



Uboho Doctor Dashboard — Privacy, Settings, and Ethics Document

1. Introduction

Welcome to the Uboho Doctor Dashboard. This platform is designed to provide medical professionals with real-time access to patient health insights, specifically related to seizure prediction and emergency response. This document outlines ethical guidelines, privacy responsibilities, data-handling practices, and legal compliance requirements expected of users.

2. Dashboard Usage Guidelines

2.1 Access Control and Authorization

Only verified medical professionals authorized by the Uboho management system may access the dashboard. Unauthorized access, sharing credentials, or accessing data outside your assigned patient panel is strictly prohibited.

2.2 Supported Use Cases

The dashboard supports:

- Real-time monitoring of seizure risk
- Review of patient sensor data (accelerometer and gyroscope)
- Communication with patients via end-to-end encrypted chat
- Access to patient location during emergency alerts
- Logging and review of seizure events

You must not use this dashboard for any diagnostic or therapeutic action outside the scope of assigned Uboho protocols.

3. Privacy and Data Protection

3.1 Patient Data Confidentiality

All patient data—including health patterns, location, and communications—must be treated as confidential and must not be downloaded, screen-captured, or shared outside the platform without patient consent.

3.2 End-to-End Encryption

The chat functionality and seizure alerts are encrypted using AES-256 encryption in transit and at rest. Doctors are expected to maintain this privacy by:

- Not sharing sensitive chat data externally
- Not copying messages outside the Uboho context

3.3 Storage and Security

All data is stored securely in Firebase Cloud Firestore under partitioned hospital structures. Doctors must never attempt to access Firestore documents via external clients or tools.

4. Ethical Considerations

4.1 Respect for Autonomy

You must respect patients' rights to decline seizure alert responses, especially when manually dismissed via the mobile app. Do not override patient judgment unless explicitly authorized in a care protocol.

4.2 Emergency Communication

You are ethically responsible to review all seizure alerts immediately and respond via the dashboard. Uboho logs your message response time and may notify admins in case of delay.

4.3 Notification Review

You are expected to monitor and acknowledge all system notifications, including:

- Patient-reported concerns
- High peak activity alerts

- Manual SOS triggers
This is part of your clinical vigilance.

5. Compliance With Regulatory Standards

5.1 FHIR/NON-FHIR Conformity

Uboho aligns partially with FHIR-compliant data structures. While real-time data like motion and chat are not FHIR-formatted, core patient records (ID, seizure events, contact logs) follow consistent field naming and audit structures. You must:

- Treat Uboho data with the same regulatory care as FHIR systems
- Refrain from exporting patient records for 3rd-party use
- Not use Uboho data for research without ethical clearance

5.2 Legal Oversight (HIPAA/Rwanda eHealth)

The dashboard complies with HIPAA-equivalent provisions and Rwanda eHealth national standards. You are individually liable for:

- Data misuse
- Inappropriate access
- Breach of consent or location exposure

6. Incident Reporting and Ethics Escalation

If you observe:

- Unauthorized access to a patient
- Misuse of patient location data
- Delayed response to a seizure
Please report this immediately to the Uboho compliance officer via the secure channel on the dashboard.

7. Closing Statement

By using this dashboard, you agree to uphold these principles in your interaction with patient data. Uboho exists to save lives—your responsibility is to uphold trust, privacy, and professionalism.