

# eHealth Data Security and Privacy: Perspectives from Diverse Stakeholders in Malawi

LISA ORII, University of Washington, USA

CARYL FELDACKER, University of Washington, USA

HANNOCK TWEYA, University of Washington, USA and International Training and Education Center for Health (I-TECH), Malawi

RICHARD ANDERSON, University of Washington, USA

The development and adoption of eHealth in low- and middle-income countries has potential to advance the quality of care in healthcare settings that are challenged by weak infrastructure. Especially in the countries where HIV rates are high, there is need to implement electronic medical record systems to enhance care and improve treatment outcomes. Due to the sensitivity of HIV-related information, eHealth applications in HIV care necessitate the attention and prioritization of data security and privacy. We explored diverse stakeholders' views on data security and privacy in Malawi's public HIV care program to expand the understanding of gaps and opportunities in improving data protections. This work connects data security and privacy goals and practices with previous work on mobile device usage as well as global best practices for security and privacy in healthcare settings. A key finding articulated by stakeholders is the importance of establishing strong data security governance.

CCS Concepts: • **Security and privacy** → **Privacy protections**;

Additional Key Words and Phrases: medical and health support, security and privacy, mobile devices

## ACM Reference Format:

Lisa Orie, Caryl Feldacker, Hannock Tweya, and Richard Anderson. 2024. eHealth Data Security and Privacy: Perspectives from Diverse Stakeholders in Malawi. *Proc. ACM Hum.-Comput. Interact.* 8, CSCW1, Article 46 (April 2024), 26 pages. <https://doi.org/10.1145/3637323>

## 1 INTRODUCTION

The applications of eHealth<sup>1</sup> systems offer great promise to optimize the management of patient health and data, increase collaboration, and improve service delivery and outcomes [47]. In many low- and middle-income countries (LMICs) where human immunodeficiency virus (HIV) prevalence is high, eHealth interventions have potential to support health systems in improving monitoring adherence to antiretroviral therapy (ART), provider decision-making, and management of patient information [15, 20, 76, 83]. However, this potential has yet to be fulfilled due to well-documented

---

<sup>1</sup>We use the term eHealth to refer to digital information systems used in the health system. This includes centralized management of medical record systems, mobile devices for working with data, as well as national health indicator reporting.

---

Authors' addresses: Lisa Orie, [lisaorie@cs.washington.edu](mailto:lisaorie@cs.washington.edu), University of Washington, Paul G. Allen School of Computer Science & Engineering, Seattle, Washington, USA; Caryl Feldacker, [cfeld@uw.edu](mailto:cfeld@uw.edu), University of Washington, International Training and Education Center for Health (I-TECH), Department of Global Health, Seattle, Washington, USA; Hannock Tweya, [tweyah@uw.edu](mailto:tweyah@uw.edu), University of Washington, Department of Global Health, Seattle, Washington, USA and International Training and Education Center for Health (I-TECH), Lilongwe, Malawi; Richard Anderson, [anderson@cs.washington.edu](mailto:anderson@cs.washington.edu), University of Washington, Paul G. Allen School of Computer Science & Engineering, Seattle, Washington, USA.

---

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from [permissions@acm.org](mailto:permissions@acm.org).

© 2024 Copyright held by the owner/author(s). Publication rights licensed to ACM.

ACM 2573-0142/2024/4-ART46  
<https://doi.org/10.1145/3637323>

challenges, including poor infrastructure [69] and weaknesses in management and regulation [7, 28, 42, 69].

Another critical challenge in expanding eHealth applications is ensuring patient data security and privacy<sup>2</sup>. Applications of eHealth, such as electronic medical record (EMR) systems, accumulate an abundance of sensitive and private information that, if jeopardized, could inflict harm to social status and social stability [33]. Especially in the domain of HIV care, the protection of health information requires extreme care and attention, as exposure of data could leave people living with HIV vulnerable and in the face of stigma or discrimination. Moreover, addressing security and privacy in digital development is a core principle that allows for the integration of best practices in technology-enabled programs, such as eHealth [1].

There is an abundance of work in the CSCW literature [23, 39, 49, 60] and beyond [32, 33, 61, 62] that has brought attention to the importance of addressing security and privacy concerns in eHealth applications in high income countries (HICs). However, the examination of eHealth security and privacy in healthcare settings of LMICs remains limited, especially in CSCW.

To address this gap in the literature and with the approval of Malawi's Ministry of Health (MoH), we explored how stakeholders of, and key staff within Malawi's largest public service delivery partner for HIV-related care, Lighthouse Trust (hereafter referred to as Lighthouse), perceive the security and privacy of electronic patient data. By investigating diverse stakeholders' views on data security and privacy, we expand the understanding of gaps and opportunities in addressing patient data protections. The impetus of this investigation is a collaboration between Lighthouse and the MoH that aims to optimize tablet-based data collection, including its data security and privacy processes, in rural and low connectivity settings. This work is concerned with broader security and privacy practices and concerns around electronic patient data at Lighthouse healthcare facilities and the MoH. We explored the following research questions:

- **RQ1:** How do stakeholders of Malawi's public-sector HIV care perceive the security of eHealth systems and implement data protection practices?
- **RQ2:** What changes or considerations in local or national governance of eHealth systems could strengthen security and privacy of patient data?

We conducted interviews with stakeholders who collect or manage routine ART data from EMRs or who inform EMR data policy or practice. Our participants included nurses, data clerks, and IT officers of Lighthouse as well as data decision makers who require or review data as part of their ART-related work.

Our findings highlight stakeholders' commitment to enact data protection practices and to establish clear and enforced management procedures for standardizing best practices for security and privacy. With respect to **RQ1**, stakeholders acknowledged their responsibility to protect patient confidentiality and implement data protection practices at group and individual levels. They expressed their keen understanding of the threats to data protection at various levels of management and stages in the HIV data pipeline and identified room for improvement through technical, behavioral, and structural measures. With respect to **RQ2**, stakeholders hoped to see reforms in device and data management from the facility to national levels. These changes should include the development of agreements that outline expectations for work at the data collection level, centralized data management at the national level to enforce the same standards for all service delivery partners, and consistent updating of data management procedures.

More broadly, we contribute (1) a report on stakeholders' perceptions towards security and privacy of patient data in Malawi's HIV care, (2) an analysis of how stakeholder views and practices

<sup>2</sup>We refer to "security" as the mechanisms used to protect against threats to patient data protections, and "privacy" as the right to control how one's patient data is viewed, shared, and used.

align with global best practices for security and privacy, and (3) an argument that highlights the strengths of Malawi's HIV care program response that prioritizes strong data governance and seeks to consistently improve data protection practices.

## 2 BACKGROUND

In 2021, sub-Saharan Africa had approximately 25.6 million people living with HIV [2]. In this region of Africa, where there is high HIV incidence, countries are increasingly integrating EMR systems into their healthcare settings. These systems have shown promising results for supporting comprehensive HIV care [55] through effectively tracking patient outcomes and medical adherence, delivering laboratory results to clinics in a timely fashion, and tracking drug supplies and expected drug usage [30, 31].

This research was conducted in Lilongwe, the capital city of Malawi, a country in Southern Africa of over 19 million people [3] where the poverty rate is over 50% [19]. Over 900,000 adults in Malawi are living with HIV, which is approximately 8% of the adult population [4]. Despite scarce resources, in 2010, Malawi launched a real-time point-of-care national EMR system, which provides over 700 healthcare facilities with real-time data collection and high-quality monitoring and evaluation (M&E) support [26, 81]. Lighthouse, the largest public provider of ART in Lilongwe, employs Malawi's national EMR system to ensure that ART services comply with global HIV guidelines and to ease routine M&E reporting. Lighthouse provides integrated HIV prevention, testing, treatment, and care clinics in two flagship urban facilities as well as seven satellite clinics in the greater Lilongwe District in partnership with the Malawi MoH. Lighthouse also provides community-based care (CBC) in rural and low connectivity areas as part of client-centered service delivery, with over 120 distribution points where nurses provide care and medications for stable patients. In CBC settings, patient data is collected on paper or tablet-based data collection tools that can operate in areas that do not have reliable connectivity. While paper and tablet-based data collection expands care, the approach is inefficient and error-prone as compared to EMR-based data collection at the facilities. As demand for CBC increases, Lighthouse is testing an innovation to improve the quality of CBC care by extending the EMR to CBC settings through a new offline-first app. The use of mobile health applications for HIV-related data calls for redoubling of efforts to focus on optimizing tablet-based data collection in CBC settings, including enhancing data security and privacy processes in device and data management. Therefore, Lighthouse sought to explore barriers and facilitators to patient data protections in both facilities and CBC settings, leveraging lessons learned to inform overall data security and patient privacy improvements across all implementation settings.

## 3 RELATED WORK

### 3.1 Security and Privacy in Low- and Middle-Income Countries

Scholars posit that there are differences in notions of security and privacy between countries based on income levels [14, 37]. The understanding that privacy notions from the West and high-income countries (HICs) cannot be fully applied, unchanged and uninformed, to address the needs of people in dissimilar settings is evident in the literature that examines security and privacy in computing contexts of LMICs [8, 11, 38, 67, 70, 78]. Such work identifies culture [8, 9, 27, 53, 78], socioeconomic background [67, 70], gender [53], and digital literacy [27] as several of the factors that influence preferences, expectations, and notions of security and privacy. This understanding of privacy as being contextual and culturally specific [54] focuses on local perceptions to inform threats, knowledge gaps, and influences to strengthen local security practices [78].

There is nevertheless a universal desire for safeguarding and protecting privacy [8, 67, 70]. In a threat modeling for deployments of Open Data Kit (ODK), a data collection tool used in LMICs [34], Cobb et al. [25] identify data confidentiality, integrity, and availability, as possible security and privacy goals that are had by stakeholders in ODK deployments. These goals, which are referred to as the 'CIA triad' in computer security literature, are understood and desired throughout both HICs [23, 43, 63] and LMICs [21, 22, 38, 65, 70]. Moreover, the work by Cobb et al. [25] demonstrates that the challenges of implementing computer security in LMICs resemble the well known challenges seen in HICs. For example, both contexts face trade-offs between security and other goals in usability or functionality [12, 29, 40, 59, 69, 82]. Standard best practices are found and recommended in both contexts, ranging from technical safeguards, such as encryption [44] and access control [8, 23, 64, 84], to behavioral practices, such as training and education to raise awareness on threats [22, 62, 63]. In fact, a combination of technical and behavioral measures for protecting privacy is considered to be a strong approach for responding to privacy threats [9, 31, 49, 62, 69, 80].

The approach of combining technical and human protocols to respond to threats is also promoted in healthcare settings across contexts [23, 61, 62], where protecting privacy is essential to technology mediated healthcare work. There is a significant amount of CSCW literature that explores privacy threats, defenses, and practices in healthcare settings in HICs. A large portion of this work focuses on how security and privacy practices are enacted in the collaborative nature of healthcare work [16, 23, 49, 60]. However, security and privacy has not been similarly examined with depth in healthcare settings in LMICs as it has been in HICs, especially from the perspective of people managing healthcare programs in LMICs. This perspective is critical for ensuring that the initiatives aimed at strengthening eHealth systems achieve high standards of patient data protection.

