World Journal of Pharmaceutical and Life Sciences
WJPLS
www.wjpls.org
SJIF Impact Factor: 6.129

CHALLENGES AND OPPORTUNITIES ON DATA PROTECTION AND PRIVACY IN HEALTHCARE

[*1]Dr. Salim Omambia Matagi and [2]Prof Satoshi Kaneko

[1]Department of Health Information and Research Kenya Medical Training College P.O. BOX 30195-00100 Nairobi, Kenya.
[2]Department of Eco-epidemiology, Institute of Tropical Medicine, Nagasaki University, Japan.

***Corresponding Author: Dr. Salim Omambia Matagi**
Department of Health Information and Research Kenya Medical Training College P.O. BOX 30195-00100 Nairobi, Kenya.
Email ID: omasalim@yahoo.com

Article Received on 09/02/2023 **Article Revised on 01/03/2023** **Article Accepted on 22/03/2023**

ABSTRACT

The envisage is the next big thing globally is information. It is the wellspring of literally everything and thus the saying ''INFORMATION IS POWER'' Any continent, country, or organization that is considered a superpower is arguably among the best if not the best in handling information. Healthcare is no exclusion on information demands. The best hospitals in the world have practices and a culture of nurturing data/information. Healthcare data is the impetus to improve patient outcomes, predict outbreaks of epidemics, gain valuable insights, avoid preventable diseases, reduce the cost of healthcare delivery and improve the quality of life in general. In Kenya and many developing countries majority of families are a stone's throw away from poverty if a family member develops. People who do not have access to healthcare are stuck in a vicious circle of poverty and poor health, which can also lead to social instability and migration consequently, health is a prerequisite to prosperity. No country is considered developed without a good health system and the antithetic applies to developing countries. Health management problems are increasing with the growing population, especially with the increasingly larger aging population. Sometimes no response from the hospital for emergencies creates social issues. Similarly, the medical staff in rural areas do not have sufficient resources for treatment and do not have the expertise to diagnose complex diseases. Due to these reasons, people in rural areas focus on big hospitals for proper medical attention, increasing the load on hospitals. The late detection of diseases and severe health problems of older people also complicates the diagnosis process. Therefore, there is a need to provide better medical facilities using an optimized healthcare system that includes body sensors and medical devices to remotely monitor and diagnose medical problems. A country may or may not have a law for user data protection, but the healthcare system should follow the laws of the country to which the user belongs

KEYWORDS: Data, Data Governance, Data Warehouse, Healthcare, Data Rules and Policies, Privacy, Confidentiality, Security, Accessibility, Rights, Regulations, Key Performance Indicators.

INTRODUCTION

The envisage is: the next big thing globally is information. It is the wellspring of literally everything and thus the saying ''INFORMATION IS POWER'' Any continent, country, or organization that is considered a superpower is arguably among the best if not the best in handling information. Healthcare is no exclusion on information demands. The best hospitals in the world have practices and a culture of nurturing data/information Healthcare data is the impetus to improve patient outcomes, predict outbreaks of epidemics, gain valuable insights, avoid preventable diseases, reduce the cost of healthcare delivery and improve the quality of life in general. The factions would arise from the extent of access to healthcare data considering patient's rights, privacy and confidentiality (Matagi, 2021).

Health Data is the nexus of any healthcare innovation. Research on new drugs, devices, therapies, patient to doctor or healthcare facilities communication is all pegged on health data. Healthcare spending consumes upward of 50 percent of government revenue, and its share continues to climb. As stated by (Boysen, 2022) The topology of health care is one of the most diffuse sectors of the economy, with no organizing force between government, hospitals, doctors, labs, researchers, patients, medical device makers and healthcare foundations and registries. Some patients access health care every day; others access services every few years. Some patients are very internet savvy,

while others don't want anything to do with online services that require a perpetual mindset of vigilance and active suspicion, as well as evergreen technical acumen. The current situation with healthcare data security is extremely dangerous, as patient health information can be sold or used for crimes such as identity theft and insurance fraud, or to illegally obtain prescription drugs. Outsider threats continue to present new challenges, but hidden insider threats are even more dangerous. Only the most basic and low-risk services are online today, and even those are beset by the huge overhead cost of data breaches and password resets. This is a global issue that plays out in communities everywhere.

