prove that an executive knew of a regulatory obligation or technical risk and failed to act. Documented warnings (e.g., Slack messages) can constitute formal legal notice of this awareness and prove willful disregard.
5-page DO Insurance Reality Check

Liability doctrines like the :

- **Responsible Corporate Officer Doctrine** allows for criminal charges based solely on oversight failure, without requiring direct knowledge. Furthermore, the Department of Justice (DOJ) categorizes reliance on manual audits or spreadsheets as
- **Willful Blindness**, treating it as a standard rather than a defense.

The volume of federal and state regulations exceeds human capacity for compliance, leaving no margin for error without our proactive software.
2 Articles: DOJ Prosecutor Guidelines article. Your Total cost of a DOJ violation

The DOJ DSP penalizes you if China, Russia, or Iran accesses large amounts of US data. Up to $ 1 million per violation and 20 years in prison. Traditional privacy frameworks and user "I agree" clicks do not exempt a company from these national security requirements.

A three-layered PQC+ approach mitigates traditional security flaws (static controls, single points of failure):

- **Layer 1: Secure Transport**: Uses "perfect forward secrecy" with unique, ephemeral keys per transfer.
- **Layer 2: Distributed Storage**: Employs DT to encrypt and scatter data fragments across a network, preventing mass theft.
- **Layer 3: Smart Compliance:** A real-time policy engine automatically masks or blocks access based on location/identity, ensuring compliance with schemas like FHIR and FIBO.

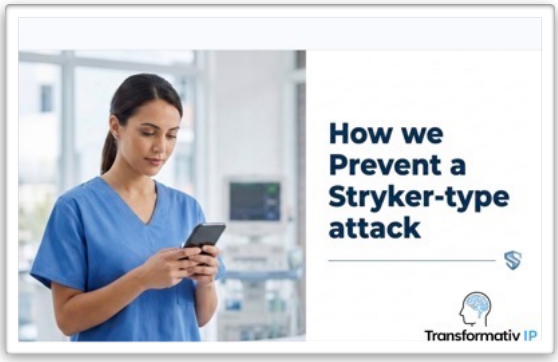
Our Educational Videos and Articles

- **Deadline**: IBM, Google, and Microsoft predict quantum hardware will break RSA/ECC encryption by 2029.
- **Harvest Now, Decrypt Later**: Adversaries are stockpiling intercepted, encrypted data (e.g., genomic, classified communications) for future quantum decryption.
- Learn about how regulators and prosecutors weave together legal doctrines to convict you. To be forewarned is to protect your C-suite team.
- **Permanent Liability:** Siphoned data creates a long-term liability for organizations and the C-Suite on Q-Day. Download our Q-Day 2029 Article

RHT or RHTP: States need an Authorization to Operate, requiring compliance with 10 regulatory domains and over 60 controls (e.g., NIST SP 800-53). Non-compliance risks include funding stalls and data breaches. Key challenges are securing HIPAA/Cures Act data (8 sensitive categories), 42 CFR Part 2 substance use records, and governing AI consent (5 categories) and 9 legal proxies.

The platform is an integrated, unique solution with a hybrid access model. It secures data and uses protocol parsers/behavioral analytics for OT protection outside standard HIPAA. It uses post-quantum cryptography and treats consent as a cryptographic primitive to mitigate quantum threats. Leveraging existing FDA authorization, the platform provides complete compliance, cutting implementation time from 12 months to 6–8 weeks and reducing assessment costs by 80%.

Download our 11-page RHTP article



The $25M Stryker breach by an Iranian hacker exposed a major security flaw in enterprise Mobile Device Management (MDM) systems, such as Microsoft Intune. Intune's device-only verification leaves files vulnerable to credential theft.
Our Defense-in-Depth solution shifts security from the device to the data object, integrating with Intune:

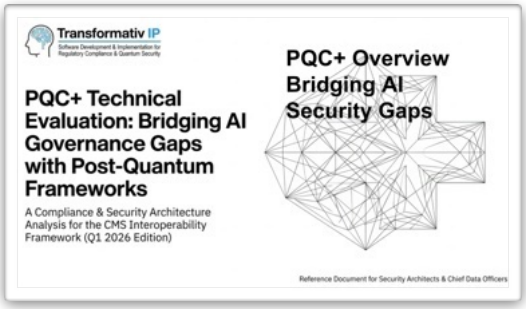
1. **Gatekeeper (Intune):** Verifies device security.
2. **Vault (PQC+ smart compliance):** Uses data owner location to generate a strict, regulation-mapped Access Control List (ACL).
3. **Enforcer:** Applies object-level encryption and embeds the ACL. Compromise instantly locks the data.

This platform uses Post-Quantum Cryptography (PQC+) and TLS 1.3 for future-proof protection, ensuring perfect forward secrecy, and meets all FDA, SBOM, and 2026 vulnerability disclosure requirements. Slide deck PDF

Key Architectural Features:

- **Smart Compliance (Automated AI Gateway):** Intercepts AI requests, enforces consent rules, dynamically masks data, and securely releases it.
- **Dynamic Enforcement:** Granularly enforces consent and jurisdiction in real-time, separating permissible clinical use from restricted third-party training, while adhering to federal and state laws.
- **Mathematical-Level Post-Quantum Cryptography (PQC+):** Utilizes NIST-validated standards: FIPS 203 (key encapsulation), FIPS 204 (digital signatures), and FIPS 205 (mathematical archival).