### 3.2 Governance of Health Information Systems

The adoption of health information systems, which are clinical systems that focus on patient documentation such as EMR systems, is considered to alleviate the healthcare supply and demand gap [46]. Initiatives to implement EMR systems are spreading throughout LMICs, where some have improved data management [76], data quality [20], and clinical productivity [41]. However, many EMR system implementations are unsuccessful due to the weak healthcare infrastructure [69]. While the reasons for failure are commonly attributed to the high cost of set up and maintenance [10] and technical pitfalls [30], researchers also argue that the challenges of adoption and implementation of EMR systems in LMICs are rarely related to technology itself, but rather the weaknesses in management [7, 69] and lack of regulations and guidance [28, 42]. In fact, many LMICs have not yet been successful with developing, implementing, and enforcing comprehensive legal frameworks and governance for eHealth [17, 52].

Mutale et al. [50] argue that African countries successfully strengthened their health systems through the development and refinement of health information systems. These countries recognized the importance of aligning health information system efforts with their respective countries' priorities. For example, in Rwanda and Zambia, mobile phone technology facilitated the introduction of EMR systems in under-resourced environments. In Rwanda, a collaboration between the MoH and an international public health organization led the national implementation of OpenMRS, an important open source EMR system [48]. This partnership played a key role in ensuring that the national health information system integrated well with the EMR components [50]. While this is an example of success through partnership, eHealth interventions in the health system that involve development partners often lead to complications. Divergent strategies or priorities between partners and between a partner and the country may impede health systems from being strengthened [51] or overwhelm national systems with duplicative processes [57]. To effectively

navigate collaboration, emphasis should be placed on aligning the goals of eHealth initiatives to the countries' needs, priorities, and policies [50, 51], standardizing protocols for project management [5, 66], and closing the gap between the execution and objectives of management systems and structures [35].

## 4 METHODS

Our goal was to understand how a range of stakeholders perceive security and privacy in the HIV data pipeline and to identify opportunities to strengthen patient data protection. To do this, we conducted semi-structured interviews with 14 participants from Lighthouse and Malawi's MoH, which were analyzed using thematic analysis. The interviews for our study took place in Lilongwe, Malawi in September 2022. This study was approved by the IRB at the University of Washington and the Malawi MoH IRB, the National Health Science Research Committee.

### 4.1 Participants

To gain perspectives on stakeholders' understandings and concerns with the security and privacy of patient data, we recruited 14 participants who require or review data as part of their ART-related work. A sample of 14 participants was considered both feasible and appropriate for this exploratory study and is in line with a recent review of qualitative studies that noted that interviews with 9-17 people were sufficient for thematic saturation [36]. Participants were stakeholders from Lighthouse and the MoH who collect, use, synthesize, manage, or aggregate routine ART data from the EMRs or who inform EMRs data policy or practice. While most participants were not information technology experts, we aimed to recruit experts with different areas of data-related expertise to capture diverse security- and privacy-related perspectives and experiences of representative roles within Lighthouse and the MoH. Thus, participants were intentionally recruited through purposive sampling [75] with the support of the Malawian study team who were deeply embedded in the Lighthouse's health system and understood the various roles within it.

In consultation with Lighthouse, participants were grouped by the study team into three data stakeholder groups: (1) community-based care (CBC) nurses, (2) data clerks and IT officers, and (3) data decision makers. Participants in the same stakeholder group had similar roles and responsibilities within the HIV data pipeline. In total, there were three CBC nurses, five data clerks and IT officers, and six data decision makers. Recruitment for participants within a stakeholder group was stopped once saturation was reached. We refer to CBC nurses as nurse-#, data clerks and IT officers as tech-#, and data decision makers as data-# without detailed demographic information to protect the anonymity of participants' responses. Most, but not all, of the participants were male. Demographic information of the participants are described in Table 1. We now describe the roles of each of the three stakeholder groups.

**4.1.1 CBC Nurses.** CBC nurses at Lighthouse are responsible for providing care to stable patients on ART at CBC settings outside of facilities. The care that they provide is similar to that offered at facilities, including adherence monitoring (pill count), refill of prescriptions, documentation of side effects, necessary referrals, and issuing of next appointment date. The nurses use paper and tablet-based data collection and documentation at CBC settings. In its current version, the tablet-based app locally stores collected data until tablets are returned to the facility, because of limitations with connectivity and automatic data synchronization to the EMR system at the facility. After nurses complete the appointments at the CBC setting, they transport the tablets and paper records back with them to the main Lighthouse facility.

**4.1.2 Data Clerks and IT Officers.** To transfer the data in the tablets into the EMR system at the facility, the data clerks connect the tablets to the facility's local network and generate CSVs from

the data in the tablets. Data clerks print the CSV files and refer to the printed data sheet to enter all of its contents into the EMR system at the facility. IT officers are most knowledgeable about the technical protections and current technology practices at Lighthouse and are relied upon to monitor the data flow, transfer, and quality at Lighthouse.

**4.1.3 Data Decision Makers.** Data decision makers include Lighthouse program managers who are well-versed in client data protections, data collection training, facility- and community-based data collection, data verification efforts, and processes to ensure quality data aggregation across settings. Also included are MoH members who are knowledgeable about the management and usage of individual-level and aggregate HIV-related data at the national level.

Table 1. Demographic details of study participants.

| Participant | Affiliation               | Position                   | Approx. Years of Experience |
|-------------|---------------------------|----------------------------|-----------------------------|
| nurse-1     | Lighthouse                | CBC Nurse                  | >5                          |
| nurse-2     | Lighthouse                | CBC Nurse                  | >10                         |
| nurse-3     | Lighthouse                | CBC Nurse                  | >5                          |
| tech-1      | Lighthouse                | Data Clerk/IT Officer      | >10                         |
| tech-2      | Lighthouse                | Data Clerk/IT Officer      | >5                          |
| tech-3      | Lighthouse                | Data Clerk/IT Officer      | >10                         |
| tech-4      | Lighthouse                | Data Manager               | >5                          |
| tech-5      | Lighthouse                | Data Clerk/IT Officer      | >15                         |
| data-1      | Lighthouse                | Health Informatics Advisor | >20                         |
| data-2      | Lighthouse                | Program Manager            | >20                         |
| data-3      | Dept. of HIV & AIDS (MoH) | MoH Key Personnel          | >25                         |
| data-4      | Dept. of HIV & AIDS (MoH) | MoH Key Personnel          | >25                         |
| data-5      | Dept. of HIV & AIDS (MoH) | MoH Key Personnel          | >25                         |
| data-6      | Dept. of HIV & AIDS (MoH) | MoH Key Personnel          | >25                         |

4.2 Study Procedure

We developed three separate interview guides, making a distinction between the questions we asked each of the three stakeholder groups, given the differences in groups’ interactions with the EMR system and patient data. We incorporated feedback on the interview guides from Lighthouse’s study team to improve question clarity, content, and contextualization. Modifications based on the stakeholder group allowed for an interview that tailored to the participant’s area of expertise and role within the health system. All three interview guides are included in Appendix A. We describe the interview flow for each of the three stakeholder groups.

**4.2.1 CBC Nurses.** Interviews with CBC nurses were focused on inquiring about tablet usage during data collection in CBC settings, daily security- and privacy-related practices during data collection, and attitudes towards device and data management. More specifically, we asked about concerns related to electronic data collection and management, security protocols that the nurses follow while using the tablets, understanding of data flow, and perceptions towards data sharing.

**4.2.2 Data Clerks and IT Officers.** Interviews with the data clerks and IT officers focused on participants’ understandings of security and privacy during the data review and management process, including Lighthouse’s technical security measures. We inquired about participants’ definitions of the security and safety of EMRs, potential threats in electronic data collection, vulnerabilities

in data handling and management, individual security practices, technical security measures for various technologies at Lighthouse, and proper usage of tablets.

**4.2.3 Data Decision Makers.** Interviews with data decision makers were aimed to gather participants' perceptions towards device and data management, data pipeline supervision, and aggregation of data to inform data-related policy or practice decision-making. These participants were asked about concerns around data collection in specific settings, concerns around data storage and data transfer, data usage at the national level, perceptions towards tablet-based data collection, perceptions towards policies for patient data protections, and recommendations for enhancing security at the facility and CBC levels.

In all interviews, we asked participants to compare the security of electronic data collection to that of paper-based data collection. All interviews ended by inquiring about other concerns or opinions around security and privacy that were not addressed during the interviews and recommendations for improving the security of patient data. All interviews were conducted by the first author in English, an official language of Malawi, and audio recorded with participants' consent. Audio recordings of interviews were transcribed for analysis. Interviews lasted approximately 45 minutes.

### 4.3 Data Analysis

We used a mixture of deductive and inductive thematic analysis [18] to code the transcripts. The first author conducted a detailed reading of all transcripts and developed a codebook, which expanded as more transcripts were coded. The final codebook was applied to all transcripts by the first author. The second author reviewed the code application and disagreements were resolved through discussion with the first author. Similar codes were grouped into higher level themes, which reflected those suggested a priori from the interview guide (deductive) and from reviewing the contributions from the participants themselves (inductive). The first and second author discussed and refined the coding.

## 5 FINDINGS

We organize our findings into the following sections. *Multi-Level Dedication to Best Practices in Security and Privacy* describes the commitment to protect patient data at multiple levels of the HIV health system. *Threats to Data Protection* details participants' understandings of threats to patient data across various settings and stages of the HIV data pipeline. Lastly, *Opportunities for Multi-Level Policies for Device and Data Management* describes the data protection mechanisms and protocols that participants hoped to see in the future for more secure device and data management.

### 5.1 Multi-Level Dedication to Best Practices in Security and Privacy

Participants shared the understanding that they collectively and individually have a responsibility to protect patient data. Trust was placed in multiple layers of the HIV health system and drove forward the collaborative and collective efforts to protect patient data. Aside from the group-level commitment to enact best practices in security and privacy, individuals carried out additional tasks in their day-to-day work to ensure that patient data was protected.

**5.1.1 Trust as the Key Driver of Collaboration and Collective Commitment.** Trust directs collaboration and is foundational to stakeholders' reliance on technologies and staff to protect patient data.

*Organizations and Partners.* Participants expressed their strong belief that the groups involved with collecting, managing, and using HIV patient data are committed to protecting patient data. Participants were confident that Lighthouse as a whole "know[s] the importance of confidentiality"

(data-2) and has “*high integrity*” (tech-4). Data-2, a Lighthouse program manager, described the MoH as “*the first people or the primary kind of interested parties in this particular field,*” implying their trust that protecting the confidentiality of HIV data is of paramount importance to the MoH. Partners also play a critical role in the data pipeline, for example in the process of approving data sharing. These partners are not only well known by the MoH, but they are also “*in the same field of taking care of people living with HIV*” and so are trusted to understand the sensitivity of HIV (data-2).