However, as sophisticated as the healthcare system is today, there are lurking threats that have enclaved health data and information handling. One of the glaring issues currently plaguing the healthcare industry is the privacy and security surrounding healthcare data. Various studies allow for healthcare data to be captured and gathered. Throughout the process, it's critical to manage consent, ensure privacy and protect access to patient healthcare data. Today, passwords and passcodes are the only barriers to accessing sensitive systems and data; however, a good digital identity system will move us beyond this limitation so that consumers of health data can do more online, the concept is a new frontier in value creation for individuals and institutions around the world. A good digital identity is something that should be portable, simple to use and accepted everywhere, much like a credit card or mobile phone. It should be trustworthy and cost-effective for accessing healthcare and other services consequently, will provide users with more choice, control and convenience (Shahid, 2022).

According to (WHO,2022) Leadership and governance involve ensuring strategic policy frameworks exist and are combined with effective oversight, coalition-building, regulation, attention to system-design and accountability. In recent years, countries across the world have implemented either new or considerably stricter data protection and cybersecurity laws. These laws continue to have a substantive impact on health information systems (HISs) and most public health activities in a wider sense.

The only thing that will never change is change and this is affirmed by the new norm in the global healthcare sector. What you sleep with is not what you wake up to technically because technology and specifically digitization of health and patient data is undergoing a dramatic and fundamental shift in the clinical, operating and business models and generally in the world of the economy for the foreseeable future. This shift is being spurred by aging populations and lifestyle changes; the proliferation of software applications and mobile devices; innovative treatments; heightened focus on care quality and value; and evidence-based medicine as opposed to subjective clinical decisions all of which are leading to offer significant opportunities for supporting clinical decisions, improving healthcare delivery, management and policy-making, surveilling disease, monitoring adverse events, and optimizing treatment for diseases affecting multiple organ systems(Abouelmehdi et al, 2018).

Currently, at least half of the people in the world do not receive the health services they need. About 100 million people are pushed into extreme poverty each year because of out-of-pocket spending on health. This must change.

As indicated by (WHO,2022) The pandemic covid-19 confirmed Health goes beyond borders and mostly it is a loss that teaches us the worth of things. It is crucial to consider health globally and universally to work vigorously collectively towards Universal Health Coverage and Health for All. Neglecting to do so would undermine the importance and influence of health in our societies. To expedite the process towards Universal Health Coverage, the United Nations identified Good Health and well-being as one of the Sustainable Development Goals. Besides, having equal access to quality healthcare is a basic human right. Yet, for many, the reality is healthcare is either too far away or too expensive. Universal health coverage means that all people have access to the health services they need, when and where they need them, without financial hardship. It includes the full range of essential health services, from health promotion to prevention, treatment, rehabilitation, and palliative care.

As stated by D'Ambrogio (2020), Japan is aging fast. Its 'super-aged' society is the oldest in the world: 28.7 % of the population are 65 or older, with women forming the majority. The country is also home to a record 80 000 centenarians. By 2036, people aged 65 and over will represent a third of the population. Japan's demographic crisis is the consequence of the combination of two elements: a high life expectancy and a low fertility rate. Tokyo is engaged in global health cooperation and succeeded in incorporating the concept of human security into the sustainable development goals. It has also been active in international cooperation on aging, with a focus on the Association of Southeast Asian Nations (ASEAN) region. The consequences of the country's aging and shrinking population include economic crisis, budgetary challenges, pressure on job markets and depopulation of rural areas. The silver economy is meanwhile flourishing and Japan is at the forefront of robot development to face a declining labor force and to take care of its elderly. The government's efforts to address the demographic crisis have yet to succeed, however, and immigration has been limited. Japan longevity is due to public health sensitization, some 40-50 years ago Japan longevity was low but with emphasis on public health sensitization the country is currently at the apex in longevity.

To make health for all a reality, we need individuals and communities who have access to high-quality health services so that they take care of their health and the health of their families; skilled health workers providing quality, people-centered care; and policy-makers committed to investing in universal health coverage. Universal health coverage should be based on strong, people-centered primary health care. Good health systems are rooted in the communities they serve. They focus not only on preventing and treating disease and illness but also on helping to improve well-being and quality of life.

