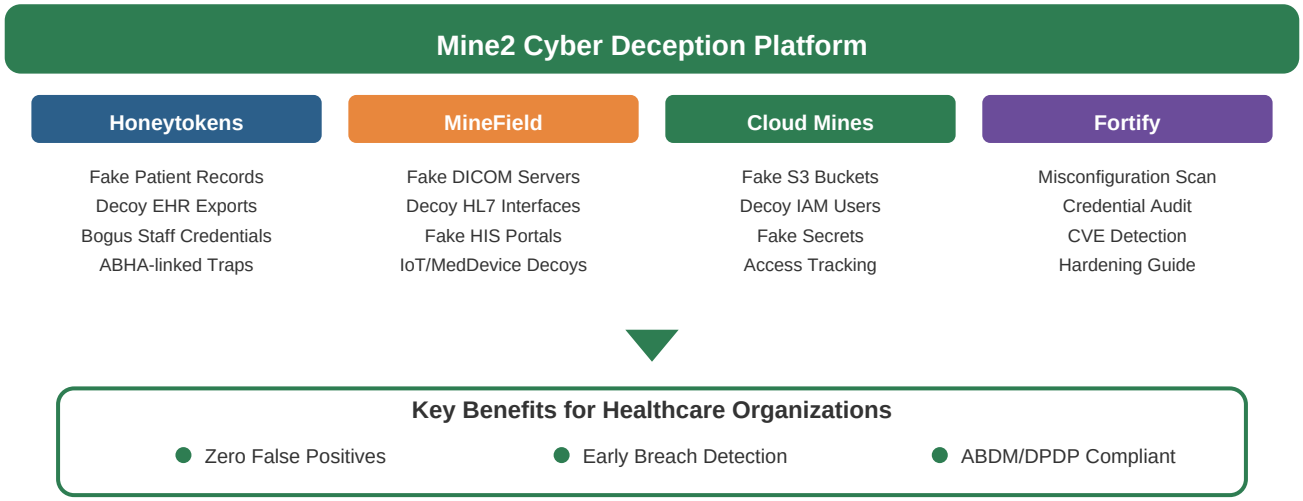
SECURING INDIAN HEALTHCARE

Cyber Deception Strategies for Hospitals and Health Systems

A Mine2 Industry Whitepaper



DPDP Act 2023 Aligned | CERT-In Ready | ABDM Compatible | NABH/NMC Guidelines

www.mine2.io | info@mine2.io

The Threat Is Real, Not Theoretical

Indian healthcare is under siege. The India Cyber Threat Report 2025 ranked healthcare as the most targeted sector in the country, accounting for 21.82% of all cyberattacks -- up 8 percentage points from 2023. This is not a distant risk; it is an active, accelerating crisis.

What Has Already Happened

AIIMS Delhi (Nov 2022): India's premier government hospital was crippled by the ChamelGang APT group using CatB ransomware. 1.3 TB of data encrypted across 5 servers. Hospital reverted to manual operations for 10+ days. Records of an estimated 4 Crore patients were at risk, including those of VIPs and political leaders. Ransom demand: Rs 200 Crore.

Star Health Insurance (Sep 2024): Sensitive data of 3.1 Crore policyholders compromised and offered for sale on a custom website -- medical histories, financial details, and identity documents.

Fortis Healthcare (Oct 2024): One of India's largest private hospital chains suffered a major breach claimed by the Kill Security group. Patient names, dates of birth, addresses, patient IDs, financial statements, and medical records were reportedly exfiltrated.

21.8%	4 Cr+	200+
of all cyberattacks in India target healthcare	patient records at risk in AIIMS attack alone	days average attacker dwell time before detection

Why Healthcare Is Uniquely Vulnerable

Healthcare faces a perfect storm that no other sector experiences in quite the same way:

