Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

Enhanced Security and Privacy Framework for Electronic Healthcare Systems (EHCS), A Case of Jaramogi Oginga Odinga Teaching & Referral Hospital (JOOTRH)

Dr. Fredrick Ochieng' Omogah

Lecturer, Uzima University and currently Postgraduate Research Studies at Jaramogi Oginga Odinga University of Science & Technology (JOOUST), Kenya,

(Received: 07 October 2023 Revised: 12 November Accepted: 06 December)

KEYWORDS

Electronic Healthcare Systems, High value of healthcare data on distributed clinical environments, Privacy and Security on Patients' data, Security and Privacy Framework

ABSTRACT:

As healthcare sector becomes more populated with Technology driven connected IoT medical devices, privacy and security on patients' data exchanged through these devices is critical, and therefore becomes an issue of concern. Electronic Healthcare Systems' (EHCS) run very critical applications that manipulate patients' data to support timely and effective healthcare service delivery. This begins from patient's admission, history taking, diagnosis, referral management, disease prevention and treatment among others. Many studies have revealed that in most developing countries, the available Electronic Healthcare Systems (EHCS) in modern hospitals and the allied facilities have been mishandled, posing a lot of risks to patients' lives. This has been happening both internally by novice or rouge system users, and more so externally by organized online criminal gang. Considering worldwide emergence of the high value for healthcare data, and the associated online criminality, patients' lives remains hanging in a balance with the absence of enhanced security and privacy framework. This could cause very serious healthcare security breaches and vulnerabilities on Electronic Healthcare Systems (EHCS), especially in the distributed clinical environments, where health data MUST be exchanged between the facilities for continued healthcare services. This study adopted both qualitative and quantitative research methods, and uses a descriptive cross sectional study to access and examine the level of security and privacy of patients' data in EHCS at Jaramogi Oginga Odinga Teaching and Referral Hospital (JOOTRH) and its allied facilities (health services sub contraction level) in Kisumu, Kenya that serves more than five (5) million patients from more than ten (10) counties in the Western Kenya Region. Finally, it identified security and privacy challenges in EHCS, and developed an Enhanced Security and Privacy Framework, which would guarantee quality and secure healthcare service delivery to patients in Healthcare facilities within interoperable environments.

1. Introduction

In the contemporary healthcare landscape, Information Security and Privacy have emerged as pivotal concerns on a global scale, fueled by the escalating frequency of cyber threats targeting electronic healthcare systems. While healthcare data may not yield immediate financial gains comparable to financial records, it has become a prime target for cybercriminals aiming to exploit and monetize this inherently sensitive information. Recent research underscores the intensifying focus of cyber threats on healthcare data breaches. The Electronic Health Care Systems (EHCS) play a critical role in supporting healthcare service delivery, yet they struggle with complicated challenges emanating from external cyber-attacks and internal resistance, notably prevalent in developing nations such as Kenya.

The vital nature of healthcare information, often paralleled with human life, emphasizes the imperative need to fortify Electronic Health Care Systems (EHCS). Regrettably, resistance from healthcare professionals has become an obstacle hindering the growth and efficacy of EHCS, particularly in developing nations like Kenya. This resistance not only jeopardizes the advancement of healthcare service delivery but also obstructs essential functions of EHCS, encompassing admissions, history tracking, and diagnosis, treatment, and disease prevention. The subsequent security and

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

privacy challenges arising from human-machine conflicts within EHCS have far-reaching consequences, potentially exposing patient medical information to clinical risks, socio-legal complications, and societal stigmatization.

2. Current Security and Privacy Situation of Patients' Information

Security and privacy are fundamental pillars in healthcare, especially within electronic health care systems (EHCS) where patient cooperation is vital for accurate diagnosis and treatment. The global impact of events like the Covid-19 pandemic has heightened concerns regarding vulnerabilities in healthcare systems, as the shift from manual to electronic health data has presented both benefits and persistent challenges. Despite growing attention to information security in various sectors, the heavily regulated healthcare industry still lacks comprehensive research on security risks.

The adoption of Electronic Health Records (EHR) in developing countries, particularly for diseases like HIV/AIDS, offers potential advantages but introduces issues such as single points of failure and inadequate security measures. Privacy breaches and unauthorized access to patient information on the internet raise concerns about reputational damage and emotional distress. Developing countries face additional challenges due to the absence of defined EHR information policies and strategies, necessitating the establishment of robust security infrastructure, proper policies, and control strategies. In Africa, where Cybersecurity awareness and legislation are lacking, there is a pressing need to address privacy, ownership, and guidelines for securing electronic patient information.

The introduction of Electronic Medical Record (EMR) systems in Kenya, focused on HIV/AIDS, underscores the urgency of addressing security and privacy concerns, particularly in the absence of e-legislation and e-health standards. As technology advances, the increasing use of technology in health interventions poses both benefits and challenges, emphasizing the need for comprehensive studies and frameworks to ensure patient information security and privacy, especially in decentralized patient management scenarios.

3. Assessment of Information Security and Privacy Research Landscape

This study explores the Information Security and Privacy Research landscape in healthcare, building upon the foundational work of Ajit Apari and Johnson M.E (2008). Conducting an extensive literature review, embraced a multidisciplinary approach, synthesizing insights from information systems, health informatics, public health, medicine, and law. The investigation spans scholarly articles, reports, and reputable publications, aiming for inclusivity across diverse fields. Fig 1 visually represents the results, highlighting the wealth of information sourced from reliable outlets, contributing to a nuanced understanding of information security and privacy in healthcare.as depicted in Fig 1 below.

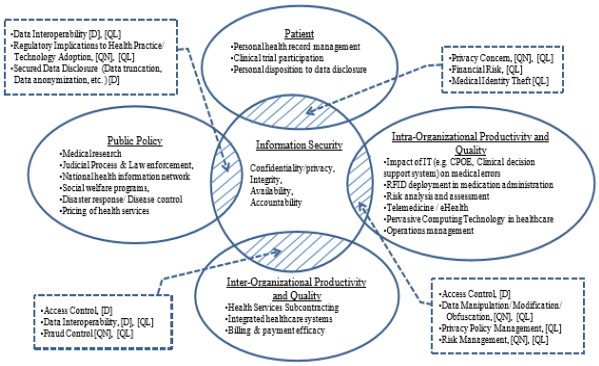

Fig 1: Research domains in Healthcare Information Security and Privacy, Ajit Apari and Johnson M.E (2008)

This study holds particular significance within the Inter-organizational Productivity and Quality category, with a specific focus on the realm of healthcare services subcontracting. The intentional placement within this category, as depicted in Fig 1, reflects a thoughtful decision by the researcher. This strategic alignment precisely aligns with the study objective and parameters, emphasizing a resonance with the intricacies of healthcare services sub contraction.

4. Overview of Kenyan Health Sector

The healthcare landscape in Kenya is characterized by a diverse structure that includes the Ministry of Health (MoH), parastatals, and county government authorities. The sector further covers privatized entities, specifically Faith-Based (FB) facilities and Non-Governmental

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

Organizations (NGOs). Notably, the public sector holds a majority share, accounting for approximately 60%, while the remaining 40% is distributed among Faith-Based institutions and NGOs, as reported by the Ministry of Health Performance Status Reports in 2003 and 2004. This multi-layered composition underscores the collaborative and multi-stakeholder nature of healthcare delivery in Kenya, reflecting a dynamic interplay between governmental bodies, private organizations, and non-profit entities in the pursuit of comprehensive healthcare services.

5. Available Kenyan Ministry Of Health (Moh) Frameworks

5.1 Kenya's Healthcare Information Systems Interoperable frameworks

In response to the global push for enhanced data quality to achieve the United Nations' Sustainable Development Goals (SDGs) and the ambitious Five-Year Big 4 Agenda (2018-2022) in Kenya, the government recognized the pivotal role of Information and Communication Technology (ICT) in healthcare transformation. The Ministry of Health (MoH) spearheaded a vision for patient-centric healthcare service delivery, emphasizing the need for quality and secure health data exchange. This vision aligned with the broader eHealth landscape, aiming for seamless, frictionless, and timely sharing of health information to support informed decision-making and achieve Universal Health Coverage (UHC).

5.2 Kenya National eHealth Policy framework (2016-2030)

To continue transforming Healthcare, Kenyan Ministry of Health (MoH) launched the Kenya National eHealth Policy (2016-2030) to elevate healthcare standards by strategically incorporating and utilizing Information and Communication Technology (ICT). Recognizing shared challenges in healthcare delivery, both in developed and developing nations, the focus on eHealth emerges as a crucial solution to overcome obstacles. This innovative approach utilizes ICT infrastructure to facilitate seamless and efficient healthcare service delivery. Despite the creation of eHealth interventions in sub-Saharan Africa, a joint survey by the World Health Organization (WHO) and the International Telecommunication Union (ITU) in 2014 revealed that many initiatives remained confined to weak platforms, hindering their transformative impact on the ground.

While the already existing frameworks hold significance in the healthcare sector, a notable gap exists in addressing the complex landscape of Teaching and Referral Hospitals and their interconnected allied facilities, specifically in terms of security, privacy, and governance within Electronic Health Care Systems (EHCS). The MoH/KHIS2 framework primarily concentrates on external systems and stakeholders, neglecting crucial concerns regarding patients' security and privacy, particularly in the distributed clinical environments. Similarly, the available Framework for eHealth Policy comprehensively addresses general challenges but falls short in catering specifically to clinical placements, where EHCS utilization poses patient-centric issues. Both frameworks overlook these critical facets, urging an urgent revisit and protection by the Ministry of Health at both national and county levels.