Health management problems are increasing with the growing population, especially with the increasingly larger aging population. Sometimes no response from the hospital for emergencies creates social issues. Similarly, the medical staff in rural areas do not have sufficient resources for treatment and do not have the expertise to diagnose complex diseases. Due to these reasons, people in rural areas focus on big hospitals for proper medical attention, increasing the load on hospitals. The late detection of diseases and severe health problems of older people also complicates the diagnosis process. Therefore, there is a need to provide better medical facilities using an optimized healthcare system that includes body sensors and medical devices to remotely monitor and diagnose medical problems (WHO,2022).

Big data has come to medicine. Its advocates promise increased accountability, quality, efficiency, and innovation. Most recently, the rapid development of machine-learning techniques and artificial intelligence has promised to wring even more useful applications from big data, from resource allocation to complex disease diagnosis. But with big data comes big risks and challenges, among them significant questions about patient privacy. Big Data Issues Integrating healthcare data notably raises security and privacy issues. Patient information is processed at different levels of security in data centers. In America, most organizations have Health Insurance Portability and Accountability Act of 1996 (HIPAA) certification, but this does not guarantee a patient's record safety because HIPAA is more inclined towards ensuring security policies rather than implementation. Moreover, the transmission of large data sets from different locations poses an extra burden on processing and storage. Conventional security solutions are inadequate for large and inherently changing data sets. With the emergence of cloud healthcare solutions, security demands are becoming more complex and there are no specified policies written in existing healthcare data protection laws (Price and Cohen2020).

According to (Ekran Systems, 2019) Almost all healthcare providers use Electronic Health Record (EHR) systems to store and manage sensitive healthcare data. Not only does the healthcare industry suffer from the highest costs for data breaches – it also takes the most time to identify and contain them: on average, it takes healthcare organizations 236 days to identify a problem and 93 days to contain it. According to the 2019 Cost of a Data Breach Report by the Ponemon Institute, for the ninth year in a row, healthcare organizations have had the highest average cost of a data breach at $6.45 million – over 60% more than the global average for all industries. Outsider threats continue to present new challenges, but hidden insider threats are even more dangerous. The current situation with healthcare data security is extremely dangerous, as patient health information can be sold or used for crimes such as identity theft and insurance fraud, or to illegally obtain prescription drugs.

The health information production market is now open and deregulated, with data analyzed by multiple people with or without epidemiological expertise—who make their analyses available through different types of traditional and social media, and who compete with traditional information producers. In Africa, routinely collected data from healthcare providers are usually event based rather than population based, and the population using the services of these providers is changing, unpredictably, across time. These data are further exposed to surveillance bias and streetlight effect. Defining the source population is also very difficult with data from social media networks or internet queries, and it is not clear of which population there are representative. As a result, how to infer information derived from these data to a target population is a serious challenge for decision-makers. Further, there is not only a multiplication of new data sources but also a multiplication of information producers. While poor quality and huge volume of data can lead to the production of information of questionable utility, a related problem is an infodemic. Scientists have not helped substantially to mitigate the effects of infodemic and to prevent misinformation. Actually, they might have contributed to these trends (Chiolero, 2022).

Data is collected in majority if not all of African countries because it has an economic constituent but usability is a challenge. This is simply because they don't know or understand the importance of data but have an economic interest and not the ultimate purpose of data. Basic information literacy is not there. Maybe more emphasis should be towards information education to sensitize the importance of data. If you don't understand the importance of data you wouldn't care much about data quality as a result, just collect data for economic purposes.

In Kenya and many developing countries majority of families are a stone's throw away from poverty if a family member falls sick. People who do not have access to healthcare are stuck in a vicious circle of poverty and poor health, which can also lead to social instability and migration consequently, health is a prerequisite to prosperity. No country is considered developed without a good health system and the antithetic applies to

developing countries. A properly functioning health system is like a constellation; it requires skilled healthcare professionals, quality equipment, accessible facilities, an uninterrupted supply of quality medicine, the involvement of the community, and an affordable and accessible operation in place that sustains the flow of quality healthcare. Poor data quality leads to increased bottlenecks, decreased efficiency, and patient mistreatment. That is where a well-maintained data quality management system steps in and saves the day. In their report (Folio3, 2022), states that healthcare providers must ensure that they properly manage patient data to create a culture of trust and transparency with patients while meeting strict data privacy and legal regulations. In Kenya there is a high enrollment in education which by default is supposed to have an impact on positive cultural practices that should yield positive results in the society, nevertheless, it's like Kenya keeps producing the same product every time despite the high enrollment numbers and high quality education, consequently, no improvement in terms of healthcare insight or positive change. Economic objectives pervasively overcome all the other vital objectives.

