WEEK 1

ARGO MODULE 1 | DATA SECURITY, PRIVACY, AND ETHICS IN LMIC HEALTH SYSTEMS

Security Realities in Low-Resource Health Systems

Threat modeling for the infrastructure we actually have, not the one we wish existed.

Topic 1
The threat landscape for LMIC health data

Topic 2
Access control on shared devices

Topic 3
Infrastructure vulnerabilities

Lecture notes | Distributed as PDF for portability | Live session: threat modeling a district health system

FRAMING

Why this week matters

- Health data is among the most sensitive information a state holds, and LMIC health systems are digitizing faster than the governance around them.
- Most cybersecurity curricula assume enterprise IT: managed endpoints, segmented networks, a security operations centre. That is not the operating reality.
- This week builds security thinking inside real constraints: shared phones, intermittent power, thin IT staffing, donor-fragmented systems.
- Everything is grounded in documented incidents, because the failure modes are not hypothetical.

279M

records affected in the 2021 breach of Indonesia's BPJS Kesehatan national health insurance database

OBJECTIVES

What Week 1 asks of participants

- **1.** Describe the threat categories that actually recur in LMIC health settings, using documented incidents as evidence.
- **2.** Evaluate access control options where devices are shared, connectivity is intermittent, and users may have low literacy.
- **3.** Trace where data sits at rest, in transit, and exposed across a district health information system.
- **4.** Produce a threat model using the modified STRIDE framework, with mitigations filtered for cost and staffing feasibility.

Keep in view: The Week 1 deliverable (Security Risk Assessment Report, 40% of the module grade) is graded on realism and implementability as heavily as technical accuracy.

THE OPERATING ENVIRONMENT

Two different worlds

What standard curricula assume

- Managed, single-user endpoints
- Segmented networks and monitored perimeters
- Dedicated security staff and a helpdesk
- Stable power and connectivity
- Procurement control over software

What facilities actually run

- Shared Android phones across multiple health workers
- Locally hosted servers on intermittent power, no automated backups
- Mobile hotspots and public Wi-Fi for transmission
- One overloaded IT focal person, or none
- Unvetted third-party apps integrated into the HIS

Bottom line: Controls designed for the left column fail quietly in the right column. The week designs for the right column.

DOCUMENTED INCIDENT

Indonesia: BPJS Kesehatan breach (2021)

1

- The national health insurance database was breached; data on roughly 279 million people was offered for sale on a criminal forum.
- Records linked identity data to enrollment and clinical information, raising fraud, extortion, and discrimination risk at population scale.
- A single national system meant a single failure exposed nearly the whole population, including people with no realistic way to opt out.

Lesson: Centralized national databases concentrate risk. Scale of aggregation is itself a security decision, not just an efficiency one.

DOCUMENTED INCIDENT

South Africa: NHLS data exposure (2020)

2

- Data held by the National Health Laboratory Service, the diagnostic backbone for the public health system, was exposed.
- A national laboratory network is a single point of failure: when it is compromised or unavailable, diagnostics degrade everywhere at once.
- Downstream harm lands on clinical care and on public trust, not on an IT dashboard.

Lesson: Availability is a patient-safety property. Security failures in health systems are measured in delayed results and missed diagnoses.

DOCUMENTED INCIDENT

DHIS2 national deployments: transmission and configuration

3

- DHIS2 is the aggregation platform for dozens of national health systems, which makes deployment quality a population-level issue.
- Documented findings across several national deployments include unencrypted data transmission and weak instance configuration.
- The platform is not the problem. A securable platform, deployed without encryption, hardening, or patching, is an insecure system.

Lesson: Configuration is a governance act. Ask who owns deployment security, not just which platform was chosen.

SYNTHESIS

What the three incidents share

- None required an exotic adversary. The failure modes were known, cheap to exploit, and visible in advance.
- Each had a governance gap underneath the technical gap: unclear ownership of security decisions.
- Harm concentrated on people with the least power to protect themselves and the least ability to exit the system.
- Policy documents existed in every case. Paper controls did not translate into operational ones.

Carry forward: The recurring threat categories in LMIC health settings: insider access and sharing (usually non-malicious), device theft and power events, interception on unsecured networks, and supply-chain exposure from unvetted applications.