The need is emphasized to confront multilayered security and privacy challenges in distributed clinical environments, ensuring a truly comprehensive and patient-sensitive healthcare landscape. It was therefore concluded that security and privacy of patients' health data are global concerns, with increasing emphasis on safeguarding health records from intrusion, unauthorized use, corruption, damage, theft, and fraud. Research addressing inter-organizational issues like health services subcontracting, inter-organizational health network development, and EDI adoption reveals security and privacy challenges such as access control, data interoperability, network security, and fraud control. In Kenya, the healthcare sector's policy frameworks primarily address national challenges, overlooking specific concerns in clinical placements where healthcare is delivered. This gap, particularly in multilayered security and privacy challenges, poses a significant concern for patients. The literature also highlights an electronic information security lapse within main health facilities and allied industries, intensifying worries about patient information security and privacy.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

6. Vii. Materials and Methods

The researcher conducted a descriptive cross-sectional study to identify security challenges in patients' electronic medical data at Jaramogi Oginga Odinga Teaching and Referral Hospital (JOOTRH) and its allied healthcare facilities in Kisumu County, Kenya. The study encompassed over five million patients across ten counties in Western Kenya. Data was collected using structured questionnaires, interviews, and document analysis, targeting EHCS users and various professionals. Key informant interviews (KII) provided in-depth insights. The research, involved 50 respondents and covered administrators, IT assistants, doctors, nurses, and other staff, employed statistical tools like SPSS and Excel. It focused on operational challenges, threats, data breaches, reporting, and technical-managerial challenges during EHCS implementation.

7. Results

Data Presentation and Analysis - The response rate was within the expected threshold. Out of the 50 questionnaires administered, only 46 questionnaires were returned. This represented 92% response rate. Forty-four of the administered questionnaires were used in the analysis because they were completely filled representing 88%. Two which is 4% of the returned questionnaires were not completely filled and were therefore removed.

Demographic Statistics - The following is a summary of the facilities and their respondents' demographic statistics. Four (4) Medical officers (Doctors) representing 9.1%, four (4) clinical officers representing 9.1%, six (6) Nurses representing 13.6%, three (3) Administrative clerks at 6.8%, I.T officers/Assistants at 11.4% Pharm Tech at 3%, eight (8) Lab Technicians at 18.2% , eleven (11) Affected/Patients at 25.0%. This therefore totaled to 100%

The research revealed that 22.7% of respondents were in laboratory services, 18.2% were patients and outpatients each, 11.4% in ICT, 6.8% in pharmacy, and 4.5% in other departments. Only 2.3% served in counseling services. The distribution covered various sections at the main hospital (JOOTRH) and allied Healthcare Facilities.

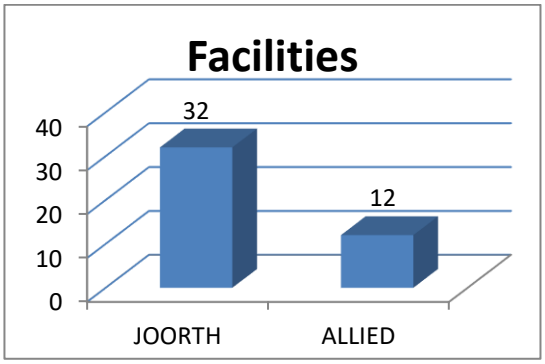

Fig 2: Facility composition

The respondents were drawn from various departments of the main hospital and the allied facilities. These included: ICT Department; Hospital Administration; Pharmacy; ICU/Isolation; Accident and Emergency; ICU/Renal; Casualty; Records Department; Pediatrics; Out-Patient; In-Patient; Female Surgical Ward; Male Surgical Ward; Barrack Obama Children Ward; Laboratory; Road Transport Accidents (RTA) patients; and Patients (the affected)

Allied Healthcare Composition - The composition of the allied Healthcare facilities were the Regional Blood Transfusion Center for western Kenya (Blood Bank), Path Care Laboratory diagnostics Ltd, VCT/ Counseling facility, West Kenya Diagnostics, Lake Pharmacy and KEMRI C.D.C.

The study assessed ICT and medical tools in the main hospital and allied facilities to enhance the security and privacy framework for Electronic Healthcare Systems (EHCS). The availability and scope of these tools are summarized in the table below.

Table I: ICT equipment and medical technologies/tools

	Connected Medical Devices	Desktop	Laptop	PDAs	Smart Phone	iPad	Tablet Pc	Printers
0-5	28 (63.6%)	15(34.1%)	24(54.5%)	36(81.8%)	24(54.5%)	34(77.3%)	29(65.9%)	24(54.4%)
6-15	4 (9.1%)	12(27.3%)	5 (11.4%)	3(6.8%)	6(13.6%)	3(6.8%)	7(15.9%)	4(9.1%)
16-25	5 (11.4)	1(2.3%)	5 (11.4%)	2(4.5%)	0	3(6.8%)	3(6.8%)	2(4.5%)
26-35	1 (2.3%)	3(6.8%)	3(6.8%)	1(2.3%)	2(4.5%)	2(4.5%)	1(2.3%)	2(4.5%)
36-45	0	2(4.5%)	3 (6.8%)	1(2.3%)	3(6.8%)	2(4.5%)	3(6.8%)	3(6.8%)
Above 45	6 (13.3%)	11(25%)	4(9.1%)	1(2.3%)	9(20.5%)	0	1(2.3%)	9(20.5%)
Total	44(100%)	44 (100%)	44 (100%)	44(100%)	44(100%)	44(100%)	44(100%)	44(100%)

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

The main hospital and allied healthcare departments predominantly used connected medical devices, desktops, laptops, PDAs, smartphones, iPads, tablets, and printers. Most departments had 0-5 devices, with desktop computers being the most utilized, especially in 25% of the departments with over 45 units. All departments had a minimum of four ICT tools.

The study aimed to address security and privacy challenges in EHCS, developing a framework for secure healthcare services in interoperable environments. The study covered operational challenges, threats, data breaches, reporting, and technical-managerial issues during EHCS implementation, with results presented accordingly.

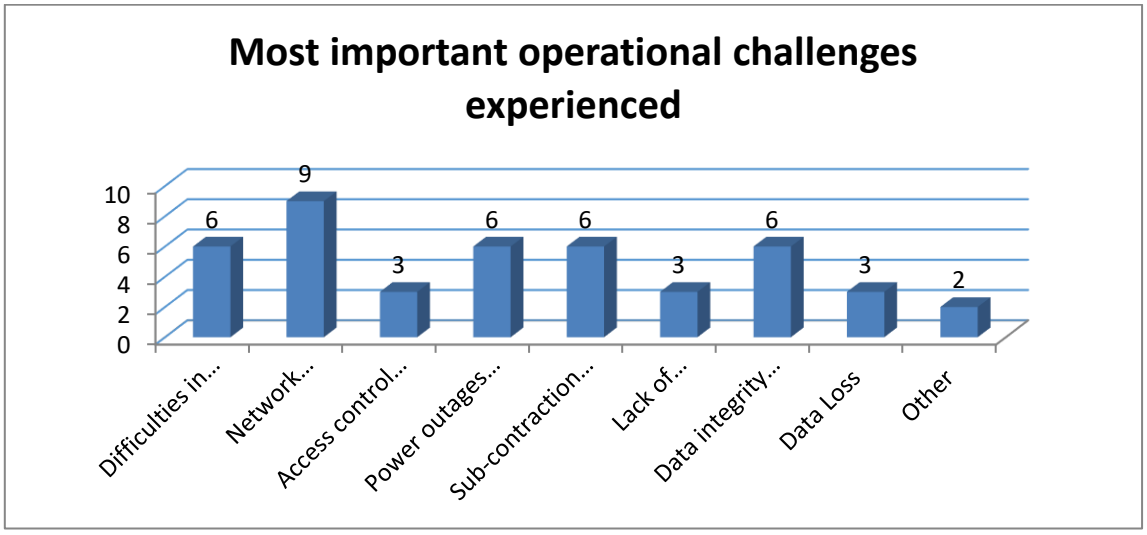

Fig 3: Most important operational challenges experienced

Out of 44 respondents, 20.7% cited network breakdown/wiretapping and security as major operational challenges. Power outages/system unavailability were reported by 13.6%, while 6.8% mentioned difficulties in access control, authentication, lack of interoperability, and data loss each.

