WEEK 2

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

Privacy, Regulation, and Consent in Practice

Two legal layers, one operational reality, and the gap between them.

Topic 1
The regulatory landscape, plus the criminal law layer

Topic 2
Consent where consent is complicated

Topic 3
When regulation meets WhatsApp

Lecture notes | Live session: The WhatsApp Problem

FRAMING

Why this week matters

- The laws are real: Nigeria's NDPA, Kenya's Data Protection Act, India's DPDP Act, South Africa's POPIA, and their cybercrime counterparts.
- Enforcement in the health sector is uneven, and the gap between law and practice is the actual terrain practitioners work in.
- The goal is to read statutes as practitioners: what is required, where it falls short, what implementation has stalled.
- New this week: the criminal law layer, taught through Nigeria's Cybercrimes Act 2015 as amended in 2024.

Working assumption

Compliance theater helps no one. This week treats each legal instrument as a tool with a shape: some problems it fits, some it does not, and some it creates.

CORE CONCEPT

A health facility answers to two legal layers at once

Data protection law

- Governs how personal data must be handled
- Administered by a regulator (NDPC, ODPC, Data Protection Board)
- Remedies are mostly administrative: orders, fines, enforcement notices
- Examples: Nigeria NDPA 2023, Kenya DPA 2019, India DPDP 2023, POPIA

Cybercrime law

- Criminalizes attacks on and misuse of computer systems and data
- Enforced by police, prosecutors, and courts
- Remedies include imprisonment, criminal fines, forfeiture
- Examples: Nigeria Cybercrimes Act 2015 (amended 2024), Kenya Computer Misuse and Cybercrimes Act 2018

Bottom line: One incident can trigger both layers, on separate clocks, owned by different people in the facility.

NIGERIA, LAYER ONE

From NDPR (2019) to NDPA (2023)

- The NDPA created the Nigeria Data Protection Commission and put the framework on a statutory footing.
- Health data is sensitive personal data, with correspondingly narrower lawful bases for processing.
- Breach notification to the NDPC within 72 hours of becoming aware, and to affected data subjects where risk is high.
- Data protection officers are expected for controllers of major importance; enforcement practice is young but growing.

The point: The NDPA governs the handling of health data. It says nothing about who goes to prison for stealing it. That is the other layer.

NIGERIA, LAYER TWO

The Cybercrimes Act 2015, amended 2024

- A criminal statute with three jobs: define offenses, impose duties on system operators and service providers, and protect designated critical infrastructure.

- **Definition 1:** A computer system includes mobile phones (Section 58). The ward's shared Android and the WhatsApp group are inside the statute.
- **Definition 2:** Damage under the Act expressly includes harm to the medical examination, diagnosis, treatment, or care of any person (Section 58).
- Few cybercrime statutes name medical harm in their definitions. This one does, which makes it unusually teachable for health audiences.

s.58

the definitions section that pulls phones, and patient care itself, into the scope of the Act

Offenses that matter in health settings

Provision	What it prohibits (paraphrased)	Health-sector relevance
Section 6	Unauthorized access to computer systems	Record snooping; stolen or shared credentials
Sections 8, 16	System interference; unauthorized modification	Ransomware, sabotage, falsified records
Sections 13, 14	Computer-related forgery and fraud	Altered results; payroll and claims fraud through the HIS
Section 22	Identity theft and impersonation	Medical identity fraud; impersonating clinicians
Sections 28, 31	Password trafficking and disclosure; duty to surrender access codes on exit	Credential-sharing culture; offboarding controls; written authorization before security testing
Section 32	Phishing, spamming, malware distribution	The most common initial access vector in health incidents

Note: Conduct facilities treat as a workflow or disciplinary matter can carry personal criminal liability for the individuals involved.

Duties with statutory clocks

- **Section 21, reporting:** Operators of systems and networks must report attacks and intrusions. The 2024 amendment routes reports through sectoral CERTs or security operations centres to the National CERT within 72 hours, replacing the seven-day window.
- **Section 38, retention:** Service providers retain traffic data and subscriber information for two years and release it to law enforcement on request, subject to a constitutional privacy proviso.
- **Section 39, interception:** A judge may authorize interception of content and traffic data for criminal investigations.

Read carefully: Sections 38 and 39 are threat-model inputs, not compliance footnotes. They are a designed-in lawful access channel to the metadata of clinical communications, even where content is end-to-end encrypted.

NIGERIA, LAYER TWO

Critical National Information Infrastructure

- Sections 3 to 5 let the President designate systems as CNII on the National Security Adviser's recommendation.
- The Designation and Protection of CNII Order, signed June 2024, lists 13 sectors. Health is one of them.
- Consequences: offenses against covered systems carry up to 10 years, 15 where grievous bodily harm results, and life imprisonment where death results.
- Covered systems also fall within the audit and inspection remit of the Office of the National Security Adviser.

Discussion: Which systems in your own national health architecture would meet a critical-infrastructure test, and who would know if they were designated?