*IT Team.* Nurses and data clerks viewed the IT team as playing a key role in upholding the technical security at Lighthouse, as summarized by tech-5: “*I trust that the IT personnel have worked hard to...install some security measures in our systems.*” Knowing that the technologies used at Lighthouse are “*Lighthouse gadgets*” (tech-3) that are managed by the IT team increased participants’ confidence in the security of the technologies themselves. For example, tech-1 attributed their trust in data handling devices to their trust in Lighthouse’s servers: “*the technology we are using [for data handling]...it’s the same [as the] server that we trust.*” Even more, tech-1’s confidence in the security of the servers extends from their knowledge that “[n]obody can go in and access the server, unless the IT guys,” which was similarly expressed by other participants (data-1, nurse-1, tech-4). In such a way, trust in one technology extends to another technology because all technologies are managed by reliable IT officers.

*Lighthouse Staff Working with Patient Data.* Participants expressed their trust in the staff who collect and manage patient data, including CBC nurses and data clerks. The data collection processes happening across facilities and CBC settings were considered to be secure because “*the [nurses] that are handling the data are Lighthouse-oriented staff*” (tech-5) and moreover, the individuals handling patient data are “*trained in terms of confidentiality*” (data-4). From the perspective of one data clerk, tech-1, signing the confidentiality form was an indicator of commitment to protect patient data and a reflection that “*everybody in that office...knows about the health data, the HIV data we are handling.*” Participants’ confidence that individuals who handle patient data have a clear purpose and meaningful role in the HIV data pipeline reassured their sense of security in these individuals.

**5.1.2 Individual-Level Security and Privacy Practices.** While participants relied on various stakeholder groups to commit to best practices, they also understood the importance of individual responsibility in protecting patient data. Participants shared voluntary practices that they incorporated into their day-to-day work that were not necessarily required, but were rather additional tasks to ensure that their daily practices are secure. While removing personally identifiable information (PII) when sharing data is required and commonly practiced, tech-4 added an additional layer of security to ensure that no one can identify the patients by completely replacing patient identification numbers with random numbers. When printing data, which could include PII, tech-1 said they quickly retrieve the paper once it is printed. All three CBC nurses were conscious of the positioning of the tablets during data collection to avoid the data on the screens being viewable to others, as summarized by nurse-1: “*...you position [the device] towards your own direction. The client is sitting in that direction [facing away from the device]. Everyone else is at that end [away from the client and the device].*” Nurse-1 also mentioned their attention to deleting data from the tablets after CSV files are generated, noting that this is a personal preference and may not be practiced by other nurses:

*“For myself, with the tablet I’m using,...I check on auto delete after syncing [the tablet] with the server. So the moment I’m [at the facility], [the tablet] has synced to the server, the data is gone in the tablet. There’s nothing else I can access in the tablet...The raw data*

*is synced and is deleted [from the tablet]. That's what I do but for other individuals, I cannot say, I'm not sure."*

## 5.2 Threats to Data Protection

While acknowledging that trust is central to work practices, participants also recognized that an overreliance on trust could lead to mishaps or breaches due to a lack of caution or carelessness. Here, we describe threats to data security and privacy at Lighthouse facilities, CBC settings, and at the national level.

### 5.2.1 Threats at the Facility Level.

*Concerns over Regulating Access to EMRs.* Notable components of security measures at facilities include restrictions of EMR-related work to the local network and passwords for accessing EMRs. Participants elaborated on the potential for mismanagement or neglect of security mechanisms that are intended to protect EMRs.

To ensure that any individual attempting to access the EMR system is authorized to do so, the EMR system requires that the individual enters correct login credentials, namely username and password. The requirement of passwords was commonly seen as a sufficient security measure because password knowledge is exclusive, as stated directly by tech-1: "[t]hat password you know is only known to you." However, participants described hypothetical situations that show that the password requirement alone *"doesn't make the data more secure"* (data-4). For example, participants (tech-1, tech-2, tech-4, data-3, data-4, data-6) recognized that an authorized individual who logs into the tablet or EMR system could leave their work station and forget to log out, allowing for an unauthorized individual to access the EMRs. Access to the EMRs is also restricted to authorized users who are connected to Lighthouse's local network. However, tech-3 indicated that this precaution may be insufficient and theoretically, an unauthorized individual could access, enter, and download sensitive and confidential patient data, risking patient HIV status exposure. Rather than relying solely on the technical security mechanisms to protect patient data, tech-2 stated the importance of recognizing that *"security is only coming in terms of the individual user,"* meaning that each individual is responsible for ensuring data security and privacy.

Access to the server room is strictly limited to the IT officers. However, there were concerns that unauthorized individuals could enter the server room because there were no *"proper policies on how...to govern those systems"* (data-6) and there *"hasn't been any sort of security audit for the...IT center"* (data-5). Another challenge with regulating EMR access arises when people move between jobs: *"people we employ, they don't always stay with the same company or partner, and so as people transition, information gets potentially shared"* (data-3).

*Concerns over Managing Paper Records.* Paper records are still used for a few, discrete patient-level data collection activities at Lighthouse facilities and CBC settings. Participants (tech-1, tech-2, tech-3, tech-5, nurse-2, data-4, data-6) noted unease with paper records, which stemmed from the difficulty of upholding secure protocols and the recognition that human errors are the main vulnerability that could harm patient confidentiality.

Distractions can inhibit secure storage of the paper records, such as forgetting to lock the paper file cabinet due to an interruption, increasing the chances of misplacing the paper record (tech-1, tech-2, tech-5). Even if paper records were to be stored properly, tech-2 said that the security measures for paper records are much weaker than those for EMRs because *"we only may be relying on the local cabinets, which maybe at times can be easily broken into."* Concerns around the disposal of paper records also motivate the shift away from reliance on paper. Based on these concerns, data-3 and data-4 emphasized the importance of establishing security measures for paper records:

*“clearly managing paper records requires a whole set of other measures to protect, to make sure that that paper is shredded and destroyed properly and it doesn’t find its way back somewhere it shouldn’t be”* (data-3).

**5.2.2 Threats in CBC Settings.** Here, we explain participants’ concerns surrounding tablet-based data collection in CBC settings, specifically tablet usage and management.

*Data Loss or Exposure.* Data collection at CBC settings involves a set of unique concerns because the chance of theft, loss, or damage to a tablet used in CBC settings is much higher than that of a computer at Lighthouse facilities. While no tablet has yet been lost or stolen in Lighthouse programs, one of the most common concerns raised was the consequences of tablet theft or loss while the device is being transported back to the facility after data collection. Because the current tablet-based app cannot automatically sync its data to the EMR system at the facility, the tablet is the only source of data storage until the tablet is returned to the facility. If the tablet is lost in transportation, then all of the captured data will be lost. This could complicate the continuation of patients’ care because CBC nurses rely on a previous visit’s data to know where to start for the next visit (nurse-2). According to nurse-1, if data were to be lost, CBC nurses must return to the CBC setting and revisit all patients, which is certainly not a trivial task.

If a tablet were to fall into the wrong hands, the data stored on the tablet is at risk of being wrongfully exposed. Tech-3 feared the possibility that someone with technical expertise could *“crack into”* a lost or stolen tablet to gain access to patient data. The main difficulty with CBC settings is that Lighthouse does not have full control over the data collection process happening outside of its facilities, as summarized by tech-4: *“...we have control over how data is being collected at the facility. But at the community, we don’t know what’s happening.”*

*Inappropriate Usage of Tablets.* Participants shared hypothetical situations in which tablets used inappropriately for personal use could harm the security and privacy of the data in the tablets. More specifically, installing external applications that are not approved by Lighthouse could *“introduce risks into the setup”* (tech-3) and distract CBC nurses from using the tablets for the correct purpose. Data-1 cautioned against the temptation to bring the tablets home and use them as personal devices. Bringing tablets into personal environments, such as homes, creates room for unauthorized and untrained individuals (e.g., children of Lighthouse staff) to use the tablet, increasing the chances of harming patient data. The root of this concern lies in policy weakness: *“As it is now, I think the policies are not really enforced and...some of them I think are not clearly outlined...to the [tablet] users...As long as [the tablet is] working, they are not really looking at the security part”* (tech-3).

Similarly, data-6 worried that because some partners of the MoH appear to be more interested in data collection than reporting the data properly, *“everyone has just been given the freedom to just use the device anyhow,”* without proper instruction or guidelines on how devices should be used. Participants (tech-3, data-6) urged for the greater enforcement of policies that will restrict the technical functionalities of tablets and confirm the importance of using the tablets solely for data collection.

**5.2.3 Threats at the National Level.** Participants described the threats to data security and privacy at the national level if there are gaps or weaknesses in policy and practices.

*Inconsistent Practices among Implementing Partners.* Like Lighthouse, other implementing partners and NGOs funded by international donors are tasked with providing HIV services in partnership with the MoH, meaning that they manage HIV service delivery and handle sensitive data. However, participants believed that not all implementing partners follow the MoH’s recommendations:

*“There are implementing partners that abide by the Ministry’s recommendations. They make databases. We know where their database is stored. And then we have other partners that... have a database but we don’t know where their database is stored. Some transfer that information to the U.S., you have no idea. So, it varies according to which partner is storing that data.” - data-4*

Implementing partners that may be less transparent about their management pose a concern to the MoH because there is a possibility that highly sensitive, patient-level data could be stored in foreign countries, which goes against MoH expectations and data governance policies (data-4). This concern has pushed forth the agenda to establish policies that restrict data hosting to Malawi, specifically within Malawi’s MoH. To ensure that all parties involved guarantee the protection of patient data, the MoH is motivated to improve monitoring of implementing partners’ data sharing and management processes.

When external organizations, including implementing partners or research teams, bring new technologies into Malawi for their own projects, there is difficulty with the technical management of security because *“different projects are doing their things in different ways”* (tech-3). Additionally, tech-3 expressed concern over implementing partners’ potential lack of attention to updating technical security and privacy measures, such as changing passwords frequently and using encryption, which could introduce risks into the patient data protection.

Data-6 described a case in which an abrupt termination of services led by an implementing partner disrupted the support of an EMR system in its early stages. This incident led the MoH to quickly address a leadership gap *“to manage the EMR from the Ministry”* and ensure prompt responses (data-6). This example sheds light on the importance of centering the MoH in identifying, managing, and sustaining activities to strengthen data systems.

*Unclear Data Sharing Protocol.* Participants raised doubts about the sufficient strength of data sharing protocols. When discussing procedures for data sharing, data-3 expressed uncertainty, saying, *“I’m not sure there’s a clear protocol for it.”* Although there is a division of the MoH that is responsible for granting individual or organizational permissions to access health data, according to data-5, these guidelines and standards have yet to be disseminated, leaving procedures for data sharing unclear. This in turn complicates the search for data sharing protocols because *“officially there’s no document that states how data has to be transferred”* (tech-4). The lack of guidelines around data sharing also creates room for improper data sharing procedures, such as sending unprotected files with patient data content through email (tech-4). One participant (data-3) attributed negligent practices around data sharing to the lack of oversight and enforcement, while noting the differences in attitudes towards data sharing between HICs and LMICs: *“...in the West and in the North, there are severe consequences for sharing, inadvertently or negligently, somebody’s data and that raises people’s fears of course, and they pay more attention. And here [in Malawi], it’s like a gentleman’s mistake and nobody cares.”*

### 5.3 Opportunities for Multi-Level Policies for Device and Data Management

Participants shared various approaches for improving the security of data, to be executed at the facility, CBC, and national levels. They also detailed the importance of reviewing and updating security and privacy standards to prioritize the improvement of patient data protection.