Data privacy in healthcare is constantly evolving with continuously updated laws and regulations. As for infodemic, we suggest media literacy to deal with the menace since the hoi polloi will easily decipher what is genuine information and what is not. In this way, patients will get the data knowledge and privacy they deserve and expect. In this paper, we will discuss the challenges and opportunities in data protection and privacy.

DISCUSSION

According to a study (Folio3, 2022), Several issues are related to the importance of data quality in healthcare, leading to the mistreatment of patients and a lack of trust between the patient and the organization. This is because inaccurate data leads to misinterpretation of patient information and misdiagnoses, which can even lead to death. In addition to this, it also leads to inefficiency within the organization since manual interventions to correct inaccurate medical records lead to further data entry errors, affecting the organization. A crucial part of a healthcare organization is making sure the importance of data quality in healthcare is maintained. The fact that inaccurate diagnoses are due to duplicate EHR is a prime example of the importance of data quality. Healthcare is all about establishing trust between the patient and the physician, and poor data quality affects this adversely while damaging the healthcare provider's reputation completely. The US government found that the third-leading cause of death in their country is patient misidentification. Because the number of duplicate records in hospitals is increasing, which results in the misidentification of 10% of incoming patients, sharing patient data from disparate sources further increases the probability of duplicate records generation. This shows that the current quality of data in healthcare is questionable.

As an alternative to creating a health-specific functional identification system, some countries have instead opted to use existing foundational identification systems, such as population registers, unique identification numbers (UINs) or national ID (NID) cards, as the basis for patient identification, verification, and authentication. Leveraging a foundational system in this way may create additional benefits beyond those offered by a functional system. There are many identifiable benefits to the use of electronic medical record systems, considering the possibility of accessing online records, while still evaluating the provision to patients of access to their health records (Lodhia et al., 2016). Handwritten documents are subject to spelling errors and illegible writing, which in general is typical of doctors. Health records are migrating to digital formats as technology evolves. These problems can be avoided through electronic medical record systems, minimizing errors in medical records and providing a way to eliminate inconsistencies, while patient care becomes more agile, as they also standardize patient histories. Similar benefits may be seen through the centralization of health information, practices and services free from tracing by paper records. However, strong cybersecurity measures are needed, which require appropriate administrative, physical and technical protections, to maintain and guarantee the protection, privacy, confidentiality, integrity and security of data and health records in all formats. These electronic medical record systems give health professionals the ability to share information instantly with other health professionals (Ekransystem, 2022). Besides, it is currently common for health organizations to think about the security of their data, still reflecting on the horizon of medical care crossing barriers and expanding outside health institutions such as hospitals, laboratories, operators and clinics. It is worth assessing that electronic systems create a safer way to store medical records, since digital security needs to keep pace with digital transformations. These data are sensitive, targeted by cybercriminals, and in this type of context cyber governance is not simple if there is no use of a digital solution that helps in protection and digital privacy (Ahmed et al,2021). One of the main aspects of health data sharing is ensuring that this is done securely, with solutions such as digital signature, encryption of data at rest (stored data) and derivatives and a platform that helps in the governance of that information, and that does not compromise patient information. Concerning data encryption, it is obtained using some algorithmic process to transform data in order to decrease the probability of giving meaning to that information, without using a specific process or a confidential key (Fernandes, 2022). Moving data are information sent from one individual (patient) or private device to another via direct messages, e-mail or other means of exchanging data and messages. In that respect, that unencrypted data can be intercepted while moving from one location to another. Data at rest refers to that information stored

somewhere, and not transported, i.e., being stored on hard disk, a removable disk, pen drive, on Data Privacy in Healthcare in the Current Age 9 a local server or even mobile devices, such as notebooks, tablets and smartphones. Even so, the privacy and integrity of health data must be protected not only against external threats, but also against unauthorized (Tigahealth, 2022).