Architectural Defense Paradigm Shift: The access policy is embedded directly in the keys via post-quantum Attribute-Based Encryption (ABE), making decryption impossible unless a user's attributes match the policy.



Why PQC+ is Superior

Detailed Tech Articles for CTOs and CISOs

What caused the Stryker Attack and How to Prevent a Similar Attack Happening to You

On March 11, 2026, Stryker Corp suffered a highly effective Living-off-the-Land (LotL) attack. Threat actors compromised an administrator account via an Adversary-in-the-Middle (AiTM) phishing campaign, weaponizing Microsoft Intune to bypass MFA. Within three hours, mass remote wipe commands were issued to 80,000 devices. Conventional security failed because the malicious actions were legitimate administrative functions, exposing a critical deficiency in identity governance (e.g., lack of PIM or Conditional Access).

Download 4 pg Article

To prevent similar attacks, organizations must implement:

- ☆ **Behavioral Analytics:** Deploy PQC Monitoring for immediate anomaly detection, or
- ☆ **Post-Quantum Cryptography (PQC) Protections:** Utilize quantum-resistant authentication, multi-admin approval, and command signing.
- ☆ **Zero-Trust Architecture:** Critical infrastructure must adopt a zero-trust model.
- ☆ **Identity Hardening:** Implement phishing-resistant MFA and robust Privileged Identity Management (PIM).
- ☆ **BYOD Security:** Secure Bring-Your-Own-Device environments through containerization.

PQC+ Technical Deep Dive for Hospital Leadership

PQC+ integrates with existing systems (like Epic and Cerner) without requiring a "rip-and-replace." PQC+ functions as a compliant connecting layer between external networks (like QHINs under TEFCA) and your existing hospital systems.

Download 25 pg White Paper

Some of the Key Benefits:

1. **Data Security:** The **SMARTInfoSecur** module uses certified Post-Quantum Cryptography (PQC) to embed access controls directly into the encryption key. This means stolen, encrypted data is useless unless it satisfies the access rules.
2. **Compliance: SMARTCompliance** provides automated, jurisdiction-aware consent enforcement and uses an **AI Compliance Gateway** to control and mask access to patient data by AI applications.
3. **Interoperability: SMARTInteroperability** acts as a universal translator for all major healthcare data formats (FHIR, HL7, DICOM).
4. The **SMARTEntityResolution** module uses AI to address duplicate patient records and maintain a unified Master Patient Index.

Technical Guide to the PQC+ Architecture: Q-InfoSecur™ and Q-SecurKey™

Quantum Data Security for CTOs/CIOs: Glossary, Executive Summary, and 8 Key Concepts.

1. **The Converging Threat:** Why the threat is different now.
2. **Architectural Failures:** Standard PQC migration flaws.
3. **Q-InfoSecur™:** Eliminating the target.
4. **Q-SecurKey™:** Self-enforcing data.
5. **Defense in Depth:** How components work together.
6. **Implementation Strategies:** Flexible and practical approach.
7. Use Cases & Benefits: Real-world strategic value.

Download 26 pg White Paper

Your Path Forward: Architectural resilience for peace of mind.

Quantum-Proof Your Leadership: The PQC+ Legal Advantage

Adopting Post-Quantum Cryptography (PQC+) is the ultimate demonstration of corporate foresight. It's not just technology; it's a critical legal shield for the organization and its leadership, which this table and video explain. Download 5 pg Article for CEO and General Counsel

Key Legal Protection	Benefit of PQC+ Adoption
CEO/Board Liability	**Park Doctrine & Caremark:** Provides "extraordinary diligence" evidence, mitigating personal criminal and oversight liability.
HIPAA Data Security	**Safe Harbor:** Protects against "Harvest Now, Decrypt Later" threats, securing sensitive data for its full lifespan.
DOJ Compliance	**Proactive Compliance:** Demonstrates a well-resourced program, potentially leading to lower fines or avoided prosecution.
CTO/CISO Negligence	**Learned Hand Calculus:** Avoids personal negligence claims, as implementation cost is minimal compared to catastrophic loss.
Data Sharing (Cures Act)	**Security Exception:** Justifies denying insecure data requests without triggering information-blocking penalties.
National Security	**DOJ Data Security Program:** Meets the high bar that restricted data must not be "decryptable using commonly available technology" by quantum adversaries.

PQC+ is the definitive legal move for corporate vigilance and due care in the Quantum era.

Healthcare and FDX solution for AI Regulatory noncompliance if using Anthropic AI MCP.

The AI adoption push faces costly compliance gaps. Healthcare breaches average $10.9M, with HIPAA fines up to $1.9M yearly. The industry also spends $13B on prior authorization. In Open Finance, non-compliance with FDX, FAPI, and OAuth 2.0 can lead to enforcement, lawsuits, and lost partnerships. The core issue is AI accountability, not capability. Our PQC+MCP, based on Anthropic's Model Context Protocol, embeds compliance, consent, and traceability into the AI architecture rather than retrofitting them. 9-pg article explains the problem and the solution

CMS FAQ 13 Questions · 32-Term Glossary

A comprehensive review of the CMS Interoperability Framework, the emerging challenges associated with healthcare AI, and the technical solutions provided by the PQC+ platform. It is designed to evaluate understanding of regulatory requirements, security standards, and the integration of AI within the modern healthcare data ecosystem. 7-pg Article