# APPENDIX III: INTERVIEW GUIDE

INTERVIEW GUIDE FOR IT PROFESSIONALS, CYBERSECURITY EXPERTS, ADMINISTRATORS FOR A SECURITY FRAMEWORK FOR INFORMATION SHARING-ENABLED INTERNET OF MEDICAL THINGS IN SELECTED HEALTH INSTITUTIONS IN UGANDA

|  |
| --- |
|  |

**INTRODUCTION**

Purpose of the Interview: To gather insights on security functionalities, compliance, IT alignment with business goals, and moderating variables in the context of the Internet of Medical Things (IoMT) in Ugandan health institutions.

Confidentiality Assurance: the interviewee assures that responses will remain confidential.

|  |
| --- |
|  |

What specific security measures are in place for medical devices connected to the IoMT?

How do you manage the authentication and access control for these devices?

What protocols are in place for regular security updates or patches?

What network security protocols are implemented to protect IoMT systems from threats?

How do you monitor network traffic for potential security breaches?

Can you describe your incident response plan for network security incidents?

What practices do you have to ensure the confidentiality and integrity of medical data?

How is sensitive data encrypted both in transit and at rest?

What procedures are followed in the event of a data breach?

Which compliance standards (local and international) are you required to adhere to for IoMT?

How do you collaborate with regulatory bodies to ensure compliance?

What role do training and awareness programs play in maintaining compliance?

What strategies do you employ to assess and manage risks associated with IoMT?

How do you ensure business continuity in case of a security incident?

Can you share an example of a risk that was successfully mitigated?

How does the IT strategy support the overall mission of the health institution?

Can you provide an example of an IT initiative that directly improved patient care?

How do you measure the success of IT projects in relation to business goals?

How do local socio-economic conditions impact your IT security strategies?

What challenges do you face in securing funding for IoMT initiatives?

How does the economic environment influence staff training and awareness?

How does the culture within your institution affect adherence to security protocols?

What methods are used to promote a culture of security among staff?

How do you address resistance to security measures from personnel?

How confident do staff feel in their ability to follow established security protocols?

What resources are provided to help staff improve their security practices?

How do you evaluate the effectiveness of training programs on staff behavior?

What secure data sharing mechanisms do you have in place with external partners?

How do you ensure compliance with data protection regulations during data sharing?

What challenges do you face when sharing sensitive medical data?

How is patient consent obtained for data sharing in your systems?

What measures are in place to ensure patient privacy during data transactions?

How do you handle situations where consent cannot be obtained?

What authentication methods are currently in use for IoMT systems?

How do you regularly assess the effectiveness of your authentication methods?

What steps are taken to enhance user awareness of secure authentication practices?

What frameworks guide your data governance practices within IoMT?

How do you ensure ongoing compliance with data protection laws?

What challenges have you encountered in implementing data governance policies?

How does collaboration among departments support IoMT security decision-making?

Can you provide an example of a successful collaborative project in this area?

What tools or platforms do you use to facilitate collaborative decision-making?

What emerging technologies related to IoMT are currently being explored?

How do you assess the security risks associated with adopting these technologies?

What steps are taken to integrate new technologies into existing security frameworks?

How do ethical considerations shape your approach to IoMT security?

What legal challenges have you faced regarding data security and compliance?

How do you ensure that ethical guidelines are followed in your security practices?

# APPENDIX IV:

# CHECKLIST INFORMATION SHARING-ENABLED INTERNET OF MEDICAL THINGS (IOMT)

|  |
| --- |
|  |

**SECTION A: SECURITY FUNCTIONALITIES**

**Device Security**

Are all medical devices used in the institution secured with unique identifiers?  
☐ Yes ☐ No

Are regular security updates and patches applied to medical devices?  
☐ Yes ☐ No

Is there a process for reporting suspicious device behavior?  
☐ Yes ☐ No

**Network Security**

Is the network used for IoMT devices protected by firewalls and intrusion detection systems?  
☐ Yes ☐ No

Are there protocols for monitoring network traffic for unauthorized access?  
☐ Yes ☐ No

Are there established procedures for responding to network security incidents?  
☐ Yes ☐ No

**Data Security**

Is patient data encrypted during transmission and storage?  
☐ Yes ☐ No

Are access controls in place to limit data access to authorized persons only?  
☐ Yes ☐ No

Is there a process for data backup and recovery in case of breaches?  
☐ Yes ☐ No

**SECTION B: COMPLIANCE**

**Standardization and Collaboration**

Is the institution compliant with local and international data protection regulations?  
☐ Yes ☐ No

Are there collaborative efforts with regulatory bodies for maintaining compliance?  
☐ Yes ☐ No