**5.3.1 Lighthouse Level Management.** Participants proposed various considerations that will ensure that the data is secure, including enhanced monitoring of tablets, control of data access, and enforcement of work expectations. These opportunities can be executed at Lighthouse facilities and in CBC settings.

*Mobile Device Management.* Mobile device management, which is the remote management of all devices, is under consideration for improving data protection mechanisms, should tablets containing data be lost or stolen. In the case that a tablet is lost or stolen, tech-3 recommended to “*wipe, to reset the tablets remotely*” before any data is accessed by unauthorized users. Mobile device management should also allow the IT personnel to remotely “*lock [the tablet] so that even if someone picks it up, they can use the parts but they cannot use the information that is in that gadget*” (data-4). Additionally, to prevent the improper usage of tablets, nurse-2 suggested making the tablets “*restricted gadget[s]*” that could only be used for data collection and prevent distracting functionalities such as web browsing and sending or receiving text messages and calls. Data-3 and data-6 proposed remote tracking of tablets as a mechanism that ensures that there is “*remote ability to understand what people are doing on there*” (data-3).

While technology-driven supervision could boost security, the protection of patient data also relies heavily on the individuals who use the tablets. Participants (nurse-3, data-1, data-2, data-4) agreed that Lighthouse staff should ensure that tablets are left in a safe place within Lighthouse facilities, as opposed to bringing them to their homes, where there is risk of damage. Data-3 said that there should be a “*clear chain of custody*” for every device that is used within and outside of facilities.

*Granular Access Levels.* Another technical suggestion that was mentioned frequently is role-based access control, a mechanism for restricting EMR access based on job responsibilities. In order to “*restrict the number of people who deal with data as much as possible*” (data-3), the EMR system should assign “*leveled rights*” as opposed to “*universal rights*” (data-4). More specifically, participants wanted the EMR system to grant and deny access to EMRs based on users’ job responsibilities, so that only relevant Lighthouse staff can access patients’ health data: “*...if you’re just a mere vitals clerk, you shouldn’t be able to see information about consultations or prescriptions that are done in the system*” (tech-5). Nurse-1 also pointed out that data clerks, whose jobs include checking which patients have missed their appointments, should not be granted full access to EMRs because they are not medically trained.

Participants also mentioned an existing protocol for changing access levels, noting its strengths, and additional measures that can be taken. Before creating a new user with access to the EMR system, data clerks and IT officers must consult with one another. Tech-2 suggested that security questions should be asked to IT officers, who are responsible for updating access privileges, to confirm their permissions to grant new access privileges.

*Clear and Enforced Work Expectations.* In addition to a universal recognition of the importance of securing passwords and establishing policies for frequently updating passwords, participants suggested other critical actions for ensuring that day-to-day work practices are more secure.

Participants emphasized the importance of reminding Lighthouse staff of the sensitivity of patient data. Tech-4 suggested having collective efforts to raise awareness, such as “*an orientation on awareness to whoever deals with the patient-level data, or whoever is entering the data, storing the data, or transferring the data,*” especially because harms to data security and privacy could affect the entire organization.

Participants (tech-3, data-1, data-2, data-5) highlighted the importance of developing clear expectations for individuals working with patient data. Data-1 elaborated on protocols that should be developed between those responsible for the HIV program and those handling electronic patient data, noting that this practice is commonly observed in HICs:

*“...developing protocols that clearly outline...expectations of IT and [data clerks] as far as the electronic data capture is concerned. So the government may bring in a policy but the*

*HIS [health information systems] partner or HIV department, who are responsible for the HIV program, should work on creating these protocols on how data should be managed. Then people who are working should go through the protocols. After they go through the protocols, they sign an agreement...So people would have that sense of responsibility that the data that I'm working on is confidential data."*

In addition to agreements that outline expectations for Lighthouse staff to manage data, nurses should be thoroughly trained on the devices they use regularly. Tech-5 said that nurses should understand the purpose of security measures, such as automatic lockouts, which can be perceived as annoying but are implemented with the intention to protect patient data. To ensure that Lighthouse manages the devices and data properly, data-6 suggested that there should be a *"terms of references on usage of this data or protocols on how these applications are supposed to be used."*

Policies should go beyond outlining proper work practices and also clarify the consequences of inappropriate work practices. In light of concerns around workers' negligence and the lacking sense of responsibility (data-3), data-2 suggested implementing *"very strict, punitive laws"* when patient data is dealt with improperly.

**5.3.2 National Level Management.** Participants advocated for centralized and standardized data governance because *"supervision and oversight become much harder if things are decentralized"* (data-3). Here, we elaborate on how centralization and standardization can be achieved and the benefits it brings to data security.

**Standardization of Project Implementation.** Many technology-involving projects follow different standards and management procedures, as they are led by various external organizations and partners, such as international NGOs. To resolve the lack of unification in project implementation and management by different partners, tech-3 said that the MoH should *"harmonize the projects"* by becoming the main manager of partners' projects and the main data custodian. The MoH should be at the center of establishing agreements that are communicated to different partners and then signed by partners to confirm their commitment to proper data management (tech-3). Implementing partners should abide by MoH data requirements that govern data ownership, including being *"the core owner of the data during the study period"* (data-5) and transferring data ownership to the MoH upon study completion. The establishment of common standards for implementing partners is to ensure that *"everyone will be subjected to the same standard"* (data-5).

**Standardization of Procedures for Data Collection, Usage, Sharing, and Transfer.** First and foremost, data collection should be restricted to data that is actually necessary for care. There should be a *"really strong rationale of every piece of information that's being collected"* especially because unnecessary data collection places additional burden on healthcare providers and is not meaningful for patient services (data-3). The reason for minimizing the amount of data collected lies in the fact that very little of the data that is currently collected is actually aggregated and transferred to the MoH for improving patient services (data-3). While efficient data collection has benefits, recognizing the utility of data is also important.

Assuming that data collection was executed properly and with purpose, various management changes can further contribute to the security of data. To ensure that patient data usage aligns with the MoH's standards, there should be an agreement between the MoH and Lighthouse:

*"I think the government and also Lighthouse should have a data agreement on how this data is going to be used. And it's not supposed to be used outside the stipulated agreements that the government had set up with Lighthouse or these partners. I think it just needs to have that proper agreement and policies on how data is supposed to be used."* - data-6

In terms of data sharing, if a research team or an organization requests a facility to share patient data, there should be a clear procedure for determining whether or not the data should be shared with them. While there are procedures in principle for data sharing with researchers or organizations, the lack of clarity referred to by participants reflects a gap in policy. This gap can be minimized by developing “a structure, a document, a standard or a protocol where they look at the requests to say, ‘does it meet this standard in terms of data security?’” (data-5). The increased sensitivity of patient-level data also necessitates more care and caution than aggregate data. Participants (tech-2, data-1, data-2, data-3, data-4, data-6) agreed that patient-level data that includes PII, such as name, date of birth, and address should never be shared outside of Lighthouse and the MoH. Participants recognized the importance of ensuring that the data requester is credible and responsible, by confirming their position or responsibility in an organization (data-2) and their rationale for requesting data (nurse-2). The data requester should also obtain written permission from the MoH to have access to the data and to use the data (data-4). Establishing a clear protocol for data sharing will “help us enforce how data is being shared and [how not to] share the data” (tech-4). To ensure that data transfer procedures are secure, data-5 and data-6 preferred that international standards are met, noting that the adherence to globally accepted security and privacy standards is “key in data security” (data-5).

**5.3.3 Building an Environment for Security and Privacy Prioritization.** Outlining policies and protocols can only ensure security improvements to a certain extent. Individuals and organizations should continuously enforce policy implementation in practice. Data-3 emphasized that regular reminders and supervision will “sensitize people about the issue of managing...sensitive data about patients” and is critical to upholding secure practices. A concrete approach to regular enforcement is “a [reoccurring] six month reminder of the rules and documentation of...supervision of what people do and what current actions has been taken” (data-3).

Participants also encouraged the continuous review of security protocols. Data-5 recommended security audits for the IT department to “review more of the gaps that are there” in the process of granting physical access to the server rooms and access to EMRs. While there are policies that have been developed to protect the data storage center, data-6 said that the involvement of an external organization to scrutinize the data protection mechanisms could create opportunities for future system improvements.

## 6 DISCUSSION

Our main claims from analyzing stakeholder interviews are as follows:

- (1) Communal trust among stakeholders to uphold confidentiality is central to collaborative and collective efforts to protect patient data. While trusting stakeholders at various levels in the HIV health system to follow best practices for security and privacy, participants also understood the importance of individual responsibility to protect patient data.
- (2) Threats to data protection can arise when technical security measures are insufficient and when stakeholders are not vigilant enough in their day-to-day work practices. Participants were also concerned about how inadequate supervision, noncompliant implementing partners, and a lack of national policy enforcement may weaken data and device management.
- (3) While there are existing protocols in principle for managing data and devices, participants expressed strong interests in further standardization, dissemination, enforcement, clarity, and consistent updating of data and device management procedures.

## 6.1 Alignment with Best Practices in Security and Privacy

CSCW and HCI literature on privacy protections and practices argues that the notion of privacy differs between HICs and LMICs [8, 38, 78]. In contrast, our findings suggest that stakeholders' motivation to review, adapt, and refine best practices for the Malawian context demonstrates the intention to align Malawi's data security and privacy practices with existing efforts in HICs. At the facility and CBC levels, participants were aware of and aimed to adhere to common protections like passwords, mobile device management, and user restrictions. At the national level, participants identified gaps in governance that challenge consistent implementation of best practices and promoted adherence to guidance on data security and privacy that align with international standards. In this section, we highlight how participants' practices and ideals intersect with best practices in security and privacy in healthcare settings. Factors that could explain the alignment of our study participants' views on security and privacy with recognized standards and norms include high level of education, familiarity with technology, and values that promote patient data protections established by the Malawian public health system.

Most notably, participants presented similar understandings of security and privacy and their threats to those observed among the stakeholders of ODK deployments [25], which is the same technology that is currently used for tablet-based data collection in Lighthouse's CBC settings. Participants' identification of threats to data security and privacy are similar to the itemization of security and privacy concerns that Cobb et al. [25] mention, namely physical theft of a data collection device and unauthorized access to data on a device. Among the three goals of the CIA triad, - confidentiality, integrity, availability - our participants were most concerned with data confidentiality, which is the protection of private information about patients from being revealed to any individual who should not have access to it.

Participants' understandings of and practices in protecting confidentiality are similar to those observed in other work that focuses on confidentiality management in healthcare work in three ways. First, participants understood that different levels of information sensitivity entail different degrees of data protection. The recognition that confidentiality is of greater importance with patient-level data than with aggregate data is an understanding that is shared with healthcare staff in other settings [49]. Participants also supported the implementation and reinforcement of role-based access control in the EMR system, which would grant and deny EMR access based on users' job responsibilities. The recognition of different levels of sensitivity within a single patient's medical record aligns with understandings of health information sensitivity and information flow that are reinforced in other healthcare settings as best practices for protecting patient data [23].