FRAMEWORK

Modified STRIDE for LMIC health systems

Category	Classic meaning	How it shows up in an LMIC facility
S – Spoofing	Pretending to be another user or system	Shared logins make every action deniable; anyone can be anyone
T – Tampering	Altering data or systems	Edited registers, falsified aggregates, quiet fixes to bad numbers
R – Repudiation	Denying an action occurred	No audit trail on a shared phone; accountability evaporates
I – Information disclosure	Data exposed to the wrong eyes	WhatsApp forwards, unencrypted sync, records on personal devices
D – Denial of service	Availability lost	Power cuts and connectivity loss count here, alongside ransomware
E – Elevation of privilege	Gaining rights one should not have	One admin password for the whole district

Note: The modification: availability threats include infrastructure failure, not only attackers; likelihood and impact are rated with local knowledge; mitigations are filtered by cost and staffing feasibility before they are proposed.

DEEP DIVE

Access control when the control is a shared phone

- **Role-based access:** DHIS2 and OpenMRS support granular roles; the constraint is maintaining them with no dedicated administrator.
- **Shared devices:** Individual credentials collapse when three health workers rotate one Android phone. Design for it: fast user switching, PIN discipline, session timeouts.
- **Low-literacy users:** Biometric authentication reduces password failure modes but introduces consent and data-sensitivity questions of its own.
- **Offline-first models:** Health posts with intermittent connectivity need local caching, which relocates the security boundary onto the device.

Implementation evidence

The asynchronous content draws on the Rwanda national HMIS rollout, the Living Goods community health worker platform in Uganda and Kenya, and the OpenSRP deployment in Pakistan. Participants evaluate real facility-level access configurations and identify where they fail.

DEEP DIVE

Infrastructure: where the data actually sits

- **At rest:** Facility servers without climate control or redundant power; health data on personal devices; no automated backup protocol.
- **In transit:** Mobile hotspots and public Wi-Fi as the default transmission path; sync jobs that fail silently and retry over whatever network is available.
- **At the edges:** Paper-to-digital transcription points, USB transfers, and printout circulation are part of the data flow even when the diagram omits them.
- Exercise: trace a representative district HIS architecture and mark where data is exposed at each stage.

The point: A data flow diagram that only shows the digital path is fiction. The assessment requires the real path.

BRIDGE TO WEEK 2

Threats have legal names

STRIDE category	Nigeria Cybercrimes Act 2015 (as amended 2024)
Spoofing	Section 22 identity theft and impersonation; Section 13 computer-related forgery
Tampering	Sections 8 and 16: system interference and unauthorized modification
Repudiation	Section 17: electronic signatures are binding; disputing one shifts the burden of proof
Information disclosure	Section 12 unlawful interception; Section 29 breach of confidence; Sections 38 and 39 define lawful access
Denial of service	Section 8: serious hindering of a computer system's functioning
Elevation of privilege	Section 6 unauthorized access; Section 28 password trafficking and intrusion tools

Note: Nigeria is the worked example; Week 2 pairs every jurisdiction's data protection law with its cybercrime law. Under the 2024 CNII Order, health is designated critical national information infrastructure, with elevated penalties for attacks.

LIVE SESSION (90 MINUTES)

Threat modeling a West African district health system

- **The case:** A DHIS2 instance on a locally hosted server, community health workers on a mix of personal and program-issued Android devices, and a referral pathway that runs on WhatsApp.
- **The task:** In small groups, build a threat inventory with the modified STRIDE framework, rate likelihood and impact with local knowledge, and propose mitigations that survive the staffing and budget constraints in the case.
- **The closing step:** Map the top-rated threats to the offenses and statutory duties they would engage under national law, previewing Week 2.

The point: Groups are graded on nothing here. The session exists so the assessment method has been practiced once before it counts.

ASSESSMENT

Security Risk Assessment Report (40% of module grade)

- **Scope:** Select a real or realistic LMIC health information system. 2,000 to 2,500 words plus diagrams. Due end of Week 2.
- **Required sections:** System description with data flow diagram; threat identification using the adapted STRIDE framework; vulnerability analysis across infrastructure, human capacity, and governance; risk rating matrix; prioritized mitigations with feasibility analysis.
- **Grading:** Realism and implementability weigh as heavily as technical accuracy. A sophisticated plan the facility cannot run scores below a modest plan it can.

Standard: Strong reports read like something a district health management team could act on Monday morning.

THIS WEEK

Before the live session

- Work through the three asynchronous topics and the three documented incidents.
- Complete the facility access-configuration evaluation exercise.
- Post to forum thread 1.1: one threat in your context that outsiders underestimate, classified with STRIDE.
- Engage threads 1.2 and 1.3: which documented failure mode is most plausible for you, and one low-cost control that actually worked.

The stance for Week 1

No catastrophizing, and no false comfort. The systems described here deliver care every day under conditions most security literature ignores. The job is to make them safer without making them stop working.