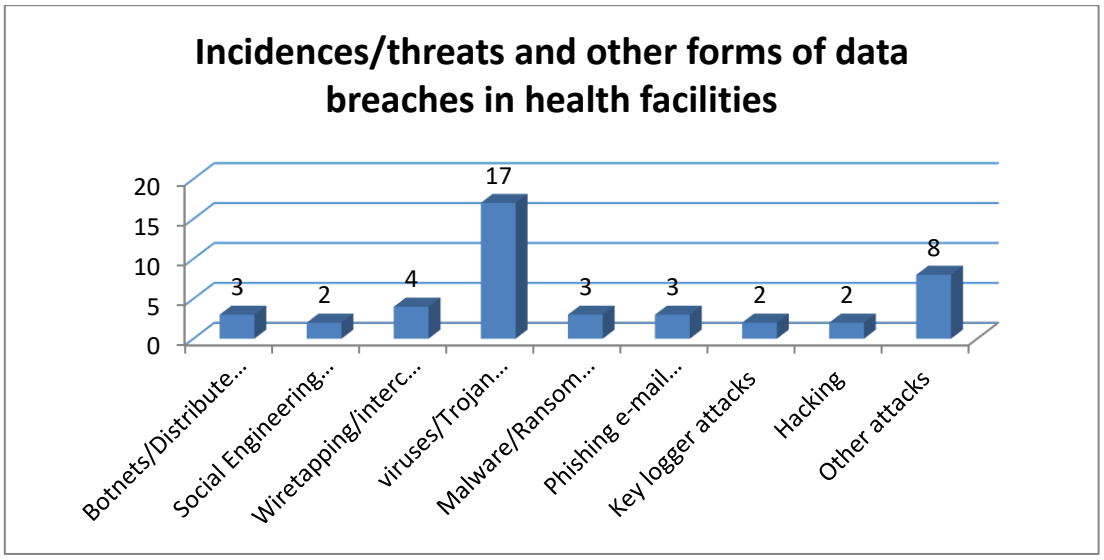

Fig 4: Incidences/threats and other forms of data breaches in the health facilities

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

Out of 44 respondents, 38.9% identified computer viruses as the main threat, while 18.1% faced other attacks. Wiretapping was reported by 9.1%, and 6.8% faced phishing emails, botnets, and malware attacks. Social engineering, fraud, key logger attacks, and hacking were each reported by 4.5%. Computer viruses were the predominant threat.

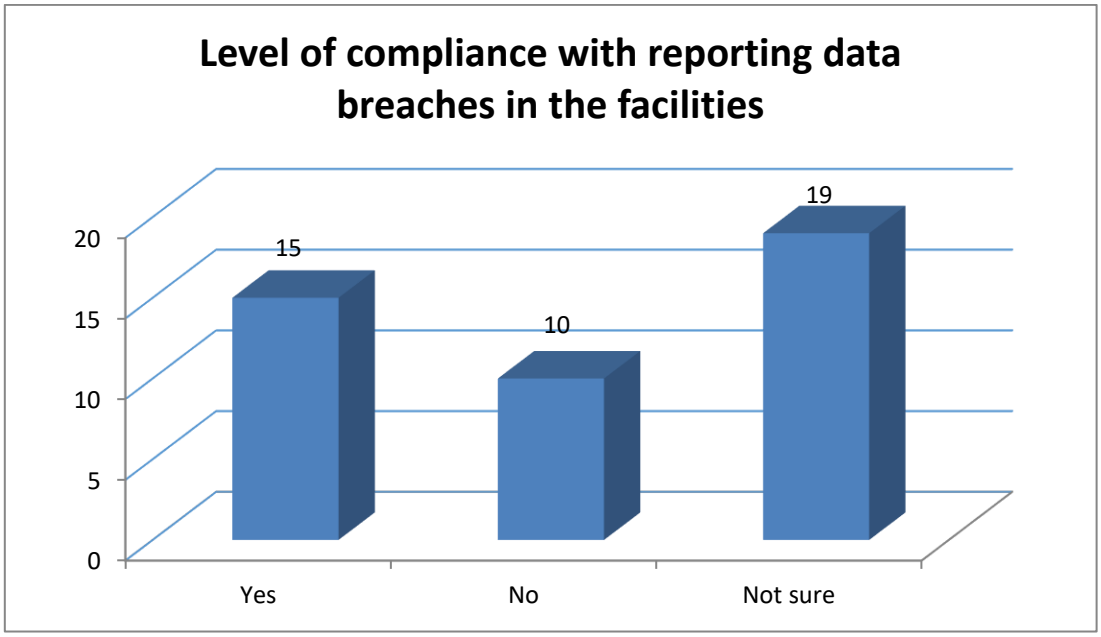

Fig 5: Level of compliance with reporting data breaches in the facilities

Out of the 44 respondents, 34.1% agreed that they do report data breaches and attacks to the support team, 43.2% were not sure and 22.7% noted that they did not report.

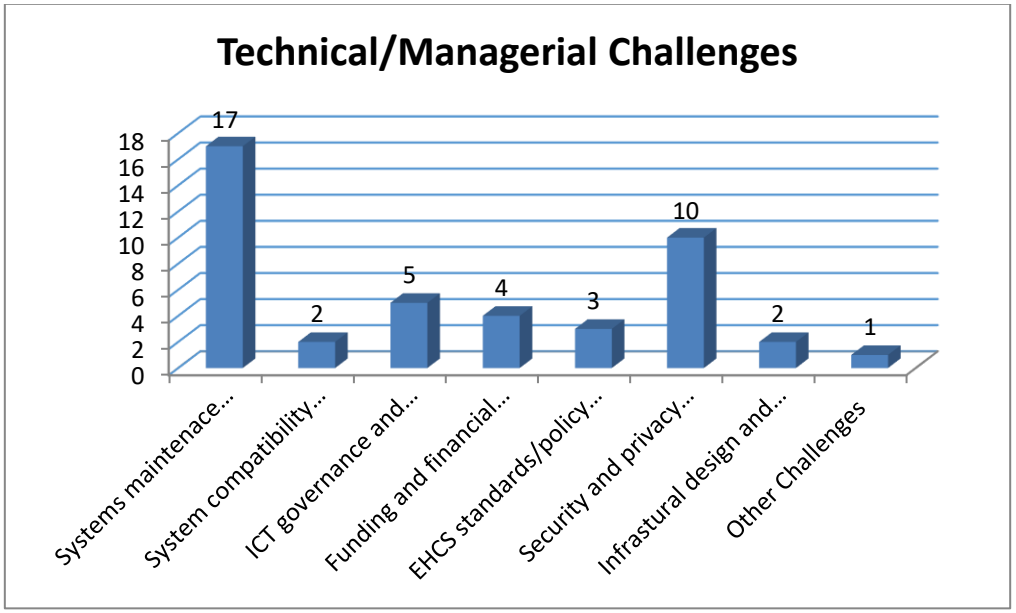

Fig 6: Technical/managerial challenges being experienced

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

Out of 44 respondents, 38.7% faced system maintenance challenges, 22.7% encountered security and privacy framework challenges, and 11.4% dealt with ICT governance and strategy challenges. Funding and financial support challenges were reported by 9.1%, EHCS standards ambiguity/absence by 6.8%, while system compatibility and infrastructural design challenges were faced by 4.5% each. Other challenges were experienced by 2.3%.

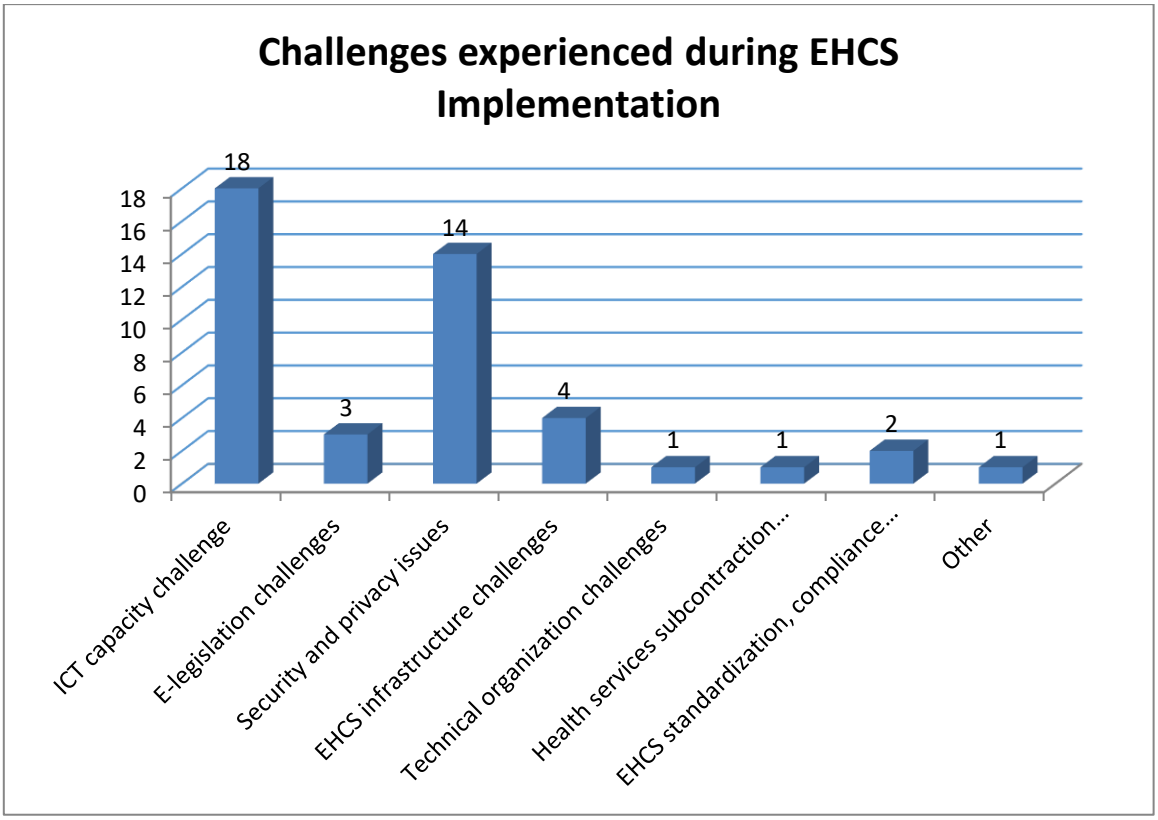

Fig 7: Challenges experienced during EHCS Implementation

Out of 44 respondents, 40.9% faced ICT capacity challenges during EHCS implementation, while 31.8% encountered security and privacy issues. EHCS infrastructure challenges were reported by 9.1%, E-legislation challenges by 6.8%, and EHCS standardization challenges by 4.5%. Health services sub-contraction and technical organization challenges each affected 2.3%. To address these issues comprehensively, the study initiated the development of an enhanced Security and Privacy framework in Electronic Health Care Systems (EHCS).