Second, CBC nurses and data clerks engaged in invisible work - a series of informal tasks that occur in the background [71, 73] - to support data security and privacy at the individual level. Invisible work is commonly observed in healthcare settings globally [16, 49, 60, 72, 79] and is examined in the accomplishment of privacy practices [60]. We found that participants quickly retrieved printed data, digitally obscured PII when sharing data, positioned tablets away from other people's eyes, and checked to see that the data in the tablets were deleted after saving the data elsewhere. None of these tasks were strictly required, but were rather tasks that stakeholders incorporated into their day-to-day work to go above and beyond in achieving the broader goal of protecting patient data. The invisible work reflects the recognition of the sensitivity of HIV care and the circumstances of mismanaging HIV-related data, which is the public exposure of HIV positive patients. At the same time, stakeholders demonstrate that technical security measures, such as unique passwords, cannot be relied upon as the sole mechanism for patient data protections. In addition to strong technical measures, such as mobile device management and role-based access control, each individual in the health system has the responsibility to properly perform their

work and respond to threats in healthcare settings [23, 24, 45, 61, 62]. At the same time, the policies that participants recommended could potentially shift the nature of certain work practices from being behind-the-scenes to more visible, collaborative work. More specifically, participants were enthusiastic about creating documents and agreements that clarify proper tablet usage and data sharing and transferring protocols. Not only do these recommendations align with global guidelines for protecting HIV information [77], but forthcoming changes in protocols could also standardize the execution of existing practices that are carried out based on individual decisions. Overall, participants' push towards implementing new policies reflects the recognition that the incorporation of technologies into Lighthouse's health system necessitates the reconfiguration of work practices and responsibilities [74].

Third, participants highlighted the importance of governance in delivering best practices for technology-based healthcare. Developing strong governance for creating an enabling environment for eHealth is recognized by the WHO as a core component of eHealth innovation and implementation [56, 58]. The significance of governance is reflected in participants' proposals for placing the MoH at the center of project and data management so that the MoH can enforce the same standards and expectations onto various stakeholder groups. Not only are participants' desires to establish centralized management a practical step towards recognizing and communicating national goals to partners, but also an indicator of efforts to establish interoperability at administrative and technical levels. More specifically, participants suggested standardizing implementing partners' project implementations and protocols for data collection, usage, sharing, and transferring. The recognition that standardization is a key driver of interoperability and that standards must be coordinated at a national level is critical for the successful application of technologies that can protect patient data [66] and is similarly acknowledged in global healthcare settings as a foundational element of successful eHealth initiatives and adoption [5].

## 6.2 Strengthening Data Security and Privacy in Malawi

We present our own analysis of the study setting, highlighting participants' actions and aspirations as indicators of the strengths of Malawi's HIV health system. Our findings reveal that stakeholders want to bolster procedural governance to securely sustain the EMR system for continued strengthening of Malawi's health system, which is a sentiment that is echoed by stakeholders in other LMICs' health systems [7, 28, 42].

At the same time, we recognize that there are challenges in implementation of recommended security practices. MoHs in LMICs face difficulty with hiring, training, and retaining experienced data privacy technicians due to competition with the private and NGO sectors, both domestically and abroad [6]. However, there is recognition that both clinic- and MoH-level data security experts are required to identify, predict, and solve existing and emerging threats to eHealth data security and privacy. The need for more expertise is also reflected in the noted challenge of governance for health partners' data management processes. Management and oversight for data security and privacy across multiple implementing partners necessitate strong policy. Yet, in LMICs, severe shortages of healthcare workers across all levels [6], policy dissemination weaknesses, supervision gaps, and healthcare worker complacency may present obstacles to immediate data privacy improvements, resulting in reduced emphasis or enforcement of security practices and policies. As challenges in achieving data security and privacy continue to evolve in response to innovations in eHealth, global donor and stakeholders will need to prioritize funding and human resources to meet emerging and persistent needs.

While new challenges may arise, our findings suggest that the collaboration between different stakeholders in Malawi's HIV health system speaks to the future success of efforts to protect sensitive patient data. Stakeholders recognized the dedication to patient data protections among

multiple levels in the HIV health system, namely organizations (Lighthouse and MoH) and partners, the IT team, and Lighthouse staff working with patient data on a daily basis. These groups co-manage sensitive patient data in their collective sharing, usage, and transferring of data, which is crucial to managing patient privacy in a collaborative environment such as a healthcare setting [49]. While trust facilitated the group-level collaboration and commitment to data protections, stakeholders were incentivized to improve the co-management of patient data, as reflected in their interest to develop national level policies and practices around device and data management. Stakeholders articulated the strengths and weaknesses of current practices and expressed the need for change in the form of strong governance. In the desire to develop, adopt, and implement strong governance at the national level, stakeholders reflected their understanding of how national level governance extends to day-to-day security and privacy practices at the facilities and CBC settings. The governance proposals that were made by stakeholders suggest that there is considerable effort to refine existing work practices at the facility and CBC levels to match the ideal management systems and structures that are defined at the national level [35]. At the same time, the collaboration between Lighthouse and the MoH offers a unique possibility that forthcoming governance will align with Lighthouse staff's work practices. This possibility is substantiated by the shared vision between Lighthouse and the MoH to protect patient data and improve the quality of HIV care. Lighthouse and the MoH operate as a cooperative unit, exemplifying a collaboration that enables integrated efforts for building a strong health system [13, 50, 68]. Further, the MoH is interested in understanding Lighthouse's work practices, which is evident in the MoH's approval for us to conduct this study. Ensuring that policies do not hinder workflow and work practices of healthcare staff is critical for overall privacy compliance [49] and this study offers insight into a strong partnership that could manifest meaningful governance.

### 6.3 Limitations and Future Work

While this study has a sufficient sample size of participants to reach data saturation, as with all qualitative work, the findings of this study are not generalizable to all stakeholders from Lighthouse or the MoH. We also acknowledge that while we argue that our findings from Lighthouse's health system align with global best practices, this argument may not necessarily extend to health systems in other LMICs. In particular, we recognize that countries have different levels of maturity in incorporating digital health into their health systems.

While this paper focuses on stakeholders' views on data security and privacy, exploring the security and privacy perceptions of HIV patients could illuminate the gaps in patient understanding to inform future improvements on patient education. The investigation of patient perspectives is forthcoming in an additional qualitative study.

## 7 CONCLUSION

There is broad recognition that eHealth governance must prioritize security and privacy considerations for robust eHealth scale-up, including EMR systems in LMICs. Our findings suggest that stakeholders in Malawi's public HIV care program have a strong commitment to protecting patient data, understand security concerns, and are able to identify clear pathways for improving privacy practices. Aligning Malawi's patient data protections with global best practices is not only desirable, but critical for strengthening Malawi's health system.

Overall, this work highlights the importance of supporting national MoH efforts in building eHealth governance that strengthens under-resourced health systems in an effective, appropriate, and collaborative manner reflecting local contexts and priorities. At the same time, we shed light on the challenges of actualizing strong governance and enforcing security in public health programs in LMICs, like Malawi. We encourage CSCW researchers to explore how other LMICs are considering

enhancing security and privacy practices and policies to better protect patients and their data as health systems continue to adopt eHealth applications.

## ACKNOWLEDGMENTS

Research reported in this publication was partially supported by the National Institutes of Health (NIH), National Institute of Mental Health (NIMH) under award number R21MH127992 (“The Community-based ART REtention and Suppression (CARES) App: an innovation to improve patient monitoring and evaluation data in community-based antiretroviral therapy programs in Lilongwe, Malawi”), under multiple principal investigators, Feldacker and Tweya. The authors would also like to thank the Lighthouse Trust and the Ministry of Health, Malawi, for their contributions, insights, and recommendations to this important area of study. The content is solely the responsibility of the authors and does not necessarily represent the official views of the NIH, NIMH, Lighthouse Trust, nor Malawi MoH.

## REFERENCES

- [1] 2020. Principles for Digital Development. <http://digitalprinciples.org/>.
- [2] 2021. AIDSinfo. <https://aidsinfo.unaids.org/>.
- [3] 2021. Population, total - Malawi. <https://data.worldbank.org/indicator/SP.POP.TOTL?locations=MW>.
- [4] 2023. Malawi HIV and AIDS Estimates. <https://www.unaids.org/en/regionscountries/countries/malawi>.
- [5] Funmi Adebisin, Paula Kotze, Rosemary Foster, and Darelle Van Greunen. 2013. A Review of Interoperability Standards in E-health and Imperatives for their Adoption in Africa. *South African Computer Journal* 50, 1 (2013), 55–72.
- [6] Ehui Adovor, Mathias Czaika, Frédéric Docquier, and Yasser Moullan. 2021. Medical brain drain: how many, where and why? *Journal of Health Economics* 76 (2021), 102409.
- [7] Hossein Ahmadi, Mehrbakhsh Nilashi, Leila Shahmoradi, and Othman Ibrahim. 2017. Hospital Information System adoption: Expert perspectives on an adoption framework for Malaysian public hospitals. *Computers in Human Behavior* 67 (2017), 161–189. <https://doi.org/10.1016/j.chb.2016.10.023>
- [8] Syed Ishtiaque Ahmed, Md. Romael Haque, Jay Chen, and Nicola Dell. 2017. Digital Privacy Challenges with Shared Mobile Phone Use in Bangladesh. *Proc. ACM Hum.-Comput. Interact.* 1, CSCW, Article 17 (dec 2017), 20 pages. <https://doi.org/10.1145/3134652>
- [9] Syed Ishtiaque Ahmed, Md. Romael Haque, Shion Guha, Md. Rashidujjaman Rifat, and Nicola Dell. 2017. Privacy, Security, and Surveillance in the Global South: A Study of Biometric Mobile SIM Registration in Bangladesh. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (Denver, Colorado, USA) (CHI '17). Association for Computing Machinery, New York, NY, USA, 906–918. <https://doi.org/10.1145/3025453.3025961>
- [10] Maxwell O Akanbi, Amaka N Ocheke, Patricia A Agaba, Comfort A Daniyam, Emmanuel I Agaba, Edith N Okeke, and Christiana O Ukoli. 2012. Use of electronic health records in sub-Saharan Africa: progress and challenges. *Journal of Medicine in the Tropics* 14, 1 (2012), 1.
- [11] Mahdi Nasrullah Al-Ameen, Tanjina Tamanna, Swapnil Nandy, M. A. Manazir Ahsan, Priyank Chandra, and Syed Ishtiaque Ahmed. 2020. We Don't Give a Second Thought Before Providing Our Information: Understanding Users' Perceptions of Information Collection by Apps in Urban Bangladesh. In *Proceedings of the 3rd ACM SIGCAS Conference on Computing and Sustainable Societies* (Ecuador) (COMPASS '20). Association for Computing Machinery, New York, NY, USA, 32–43. <https://doi.org/10.1145/3378393.3402244>
- [12] Wei Bai, Moses Namara, Yichen Qian, Patrick Gage Kelley, Michelle L Mazurek, and Doowon Kim. 2016. An Inconvenient Trust: User Attitudes toward Security and Usability Tradeoffs for {Key-Directory} Encryption Systems. In *Twelfth Symposium on Usable Privacy and Security* (SOUPS 2016). 113–130.
- [13] Catharina Barkman and Lars Weinehall. 2017. Policymakers and mHealth: roles and expectations, with observations from Ethiopia, Ghana and Sweden. *Global health action* 10, sup3 (2017), 1337356.
- [14] Yahel Ben-David, Shaddi Hasan, Joyjeet Pal, Matthias Vallentin, Saurabh Panjwani, Philipp Gutheim, Jay Chen, and Eric A. Brewer. 2011. Computing Security in the Developing World: A Case for Multidisciplinary Research. In *Proceedings of the 5th ACM Workshop on Networked Systems for Developing Regions* (Bethesda, Maryland, USA) (NSDR '11). Association for Computing Machinery, New York, NY, USA, 39–44. <https://doi.org/10.1145/1999927.1999939>
- [15] Brandford Bervell and Hosam Al-Samarraie. 2019. A comparative review of mobile health and electronic health utilization in sub-Saharan African countries. *Social Science & Medicine* 232 (2019), 1–16.