Are staff trained on compliance standards regularly?  
☐ Yes ☐ No

**Resilience and Risk Management**

Are risk assessments conducted regularly to identify potential vulnerabilities?  
☐ Yes ☐ No

Is there a business continuity plan in place for health services during security incidents?  
☐ Yes ☐ No

Are incident response drills conducted to prepare staff for potential threats?  
☐ Yes ☐ No

**SECTION C: IT ALIGNMENT TO BUSINESS GOALS**

**Business Objectives**

Does the IT strategy support the overall mission of the health institution?  
☐ Yes ☐ No

Are IT initiatives evaluated for their impact on patient care?  
☐ Yes ☐ No

Are patients informed about how IT improvements benefit their healthcare experience?  
☐ Yes ☐ No

**SECTION D: MODERATING VARIABLES**

**Socio-Economic Factors**

Are there considerations for how socio-economic factors may affect access to secure IoMT?  
☐ Yes ☐ No

Is there a process for addressing barriers patients may face due to economic conditions?  
☐ Yes ☐ No

Are resources allocated to support vulnerable populations?  
☐ Yes ☐ No

**Subjective Norms**

Is there a culture of security awareness among staff that extends to patient interactions?  
☐ Yes ☐ No

Are patients encouraged to report security concerns or suspicious activities?  
☐ Yes ☐ No

Do staff regularly communicate the importance of security to patients?  
☐ Yes ☐ No

**Perceived Behavioral Control**

Are patients provided with resources to understand their rights regarding data security?  
☐ Yes ☐ No

Is there support for patients to easily access their medical data securely?  
☐ Yes ☐ No

Are training programs available to help patients understand how to protect their data?  
☐ Yes ☐ No

**SECTION E: INFORMATION SHARING-ENABLED IOMTs**

Data Sharing Mechanisms

Are patients informed about how and with whom their medical data is shared?  
☐ Yes ☐ No

Is there transparency regarding data sharing agreements with third parties?  
☐ Yes ☐ No

Are patients given the option to opt-out of data sharing if desired?  
☐ Yes ☐ No

**Privacy and Consent Management**

Is there a clear process for obtaining informed consent from patients for data sharing?  
☐ Yes ☐ No

Are patients informed about their rights regarding data privacy?  
☐ Yes ☐ No

Are measures in place to ensure that patient data is anonymized when shared for research?  
☐ Yes ☐ No

**Security and Authentication**

Are robust authentication methods employed to protect patient data access?  
☐ Yes ☐ No

Are patients educated on the importance of secure passwords and login practices?  
☐ Yes ☐ No

Is there a two-factor authentication process in place for accessing sensitive information?  
☐ Yes ☐ No

**Data Governance and Compliance**

Is there a governance framework in place to manage patient data security?  
☐ Yes ☐ No

Are there regular audits to ensure compliance with data governance policies?  
☐ Yes ☐ No

Are patients informed about how their data is governed and protected?  
☐ Yes ☐ No

**Collaborative Decision Support**

Are there collaborative tools that involve patients in their healthcare decisions?  
☐ Yes ☐ No

Is patient feedback considered in security policy updates?  
☐ Yes ☐ No

Are there mechanisms for patients to communicate their security concerns effectively?  
☐ Yes ☐ No

**Emerging Technologies**

Are patients informed about new technologies being implemented in their care?  
☐ Yes ☐ No

Is there an assessment process to evaluate the security of emerging technologies?  
☐ Yes ☐ No

Are patients provided with resources to understand the benefits and risks of new technologies?  
☐ Yes ☐ No

**Ethical and Legal Considerations**

Are ethical guidelines followed in the handling of patient data?  
☐ Yes ☐ No

Are patients informed about their legal rights regarding their data?  
☐ Yes ☐ No

Is there a process for addressing ethical concerns raised by patients?  
☐ Yes ☐ No

# **APPENDIX VI:** ENROLMENT CRITERIA (INCLUSION AND EXCLUSION)

This is an Enrolment Criteria (Inclusion and Exclusion) section for this study titled:" Development of a Security Framework for Information Sharing-Enabled Internet of Medical Things in Selected Health Institutions in Uganda"

Enrolment Criteria

1. Inclusion Criteria

Participants must meet all of the following conditions to be eligible:

Healthcare professionals or ICT personnel actively involved in Internet of Medical Things (IoMT) implementation, management, or usage in the selected hospitals.

Institutional administrators or policy/decision-makers responsible for overseeing health ICT systems, medical devices, or patient information sharing.

Aged 18 years and above.

Have at least six (6) months of continuous work experience at either St. Francis Hospital Nsambya or Uganda Martyrs Hospital Lubaga.

Willing and able to provide informed consent to participate in interviews, FGDs, or related research activities.

For Focus Group Discussions: Must be able to comfortably engage in group discussions in English or Luganda.