The researcher precisely examined existing EHCS infrastructures at the main hospital (JOOTRH) and allied facilities to identify vulnerabilities and enhance security measures. The goal was to protect patient data, ensuring confidentiality and fostering trust between healthcare providers and patients. This contribution aligns with the increasing importance of data security and privacy in healthcare, promoting responsible and ethical technology use for improved patient care.

8. Existing EHCS framework Between JOOTRH and its Allied Facilities

The figure below outlines the framework developed through intensive Key Informant Interviews, involving researchers, administrations, I.T teams, and healthcare personnel at JOOTRH and allied facilities.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

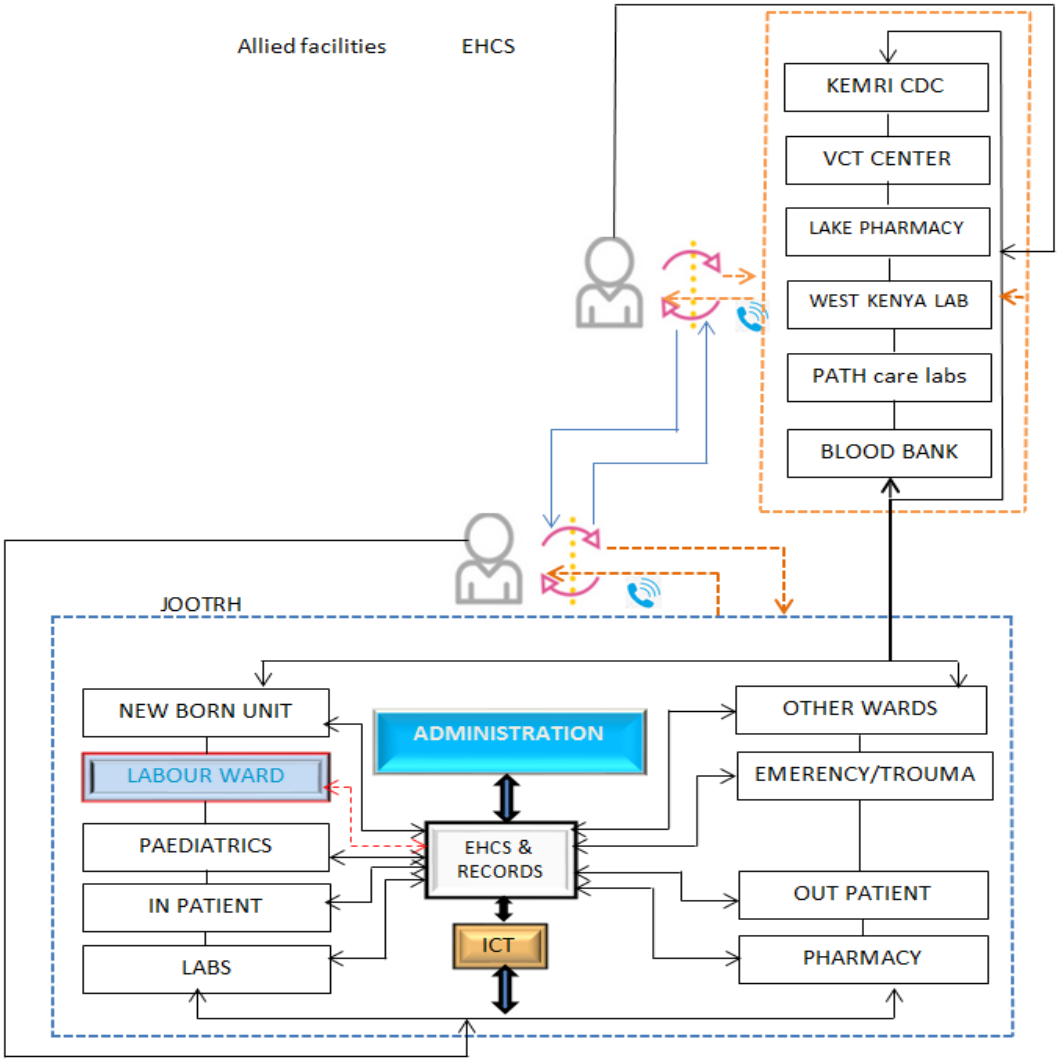

Fig 8: Current EHCS framework between JOOTRH and its allied facilities

The above framework in fig 8 supported interoperable clinical environments between JOOTRH and allied healthcare facilities but revealed critical gaps, necessitating an enhanced Security and Privacy framework for EHCS. Identified challenges include isolated EHCS sections, interoperability issues causing delays in healthcare service delivery, reliance on insecure communication methods leading to security and privacy concerns, misinterpretation of information impacting patient safety, confusion in prioritizing emergencies, lack of a centralized database hindering data synchronization, network connectivity issues affecting data exchange, and a lack of governance standards creating regulatory gaps.

To address these, the researcher proposes an alternative framework focusing on standardized governance, interoperability, and secure patient information exchange to enhance patient safety, healthcare delivery, and protect sensitive information across JOOTRH and its allied facilities.

9. Enhanced Security and Privacy Framework Developed for EHCS

The figure below is an enhanced Security and Privacy framework for Electronic Health Care Systems (EHCS), aiming to address interoperability gaps, enhance information security and privacy, and serve as a model for a regulatory authority, ensuring patients' safety and confidence in quality healthcare outcomes.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

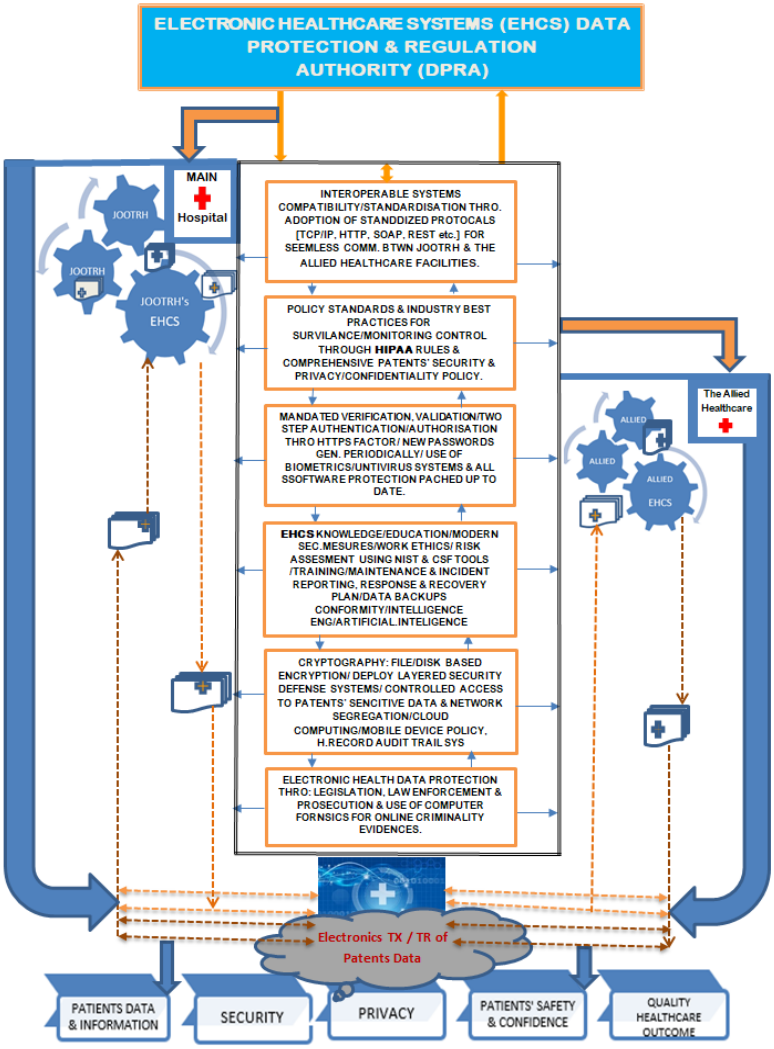

Fig 9: Enhanced Security and Privacy Framework in EHCS

Components of the above framework are as follows:

9.1 Framework's Interoperable Environments

The framework represents interoperable environments with JOOTRH as the Main Hospital and its allied facilities, including the Blood Bank, Path Care Laboratory, VCT/Counseling, West Kenya Diagnosis Lab, Lake Pharmaceutical, and KEMRI CDC.

9.2 Framework's Healthcare Data Transmission Channels

The framework's data transmission channels, represented by dotted arrow lines and a cloud symbol, utilize physical mediums like wires/cables, and broadcast waves for health data transmission.4.4.4 Framework's Security Measures.

These are *technical security measures for Interoperable Systems Compatibility.* They would constitute technical controls for deployment on medical devices and network levels. Under this, adoption of standardized protocols such TCP/IP, HTTP, SOAP and REST to aid seamless communication and to ease interoperability issues arising in the infrastructures between healthcare facilities would take place.