- [16] Claus Bossen and Erik Grönvall. 2015. Collaboration In-between: The Care Hotel and Designing for Flexible Use. In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (Vancouver, BC, Canada) (CSCW '15). Association for Computing Machinery, New York, NY, USA, 1289–1301. <https://doi.org/10.1145/2675133.2675243>
- [17] Jørn Braa and Sundeep Sahay. 2017. The DHIS2 Open Source Software Platform: Evolution Over Time and Space. In Global Health Informatics. Principles of eHealth and mHealth to Improve Quality of Care, Leo Anthony, G. Celi, Hamish S. F. Fraser, Vipani Nikore, Juan Sebastian Osorio, and Kenneth Paik (Eds.). The MIT Press.
- [18] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. Qualitative research in psychology 3, 2 (2006), 77–101.
- [19] German Daniel Caruso and Lina Marcela Cardona Sosa. 2022. Malawi Poverty Assessment : Poverty Persistence in Malawi - Climate Shocks, Low Agricultural Productivity, and Slow Structural Transformation (English). World Bank Group (2022). <http://documents.worldbank.org/curated/en/099920006302215250/P174948072f3880690afb70c20973fe214d>
- [20] Barbara Castelnuovo, Agnes Kiragga, Victor Afayo, Malisa Ncube, Richard Orama, Stephen Magero, Peter Okwi, Yukari C Manabe, and Andrew Kambugu. 2012. Implementation of provider-based electronic medical records and improvement of the quality of data in a large HIV program in Sub-Saharan Africa. PloS one 7, 12 (2012), e51631.
- [21] Sam Castle, Fahad Pervaiz, Galen Weld, Franziska Roesner, and Richard Anderson. 2016. Let's Talk Money: Evaluating the Security Challenges of Mobile Money in the Developing World. In Proceedings of the 7th Annual Symposium on Computing for Development (Nairobi, Kenya) (ACM DEV '16). Association for Computing Machinery, New York, NY, USA, Article 4, 10 pages. <https://doi.org/10.1145/3001913.3001919>
- [22] Jay Chen, Michael Paik, and Kelly McCabe. 2014. Exploring internet security perceptions and practices in urban ghana. In 10th Symposium On Usable Privacy and Security (SOUPS 2014). 129–142.
- [23] Yunan Chen and Heng Xu. 2013. Privacy Management in Dynamic Groups: Understanding Information Privacy in Medical Practices. In Proceedings of the 2013 Conference on Computer Supported Cooperative Work (San Antonio, Texas, USA) (CSCW '13). Association for Computing Machinery, New York, NY, USA, 541–552. <https://doi.org/10.1145/2441776.2441837>
- [24] Young B Choi, Kathleen E Capitan, Joshua S Krause, and Meredith M Streeper. 2006. Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. Journal of medical systems 30 (2006), 57–64.
- [25] Camille Cobb, Samuel Sudar, Nicholas Reiter, Richard Anderson, Franziska Roesner, and Tadayoshi Kohno. 2016. Computer Security for Data Collection Technologies. In Proceedings of the Eighth International Conference on Information and Communication Technologies and Development (Ann Arbor, MI, USA) (ICTD '16). Association for Computing Machinery, New York, NY, USA, Article 2, 11 pages. <https://doi.org/10.1145/2909609.2909660>
- [26] Gerald P. Douglas, Oliver J. Gadabu, Sabine Joukes, Soyapi Mumba, Michael V. McKay, Anne Ben-Smith, Andreas Jahn, Erik J. Schouten, Zach Landis Lewis, Joep J. van Oosterhout, Theresa J. Allain, Rony Zachariah, Selma D. Berger, Anthony D. Harries, and Frank Chimbandira. 2010. Using Touchscreen Electronic Medical Record Systems to Support and Monitor National Scale-Up of Antiretroviral Therapy in Malawi. PLOS Medicine 7, 8 (08 2010), 1–6. <https://doi.org/10.1371/journal.pmed.1000319>
- [27] Elizabeth Dunbar, Helen Elizabeth Olsen, Erika Salomon, Shreya Bhatt, Regina Mutuku, Beatrice Wasunna, Jacqueline Edwards, Beth Kolko, and Isaac Holean. 2021. Towards Responsible Data Practices in Digital Health: A Case Study of an Open Source Community's Journey. In Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems (Yokohama, Japan) (CHI EA '21). Association for Computing Machinery, New York, NY, USA, Article 42, 8 pages. <https://doi.org/10.1145/3411763.3443438>
- [28] Ryan A. Ebarido and Nelson J. Celis. 2019. Barriers to the Adoption of Electronic Medical Records in Select Philippine Hospitals: A Case Study Approach. In Proceedings of the 2019 5th International Conference on Computing and Artificial Intelligence (Bali, Indonesia) (ICCAI '19). Association for Computing Machinery, New York, NY, USA, 123–128. <https://doi.org/10.1145/3330482.3330503>
- [29] Adrienne Porter Felt, Alex Ainslie, Robert W. Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettles, Helen Harris, and Jeff Grimes. 2015. Improving SSL Warnings: Comprehension and Adherence. In Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (Seoul, Republic of Korea) (CHI '15). Association for Computing Machinery, New York, NY, USA, 2893–2902. <https://doi.org/10.1145/2702123.2702442>
- [30] Hamish SF Fraser, Paul Biondich, Deshen Moodley, Sharon Choi, Burke W Mamlin, and Peter Szolovits. 2005. Implementing electronic medical record systems in developing countries. Informatics in primary care 13, 2 (2005).
- [31] Hamish S F Fraser, Darius Jazayeri, Patrice Nevil, Yusuf Karacaoglu, Paul E Farmer, Evan Lyon, Mary Kay C Smith Fawzi, Fernet Leandre, Sharon S Choi, and Joia S Mukherjee. 2004. An information system and medical record to support HIV treatment in rural Haiti. BMJ 329, 7475 (2004), 1142–1146. <https://doi.org/10.1136/bmj.329.7475.1142> <https://www.bmj.com/content/329/7475/1142.full.pdf>

- [32] Harsha S. Gardiyawasam Pussewalage and Vladimir A. Oleshchuk. 2016. Privacy preserving mechanisms for enforcing security and privacy requirements in E-health solutions. *International Journal of Information Management* 36, 6, Part B (2016), 1161–1173. <https://doi.org/10.1016/j.ijinfomgt.2016.07.006>
- [33] Arash Ghazvini and Zarina Shukur. 2013. Security Challenges and Success Factors of Electronic Healthcare System. *Procedia Technology* 11 (2013), 212–219. <https://doi.org/10.1016/j.protcy.2013.12.183> 4th International Conference on Electrical Engineering and Informatics, ICEEI 2013.
- [34] Carl Hartung, Adam Lerer, Yaw Anokwa, Clint Tseng, Waylon Brunette, and Gaetano Borriello. 2010. Open Data Kit: Tools to Build Information Services for Developing Regions. In *Proceedings of the 4th ACM/IEEE International Conference on Information and Communication Technologies and Development* (London, United Kingdom) (ICTD '10). Association for Computing Machinery, New York, NY, USA, Article 18, 12 pages. <https://doi.org/10.1145/2369220.2369236>
- [35] Richard Heeks. 2006. Health information systems: Failure, success and improvisation. *International journal of medical informatics* 75 (03 2006), 125–37. <https://doi.org/10.1016/j.ijmedinf.2005.07.024>
- [36] Monique Hennink and Bonnie N. Kaiser. 2022. Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine* 292 (2022), 114523. <https://doi.org/10.1016/j.socscimed.2021.114523>
- [37] Geert Hofstede. 2011. Dimensionalizing cultures: The Hofstede model in context. *Online readings in psychology and culture* 2, 1 (2011), 2307–0919.
- [38] Margaret C. Jack, Pang Sovannaroeth, and Nicola Dell. 2019. "Privacy is Not a Concept, but a Way of Dealing with Life": Localization of Transnational Technology Platforms and Liminal Privacy Practices in Cambodia. *Proc. ACM Hum.-Comput. Interact.* 3, CSCW, Article 128 (nov 2019), 19 pages. <https://doi.org/10.1145/3359230>
- [39] Maia L. Jacobs, James Clawson, and Elizabeth D. Mynatt. 2015. Comparing Health Information Sharing Preferences of Cancer Patients, Doctors, and Navigators. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) (CSCW '15). Association for Computing Machinery, New York, NY, USA, 808–818. <https://doi.org/10.1145/2675133.2675252>
- [40] Yeongjin Jang, Chengyu Song, Simon P. Chung, Tielei Wang, and Wenke Lee. 2014. A11y Attacks: Exploiting Accessibility in Operating Systems. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (Scottsdale, Arizona, USA) (CCS '14). Association for Computing Machinery, New York, NY, USA, 103–115. <https://doi.org/10.1145/2660267.2660295>
- [41] Raoul M Kamadjeu, Euloge M Tapang, and Roland N Moluh. 2005. Designing and implementing an electronic health record system in primary care practice in sub-Saharan Africa: a case study from Cameroon. *Informatics in primary care* 13, 3 (2005).
- [42] Sana Z Khan, Zahraa Shahid, Karin Hedstrom, and Annika Andersson. 2012. Hopes and fears in implementation of electronic health records in Bangladesh. *The Electronic Journal of Information Systems in Developing Countries* 54, 1 (2012), 1–18.
- [43] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. 2009. "When I Am on Wi-Fi, I Am Fearless": Privacy Concerns & Practices in Eeryday Wi-Fi Use. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Boston, MA, USA) (CHI '09). Association for Computing Machinery, New York, NY, USA, 1993–2002. <https://doi.org/10.1145/1518701.1519004>
- [44] Eike-Henner W. Kluge. 2007. Secure e-Health: Managing risks to patient health data. *International Journal of Medical Informatics* 76, 5 (2007), 402–406. <https://doi.org/10.1016/j.ijmedinf.2006.09.003> "Virtual Biomedical Universities and E-Learning" and "Secure eHealth: Managing Risk to Patient Data".
- [45] Clemens Scott Kruse, Brenna Smith, Hannah Vanderlinden, and Alexandra Nealand. 2017. Security techniques for the electronic health records. *Journal of medical systems* 41 (2017), 1–9.
- [46] D.A. Ludwick and John Doucette. 2009. Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries. *International Journal of Medical Informatics* 78, 1 (2009), 22–31. <https://doi.org/10.1016/j.ijmedinf.2008.06.005>
- [47] D Luna, C Otero, and A Marcelo. 2013. Health Informatics in Developing Countries: Systematic Review of Reviews Contribution of the IMIA Working Group Health Informatics for Development. *Yearbook of medical informatics* 22, 01 (2013), 28–33.
- [48] Burke W Mamlin, Paul G Biondich, Ben A Wolfe, Hamish Fraser, Darius Jazayeri, Christian Allen, Justin Miranda, and William M Tierney. 2006. Cooking up an open source EMR for developing countries: OpenMRS—a recipe for successful collaboration. In *AMIA Annual Symposium Proceedings*, Vol. 2006. American Medical Informatics Association, 529.
- [49] Alison R. Murphy, Madhu C. Reddy, and Heng Xu. 2014. Privacy Practices in Collaborative Environments: A Study of Emergency Department Staff. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Baltimore, Maryland, USA) (CSCW '14). Association for Computing Machinery, New York, NY, USA, 269–282. <https://doi.org/10.1145/2531602.2531643>

