

SentinelWear data is locked with military-grade encryption before it even leaves your phone. No one — not even us — can see it unless you give explicit permission or a court compels it, and even then, every file access leaves an indelible fingerprint in the system. It's like a black box for your body — sealed, protected, and unreadable unless something goes seriously wrong.

Here's a roadmap to building a **military-grade digital evidence custody and privacy architecture** with civil liberties and trauma sensitivity at its core.

1. **Guiding principles**
 2. **System architecture** (phone → storage → access control)
 3. **Spec sheet** of technologies and standards
 4. **Vendors or tools** that could support each layer
-

1. Guiding Principles for SentinelWear Evidence Architecture

- **Zero Trust, Even to the App:** Data is encrypted on-device. No one — not even the developers — can read it.
 - **End-to-End Encryption:** Data is encrypted before it leaves the phone and never decrypted except in strict, auditable cases.
 - **Proof of Integrity:** Every packet of data is signed and timestamped.
 - **Zero Access by Default:** Nothing is retained longer than 72h unless an unlock protocol (with user or legal initiation) is triggered.
 - **Immutable Chain of Custody:** Any access, copy, or retrieval is cryptographically logged.
 - **Two-Key Escrow:** Decryption requires *two parties* — e.g., the user and law enforcement, or court-issued authorization + system attestation.
-

2. System Architecture Overview

A. On-Device Layer (Smartphone / Wearables)

- **Real-time data collection** (audio, biometrics, motion, etc.)
- **AES-256 encryption** applied immediately to each time-chunked buffer (e.g., 1 min audio, 5 min motion data)
- **Ephemeral buffer** holds data for 72 hours, then auto-deletes unless escalation is triggered

B. Cloud Layer (Encrypted Cold Storage)

- Data is **re-encrypted at rest** with unique keys per session/device/event
- **Metadata only (hash, timestamp, geotag)** is stored in an immutable **audit ledger**
- Storage is **region-aware** and redundant (AWS S3 with KMS or Google Cloud + Confidential Compute)

C. Access & Retrieval Layer

- **No user or admin access by default**
- **Unlock protocol requires:**
 - **User consent** (biometric or passcode auth) *OR*
 - **Valid legal request + warrant + audit trigger**
- **Dual-key escrow:** Data can only be decrypted when:
 - User key + server key are both presented *or*
 - Law enforcement key + time-locked system key are activated

D. Chain-of-Custody & Audit Logging

- Every:

- File write
 - Attempted access
 - Decryption event
- Is **hashed, timestamped, signed** and recorded to a **secure, append-only audit log** (like a private blockchain or Merkle ledger)

3. Spec Sheet: Military-Grade Security Standards

Feature	Technology / Protocol	Notes
Encryption at Rest	AES-256-GCM	Military standard; Google, AWS use
Encryption in Transit	TLS 1.3+ , mTLS	Modern encrypted transport
Key Management	Hardware Security Module (HSM) or KMS (AWS/GCP)	Keys never stored in software
Dual Access Escrow	Shamir's Secret Sharing or Threshold Encryption	Requires N of M parties to unlock
Access Control	OAuth2 + Zero Trust	Role- and policy-based enforcement
Tamper Logging	Merkle tree / blockchain ledger	Immutable proof of chain-of-custody
Time-Locked Release	Cryptographic time vaults (e.g. Timelock puzzles or Dead Man Switches)	For whistleblower or delayed consent cases
Facial/Bio Auth	Device-native biometrics + Secure Enclave	Android/Apple platform APIs

4. Vendor / Tool List

Layer	Vendor/Tool	Role
-------	-------------	------

On-Device Encryption	Apple Secure Enclave / Android Keystore	Hardware-based crypto
Cloud Storage	AWS S3 + KMS / Google Cloud Storage + CMEK	Encrypted object storage
Identity/Auth	Auth0, Okta, or Firebase Auth	Secure multi-factor authentication
Ledger / Logging	AWS QLDB, Hyperledger Fabric, or Google Cloud Ledger	Immutable logging
Key Escrow & Splitting	Tarsnap, OpenSSL SSS, or CloudHSM	Secure multi-party key control
Monitoring / Auditing	Splunk, Wiz, or Datadog Security	Visibility into security events
Privacy Review / Audit	TNO (Netherlands), Palantir Secure Environments, or MITRE	Policy audit and external verification
