ZENPREXI
BIO-RISK™

Privacy Architecture Framework

Structuring the Platform for BIPA, ADA, and GINA Compliance

PRIVILEGED AND CONFIDENTIAL — ATTORNEY WORK PRODUCT

I. Executive Summary

Zenprexi's PANT™ intervention system presents a novel legal challenge: how to enable real-time safety interventions based on biometric-derived fatigue scores without creating liability under biometric privacy statutes (BIPA), disability discrimination laws (ADA), and genetic information protections (GINA).

Key Finding: The platform can achieve full legal compliance while preserving core IP. The solution is architectural separation combined with contractual controls and data minimization principles.

II. The Privacy Paradox — And Its Resolution

The system must simultaneously:

- Protect worker privacy from the carrier
- Deliver interventions to specific workers/equipment
- Prevent employer misuse of health-related data for personnel decisions

Resolution: Different parties see different layers of data. The intervention capability and privacy protection operate at different architectural layers and are not in conflict.

III. Privacy Firewall Architecture

Layer 1: Worker's Wearable Device

- Raw biometrics ON-DEVICE only
- CARI™ calculated locally
- Data deleted in 24 hours

↓ *Binary Signal Only (LOCKOUT=T/F)*

Layer 2: Equipment Interlock

- Receives lockout signal only — No worker ID, No CARI score
- Mechanical safety function only

Layer 3: Employer Environment

QSA (Qualified Safety Administrator): Immediate reassignment ONLY

■■ PRIVACY FIREWALL — NO DATA PASSES ■■ HR: NO ACCESS | SUPERVISORS: NO ACCESS | MANAGERS: NO ACCESS

Layer 4: Insurance Carrier

✓ **Receives:** Anonymized risk scores, Intervention counts, Loss trends

✗ **Never Receives:** Worker IDs, Individual CARI scores, Raw biometrics, Medical inferences

IV. Layer-by-Layer Legal Analysis

Layer	Legal Effect
Layer 1	✓ Zenprexi is "collector" under BIPA (not employer) ✓ Employer never possesses biometric identifiers ✓ Satisfies BIPA consent requirements
Layer 2	✓ Employer receives no "medical information" under ADA ✓ No biometric data transmitted = no BIPA violation ✓ Intervention is purely mechanical safety function
Layer 3	✓ Creates "reasonable safeguards" defense under ADA ✓ Limits employer's "acquisition" of medical information ✓ Contractual recourse with liquidated damages ($50K+ per violation) ✓ Workers are third-party beneficiaries with direct enforcement rights
Layer 4	✓ No BIPA exposure for carrier ✓ No ADA/GINA exposure for carrier ✓ Carrier interest remains purely actuarial

V. Three-Tier Consent Model

Tier	Parties	Content	Timing
Tier 1: Platform Consent	Worker → Zenprexi	Biometric data collection disclosure, Purpose limitation (safety only), Retention schedule (24 hrs), Right to revoke/delete	Device activation
Tier 2: Intervention Consent	Worker → Employer	Safety intervention acknowledgment, Equipment may be locked out, QSA may know intervention occurred, No employment decisions from data	Employment onboarding
Tier 3: Carrier Disclosure	Worker → Zenprexi	Anonymized aggregate data sharing, Confirmation no PII shared	Device activation

VI. Risk Mitigation Summary

Risk	Mitigation	Residual
BIPA violation (Zenprexi)	Proper consent, purpose limitation, retention schedule	LOW
BIPA violation (Employer)	Employer never receives biometric data	ELIMINATED
ADA medical exam violation	Employer receives no medical information	LOW
ADA discrimination	Contractual use limitations, firewall from HR	MEDIUM
GINA violation	No genetic data collected	ELIMINATED
Worker retaliation claims	Anti-retaliation policy, normalization training	MEDIUM
Employer breach of contract	Liquidated damages, audit rights, worker enforcement	MEDIUM

VII. Competitive Moat

For Investors: This privacy architecture should be emphasized as a competitive moat. Competitors who fail to implement similar protections will face significant legal exposure, particularly in Illinois where BIPA provides a private right of action with $1,000-$5,000 per violation—no injury required.

By designing for Illinois (BIPA) compliance—the strictest jurisdiction—Zenprexi will be compliant everywhere and can position itself as the only legally-defensible solution in the market.

VIII. Conclusion

The Zenprexi Bio-Risk™ platform can be structured to comply with BIPA, ADA, GINA, and emerging state privacy laws while preserving core IP and commercial functionality. The key insight:

The intervention capability and privacy protection are not in conflict—they operate at different architectural layers.

- Raw biometrics never leave the worker's device
- Employers receive only binary intervention signals
- Individual worker data is siloed with a contractually-bound QSA
- HR and management are completely firewalled
- Carriers receive only anonymized aggregates

This memorandum constitutes legal advice and is protected by attorney-client privilege.
Zenprexi, Inc. | Patent Pending: US 63/919,896