VERTICAL EDITION 11 · PATIENT, DOCTOR & PHARMACY APPS

Stop the prescription that no doctor wrote.

Health apps carry the most sensitive category of personal data and the least tolerance for friction: a consult that stalls is a patient who does not get care. NonaShield answers a deterministic question before the request leaves the handset — was this exact request produced by the physical device holding the non-exportable key, and has it been altered since? Attestation, RASP, fingerprinting, behavioural intelligence, network defence, risk decisioning and forensic evidence run as one signed pipeline across your patient, practitioner, diagnostics and pharmacy apps.

400+	40+	9	1
Distinct threat vectors monitored across device, network and server	Behavioural vectors profiled per consult session, continuously	Architectural layers delivered as one cryptographically signed pipeline	Vendor, contract, integration and console — not four or five

IN THIS DOCUMENT

HARDWARE ATTESTATION · RASP · FINGERPRINTING · BEHAVIOURAL BIOMETRICS · GRAPH INTELLIGENCE · NETWORK DEFENCE · API GATEWAY · RISK DECISION ENGINE · EVIDENCE & COMPLIANCE

EXHIBIT 1 — EIGHT VECTORS, ONE ARCHITECTURE

The vocabulary is care. The question underneath is possession.

Every vector below reduces to the same test: was this request produced by the physical device it claims to come from, by the person entitled to hold it, in an environment that has not been tampered with? The architecture does not change per sector — what changes is the policy set in Layer 7 and the entity model in Layer 5.

VECTOR	HOW IT ARRIVES ON A HEALTH APP	LAYER
Forged & recycled prescriptions	Edited or re-used prescription images submitted across accounts to release Schedule H and H1 medicines.	**1, 3, 5**
Tele-consult identity substitution	A different person in front of the camera at consult or verification — injected video streams and replayed selfies.	**1, 4, 6**
Practitioner-credential misuse	Doctor and pharmacist apps operated by unregistered staff, or one credential shared across a chain of outlets.	**1, 3, 7**
Record access from compromised handsets	Linked health records and reports opened on rooted, hooked or remotely controlled devices.	**1–3**
Patient data lifted before transmission	Hooking frameworks reading reports, prescriptions and identifiers out of app memory before they ever reach you.	**1–2**
Cloned & repackaged health apps	Fake builds outside official stores collecting identity documents, records and payment data under your brand.	**1–3**
Diagnostics & home-collection fraud	Sample collection marked complete off-site; slot, location and report data altered on field-agent handsets.	**1, 2, 8**
Promotion, refund & repeat-order abuse	Emulators and multi-account clusters farming first-order discounts and staged refunds on medicine orders.	**3, 5, 7**

WHERE CRYPTOGRAPHY IS SILENT — STATED PLAINLY

When a registered patient on their own enrolled device requests a repeat that is clinically inappropriate, every cryptographic check passes correctly — because every check is correct. That case belongs to graph and behavioural analysis (Layers 4–6), which surface repeat-fill clusters and coordinated accounts and apply friction there, never to the consult journey as a whole.

APPS COVERED ON ONE INTEGRATION

Patient and consult apps, doctor and pharmacist apps, diagnostics and home-collection field apps, e-pharmacy checkout — Android and iOS from one Kotlin Multiplatform SDK. Layers engaged for this vertical: **1–3 and 5–9**, with Layers 8–9 producing the retained record an audit of a regulated health service asks for.

EXHIBIT 2 — ONE PLATFORM, NINE LAYERS

Six procurements, one signed pipeline — and only three layers may say no.

Device trust, app logic, network gateways, identity, backend controls and forensic chain-of-custody are conventionally six disjointed purchases correlated after the fact. NonaShield delivers them as a single pipeline in which every signal is bound to the same cryptographic assertion at the moment of capture.

BAND A · LAYERS 1–3

Deterministic device & payload truth

1 Mobile SDK — runtime signal capture, RASP, on-device enforcement

2 API Gateway & Network — edge enforcement, signed-payload validation

3 Trust Verification — server-side hardware key attestation

WHAT IT ESTABLISHES

Binary authority. These layers may allow or block outright because their error rate justifies it.

BAND B · LAYERS 4–6

Probabilistic risk enrichment

4 Fraud Intelligence — risk modelling and scoring across entities

5 Graph Intelligence — entity linkage, mule and coordinated-network detection

6 Behavioural Intelligence — continuous interaction and intent analysis

WHAT IT ESTABLISHES

Graded risk only. These layers modulate friction; they never make a binary access decision alone.

BAND C · LAYERS 7–9

Verdict & accountability

7 Decision Engine — real-time rule and model enforcement: allow / step-up / block

8 Evidence Engine — hash-chained, tamper-evident immutable record

9 Compliance — regulatory controls, WORM retention, regulator-mapped export

WHAT IT ESTABLISHES

One graded, signed verdict — and non-repudiable accountability as a by-product of the transaction path.

DETECT ——▶ ENFORCE ——▶ DECIDE ——▶ HARDENED RULES PUSHED BACK TO THE SDK

THE SEPARATION MATTERS MORE THAN THE COUNT

Most platforms fail not because they lack signals but because they let weak signals make strong decisions. Segregating binary authority (Bands A and C) from probabilistic enrichment (Band B) keeps false positives out of the journey that earns — a blocked genuine consult is a patient who does not get care — while still allowing behavioural evidence to add friction the instant a session deviates from its own baseline.

EXHIBIT 3 — POINT SOLUTIONS VERSUS ONE UNIFIED PLATFORM

The stack you would otherwise assemble has four seams.

	FOUR TO FIVE POINT SOLUTIONS	NONASHIELD (UNIFIED)
Vendors to contract & manage	4–5 separate vendors	**1**
Integrations to build & maintain	One per vendor, each with its own SDK and API	**Single SDK + gateway + backend**
Signal correlation across layers	Manual or none — each tool sees only its own slice	**Fused into one explainable risk score**
Threat vectors covered	Varies per tool; gaps at the seams	**400+, continuously correlated**
Compliance & audit evidence	Assembled after the fact from disparate logs	**Native hash-chained evidence, regulator-mapped**
Time to deploy	Sequential vendor onboarding	**A single integration cycle**

DEPLOYMENT

01 Threat-surface review — map your current stack, seams and highest-loss journeys. Two weeks.

02 Pilot — one app, one journey, production traffic, measured against your existing controls.

03 Production rollout — full journey coverage, policy tuning, evidence chain live for audit.

04 Continuous hardening — detect, enforce, decide — with hardened rules pushed back to the SDK.

COMPLIANCE & ASSURANCE

Digital Personal Data Protection Act and DPDP Rules, 2025 — health data handled on device

ABDM Health Data Management Policy and linked health-record handling

Telemedicine Practice Guidelines, 2020 — identity and record obligations at consult

Drugs and Cosmetics Rules — Schedule H, H1 and X prescription controls

CERT-In Directions 2022; ISO 27001 and NABH-aligned information security

Five-year WORM retention under compliance lock; regulator-mapped export

WHY DIMEAI

25 years of banking-technology and e-governance security experience behind the architecture

Patent published in India, grant awaited — tamper-evident evidence chain

Explainable ML risk scoring — decisions you can defend to a regulator

Android & iOS from one Kotlin Multiplatform SDK

Cloud, on-premises or hybrid — matched to your infrastructure posture

One commercial relationship, one console, one support line

NONASHIELD · HEALTHCARE & PHARMA

Stop the fraudster. Before the fraud.

contactus@diimeai.com
+91 85917 55427
DIIMEAI.COM