Undoubtedly, poor data quality has a tremendous impact on the efficiency and effectiveness of the healthcare organizations, at both operational and strategic levels All healthcare organizations have to change the way of accessing patients' data and define who is allowed to access what type of data in order to comply with external regulations(Alofaysan et al., 2014). We can still reflect on the growing use of mobile devices, as well as the subsequent collection of patient data, assessing the health area, bringing a new emphasis to the importance of certificate management, public and private key infrastructures, and digital privacy property. Many different gadgets are used, including smartwatches measuring vital signs, or ingestible sensors, or digital pacemakers, among other state-of-the-art devices, collecting data, generating and extracting information and using techniques that can improve people's lifestyles. However, the continuous effort for interoperability, i.e., the ability of different systems, devices, applications or digital solutions to connect and communicate in a coordinated manner, without the end user's effort (transparency), has helped to drive the growth of data sharing in the health field. Although data collection has its risks, the benefits for patients are undeniable, through faster and more efficient assistance in situations of low or medium complexity, reducing the number of readmissions and fraud, avoiding medication errors, reducing duplicate tests or even talking to a digital attendant, as explained above. Even so, in the face of all the imaginable advantages, healthcare institutions need to consider the rules of data protection legislation, exclusive to each country, and privacy rules related to the sharing of sensitive information (Anjarwalla & Khanna 2022). In protecting the privacy of health information, in the face of increasing numbers and the impact of data breaches, the security of medical records must be one of the main priorities of the health sector. Regarding ownership of their personal data and their own experience, both patients and digital users should not be sceptical about the non-transparent methods that institutions use to provide the many benefits of 12 Data Protection and Privacy in Healthcare personalization of care, due to control and/or manipulation of algorithms with the commercial use of personal data (Lexology, 2020). Today's personalization methods, based on robust data collection and analysis, are failing to provide transparency for users and patients. In this sense, in order to customize services, they need to be increasingly transparent, protecting and giving greater power, confidence and stability over the use of their data and information. The most common and general practice to ensure the safety of patient data is to make them anonymous. This is one of the ways in which the balance between technology and privacy is achieved. In this sense, calls, medical records and other types of interaction with patients are stored in their systems without the identification of users. The digital certificates used in the health area are similar to those used in other market segments, which include a public key, stored in your certificate, and published in a secure repository, and a private key, stored on the computer of the health professional, or in a personal hardware token (device model or smartcard), or even in a digital cloud technology structure (Healthit, 2022). Given this scenario, the data transmitted between the systems of the health institutions themselves, between clinics and hospitals, laboratories or health operators, or even others, must be treated more rigorously in the face of countless cases reported around the world concerning data leakage worldwide, whether due to failures in the security systems of health institutions, or even the improper use and provision of patient information. In addition to the need for authorization by patients, sharing of this information can only be done if the messages are encrypted (encrypted). A healthcare institution should be aware that the integration of digital signatures, electronic signatures and digital certificates through the encryption of these keys and credentials is essential and of fundamental importance. They authenticate all informed and in-transit procedures, ensuring that the files are safe and verifiable, protecting the privacy of patient data during medical and administrative procedures (Wiewiorówski, 2020).

The Internet of Things (IoT) in the health care and medical industries is at an advanced stage in some areas and sorely lacking in others. The Internet of Things (IoT) is an emerging field consisting of Internet-based globally connected network architecture (Shah & Chircu, 2018). The IoT is a technology that facilitates consumers by exchanging information with devices connected to the Internet. One primary use case of IoT is in the healthcare sector, i.e., the Internet of Healthcare Things (IoHT), designed to monitor, store, or transmit healthcare information, thus,a subset of IoT is the Internet of Healthcare Things (IoHT) that consists of smart healthcare devices having significant importance in monitoring, processing, storing, and transmitting sensitive information. Some applications such as heart and other monitors provide major amounts of data to health care professionals. However, within hospital systems, silos of data and legacy equipment hamper the broad implementation of IoT in the sector but that is changing fast. It is experiencing novel challenges regarding data privacy protection(Zakerabasali, 2022).

The IoHT describes uniquely identifiable devices connected to the Internet, communicating with each other, used in the medical area. IoHT devices help to monitor individuals' medical conditions by generating clinical data by forwarding it to a remote server or service with the help of wireless network infrastructure

(Robb, 2021). Like any other Internet-based device, IoHT devices have a unique identifier such as an IP address which enables them to connect with the network and to forward/receive data to/from intended devices. The central server manages this collected information and responds accordingly to diagnose patients' diseases. The idea is to provide reliable, efficient, and cost-effective healthcare services by facilitating physicians and medical staff by remotely monitoring their patients. IoHT implementations also enable individuals to manage their health data easily and assist them in how to use wearable health monitors (CIPIT, 2021).