- **Patient Lives at Stake:** Unlike retail or finance, a ransomware attack on a hospital doesn't just cost money -- it can delay surgeries, disable ventilators, and directly endanger lives. Hospitals are more likely to pay ransom quickly.
- **ABDM Expansion:** With 69 Crore+ ABHA IDs created and 1.5 Lakh+ facilities digitizing records, the attack surface is expanding faster than security can keep pace. Every new digital touchpoint is a potential entry.
- **Medical IoT Everywhere:** Ventilators, infusion pumps, patient monitors, CCTV, biometric systems -- thousands of connected devices with limited security, often running legacy firmware with default credentials.
- **Chronic Underfunding:** Hospital IT budgets are allocated to EHR systems and ABDM compliance, not to threat detection. Most hospitals lack dedicated cybersecurity staff.
- **Data Worth More Than Credit Cards:** A complete patient record (Aadhaar + medical history + insurance details) is worth Rs 5,000+ on the dark web -- 10-50x more than a credit card number -- because it enables long-term identity fraud.

Why Traditional Security Falls Short

Most Indian hospitals rely on firewalls, antivirus, and basic endpoint protection. These tools were designed for a different era and a different threat model. Here's where they fail:

Perimeter-Focused: Firewalls assume attackers are outside. But in healthcare, threats come from phished staff, compromised vendor credentials, infected medical devices on the local network, and even malicious insiders. Once inside, there is nothing to detect lateral movement.

Signature-Dependent: Antivirus and IDS look for known malware signatures. The AIIMS attack used CatB ransomware -- a novel strain that evades signature detection. Zero-day exploits and living-off-the-land techniques render signature-based tools ineffective.

Alert Fatigue: A mid-size hospital's SIEM can generate thousands of alerts daily. With limited staff (often 1-2 IT personnel), genuine threats are buried in noise. Critical alerts are missed, not because the tool failed, but because no one had time to investigate.

Too Late: By the time traditional tools detect a breach, attackers have already mapped the network, exfiltrated data, or deployed ransomware. Average dwell time exceeds 200 days globally. In healthcare, even 2 hours can mean compromised patient records or disabled critical systems.

What Is Cyber Deception?

Cyber deception is a fundamentally different approach to threat detection. Instead of trying to identify attackers by their behavior (which produces false positives) or their tools (which misses novel attacks), deception places realistic-looking fake assets throughout your environment.

These decoys -- fake credentials, fake databases, fake servers -- have no legitimate business purpose. No real user or system should ever access them. When someone does, it is a confirmed threat, not a guess.

> *The fundamental insight: legitimate users know what is real. Only attackers, who are navigating your environment blind, will interact with decoys. This is why deception achieves near-zero false positives -- something no other detection technology can claim.*

Mine2 Cyber Deception Platform

Honeytokens

Digital tripwires planted across your environment: fake AWS/DB credentials, SSH/RDP keys, VPN configs, decoy documents (Patient_Aadhaar_Export.xlsx, EHR_Backup.sql), and fake Active Directory users. Any access triggers an immediate, high-confidence alert.

MineField

Transforms any system into a decoy by running realistic fake TCP services -- MySQL, MongoDB, FTP, SMTP, web portals, and medical-specific protocols (DICOM, HL7). Any connection is a confirmed threat.

Cloud Mines

Scans your AWS environment, suggests and deploys fake S3 buckets, IAM roles, and Secrets Manager entries. Tracks all access attempts with full attribution.

Fortify

Proactive hardening: scans for misconfigurations, insecure/default credentials (critical for medical IoT), CVE vulnerabilities, and provides prioritized remediation guidance.

Healthcare-Specific Use Cases

1. Hospital Information Systems (HIS/EHR)

The Risk: HIS databases contain Aadhaar, ABHA IDs, diagnoses, prescriptions, and billing -- the complete patient identity. AIIMS proved these systems can be held hostage.
Mine2 Approach: DB honeytokens planted near production databases mimic real patient records. Decoy exports (Patient_Aadhaar_Export.xlsx) on shared drives act as early warning tripwires. MineField creates fake backup database servers that catch attackers during reconnaissance.

2. Medical Device & IoT Networks

The Risk: Ventilators, infusion pumps, CCTV cameras, and biometric systems often ship with default credentials and run unpatched firmware. Attackers compromise one device and pivot to the hospital network.
Mine2 Approach: MineField decoys emulate DICOM servers, HL7 interfaces, and DVR/NVR management consoles. Fortify continuously scans for default passwords on medical devices. Any interaction with decoys reveals lateral movement from compromised IoT segments.