CASE WITHIN A CASE

The 2024 amendment as a lesson in law-making

- **Section 24, narrowed:** The cyberstalking provision, long used against journalists and critics, was rewritten after the ECOWAS Court of Justice found the original wording incompatible with free-expression guarantees and ordered change.
- **Reporting, tightened:** The incident-reporting window moved from seven days to 72 hours, with sectoral routing.
- **The levy, suspended:** A restated 0.5 percent cybersecurity levy on scheduled businesses was implemented by Central Bank circular in May 2024 and withdrawn within two weeks after public backlash.

The point: Enactment is not implementation. The same gap the module names in data protection law runs through cybercrime law.

PRACTICE

One breach, two clocks: dual-track reporting in Nigeria

Dimension	NDPA 2023	Cybercrimes Act 2015 (as amended 2024)
Trigger	Personal data breach likely to cause harm to data subjects	Any attack, intrusion, or disruption affecting a system or network
Recipient	Nigeria Data Protection Commission; affected data subjects where risk is high	National CERT, routed through the sectoral CERT or security operations centre
Timeline	72 hours from becoming aware	72 hours from occurrence
Failure consequence	Administrative enforcement and penalties	Statutory fine to the National Cyber Security Fund; denial of internet services
Facility owner	Data Protection Officer	HIS or IT lead, jointly with the DPO

Note: Exercise: draft the first-24-hours playbook that satisfies both columns with the staff a district facility actually has.

COMPARATIVE VIEW

Kenya: Data Protection Act 2019

- The Office of the Data Protection Commissioner registers controllers and processors and has an active enforcement record.
- Health data is sensitive personal data; breach notification to the Commissioner runs on a 72-hour clock where there is real risk of harm.
- Enforcement examples span digital lenders and the 2023 suspension of Worldcoin’s biometric collection.
- Kenya’s criminal layer is the Computer Misuse and Cybercrimes Act 2018: the same dual-layer pattern as Nigeria.

Generalize: Assignment thread 2.1 asks every participant to name the two layers, and the two clocks, in their own jurisdiction.

COMPARATIVE VIEW

India: Digital Personal Data Protection Act 2023

- A consent-centred statute administered by a Data Protection Board, with obligations scaled up for significant data fiduciaries.
- Notable design choice: no separate sensitive-data category. Health data is treated as personal data like any other.
- Implementing rules notified in 2025 operationalize breach reporting, including a detailed report to the Board within 72 hours.
- For health programs, the absence of a heightened tier for health data is the point to argue about, not a footnote.

COMPARATIVE VIEW

The Malabo Convention: a continental baseline

- The African Union Convention on Cyber Security and Personal Data Protection, adopted 2014, entered into force in 2023.
- It spans data protection, cybercrime, and electronic transactions in one instrument, which is exactly the dual-layer structure this week teaches.
- Its weakness is machinery: no strong enforcement or harmonization body stands behind it.
- Its value is as a reference point for national reform and for cross-border data-sharing arguments.

COMPARATIVE VIEW

Snapshot: four frameworks side by side

Jurisdiction	Regulator	Health data status	Breach clock	Cybercrime pairing
Nigeria	NDPC	Sensitive personal data	72 hours to NDPC	Cybercrimes Act 2015 / 2024
Kenya	ODPC	Sensitive personal data	72 hours to Commissioner	Computer Misuse and Cybercrimes Act 2018
India	Data Protection Board	Personal data; no sensitive tier	72 hours to the Board (2025 Rules)	Information Technology Act provisions

Note: The Malabo Convention sits above all three as a continental baseline; implementation depends entirely on member states.

THE LIVE SESSION CASE

The WhatsApp Problem

- A maternal health referral network in East Africa runs on a WhatsApp group: patient names, gestational ages, HIV status, partograph photos, voice notes describing complications.
- A journalist discovers the group and publishes. The exposure is real, and so is the record: the group has measurably sped referrals and reduced maternal mortality in the catchment.
- The session resists easy answers. Both shutting the group and keeping it are defensible positions that must be argued, with costs owned.

Why this case anchors the week

Clinical use of consumer messaging platforms is arguably the single most significant data governance challenge in LMIC health systems today. It gets a full topic and the live session by design.

THE LIVE SESSION CASE

Working the case through both layers

Data protection lens

- Lawful basis and consent for each data element shared
- Minimization: what did the referral actually require?
- Cross-border processing on commercial infrastructure
- Breach duties once the journalist publishes

Cybercrime lens (run as if in Nigeria)

- Phones and the group are computer systems under Section 58
- MNO metadata retained two years under Section 38, despite end-to-end encryption of content
- The 72-hour reporting duty and who owes it
- Individual staff exposure under access and disclosure offenses; then find the Kenyan equivalents

Constraint: Any transition plan is graded against one constraint above all: it must not give back the referral speed.

THIS WEEK

Work for Week 2

- Complete the four asynchronous topics, including the new criminal law layer topic.
- Forum 2.1: name the two legal layers and the two clocks in your jurisdiction.
- Forum 2.2: defend or replace the WhatsApp group, citing at least one statutory provision.
- Forum 2.3: where the policy-implementation gap bites hardest for you.
- Submit the Security Risk Assessment Report by end of week (40% of module grade).

Optional self-check

The regulatory mapping worksheet walks one data-sharing scenario, a ministry sharing de-identified surveillance data with an international research consortium, through all four frameworks. Ungraded, and the best preparation for the final case analysis.