Policy Standards to protect the rights of patients adopted include Health Insurance Policy and Accountability Act (HIPAA) of 1996; Personnel Mobile Device Management Policy to govern how portals or mobile devices would be used within healthcare facilities.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

*Layered Security Defense System***,** deployment would constitute numerous forms of security apparatus and procedures composed of firewalls, malware scanners, intrusion detection Systems (IDS), and integrity auditing procedures, local storage encryption tools; Security Socket Layers/Transport Layer Security SSL/TLS, and Internet Protocol Security IPsec.

Standards for Web Services Security here are eXtensible Markup Language XML Digital Signatures, XML Encryption e.g. WS-Sec, SAML (Secure Assertion Markup Language) and XACML(Extensible Access Control Markup Language), to make the framework water proof; Antivirus software to guard against infection by malicious codes such as Viruses, worms, Trojan horses, Spyware and Ransomware.

Network Segregation/Cloud Computing Strategies which would be used to isolate and/or backup very critical network segments.

Cryptography for information security with associated subjects of encryption, decryption, authentication and other applications such as access controls on healthcare data and information from attackers.

Operational Controls measures, which would take care of employee training and awareness programs on the value and criticality of patients and their information to operationalize, and to reinforce incidence reporting system, through data recovery plan for business continuity, data back-up devices/drives and connected medical devises and physical protection using security guards, bugler proofing, Close Circuit Television (CCTV) and Alarm systems.

Forensic Computing involving - activities and behaviors for conservancy, identification, extraction, documentation and interpretation of healthcare data in EHCS where computer(s) and related IoT medical connected devices might have been used.

Access control and Authentications, - which make use of passwords, biometric systems for healthcare personnel's personal bio features.

Risk assessments and Management, - which are the apparatus for strengthening investigation of the likelihood of potential security incidences, and attacks within organizations' Network infrastructure.

National Institute of Standards and Technology (NIST) framework, the best current measures for Cyber security assessment tools to provide procedures necessary for better management and reduction in security threats and incidences targeting EHCS, and enhance communication and awareness of risks between the interoperable environments' response and Recovery and *Cyber Security Framework (CSF)* for frequent monitoring to carry out assessment and give feed-back on the threat incidences in the interoperable environment for counter measure.

Other modern security measures included in the developed framework include tools like the *Zero-Trust Environment and software-defined Perimeter*, combined to blind fold Ransomware attackers, Next generation security measures e.g. *Endpoint Detection and Response (EDR)* which is an intelligent anti-virus that have Extended Detection and Response (XDR) ties in EDR data that would have greater conspicuousness in revealing activities within interoperable environments and *Human Firewall.*

Intelligence Engineering, which is based on the innovative and related challenges in healthcare facilities; *Legal Pursuit measure involving* Legislative instruments, Law enforcement agency and Judiciary/Prosecution to respond to the emerging online criminal conducts, targeting healthcare facilities.

9.3 EHCS framework's Data Protection and Regulatory Authority (DPRA)

Electronic healthcare data breaches are widespread than ever before because criminals are trying much to capture healthcare data. In view of this landscape, patients' information is at higher risks compared to information from other sectors. This is the top most part of the developed framework. EHCS framework's Data Protection and Regulatory Authority would be a protection and regulatory authority body that would propose a legislation to push for a specific bill in Parliament for EHCS infrastructure protection as a critical infrastructure.

9.4 EHCS' developed framework product outcome.

The last component of the framework is EHCS' developed framework outcome presented at the bottom end part of the framework represents the product, and answers or solutions to this study where significant

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

security and privacy safeguards on EHCS administration would be achieved. With this, the framework would be able to deliver Security and Privacy leading to Patients' Safety, Confidence and Quality Healthcare Outcome.

10. Discussion of Results

Operational challenges in Electronic Healthcare Systems (EHCS) at JOOTRH and its allied facilities, as per figure 3, include network breakdowns (20.7%), power outages (13.6%), and healthcare subcontracting linkage issues. System unavailability poses risks to patient care, and power outages, prevalent in sub-Saharan Africa, contribute to EHCS downtime. Addressing these challenges is crucial for secure and continuous healthcare operations. EHCS systems face unavailability due to online threats like hacking and DDOS attacks.

These attacks involve flooding EHCS infrastructure with spoofed packets, seizing control, and disrupting critical healthcare operations. DDOS attacks, detailed by Omogah (2020), can result in total EHCS unavailability during medical procedures. Countermeasures involve router-level packet filtering and tools like ping broadcast, Smurf, synk4, macf, and sky dance to manage traffic. Insider threats from errors or intentional protocol violations also contribute to system unavailability.

Health data integrity is vital for patient well-being, ensuring quality in healthcare operations. Data errors, particularly at entry points, compromise integrity during capture, processing, storage, and exchange. The life of each patient hinges on data integrity. Automation in healthcare, facilitated by EHCS, consolidates vast patient information, escalating risks if not properly governed. Poor implementation malfunctions, or mishandling during operations can lead to data loss and associated threats. Faults in software, hardware, networks, security attacks, and natural disasters further contribute to potential data loss.

Automating healthcare for better outcomes necessitates secure communication of lab test results. However, EHCS advancements within interoperable environments pose efficiency challenges due to varying data presentation methods. This hinders workflow, fostering a misconception that technology complicates diagnostics. Communication difficulties can lead to missed lab tests, adversely affecting patient management. Key Informants reveal manual result exchange during communication challenges, posing additional vulnerabilities.

The study underscores the importance of interoperable environments in Electronic Healthcare Systems (EHCS), connecting main hospital JOOTRH to its allied facilities. These interconnected infrastructures encompass diverse technologies for processing, storing, and exchanging clinical data, emphasizing secure operations and timely services. Incompatibility issues, such as varying operating system versions or outdated software, hinder interoperability, raising security and privacy concerns. The inability to obtain update patches during data exchange exacerbates these challenges, emphasizing the need for standardized technologies across healthcare facilities.

The study highlights challenges in healthcare subcontracting, driven by hospitals' urgent needs for critical patient management procedures. When first-line treatments, like lab tests or diagnostics, can't be conducted in the main hospital, referrals initiate the movement of patients and their data between the main hospital and allied facilities, necessitating electronic data sharing across multiple systems, which ideally should be managed within the main hospital. The study identifies technical challenges where the technology used may not meet security and privacy thresholds for patients' information exchange. Electronic sharing of patients' data, especially when linked to the public network, raises concerns about identifying individuals in the infrastructure. Insider and outsider threats, including malice, revenge, sabotage, curiosity, and politics, pose significant risks to patients' information security in healthcare subcontracting linkages.

The study's data on threats and data breaches in health facilities revealed that, among 44 respondents, 38.9% faced major threats from computer viruses, followed by 18.1% experiencing other attacks. Wiretapping, phishing emails, botnets, and malware attacks were reported at 9.1%, while social engineering, fraud attacks, key logger attacks, and hacking each constituted 4.5%. Computer viruses were identified as the primary threat, prevalent across healthcare organizations, leading to malicious code attacks that

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

could modify patients' data, potentially causing clinical mismanagement. The study revealed that "other attacks" at 18.1% occurred after computer viruses at 38.9%, surprising the researcher. These were undocumented data breaches, likely resulting from insider threats involving negligence from EHCS users or malicious healthcare personnel activities. To explore further, the researchers conducted Key Informant Interviews with IT teams and healthcare personnel to investigate the causes of these "other attacks."

The study explored weaknesses in the EHCS framework between JOOTRH and its allied facilities, revealing a notable factor contributing to "other attacks" at 18.1%: the unreliable connection between EHCS and the subsequent fallback on telephone communications. This reliance on telephone communication introduced vulnerabilities, potentially weakening the security and privacy of patients' information and contributing to the observed increase in "other attacks."

The study identifies wiretapping or Interruption Attacks as potential outcomes of Distributed Denial of Service (DDOS) attacks on EHCS. These attacks involve flooding systems with spoofed packets, leading to EHCS unavailability. Additionally, Botnet Attacks, associated with DDOS attacks, utilize malware-infested bot armies controlled by criminals. Social engineering, a manipulative technique, poses a threat by convincing healthcare personnel to share login credentials, potentially resulting in damage, loss, or theft of critical patient and facility information within the EHCS. Phishing, a form of social engineering, involves fraudulent emails enticing healthcare workers to open links and provide EHCS login credentials, posing a potential disaster for main hospitals and allied facilities. Training and awareness initiatives can mitigate this risk. Key logger attacks involve capturing keyboard inputs, possibly leading to unauthorized access and data capture. Hacking, often initiated through identifying EHCS vulnerabilities, poses severe threats, ranging from fraud to clinical risks that can compromise healthcare delivery services. Examples include password cracking algorithms and exploiting social engineering for unauthorized access.

Analysis and presentation, data reveals that 34.1% of respondents report data breaches to support teams, 43.2% are unsure, and 22.7% do not report. Underreporting may stem from a lack of reporting knowledge, absence of established mechanisms, or fear of repercussions on an organization's image. Reporting incidents is crucial for planning and enhancing patients' information security. EHCS technical/managerial challenges include 38.7% facing system maintenance issues, 22.7% grappling with security and privacy framework challenges, 11.4% encountering ICT governance and strategy challenges, 9.1% experiencing funding obstacles, and 6.8% dealing with EHCS standards ambiguity. System maintenance is pivotal for EHCS effectiveness and requires sustained investment for long-term healthcare benefits, ensuring uninterrupted facility operations.