2. Exclusion Criteria

A person will not be eligible if they meet any of the following:

Are interns, student trainees, or short-term visiting staff not actively involved in IoMT operations or strategic decision-making.

Are patients, caregivers, or members of the general public not employed by the participating institutions.

Have worked at the selected hospital for less than six (6) months.

Are on leave, suspension, or probation at the time of data collection.

Are unwilling or unable to provide informed consent.

Have prior conflicts of interest with the research team or ongoing disciplinary proceedings that could bias participation.

APPENDIX VII: INFORMED CONSENT FORM FOR IN-DEPTH INTERVIEWS  
Study Title: Development of a Security Framework for Information Sharing-Enabled Internet of Medical Things in Selected Health Institutions in Uganda  
Principal Investigator: Arinaitwe Winfred, PhD Candidate, Kampala International University

Introduction

You are invited to participate in a one-on-one in-depth interview as part of a PhD study focused on improving the security of IoMT systems in Ugandan healthcare.

What Participation Involves

This interview will last approximately 45–60 minutes. You will be asked open-ended questions related to your role and expertise in ICT, clinical practice, or medical technology.

Voluntary Participation

Your participation is entirely voluntary. You may stop the interview or decline to answer specific questions at any time.

Confidentiality

Your responses will be kept private. No identifiable information will be disclosed in any publication or report.

Risks and Benefits

There are no anticipated risks. Your insights may contribute to the development of safer and more efficient healthcare systems.

Compensation

You will receive UGX 30,000 to compensate for your time, transport, and inconvenience, as recommended by the Uganda National Council for Science and Technology (UNCST).

Audio Recording Consent (Tick One)

☐ I agree to have the interview audio recorded.  
☐ I do not agree to have the interview audio recorded.

Consent Declaration

I have read and understood the details of this research study. I voluntarily consent to participate.

Name of Participant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Researcher Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

APPENDIX VIII: INFORMED CONSENT FORM FOR KEY INFORMANTS  
Study Title: Development of a Security Framework for Information Sharing-Enabled Internet of Medical Things in Selected Health Institutions in Uganda  
Principal Investigator: Arinaitwe Winfred, PhD Candidate, Kampala International University

Introduction

You are invited to take part in this PhD research study as a key informant. The study aims to explore experiences, risks, and institutional frameworks related to IoMT (Internet of Medical Things) technologies in healthcare institutions in Uganda.

What Participation Involves

You will participate in a one-on-one interview lasting about 45–60 minutes, focusing on your professional experience with IoMT implementation or governance.

Voluntary Participation

Participation is voluntary. You may skip any question or withdraw at any time without penalty.

Confidentiality

Your name and personal identity will not be recorded in any report or publication. All data will be kept confidential and stored securely.

Risks and Benefits

There are no anticipated risks. This study may contribute to improved healthcare data security and better patient outcomes.

Compensation

You will receive UGX 30,000 as modest compensation for your time, effort, and transport, in accordance with Section 5.3 of the National Guidelines for Research Involving Humans as Research Participants.

Audio Recording Consent (Tick One)

☐ I agree to have the interview audio recorded.  
☐ I do not agree to have the interview audio recorded.

Consent Declaration

I have read and understood the information above. I voluntarily consent to participate.

Name of Participant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Researcher Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

APPENDIX IX: INFORMED CONSENT FORM FOR FOCUS GROUP DISCUSSIONS (FGDs)  
Study Title: Development of a Security Framework for Information Sharing-Enabled Internet of Medical Things in Selected Health Institutions in Uganda  
Principal Investigator: Arinaitwe Winfred, PhD Candidate, Kampala International University

Introduction

You are invited to participate in a Focus Group Discussion (FGD) for this doctoral research study. The study seeks to gather insights from healthcare professionals on their experiences using Internet of Medical Things (IoMT) technologies.

What Participation Involves

You will participate in a group discussion with 6–8 people for about 60–90 minutes, guided by a trained facilitator.

Voluntary Participation

Your participation is voluntary. You may decline to answer any question or leave the session at any time.

Confidentiality

All discussions will be treated confidentially. Names will not be recorded or disclosed in any way. Participants will be encouraged to respect each other's privacy.

Risks and Benefits

There are no known risks. Your input will help strengthen policies and practices related to health technology and patient data protection.

Snacks and Refreshments

You will receive snacks and refreshments during the session as a courtesy and in appreciation of your time.

Compensation

You will receive UGX 20,000 for your time, effort, and inconvenience, in line with national research guidelines.

Audio Recording Consent (Tick One)

☐ I agree to have the discussion audio recorded.  
☐ I do not agree to have the discussion audio recorded.

Consent Declaration

I have read and understood the study information. I voluntarily agree to participate in this focus group.

Name of Participant: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Facilitator Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_