- [50] Wilbroad Mutale, Namwinga Chintu, Cheryl Amoroso, Koku Awoonor-Williams, James Phillips, Colin Baynes, Cathy Michel, Angela Taylor, and Kenneth Sherr. 2013. Improving health information systems for decision making across five sub-Saharan African countries: Implementation strategies from the African Health Initiative. *BMC health services research* 13, 2 (2013), 1–12.
- [51] Aziza Mwisongo and Juliet Nabyonga-Orem. 2016. Global health initiatives in Africa—governance, priorities, harmonisation and alignment. *BMC Health Services Research* 16, 4 (2016), 245–254.
- [52] Moses Namara, Darcia Wilkinson, Byron M. Lowens, Bart P. Knijnenburg, Rita Orji, and Remy L. Sekou. 2018. Cross-Cultural Perspectives on EHealth Privacy in Africa. In *Proceedings of the Second African Conference for Human Computer Interaction: Thriving Communities* (Windhoek, Namibia) (AfriCHI '18). Association for Computing Machinery, New York, NY, USA, Article 7, 11 pages. <https://doi.org/10.1145/3283458.3283472>
- [53] Sheza Naveed, Hamza Naveed, Mobin Javed, and Maryam Mustafa. 2022. "Ask This from the Person Who Has Private Stuff": Privacy Perceptions, Behaviours and Beliefs Beyond W.E.I.R.D. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems* (New Orleans, LA, USA) (CHI '22). Association for Computing Machinery, New York, NY, USA, Article 105, 17 pages. <https://doi.org/10.1145/3491102.3501883>
- [54] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.
- [55] Tom Oluoch, Xenophon Santas, Daniel Kwaro, Martin Were, Paul Biondich, Christopher Bailey, Ameen Abu-Hanna, and Nicolette de Keizer. 2012. The effect of electronic medical record-based clinical decision support on HIV care in resource-constrained settings: A systematic review. *International Journal of Medical Informatics* 81, 10 (2012), e83–e92. <https://doi.org/10.1016/j.ijmedinf.2012.07.010> Health Information Electronic Network Systems for People Living with HIV/AIDS in Underserved Communities.
- [56] World Health Organization. 2021. *Global strategy on digital health 2020–2025*. World Health Organization. 44, [12] p. pages.
- [57] World Health Organization et al. 2009. *Report on the WHO/PEPFAR consultation on maximizing positive synergies between health systems and global health initiatives through work on building and sustaining health workforce development*, Washington DC, 17–18 March 2009. Technical Report. World Health Organization.
- [58] World Health Organization et al. 2012. *National eHealth strategy toolkit*. International Telecommunication Union.
- [59] Saurabh Panjwani and Edward Cutrell. 2010. Usably Secure, Low-Cost Authentication for Mobile Banking. In *Proceedings of the Sixth Symposium on Usable Privacy and Security* (Redmond, Washington, USA) (SOUPS '10). Association for Computing Machinery, New York, NY, USA, Article 4, 12 pages. <https://doi.org/10.1145/1837110.1837116>
- [60] Chrysanthi Papoutsis and Ian Brown. 2015. Privacy as Articulation Work in HIV Health Services. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing* (Vancouver, BC, Canada) (CSCW '15). Association for Computing Machinery, New York, NY, USA, 339–348. <https://doi.org/10.1145/2675133.2675204>
- [61] Rachida Parks, Chao Chu, Heng Xu, and Lascelles Adams. 2011. Understanding the drivers and outcomes of healthcare organizational privacy responses. (2011).
- [62] Rachida Parks, Chao-Hsien Chu, and Heng Xu. 2011. Healthcare information privacy research: Issues, gaps and what next? (2011).
- [63] Vimla L. Patel, Jose F. Arocha, and Edward H. Shortliffe. 2000. Cognitive models in training health professionals to protect patients' confidential information. *International Journal of Medical Informatics* 60, 2 (2000), 143–150. [https://doi.org/10.1016/S1386-5056\(00\)00114-3](https://doi.org/10.1016/S1386-5056(00)00114-3)
- [64] Mor Peleg, Dizza Beimel, Dov Dori, and Yaron Denekamp. 2008. Situation-Based Access Control: Privacy management via modeling of patient data access scenarios. *Journal of Biomedical Informatics* 41, 6 (2008), 1028–1040. <https://doi.org/10.1016/j.jbi.2008.03.014>
- [65] Bradley Reaves, Jasmine Bowers, Nolen Scaife, Adam Bates, Arnav Bhartiya, Patrick Traynor, and Kevin R. B. Butler. 2017. Mo(Bile) Money, Mo(Bile) Problems: Analysis of Branchless Banking Applications. *ACM Trans. Priv. Secur.* 20, 3, Article 11 (aug 2017), 31 pages. <https://doi.org/10.1145/3092368>
- [66] Thomas C. Rindfleisch. 1997. Privacy, Information Technology, and Health Care. *Commun. ACM* 40, 8 (aug 1997), 92–100. <https://doi.org/10.1145/257874.257896>
- [67] Nithya Sambasivan, Garen Checkley, Amna Batool, Nova Ahmed, David Nemer, Laura Sanely Gaytán-Lugo, Tara Matthews, Sunny Consolvo, and Elizabeth Churchill. 2018. "Privacy is Not for Me, It's for Those Rich Women": Performative Privacy Practices on Mobile Phones by Women in South Asia. In *Proceedings of the Fourteenth USENIX Conference on Usable Privacy and Security* (Baltimore, MD, USA) (SOUPS '18). USENIX Association, USA, 127–142.
- [68] Tanzir Ahmed Shuvo, Rubana Islam, Shahed Hossain, Julie L. Evans, Fatema Khatun, Tanvir Ahmed, Rukhsana Gazi, and Alayne M. Adams. 2015. eHealth innovations in LMICs of Africa and Asia: a literature review exploring factors affecting implementation, scale-up, and sustainability. *health care* 8, 9 (2015).
- [69] Sanjay P. Sood, Stacie N. Nwabueze, Victor W.A. Mbarika, Nupur Prakash, Samir Chatterjee, Pradeep Ray, and Saroj Mishra. 2008. Electronic Medical Records: A Review Comparing the Challenges in Developed and Developing

- Countries. In *Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008)*. 248–248. <https://doi.org/10.1109/HICSS.2008.141>
- [70] Janaki Srinivasan, Savita Bailur, Emrys Schoemaker, and Sarita Seshagiri. 2018. Privacy at the margins| The poverty of privacy: Understanding privacy trade-offs from identity infrastructure users in India. *International Journal of Communication* 12 (2018), 20.
- [71] Susan Leigh Star and Anselm Strauss. 1999. Layers of silence, arenas of voice: The ecology of visible and invisible work. *Computer supported cooperative work (CSCW)* 8, 1 (1999), 9–30.
- [72] Allan Stisen, Nervo Verdezoto, Henrik Blunck, Mikkel Baun Kjærgaard, and Kaj Grønbaek. 2016. Accounting for the Invisible Work of Hospital Orderlies: Designing for Local and Global Coordination. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing (San Francisco, California, USA) (CSCW '16)*. Association for Computing Machinery, New York, NY, USA, 980–992. <https://doi.org/10.1145/2818048.2820006>
- [73] Anselm Strauss. 1985. Work and the division of labor. *Sociological quarterly* 26, 1 (1985), 1–19.
- [74] Charlotte Tang, Yunan Chen, Bryan C. Semaan, and Jahmeilah A. Roberson. 2015. Restructuring Human Infrastructure: The Impact of EHR Deployment in a Volunteer-Dependent Clinic. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing (Vancouver, BC, Canada) (CSCW '15)*. Association for Computing Machinery, New York, NY, USA, 649–661. <https://doi.org/10.1145/2675133.2675277>
- [75] Maria Dolores C Tongco. 2007. Purposive sampling as a tool for informant selection. (2007).
- [76] Hannock Tweya, Caryl Feldacker, Oliver Jintha Gadabu, Wingston Ng'ambi, Soyapi L Mumba, Dave Phiri, Luke Kamvazina, Shawo Mwakilama, Henry Kanyerere, Olivia Keiser, et al. 2016. Developing a point-of-care electronic medical record system for TB/HIV co-infected patients: experiences from Lighthouse Trust, Lilongwe, Malawi. *BMC research notes* 9, 1 (2016), 1–10.
- [77] UNAIDS/PEPFAR. 2007. Interim guidelines on protecting the confidentiality and security of HIV information: proceedings from a workshop. [https://data.unaids.org/pub/manual/2007/confidentiality\\_security\\_interim\\_guidelines\\_15may2007\\_en.pdf](https://data.unaids.org/pub/manual/2007/confidentiality_security_interim_guidelines_15may2007_en.pdf)
- [78] Aditya Vashistha, Richard Anderson, and Shirang Mare. 2018. Examining Security and Privacy Research in Developing Regions. In *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies (Menlo Park and San Jose, CA, USA) (COMPASS '18)*. Association for Computing Machinery, New York, NY, USA, Article 25, 14 pages. <https://doi.org/10.1145/3209811.3209818>
- [79] Nervo Verdezoto, Naveen Bagalkot, Syeda Zainab Akbar, Swati Sharma, Nicola Mackintosh, Deirdre Harrington, and Paula Griffiths. 2021. The Invisible Work of Maintenance in Community Health: Challenges and Opportunities for Digital Health to Support Frontline Health Workers in Karnataka, South India. *Proc. ACM Hum.-Comput. Interact.* 5, CSCW1, Article 91 (apr 2021), 31 pages. <https://doi.org/10.1145/3449165>
- [80] Noel Warford, Tara Matthews, Kaitlyn Yang, Omer Akgul, Sunny Consolvo, Patrick Gage Kelley, Nathan Malkin, Michelle L. Mazurek, Manya Sleeper, and Kurt Thomas. 2021. SoK: A Framework for Unifying At-Risk User Research. *CoRR abs/2112.07047* (2021). [arXiv:2112.07047](https://arxiv.org/abs/2112.07047) <https://arxiv.org/abs/2112.07047>
- [81] Evan Waters, Jeff Rafter, Gerald P Douglas, Mwatha Bwanali, Darius Jazayeri, and Hamish SF Fraser. 2010. Experience implementing a point-of-care electronic medical record system for primary care in Malawi. In *MEDINFO 2010*. IOS Press, 96–100.
- [82] Dominik Wermke, Noah Wöhler, Jan H Klemmer, Marcel Fourné, Yasemin Acar, and Sascha Fahl. 2022. Committed to Trust: A Qualitative Study on Security & Trust in Open Source Software Projects. In *Proceedings of the 43rd IEEE Symposium on Security and Privacy*. IEEE Computer Society.
- [83] Xanthe Wessels, Nicoli Nattrass, and Ulrike Rivett 1. 2007. Improving the efficiency of monitoring adherence to antiretroviral therapy at primary health care level: a case study of the introduction of electronic technologies in Guguletu, South Africa. *Development Southern Africa* 24, 4 (2007), 607–621.
- [84] Wen Zhang, Carl A Gunter, David Liebovitz, Jian Tian, and Bradley Malin. 2011. Role prediction using electronic medical record system audits. In *AMIA Annual Symposium Proceedings*, Vol. 2011. American Medical Informatics Association, 858.