Healthcare facilities in Kenya face funding challenges due to donor fatigue caused by mismanagement and corruption in the healthcare sector. With the devolution of government functions to 47 counties under the 2010 constitution, healthcare funding and management lack proper policies. Figure 22 reveals that during EHCS implementation, 40.9% faced ICT capacity challenges, 31.8% encountered security and privacy issues, and 9.1% dealt with EHCS infrastructure challenges. Implementation challenges can hinder EHCS functionality, risking patients' lives and healthcare operations. Financial constraints and devolution exacerbate the difficulties, impacting the quality and sustainability of EHCS in public healthcare facilities. During systems implementation, challenges arise from ICT capacity issues, such as inadequate technical skills among IT personnel for customizing equipment and aligning it with electronic healthcare devices.

Additional difficulties included health data migration problems, interoperability challenges, knowledge gaps among IT and healthcare personnel, resistance to change from healthcare staff, and a lack of alignment between IT equipment and healthcare services. Moreover, insufficient knowledge and laws about system documentation from vendors and developers can pose obstacles, impacting the smooth implementation and subsequent daily healthcare service delivery. Underdeveloped IT infrastructures at JOOTRH and its allied facilities hinder EHCS implementation, causing disparities and interoperability issues among critical devices. Weaknesses stem from EHCS unreliability during data transmission and challenges at healthcare services sub-contracting levels, including insufficient

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

capacity for secure communication, lack of EHCS standardization, interoperable environments issues, and inconsistencies between EHCS used across facilities.

11. Conclusion

This study identifies critical challenges in the Electronic Health Communication System (EHCS) at Jaramogi Oginga Odinga Teaching and Referral Hospital (JOOTRH) and proposes comprehensive recommendations to enhance security, privacy, and overall functionality. The reported challenges encompass both operational and technical managerial aspects, including network breakdowns, security issues, power outages, and data breaches. Noteworthy operational challenges involve healthcare sub-contracting, data integrity issues, and difficulties in communication, alongside unidentified issues hindering EHCS operations. The study underscores the significance of addressing undocumented breaches, primarily attributed to insider threats arising from negligence and malicious activities by healthcare personnel.

Technical managerial challenges further highlight neglect in EHCS maintenance, security and privacy framework issues, insufficient ICT governance, funding gaps, ambiguous standards, compatibility issues, and infrastructural design challenges. The study reveals that the major threats and data breaches include computer viruses, unidentified threats, wiretapping, e-mail phishing, and malware, with social engineering, fraud attacks, key logger attacks, and hacking constituting a smaller proportion.

An in-depth investigation, utilizing K.I.I, pinpoints the root causes of unknown threats to weaknesses in the existing infrastructure connecting JOOTRH and allied facilities. Critical factors contributing to these threats include EHCS unreliability, lack of integration, absence of standardization, no centralized database, network traffic, connectivity issues, and inadequate governance and oversight. The absence of clear oversight exposes EHCS to vulnerabilities, particularly in terms of security, privacy, and compliance with data breach reporting.

12. Recommendations

The researcher advocates a comprehensive strategy to address challenges in the Electronic Health Communication System (EHCS) at JOOTRH and affiliated facilities. A pivotal recommendation is the development and implementation of enhanced security and privacy frameworks through the proposed Electronic Healthcare (EHCS) Data Protection and Regulation Authority (DPRA) Framework. This initiative aims to bolster the security and privacy of patients' information, providing a robust foundation for reliable healthcare data management.

Operational challenges necessitate efforts to mitigate network breakdowns, enhance power reliability, and streamline communication protocols for lab test results and diagnoses. Tackling technical managerial challenges involves prioritizing EHCS maintenance, reinforcing security and privacy frameworks, and ensuring effective ICT governance. Adequate funding, clarification of EHCS standards, and addressing compatibility issues and infrastructural design challenges are imperative.

Major threats and data breaches prompt a focus on Cybersecurity measures, safeguarding against computer viruses, mitigating unknown threats, and countering wiretapping, email phishing, and malware. Special attention is given to social engineering, fraud attacks, key logger attacks, and hacking, despite constituting a lesser proportion of threats.

The root cause analysis emphasizes addressing EHCS unreliability, fostering integration, standardizing protocols, establishing a centralized database, and resolving network traffic and connectivity issues. Proper governance and oversight are crucial aspects to monitor EHCS performance and security comprehensively.

To enhance EHCS implementation, a comprehensive strategy proposes solutions for ICT capacity challenges, security and privacy concerns, infrastructure issues, legislative challenges, standardization discrepancies, sub-contracted health services, and technical organizational challenges. Establishing reporting protocols for data breaches is imperative to ensure transparency and accountability, addressing the current uncertainty and lack of reporting among respondents.

In conclusion, the recommended measures collectively aim to fortify EHCS, ensuring a seamless, secure, and privacy-focused healthcare data management system.

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

The proposed Electronic Healthcare DPRA Framework stands as a pivotal tool, promising improved patient safety, confidentiality, and overall healthcare outcomes.

References:

[1] Agrawal, R., Evfimievski, A. and Srikant, R. (2003) 'Information sharing across private databases', Proceedings of ACM SIGMOD, San Diego, CA, pp. 86–97.

[2] Ajuwon, G. A. (2003). BMC Medical Informatics and Computer and internet use by first year clinical and nursing students in a Nigerian teaching hospital. BMC Medical Informatics and Decision Making, 7, 1–7.

[3] Alberts, C. & Dorofee, A. (2003) Managing Information Security Risks: The OCTAVE Approach. New York: Addison Wesley.

[4] Anderson, R.J. (1996). Security in Clinical Information Systems. University of Cambridge.

[5] Anderson, R. (2008). Connecting for health. The British journal of general practice: the journal of the Royal College of General Practitioners, 58(549), 279–280. https://doi.org/10.3399/bjgp08X279823

[6] Anderson, R., Brown, I., Dowty, T., Inglesant, P., Heath, W. and Sasse, A. (2009). Database State. Joseph Rowntree Reform Trust, York.

[7] Angst, C.M., Agarwal, R., & Downing, J. (2006). An Empirical Examination of the Importance of Defining the PHR for Research and for Practice.

[8] Angst, Corey & Agarwal, Ritu & Downing, Janelle. (2006). An Empirical Examination of the Importance of Defining the PHR for Research and for Practice. SSRN Electronic Journal. 10.2139/ssrn.904611.

[9] Antón, A.I., Earp, J.B., Vail, M.W., Jain, N., Gheen, C.M., & Frink, J.M. (2007). HIPAA's Effect on Web Site Privacy Policies. IEEE Security & Privacy, 5.

[10] Appari, A., & Johnson, M. E. (2008). Information security and privacy in healthcare: current state of research. Center for Digital Strategies, Tuck School of business Dartmouth College.

[11] Appari, A., & Johnson, M. E. (2010). Information security and privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management, 6(4), 279. https://doi.org/10.1504/ijiem.2010.035624

[12] Appari, A., & Johnson, M. E. (2018). Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management, 9(1), 1-24.

[13] Appelbaum, P. S. (2002). Privacy in psychiatric treatment: threats and responses. American Journal of Psychiatry, 159(11), 1809-1818.

[14] Ayala, L. (2016). Cybersecurity for hospitals and healthcare facilities. Berkeley, CA.

[15] Baker, W.H., Rees, L.P., & Tippett, P.S. (2007). Necessary measures: metric-driven information security risk assessment and decision making. Commun. ACM, 50, 101-106.

[16] Ball, E., Chadwick, D.W., & Mundy, D.P. (2003). Patient Privacy in Electronic Prescription Transfer. IEEE Secur. Priv., 1, 77-80.

[17] Ball, M. J., & Gold, J. (2006). Banking on health: Personal records and information exchange. Journal of healthcare information management: JHIM, 20(2), 71–83.

[18] Bansal, G., Zahedi, F. & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. Decision Support Systems. 49. 138-150. 10.1016/j.dss.2010.01.010.

[19] Baumer, D.L., Earp, J.B., & Payton, F.C. (2000). Privacy of medical records: IT implications of HIPAA. SIGCAS Comput. Soc., 30, 40-47.

[20] Behlen, F. M., & Johnson, S. B. (1999). Multicenter patient records research: security policies and tools. Journal of the American Medical Informatics Association: JAMIA, 6(6), 435–443. https://doi.org/10.1136/jamia.1999.0060435

[21] Botkin J. (2001). Protecting the privacy of family members in survey and pedigree

research. JAMA, 285(2), 207–211. https://doi.org/10.1001/jama.285.2.207

[22] Brailer D. J. (2005). Interoperability: the key to the future health care system. Health affairs (Project Hope), Suppl Web Exclusives, W5–W21. https://doi.org/10.1377/hlthaff.w5.19

[23] Bolin, J. N., & Clark, L. S. (2004). Avoiding charges of fraud and abuse: developing and implementing an effective compliance program. The Journal of nursing administration, 34(12), 546–550. https://doi.org/10.1097/00005110-200412000-00003

[24] Bhatti, R., & Grandison, T. (2007). Towards Improved Privacy Policy Coverage in Healthcare Using Policy Refinement. Secure Data Management.

[25] Bhatti R., Grandison T. (2007) Towards Improved Privacy Policy Coverage in Healthcare Using Policy Refinement. In: Jonker W., Petković M. (eds) Secure Data Management. SDM 2007. Lecture Notes in Computer Science, vol 4721. Springer, Berlin, Heidelberg

[26] Becker, D.J., Kessler, D., & McClellan, M.B. (2005). Detecting Medicare Abuse. Experimental & Empirical Studies eJournal.