3. Pharmacy & Controlled Substance Systems

The Risk: Prescription databases and drug inventory systems are targeted for manipulation -- altering controlled substance records or stealing prescription data for illegal sale.
Mine2 Approach: Honeytokens in pharmacy databases, decoy drug inventory files (Controlled_Substance_Log.xlsx), and fake pharmacy admin accounts detect unauthorized access attempts.

4. Insurance, Billing & TPA Systems

The Risk: Business Email Compromise (BEC) targeting TPA payments, fake insurance claims, and manipulation of billing ERP systems. Star Health proved that insurance-adjacent data is a goldmine.
Mine2 Approach: Honeytokens for billing ERPs, decoy NEFT/RTGS authorization documents, fake finance admin accounts. Cloud Mines protect claims data stored in S3 buckets.

5. ABDM-Connected Infrastructure

The Risk: ABDM integration means hospital systems now exchange data with national registries, other facilities, and third-party apps. Each integration point is a potential attack vector.
Mine2 Approach: Honeytoken API credentials for ABDM integrations, fake ABHA-linked test records, Cloud Mines monitoring S3 buckets containing health record exports.

6. Ransomware Early Warning

The Risk: Ransomware groups spend days to weeks in reconnaissance before deploying encryption. In healthcare, even hours of downtime can endanger lives.
Mine2 Approach: Strategic honeytokens in backup directories catch attackers attempting to destroy backups before encryption (a hallmark of sophisticated ransomware). MineField detects network scanning and lateral movement during the crucial reconnaissance phase -- before damage occurs.

Regulatory Compliance

Indian healthcare operates under a complex regulatory landscape. Mine2 directly supports compliance with every major framework:

DPDP Act 2023 (Digital Personal Data Protection)

Patient health data is classified as sensitive personal data. Section 8 requires Data Fiduciaries (hospitals) to implement 'reasonable security safeguards.' Section 12 grants patients rights to access, correction, and erasure. Breaches affecting personal data require mandatory notification.
How Mine2 Helps: Forensic telemetry provides timestamped evidence of breach detection. Comprehensive audit trails demonstrate proactive security measures to regulators. Near-zero false positives ensure genuine threats are not lost in noise.

CERT-In Incident Reporting (6-Hour Mandate)

CERT-In mandates that cybersecurity incidents be reported within 6 hours of detection. For hospitals without 24/7 SOC coverage, meeting this timeline is nearly impossible with traditional tools that generate ambiguous alerts requiring manual investigation.
How Mine2 Helps: Immediate alerts with complete forensic context -- source IP, user identity, accessed asset, timestamp -- enable classification and reporting without lengthy investigation. SMS/email alerts ensure the right people are notified even outside business hours.

ABDM/NHA Data Security Requirements

The Health Data Management Policy under ABDM mandates that health data shall not be shared without patient consent. The federated architecture requires each facility to secure its own data. With 1.5 Lakh+ ABDM-enabled facilities, the responsibility is distributed -- and so is the risk.
How Mine2 Helps: Honeytokens detect unauthorized access to ABHA-linked records and health data repositories. Cloud Mines protect cloud-hosted health records. Fortify identifies misconfigurations in ABDM-integrated systems before attackers exploit them.

NABH & NMC Accreditation

NABH accreditation expects demonstrable IT security controls for patient data protection. NMC guidelines mandate safeguarding medical records and clinical data. Both require evidence of active security measures, not just policies on paper.
How Mine2 Helps: Mine2 provides demonstrable, working security mechanisms with low technical overhead -- ideal for hospitals that need to show active controls without building a dedicated SOC.

How Mine2 Would Have Changed the Outcome

These scenarios are modeled on real Indian healthcare incidents. We show how deception technology would have altered the timeline:

Scenario 1: The AIIMS-Style Ransomware Attack

Without Mine2: Attacker phishes a hospital administrator. Gains workstation access. Spends 5-7 days mapping Active Directory, locating backup servers, and identifying critical databases. Deploys ransomware on Day 8. Hospital discovers breach when systems go down. 10+ days of manual operations.