## A INTERVIEW GUIDES

### A.1 CBC Nurses

- (1) The patients you see are part of a vulnerable population with sensitive health information. What are your concerns with the confidentiality of the data that is electronically collected from patients?
- (a) Why do you trust electronic data collection?

- (b) What are you afraid of for your clients with the data being collected electronically?
  - (i) How well is patient data protected once it is collected?
  - (ii) What weaknesses are there in electronic data collection that could compromise the security and confidentiality of data?
  - (iii) If the data were to be leaked, what consequences are there for the patients?
    - (A) What information, if leaked, would put the patients at risk?
- (c) How much access do you have to individual electronic patient data?
  - (i) Who else do you think has access to the electronic patient data?
  - (ii) What are your concerns with the amount of access you or other providers might have to electronic patient data?
  - (iii) Are you concerned that anyone who is not supposed to access electronic patient data could access the data?
    - (A) How do you think someone who is not supposed to have access would gain access?
- (2) Now, let's talk about how you use the tablet. When being trained to use the tablet, was there something you were told to do or not to do to ensure the confidentiality of patient records?
- (3) What confidentiality protocols do you use to keep patient records confidential?
  - (a) Are you the only one with access to your tablet?
    - (i) How do you access the content in the tablet?
  - (b) Where is the tablet stored when it is not in use?
    - (i) Do you hide the tablet in a lockable place?
  - (c) Do you position the tablet so only you can see what is on the screen?
  - (d) Do you log out each time?
  - (e) Can your colleagues use the same tablet as the one you use?
    - (i) Do you log out each time you are done using, or share the same account?
- (4) Once you input patient information into the tablet, what do you think happens to the data? Where do you think the data goes?
  - (a) Where do you think the electronic patient data is stored?
  - (b) What concerns do you have with using the tablet to store electronic patient data?
- (5) Currently, how does the data you collect at the community get transferred to the EMR?
  - (a) What security concerns do you have with this process?
  - (b) With the new optimized tablet app, how will this affect the way you collect and enter data at the community?
    - (i) How will this affect the security of patient data?
      - (A) Will the new app minimize the concerns you have with the current data collection process at the community?
    - (ii) What security concerns do you have with using the new app? How will your workload change?
    - (iii) What security concerns do you have with using the new app?
      - (A) What could harm the security of patient data?
- (6) Now, let's talk about sending patient data to partners. How do you think the data from Lighthouse gets to the Ministry of Health or other partners?
  - (a) In what form is the data shared? Is the data that is transferred aggregate or individual data?
  - (b) What concerns do you have with how or with whom the data is shared?
- (7) We want to give you a chance to tell us any other concerns or opinions in the area of data safety. What else would you like to tell us about data collection, storage, and management?
- (8) Do you have any recommendations for improving data confidentiality or dealing with the concerns you mentioned today?

## A.2 Data Clerks and IT Officers

- (1) To begin, what does it mean for data to be secure and safe?
  - (a) Do you handle data confidentiality and security differently if its general health data versus HIV-related data of a patient?
- (2) Do you think electronic data collection is secure? Why or why not?
  - (a) Do you think electronic data collection more secure than paper data collection?
- (3) What is the current process of data collection and entering at the CBC setting?
  - (a) What are your concerns with data collection at the community?
  - (b) Where in the process of data collection at the community, is data security most at risk?
- (4) What is the process of data collection and entering at the Lighthouse facility?
  - (a) What are your concerns with electronic data collection at the facility?
  - (b) Do your concerns differ by location of data collection (CBC setting or facility)?
  - (c) Do your concerns differ by user?
  - (d) Where in the process of electronic data collection at the facility, is data security most at risk?
  - (e) Do you trust data collection more at the Lighthouse facility or at the CBC setting?
- (5) Are there any weaknesses or vulnerabilities in data handling in your role that could compromise the security of the data?
  - (a) What protocols could improve the security of the data?
- (6) B. What precautions and confidentiality protocols do you put into place to keep the data confidential?
  - (a) When delivering or sending data
    - (i) How do you ensure that the recipient of the data guarantees confidentiality of the data?
  - (b) When printing out data
    - (i) How do you make sure that the printed data does not fall into the wrong hands?
  - (c) When manually entering data from paper
  - (d) Other
- (7) What security features are enabled on the tablet to protect the data?
  - (a) What were the alternative security features that you considered?
  - (b) Tell me about user restrictions and permissions. Who has access to what data?
    - (i) What safeguards or permissions are put into place to grant or deny access?
    - (ii) What kind of hierarchy of accounts exists to regulate access?
  - (c) Is the tablet password protected? Is the data encrypted? If so, what kind of encryption?
  - (d) Is there software that keeps track of who, when, and where a patient's data is accessed on the tablet?
- (8) Now, let's talk about data transfer. Could you explain how the entered data in the tablet is transferred to the EMR?
  - (a) What are the encryption processes?
  - (b) Is the encryption process different for individual level data and aggregate data?
- (9) Where is the data stored?
  - (a) What kind of server is used?
    - (i) What are the security characteristics of the server?
    - (ii) How secure is the server where the data is stored?
    - (iii) What are the procedures for ensuring that the server is secure?
- (10) Let's talk about the protection of data for the new optimized tablet-based app or the new community-based EMR.

- (a) What concerns are there for making the new app strictly offline or online? What are the security benefits?
- (b) What vulnerabilities do you expect with the way the new app is designed?
- (c) Do you have any security concerns with the use of a mobile phone?
- (d) Do you prefer using the new app for data collection at the CBC setting or the current method? Why?
  - (i) How will the new app affect workload?
    - (A) What part of data handling will change with the new app?
    - (B) Are there security concerns you have with the new app that you don't have currently?
- (11) How can nurses and clinicians use the tablet and the app to ensure that the data is kept safe?
  - (a) What are precautions that the nurses and clinicians should keep in mind?
  - (b) What is the ideal way to use the tablet from start to end to ensure confidentiality?
- (12) We want to give you a chance to tell us any other concerns or opinions in the area of data safety. What else would you like to tell us about data collection, storage, and management?
- (13) Do you have any recommendations for improving data confidentiality or dealing with the concerns you mentioned today?

### A.3 Data Decision Makers

- (1) To begin, let's talk about electronic data collection, specifically the EMRs. EMRs allow healthcare workers to collect patient information electronically and to store the health information in a digital format.
  - (a) Are there elements of HIV-related health information that makes the data more sensitive?
  - (b) What are your concerns with data collection for EMRs in terms of patient confidentiality?
    - (i) Do your concerns for data collection differ by facility type?
    - (ii) Do your concerns differ by implementing partner?
    - (iii) Do your concerns differ on where the data is captured (facility vs. CBC setting)?
- (2) Next, I would like to hear about your thoughts on data storage. When data is collected via the EMRs, the system electronically stores the collected patient data in such a way that is aimed to keep the data safe and protected.
  - (a) How do you think patient data is stored once the health worker inputs information into the EMR?
  - (b) What are your concerns with EMRs data storage in terms of patient confidentiality?
    - (i) What vulnerabilities do you anticipate with electronic data storage?
    - (ii) What problems could occur if the data is not securely stored?
- (3) Now, I would like to discuss your thoughts about electronic data transfer. EMRs at Lighthouse can be shared and accessed between systems and organizations, such as the MoH. What concerns do you have about electronic data transfer?
  - (a) What are your concerns with data transfer from Lighthouse to MoH?
  - (b) Do you have different concerns for other data transfers that are happening between other facilities or clinic settings?
- (4) Now, I want to talk about how the MoH uses data and protects patient confidentiality.
  - (a) In what format is the data that MoH receives?
    - (i) How is the data sent to MoH?
    - (ii) How does the MoH protect the data that is received?
      - (A) Is the protection of data different for aggregate and individual level data?
      - (B) Does the data contain personal information of the patients?
      - (C) How does the MoH protect identifiable information?
      - (D) How does the MoH protect HIV status or treatment information of patients?

- (b) How does the MoH use the data collected?
  - (i) Does the MoH allow other parties to access the data?
    - (A) In what format does the MoH send data?
    - (B) How is the data protected when it is sent?
    - (C) How do you guarantee that the recipient will ensure confidentiality?
- (5) Currently, Lighthouse healthcare providers go off-site to collect patient data using a tablet. This tablet does not transmit the data to EMR systems until the tablet is returned to the facility. When the tablet is returned to Lighthouse, the data on the tablet is uploaded to Lighthouse server. What concerns do you have with this current approach?
  - (a) How do you think security could be compromised with this current approach?
- (6) Lighthouse is introducing a new tablet-based app for electronic data collection using a mobile phone. This is intended to be used for off-site data collection, so that the data can be immediately transmitted to the EMR system when the data is collected.
  - (a) How do you expect the new app to minimize the concerns you have for the current data collection approach?
  - (b) What are your concerns with the new app data collection in terms of the security of the data?
    - (i) What security concerns do you have with the new app app that you don't have with the current data collection process?
    - (ii) What policy or practice would make you feel more comfortable with the new app data collection?
  - (c) How should the healthcare providers use the new app to ensure data security?
- (7) MoH policy ensures strict confidentiality protections. For example, there is a policy that the data and data servers must remain within Malawi. What informed this policy?
  - (a) How does this policy protect patient data?
  - (b) What other policies or enforcement could improve data confidentiality?
- (8) What do you wish Lighthouse to do to ensure the confidentiality of patients and electronic data?
  - (a) How do you think the data should be stored to ensure data security?
  - (b) What protections or advances in data confidentiality could lead to more comfort with data storage elsewhere, like in the cloud for example?
- (9) We want to give you a chance to tell us any other concerns or opinions in the area of data safety. What else would you like to tell us about data collection, storage, and management?
- (10) Do you have any recommendations for improving data confidentiality or dealing with the concerns you mentioned today?

Received January 2023; revised July 2023; accepted November 2023