[27] Baker, W. H., Rees, L. P., & Tippett, P. S. (2007). Necessary Measures: Metric-Driven Information Security Risk Assessment and Decision Making. Communications of the ACM, 50(10), 101–106. https://doi.org/10.1145/1290958.1290969

[28] Bansal, G., Gefen, D., & Zahedi, F. M. (2007). The Impact of Personal Dispositions on Privacy and Trust in Disclosing Health Information Online The Impact of Personal Dispositions on Privacy and Trust.

[29] Barrows, R. C., Jr, & Clayton, P. D. (1996). Privacy, confidentiality, and electronic medical records. Journal of the American Medical Informatics Association: JAMIA, 3(2), 139–148. https://doi.org/10.1136/jamia.1996.96236282

[30] Campbell, B., Thomson, H., Slater, J., Coward, C., Wyatt, K., & Sweeney, K. (2007). Extracting information from hospital records: what patients think about consent. Quality & safety in health care, 16(6), 404–408. https://doi.org/10.1136/qshc.2006.020313

[31] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. Communications of the ACM, 47(7), 87-92.

[32] Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9(1), 70-104.

[33] Choi, N., Kim, D., & Goo, J. (2006). Managerial Information Security Awareness' Impact on an Organization's Information Security Performance. AMCIS 2006 Proceedings, 406.

[34] Cilliers, L. (2020). Wearable devices in healthcare: Privacy and information security issues. Health information management journal, 49(2-3), 150-156.

[35] Coiera E. (1995). Recent Advances: Medical informatics. BMJ. 310. 1381 - 1387. 10.1136/bmj.310.6991.1381.

[36] Conaty-Buck, S. (2017). Cybersecurity and healthcare records. Am Nurse Today, 12(9), 62-64.

[37] Crevecoeur, T. (2021). Developing Culturally Specific, Patient-Centered Maternity Care Models for High-Risk Immigrant Populations: Recommendations from a Study of the Haitian Population at Boston Medical Center (Doctoral dissertation, Boston University).

[38] Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio- Organizational Perspectives. Information Systems Journal, 11(2), 127–153.

[39] Fakhri, D., & Mutijarsa, K. (2018, October). Secure IoT communication using blockchain technology. In 2018 international symposium on electronics and smart devices (ISESD) (pp. 1-6). IEEE.

[40] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. ángel O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. Journal of

Biomedical Informatics, 46(3), 541–562. https://doi.org/10.1016/j.jbi.2012.12.003

[41] Fernández-Luque, L., & Bau, T. (2015). Health and social media: perfect storm of information. Healthcare informatics research, 21(2), 67.

[42] Fisher, F., & Madge, B. (1996). Data security and patient confidentiality: the manager's role. International Journal of Biomedical Computing, 43(1–2), 115–119. https://doi.org/ 10.1016/S0020-7101(96)01236-6

[43] Fraser, H., Biondich, P., Moodley, D., Choi, S., Mamlin, B., & Szolovits, P. (2005). Implementing electronic medical record systems in developing countries. Journal of Innovations in Health Informatics, 13(2), 83–95. https://doi.org/10.14236/jhi.v13i2.585

[44] Gaylin, Daniel & Moiduddin, Adil & Mohamoud, Shamis & Lundeen, Katie & Kelly, Jennifer. (2011). Public Attitudes about Health Information Technology, and Its Relationship to Health Care Quality, Costs, and Privacy. Health services research. 46. 920-38. 10.1111/j.1475-6773.2010.01233. x.

[45] Grandison, T., & Bhatti, R. (2010). HIPAA compliance and patient privacy protection. In MEDINFO 2010 (pp. 884-888). IOS Press.

[46] Greenhalgh, T., Hinder, S., Stramer, K., Bratan, T., & Russell, J. (2010). Adoption, non-adoption, and abandonment of a personal electronic health record: case study of Health Space. BMJ (Clinical research ed.), 341, c5814. https://doi.org/10.1136/bmj.c5814

[47] Goldstein, Douglas E (2007). Medical informatics 20/20: quality and electronic health records through collaboration, open solutions, and innovation. Jones and Bartlett Publishers, Sudbury, Mass

[48] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, 100059.

[49] Hasan, R., and Yurcik, W. (2006). A Statistical Analysis of Disclosed Storage Security Breaches. ACM Workshop on Storage Security and Survivability.

[50] Haux R. (2006). Health information systems - past, present, future. International journal of medical informatics, 75(3-4), 268–281. https://doi.org/10.1016/j.ijmedinf.2005.08.002

[51] Haux R. (2006). Individualization, globalization and health--about sustainable information technologies and the aim of medical informatics. Int J Med Inform,75(12):795-808. doi: 10.1016/j. ijmedinf.2006.05.045

[52] Häyrinen, K., Saranto, K., & Nykänen, P. (2008). Definition, structure, content, use and impacts of electronic health records: a review of the research literature. International journal of medical informatics, 77(5), 291–304. https://doi.org/10.1016/j.ijmedinf.2007.09.001

[53] Healey, N. M. (2008). Is higher education in really 'internationalizing'?. Higher education, 55, 333-355. Hevner, A., March, S.T., Park, J., and Ram, S. (2004). Design Science Research in Information Systems. MIS Quarterly, MIS Quarte(1), 75–106.

[54] Jayawardena, A. (2013). A systematic literature review of Security, Privacy and Confidentiality of information in Electronic Health Information Systems. Sri Lanka Journal of Bio-Medical Informatics. 4. 10.4038/sljbmi.v4i2.5740.

[55] Jha, A. K., DesRoches, C. M., Campbell, E. G., Donelan, K., Rao, S. R., Ferris, T. G., Shields, A., Rosenbaum, S., & Blumenthal, D. (2009). hospitals. The New England journal of medicine, 360(16), 1628–1638. https://doi.org/10.1056/NEJMsa0900592

[56] Kaye J. (2012). The tension between data sharing and the protection of privacy in genomics research. Annual review of genomics and human genetics, 13, 415–431. https://doi.org/10.1146/annurev-genom-082410-101454

[57] Khansa, L., & Liginlal, D. (2009). Valuing the Flexibility of Investing in Security Process Innovations. European Journal of Operational Research, Forthcoming, 192(1), 216–235.

[58] Kritzinger, E., & Von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement.

Computers and Security, 29(8), 840–847. https://doi.org/10.1016/j.cose.2010.08.001

[59] Laurie, G., Stevens, L., Jones, K. H., & Dobbs, C. (2015). A Review of Evidence Relating to Harms Resulting from Uses of Health and Biomedical Data. Nuffield Council on Bioethics. http://nuffieldbioethics.org/wp-content/uploads/A-Review-of-Evidence-Relatingto-Harms-Resulting-from-Uses-of-Health-and-Biomedical-Data-FINAL.pdf Liverpool School of Tropical Medicine website: http://www.lstmed.ac.uk(2023)

[60] Malin, B. A., Emam, K. E., & O'Keefe, C. M. (2013). Biomedical data privacy: problems, perspectives, and recent advances. Journal of the American Medical Informatics Association: JAMIA, 20(1), 2–6. https://doi.org/10.1136/amiajnl-2012-001509

[61] Malin, B., & Sweeney, L. (2004). How (not) to protect genomic data privacy in a distributed network: using trail re-identification to evaluate and design anonymity protection systems. Journal of biomedical informatics, 37(3),179–192. https://doi.org/10.1016/j.jbi.2004.04.005

[62] McGuire, A. L., Fisher, R., Cusenza, P., Hudson, K., Rothstein, M. A., McGraw, D., ... & Henley, D. E. (2008). Confidentiality, privacy, and security of genetic and genomic test information in electronic health records: points to consider. Genetics in Medicine, 10(7), 495-499.

[63] Mercuri, R. T. (2004). The HIPAA-potamus in Health Care Data Security. Communications of the ACM, 47(7).

[64] Millman A., Lee N., Kealy K. (1995). ABC of medical computing. The Internet. BMJ. 311(7002):440-443. doi:10.1136/bmj.311.7002.440

[65] Ministry of Health, Kenya.(2022). KENYA NATIONAL eHEALTH POLICY 2016-2030 DigiAfya.

[66] Ministry of Health, Kenya. (2023). Kenya Health Information Systems Interoperability Framework. Government of Kenya. [URL]

[67] Morwesy, (2019). Power outages as a cause of systems downtimes in sub-Saharan African Countries. Retrieved from https://excellerbooks.com/product/the-unrehearsed-boom-in-education-automation-amid-covid-19-flouts-online-education-in-the-midst-of-a-worlds- Pandemic-a-potential-academic-integrity-cyber-risks-aicr/

[68] Mugenda, A. G., & Mugenda, O. M. (1999). Research Methods: Quantitative and qualitative approaches. Acts Press.

[69] Mugo, David M., and David Nzuki. "Determinants of electronic health in developing countries." (2014).

[70] Myers, M. D., & Young, L. W. (1997). Hidden agendas, power and managerial assumptions in information systems development: An ethnographic study. Information Technology & People, 10(3), 224-240.

[71] National Academies of Sciences, Engineering, and Medicine. (1997). For the Record: Protecting Electronic Health Information. Washington, DC: The National Academies Press. https://doi.org/10.17226/5595.

