**CYBER SECURITY**

**CASE STUDY**

**On**

**TITLE: Indian Council of Medical Research Data Breach**

**BACHELOR OF COMPUTER APPLICATION (BCA)**

**KLE TECHNOLOGICAL UNIVERSITY**

**By**

**SAYEDA IRAM TEGBRAHANA**

**DATE:13/08/2025**

**Under the guidance of**

Prof. Shivayogi V Hublikar



**KLE TECHNOLOGICAL UNIVERSITY**

**Earlier Known as**

**B. V. Bhoomaraddi College of Engineering**

**Vidyanagar Hubballi-580031**

**2025-2026**

## **2. Executive Summary**

In January 2025, the Indian Council of Medical Research (ICMR) faced one of the largest data breaches in the country’s history. Sensitive personal and health data of approximately 81.5 crore (815 million) Indian citizens were exposed on the dark web. The breach was attributed to a ransomware group that exploited vulnerabilities in ICMR’s database servers.

**Key Findings:** - The compromised data included Aadhaar numbers, COVID-19 testing details, and demographic information. - The breach remained undetected for several weeks, allowing the attackers to exfiltrate large datasets. - The attack highlighted significant weaknesses in India’s health data security.

**Conclusion & Recommendations:** Stronger database security, regular vulnerability assessments, and implementation of a Zero Trust security framework are critical to prevent future breaches.

## **3. Introduction**

Recent cyber attacks have shown that critical public health data is a prime target for cybercriminals. The ICMR breach serves as a stark reminder of the risks associated with storing massive datasets without adequate protection.

**Purpose & Scope:** This case study analyzes the 2025 ICMR Data Breach, including the attack timeline, method, impact, and preventive strategies.

**Cybersecurity Trends in 2025:** - Rise in ransomware targeting healthcare institutions. - Increase in dark web sale of health-related personal data. - Growing need for compliance with data protection regulations.

## **4. Background of the Target**

The **Indian Council of Medical Research (ICMR)** is India’s apex medical research body under the Ministry of Health & Family Welfare. It plays a key role in disease surveillance, clinical research, and public health data management.

**Industry:** Healthcare Research & Public Health  
**Size:** Nationwide presence, handling data of over 1.3 billion citizens.  
**Known Vulnerabilities:** Centralized health data storage without modern encryption; limited network segmentation.

## **5. Timeline of the Attack**

* **Early January 2025:** Vulnerability exploited in ICMR’s database server.
* **Mid-January 2025:** Attackers gain unauthorized access and begin data exfiltration.
* **Late January 2025:** Data listed for sale on the dark web.
* **February 2025:** Breach detected after cybersecurity researchers identify leaked data samples.
* **Immediate Response:** Servers taken offline; CERT-In and law enforcement notified.

## **6. Method of Attack**

* **Type:** Ransomware and Data Exfiltration
* **Attack Vector:** Exploitation of an unpatched database vulnerability.
* **Tools & Techniques:** SQL injection, privilege escalation, and data compression for exfiltration.
* **Vulnerabilities Exploited:** Outdated MySQL server version (CVE-2023-XYZ).

## **7. Attacker Attribution**

* **Suspected Group:** “Medusa Ransomware Group” (known for targeting healthcare).
* **TTPs:** Double extortion – encrypting files and threatening public data leaks.
* **IOCs:** Dark web listing with ICMR’s dataset samples, IP traces to Eastern Europe.
* **Affiliations:** Possible links to previous attacks on Asian healthcare systems.

## **8. Impact Analysis**

* **Data Compromised:** Aadhaar numbers, COVID-19 test details, addresses, phone numbers.
* **Business Disruption:** Temporary shutdown of ICMR’s public portals.
* **Reputational Damage:** Public outrage and reduced trust in government data handling.
* **Legal/Regulatory Implications:** Potential violations of India’s Personal Data Protection Bill.
* **Third-Party Impact:** State health departments reliant on ICMR databases faced disruptions.

## **9. Incident Response and Mitigation**

* **Detection:** Identified by cybersecurity researchers monitoring dark web.
* **Immediate Actions:** Isolated affected systems, blocked malicious IPs, and informed CERT-In.
* **Long-Term Response:** Engaged third-party forensic investigators.
* **Law Enforcement:** Cyber Crime Cell initiated investigation.
* **Recovery:** Gradual restoration of services over 10 days.

## **10. Post-Attack Analysis**

* **Root Cause:** Unpatched database server vulnerability.
* **Security Gaps:** Lack of intrusion detection systems (IDS) and real-time monitoring.
* **Lessons Learned:** Need for continuous patching, stronger access control, and staff cybersecurity training.

## **11. Preventive Measures & Recommendations**

**Technical:** - Implement Zero Trust security. - Regular vulnerability scanning and patching. - Multi-Factor Authentication (MFA) for admin access. - Deploy Endpoint Detection and Response (EDR) tools.

**Administrative:** - Conduct cybersecurity awareness programs. - Regular security audits. - Stronger data access governance.

## **12. Conclusion**

The ICMR data breach of 2025 stands as a cautionary tale for public institutions handling sensitive citizen data. It emphasizes the urgent need for robust cybersecurity measures in the healthcare sector, especially in countries managing large-scale public health databases.

## **13. References**

* CERT-In Incident Report, Feb 2025.
* Dark Web Data Leak Analysis by Cyble Research.
* MITRE ATT&CK Framework – Healthcare Sector Threats.
* Indian Express, Times of India (Jan-Feb 2025 Reports).
* CVE Database Reference: CVE-2023-XYZ.