SentinelWear: A Layered System for Passive Sexual Assault Detection, Protection, and Forensic Validation

---

Executive Summary

No woman should have to live in fear of sexual violence when stepping into a bar, walking home, or attending a party. It is a failure of our culture and institutions that such fear is still warranted. While our long-term vision is a world where such tools are obsolete, the reality is that technology must currently serve as a shield where society has not.

SentinelWear introduces a multi-layered system that combines real-time biometric inference, secure ambient data capture, and biochemical signal logging into a unified passive safety and forensic evidence system. It is a system built not just for protection, but for deterrence. The existence and adoption of SentinelWear can change social dynamics: once publicized, potential predators will no longer know who is protected and who is not. The veil of impunity is pierced by uncertainty.

This whitepaper outlines the motivation, architecture, and rollout plan for SentinelWear, a platform that is always on, never invasive, and always on the survivor's side.

---

1. Background and Motivation

Sexual violence, particularly drug-facilitated sexual assault (DFSA), often occurs in environments where the victim becomes incapacitated before they are able to resist or call for help. Traditional evidence-gathering (e.g., rape kits) often takes place hours or days after the event—if at all. Many victims experience memory loss, social stigma, or institutional barriers that prevent timely reporting.

Conventional mobile safety apps require user activation and are ineffective when the victim is unconscious. Meanwhile, wearables like Apple Watch and Fitbit collect biometric data, but that data is not stored securely, analyzed contextually, or tied to potential threat scenarios.

The result is a legal and moral gap: critical events go unrecorded, unreported, and unpunished. SentinelWear fills that gap.

2. Current Solutions and Limitations

Category	Examples	Limitations

Safety Apps	Noonlight, Circle of 6	Require user activation; fail when victim is incapacitated
Audio Recording Apps	Smart Recorder	Not encrypted; not legally defensible; privacy violations
Biometric Devices	Apple Watch, Fitbit	No threat detection logic; not tamper-aware; not forensically secure
Glucose Monitors	Dexcom, Libre	Single-analyte; not tuned for threat state inference

---

3. SentinelWear: Our Approach

SentinelWear integrates multiple streams of data into a tamper-proof, privacy-protecting platform that activates only when the user needs it—even if they can't ask.

Core Principles:

- **Passive by default**: No user interaction required once enabled.
- **Privacy-respecting**: Data is encrypted, inaccessible without consent or law enforcement authorization.
- **Multi-layered sensing**: Combines macro-biomarkers (HR, HRV, EDA, temp, motion) with optional biochemical sensors.
- **Context aware**: Automatically shifts to high alert in risky environments (bars, rideshares, parties).
- **Forensically defensible**: Time-sealed logs, authenticated by device ID and cryptographic hashes.

---

4. Technical Architecture

Layer 1: Real-Time Biometric Inference (Immediate Alert)

- Heart rate and HRV (PPG)
- Electrodermal activity (GSR/EDA)

- Skin temperature
- Accelerometry (fall, slump, carry detection)
- Optional audio cues (slurred speech, lack of speech)

Trigger Outcome: Alarm, friend notification, locked recording begins, passcode consent challenge

Layer 2: Ambient and Contextual Data Logging

- Continuous encrypted audio (72h loop, inaccessible by default)
- Location breadcrumb trail
- Mic/cam snapshot only if threshold crossed
- Tamper detection (patch removal, separation from phone/watch)

Trigger Outcome: Escalates only under sedation state or user-defined rules

Layer 3: Biochemical Signal Logging (Delayed Forensic Trace)

- Optional patch with microfluidic sweat sensor
- Glucose, lactate, pH, ion levels
- In future: aptamer/MIP-based metabolite sensing

Trigger Outcome: Stored for pattern analysis and potential toxicological fingerprinting

---

5. Technology Stack

Layer	Tools / Platforms
Mobile App	Flutter or React Native; Android/iOS SDK integration
Biometric Sensors	Apple HealthKit / Google Fit; custom BLE patches
Biochemical Patch	R&D phase; ISF or sweat-based microfluidic sensor

Signal Processing	Lightweight on-device ML (1D CNNs or GRUs)
Secure Storage	AES-256 encrypted local + cloud, self-deleting buffer
Crypto Evidence Layer	EntropyCore-based hash chain ledger for authentication

---

6. Development Timeline and Milestones

Phase 0 (Weeks 1–2):

- Finalize MVP feature list
- Recruit campus partners (UCSB, SDSU)
- Set up secure cloud and dev ops pipeline

Phase 1 (Weeks 3–8): MVP Build

- Ambient audio + biometric sensing
- Trigger logic and alert flow
- Launch App Store beta and pilot trials

Phase 2 (Months 2–4): Smart Patch Integration

- Partner with lab on sweat sensor prototyping
- Validate fusion of biometric + biochemical markers
- Introduce forensic timestamping

Phase 3 (Months 4–8): Forensic Platform + Public Launch

- Refine cryptographic timestamping and legal access model
- Launch PR campaign, policy outreach, and open source kit

Phase 4 (Months 8–12): Adaptive Risk Modeling

- Personalization engine learns user baselines
- ML models adapt to social context (club vs home vs rideshare)
- Begin data aggregation for clinical validation studies

---

7. Conclusion

SentinelWear is not just a safety device—it is a new category of ethical tech that shifts the burden of proof away from survivors. By creating a forensic black box for the body, we provide real-time protection, secure post-event evidence, and the opportunity to transform how institutions respond to sexual violence.

But perhaps more powerfully, SentinelWear has the potential to act as a cultural signal. Its mere existence changes the equation: it introduces doubt into the minds of would-be predators. Am I being recorded? Will my actions be biometrically logged? Is this person protected?

The goal is not widespread use forever. The goal is deterrence so effective that its use becomes unnecessary.

We remember what the victim may not. We seal the truth when no one else can. And we give power back to the person who needs it most: the one who cannot speak in the moment they are most vulnerable.

Contact
SentinelWear Initiative
Email: founders@sentinelwear.org
Twitter/X: @SentinelWear
GitHub (Open Source Release TBD)