With Mine2: Same initial phishing succeeds. But during AD enumeration on Day 1, the attacker discovers 'IT_Admin_Credentials.txt' on a shared drive -- a Mine2 honeytoken. Alert fires immediately with source IP, username, file accessed, and timestamp. Security team isolates the workstation within 2 hours. Ransomware never deployed. Patient services uninterrupted.

Scenario 2: Compromised Medical Device Pivot

Without Mine2: Attacker exploits a vulnerable CCTV camera in the ICU ward (default credentials). Pivots from the IoT network segment to the hospital LAN. Reaches the patient database. Exfiltrates records of 50,000+ patients over several weeks. Breach discovered 4 months later during audit.

With Mine2: Same camera compromise. But while scanning the hospital network, the attacker connects to a MineField fake MySQL server that looks like the patient database. Mine2 alerts fire within seconds. IoT segment is isolated immediately. Zero patient records exfiltrated.

Scenario 3: Insider Threat in Billing

Without Mine2: A billing department employee accesses restricted patient insurance records for personal gain. Copies data to a USB drive over 3 months. Discovery comes only when a patient reports suspicious activity on their insurance account.

With Mine2: The insider opens a decoy claims database (Claims_Master_2024.sql) placed by Mine2 alongside real databases. The access triggers an alert with user identity, timestamp, and query details. HR and compliance are notified the same day. Clear evidence for investigation and action.

Getting Started

1. Assess Map your critical assets: HIS/EHR databases, backup locations, AD structure, medical device inventory, cloud resources, and third-party integration points.

2. Plan Strategic placement of deception assets along likely attack paths -- not random scattering, but informed by how attackers actually move through hospital networks.

3. Deploy Days, not months. Zero impact on production systems, patient care, or clinical workflows. No agents to install on medical devices.

4. Integrate Connect Mine2 alerts to your existing SIEM, email, or SMS notification systems. Train your IT team on response procedures.

5. Evolve As your environment changes -- new ABDM integrations, cloud migrations, new departments -- Mine2 coverage evolves with you.

Business Value Beyond Security

For healthcare leadership evaluating cybersecurity investments, Mine2 delivers measurable value across multiple dimensions:

Breach Cost Avoidance

The average healthcare breach globally costs Rs 13+ Crore in remediation, legal fees, regulatory fines, and patient notification. AIIMS-scale incidents cost multiples of that. Early detection can reduce breach costs by 50-70%.

Patient Safety Continuity

Preventing ransomware means critical care systems -- ventilators, monitors, drug dispensing -- remain operational. This isn't just a financial metric; it is a patient safety imperative.

Regulatory Penalty Avoidance

DPDP Act penalties can reach Rs 250 Crore. CERT-In reporting failures carry separate consequences. Mine2's forensic trails and rapid detection significantly reduce regulatory risk.

SOC Cost Optimization

Near-zero false positives mean your limited IT staff spends time on confirmed threats, not chasing noise. Hospitals without dedicated SOCs can achieve enterprise-grade detection.

Cyber Insurance Posture

Active deception-based detection can strengthen your cyber insurance application, potentially reducing premiums and improving coverage terms.

Minimal Operational Overhead

No agents on medical devices. No production traffic inspection. No performance impact on clinical systems. No additional software dependencies. Deployed in days, not months.

> **Why Mine2 for Healthcare:**
>
> - Near-zero false positives: every alert is a confirmed threat
> - Catches attackers during reconnaissance, before damage
> - Works alongside existing firewalls, AV, and SIEM -- not a replacement
> - Non-bypassable: unlike EDR, deception assets cannot be identified
> - Detects both external attackers AND malicious insiders

Conclusion

Indian healthcare faces a stark reality: the sector is the country's #1 target for cyberattacks, yet most hospitals operate with minimal cybersecurity beyond basic perimeter defense.

> *The question is not whether your hospital will face an attack -- AIIMS, Star Health, and Fortis have already answered that. The question is whether you will detect it before patient data is compromised, before ransomware is deployed, before lives are at risk. Mine2 ensures you will.*

Contact Mine2 Today

www.mine2.io | info@mine2.io