[72] Omogah, F. O. (2020). The Embryonic COVID-19 Themed Cyber Threats: A Looming Tragedy to Already Vulnerable Global Electronic Healthcare Systems (GEHCS)! Health Systems and Policy Research. Retrieved from https://www.hsprj.com/abstract/the-embryonic- covid19-themed-cyber-threats-a-looming-tragedy-to-already-vulnerable-global-electronic-healthcare-systems-gehcs-33136.html

[73] Orodho A.J (2005). Techniques of writing research Proposals and Reports in Education and Social Sciences Nairobi Kawezia Enterprises

[74] Pagliari, C., Detmer, D., & Singleton, P. (2007). Potential of electronic personal health records. BMJ (Clinical research ed.), 335(7615), 330–333. https://doi.org/10.1136/bmj.39279.475787.AD

[75] Pandey, A., Hasan, T., Dubey, S., Sarangi, S. R., & Kar, A. K. (2020). Mapping the dynamics of information security research: A scientometric analysis using machine learning. Journal of Information Security and Applications, 54, 102596.

[76] Pavlopoulos, S., Gerogiannis, V., & Efraimidis, P. S. (2003). Information security in healthcare environments. Computers in Biology and Medicine, 33(1), 67–83. https://doi.org/10.1016/S0010-4825(02)00043-9

[77] Policastri, A., Zaccagnino, R., Frontoni, E., & Principi, E. (2018). A comprehensive review on secure electronic health record systems. Journal of King Saud University-Computer and Information Sciences.

[78] Powers, T. M., Sharda, R., & Yadavalli, V. S. S. (2006). Security of electronic health records: Issues impacting the adoption of EHRs. Paper presented at the 39th Annual Hawaii International Conference on System Sciences (HICSS'06).

[79] Prainsack, B., & Buyx, A. (2013). A solidarity-based approach to the governance of research biobanks. Medical law international, 13(2-3), 85–109. https://doi.org/10.1177/0968533213013002002

[80] Qureshi, H., Khokhar, R. H., & Katsikas, S. K. (2016). Survey on secure communication protocols for internet of things applications. Journal of Ambient Intelligence and Humanized Computing, 7(1), 37–56. https://doi.org/10.1007/s12652-015-0335-4

[81] Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules through Technology. Texas Law Review, 76(3), 553–593. https://doi.org/10.2307/24825148

[82] Robillard, J. M., Feng, T. L., & Hu, E. (2009). Acceptance and resistance of new digital technologies in medicine: qualitative study. Journal of medical internet research, 11(2), e20. https://doi.org/10.2196/jmir.1003

[83] Rockoff, M. L., & Friedman, C. P. (1985). Towards a comprehensive medical computer science curriculum: Integration of medical informatics into medical school. In Proceedings of the 8th Symposium on Computer Applications in Medical Care (pp. 198-202). American Medical Informatics Association.

[84] Rolland, S. (2016). Privacy, health information exchange, and new models for delivery of care. Journal of General Internal Medicine, 31(6), 647–649.

[85] Rosenbaum, S., & Simon, A. (2009). Duty to Warn in the Face of H1N1 and Other Contagious Conditions: Ethical, Legal, and Practical Considerations. Loyola University Chicago Law Journal, 40(2), 257–274.

[86] Rajeev, J., & David, S. (2013). A Framework for Building a Security-Aware Culture in Healthcare Environments. Journal of Medical Systems, 37(5), 9985. https://doi.org/10.1007/s10916-013-9985-5

[87] Sankaran, R., & Damiani, E. (2018). Health Information Systems: Concepts, Methodologies, Tools, and Applications. IGI Global.

[88] Sittig, D. F., & Singh, H. (2010). A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Quality and safety in health care, 19(Suppl 3), i68–i74. https://doi.org/10.1136/qshc.2010.042085

[89] Stewart, J. E., & Halpern, A. L. (1999). Documenting professional development in medical informatics: AMIA's 1999 conference: Informatics: Across time, across the continuum, across the globe. Proceedings. Journal of the American Medical Informatics Association: JAMIA, 6(6), 430–435. https://doi.org/10.1136/jamia.1999.0060430

[90] Tang, P. C., & Ash, J. S. (2005). Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. Journal of the American Medical Informatics Association: JAMIA, 13(2), 121–126. https://doi.org/10.1197/jamia.M1700

[91] Tawileh, A. A. (2019). Information security policy effectiveness: A focus on the socio-technical facet. Computers & Security, 82, 32–45. https://doi.org/10.1016/j.cose.2019.01.003

[92] Tawileh, A. A., & El-Masri, S. (2006). Benchmarking information security implementation in financial services. Information Management & Computer

Journal of Chemical Health Risks

www.jchr.org

JCHR (2023) 13(6), 2423-3443 | ISSN:2251-6727

Security, 14(2), 168–188. https://doi.org/10.1108/09685220610662794

[93] Thompson, C. A. (2021). Mobile Health (M-Health) Technologies in Health and Wellness: A Systematic Review. International Journal of Telerehabilitation, 13(1), 3. https://doi.org/10.5195/IJT.2021.6357

[94] Toribio, N. & Díaz, G. 2015. Use of mobile technology as an education tool: Its impact on health. Journal of Applied Research and Technology, 13(3): 513–519. DOI: 10.1016/S1665- 6423(15)30022-3

[95] Treisman, K., & Brody, J. E. (2018). Will People Who Need the Most Medical Care Get It? It Depends. The New York Times. Retrieved from https://www.nytimes.com/2018/05/25/upshot/will- people-who-need-the-most-medical-care-get-it-it-depends.html

[96] Turpin, C. & Doherty, N. F. (2004). The role of expectation in the perception of e-service quality: A case of online travel and holiday services. Journal of Interactive Marketing, 18(4): 23–37.

[97] Vidyarthi, A. R., Hamill, T., Green, A. L., Rosenbluth, G., Baron, R. B., & Miloslavsky, E. M. (2014). Changing resident test ordering behavior: a multilevel intervention to decrease laboratory utilization at an academic medical center. American journal of medical quality: the official journal of the American College of Medical Quality, 29(6), 492–498. https://doi.org/10.1177/1062860613504613
Vayena E, Salathé

[98] M, Madoff LC, Brownstein JS. (2015). Ethical challenges of big data in public health. PLoS Comput Biol 11(2): e1003904. doi:10.1371/journal.pcbi.1003904

[99] Vimarlund, V., & Timpka, T. (2000). Functional requirements for electronic health records to support primary care. International journal of medical informatics, 60(2), 129–137. https://doi.org/10.1016/S1386-5056(00)00079-8

[100] Wan, J., & Zhou, K. (2010). Security and privacy for cloud computing: A review. Paper presented at the 2010 seventh international conference on grid and cooperative computing.

[101] Wang, Y. Z., & Levy, Y. (2011). Towards an understanding of the theoretical underpinnings of Chinese medicine and informatics research. European Journal of Information Systems, 20(3), 259–275. https://doi.org/10.1057/ejis.2010.89

[102] Ward, R., Stevens, C., Brentnall, P., & Briddon, J. (2018). The attitudes of health care staff to information technology: a comprehensive review of the research literature. Health Information and Libraries Journal, 25(2), 81–97. https://doi.org/10.1046/j.1365-2532.2008.00796.x

[103] Wolpert, J. (2011). Cybersecurity in healthcare. Journal of Healthcare Protection Management, 27(1), 93-101.

[104] Yao, W., Chu, C. H., & Li, Z. (2017). The adoption and implementation of RFID technologies in healthcare: A literature review. Journal of Medical Systems, 41(5), 69. https://doi.org/10.1007/s10916-017-0724-8

[105] Ye, M., & Smith, A. J. (2007). Clinical research informatics: A conceptual perspective. Journal of the American Medical Informatics Association: JAMIA, 14(2), 138–144. https://doi.org/10.1197/jamia.M2247

[106] Yusof, M. M., Paul, R. J., Stergioulas, L. K., & O'brien, C. (2008). The development of a healthcare specific enterprise architecture: A methodology. Information & Management, 45(5), 257–270. https://doi.org/10.1016/j.im.2008.04.001

[107] Zhang, X., Guo, X., Lai, K. H., & Guo, F. (2011). Research on the key technologies of health information security in clouds. Paper presented at the 2011 International Conference on Computer Science and Network Technology.

[108] Zhang, Y., Johnson, T. R., Patel, V. L., & Paige, D. L. (2002). Kubose, T. A. Using usability heuristics to evaluate patient safety of medical devices. Journal of biomedical informatics, 35(1), 23–30. https://doi.org/10.1016/S1532-0464(02)00504-4

[109] Zhao, K., Zhang, Y., Zhang, K., & Zhang, X. (2019). Ensuring information security in big data storage. Security and Communication

Networks, 2019. https://doi.org/10.1155/2019/6461562

[110] Zheng, Y., Cui, H., Chen, Z., Zhou, X., & Fan, J. (2021). A privacy-preserving data sharing method for the internet of medical things based on the combination of blockchain and homomorphic encryption. Journal of Ambient Intelligence and Humanized Computing, 12(6), 7279–7292. https://doi.org/10.1007/s12652-021-03092-7

[111] Zimmermann, B. M., Walter, Z., Teuteberg, F., & Weking, J. (2014). Assessing the potential of Near Field Communication (NFC) for medical contexts. Journal of Medical Systems, 38(7), 69. https://doi.org/10.1007/s10916-014-0069-8

[112] Zwijsen, S. A., Niemeijer, A. R., Hertogh, C. M., & Ethics in Dementia Care Research Group. (2011). Ethics of using assistive technology in the care for community-dwelling elderly people: an overview of the literature. Aging & mental health, 15(4), 419–427. https://doi.org/10.1080/13607863.2010.543655