NHS Digital plans to extract all data coded in GP held medical records in England, unless patients opt out first. These data include all physical and mental health diagnoses, physiological measurements, test results, and medications. The data will be pseudonymised, meaning that identifiers such as name, NHS number, date of birth, and the second part of the postcode will be hidden—but NHS Digital has a key to re-identify records, which it will do "where there is a legal reason." As reported by (Salisbury, 2021) The stated aim of the dataset is to assist research and planning. The list of organizations NHS Digital may share data with includes other government departments, universities, charities, research bodies, and drug companies. NHS Digital says that it only ever releases the minimum dataset necessary and is confident that it has robust systems in place to prevent breaches of confidentiality. However, not everyone is reassured, as re-identifying people from an incomplete dataset is a developing art and is likely to evolve further. The Information Commissioner's Office is clear in its most recent guidance that pseudonymised data are therefore personal data. Leaving aside the question of whether absolute data security can be guaranteed, a more fundamental question concerns consent. General practices are legally obliged to transfer data to NHS Digital under the 2012 Health and Social Care Act, but how does this square with ethical obligations to patients. There's something sacrosanct about a medical consultation, with similarities to a religious confessional: whatever patients tell practitioners, unless there's a risk to others, they are never to break the patients' confidentiality as sworn in the Hippocrates oath.

Human dignity and the right to the integrity of the person are recognized in Articles 1 and 3 of the Charter of Fundamental Rights of the European Union. Medical research on humans (also known as biomedical research or experimental medicine, including 'bench science' and applied research), is strictly subject to ethical standards and controls. Under Article 3(2)(a) of the Charter, the 'free and informed consent of the person concerned' must be respected in the field of biology and medicine. In the health sector there is, it is argued, an 'ethical and scientific imperative' to share personal data for research purposes82. The EU like governments elsewhere in the world promote the public sharing of anonymized clinical trial documents83, though techniques are not standardized (Wiewiorówski, 2020).

As indicated by (Yin, D. *et al*, 2022), Research is clearly no longer the preserve of academia, if indeed it ever was. China's first privacy law, the Personal Information Protection Law, went into effect on 1 November 2021.1 Driven by security and privacy concerns, the law established the legal framework and principles for processing the personal data of people residing within the territory of China. The law shares some of the principles and concepts in the EU's General Data Protection Regulation (GDPR), although stated in broader terms. Like GDPR, the Chinese law aims to empower individuals by giving them control over their data. Personal data are defined as "information related to an identified or identifiable natural person recorded electronically or by other means, but do not include anonymized information."1 Health data, classified as sensitive, must be processed through a rigorously regulated pathway, with clear justification for the proposed use and unambiguous consent. Importantly, while the new law does not cover fully anonymized data, it does apply to data that have been "de-identified" since such data can be reattributed to a particular person through other sources of information. Privacy aims must be reconciled with the need for medical research in the public interest. Digitization has transformed research. The cost of data processing and storage continues to decrease, processing power increases and sensors and connected devices proliferate. Researchers, particularly in medical research, often work in large collaborative networks and need to exchange large volumes of data at great speed across borders11. In the online environment researchers may have limited direct contact with participants, and large-scale genomic databases are developed for use by multiple researchers over long periods.

According to (Wiewiorówski, 2020), ethical standards for research have evolved governing primarily medical experiments on humans. They have been adapted generally to any research using human subjects. The Nuremberg Code was probably the first example of an ethical code in modern times, formulated in reaction to the medical experimentations conducted in Nazi concentration camps72. Later, in 1964, the World Medical Association's Declaration of Helsinki on Ethical Principles for Medical Research Involving Human Subjects (last amended in 2013) included within its scope 'research on identifiable human material and data', and prescribed that 'Every precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information.' It further stipulated, 'For medical research using identifiable human material or data, such as research on material or data contained in biobanks or similar repositories, physicians must seek informed consent for its collection, storage and/or reuse. There may be exceptional situations where consent would be impossible or impracticable to

obtain for such research. In such situations the research may be done only after consideration and approval of a research ethics committee' 73. The United States, following the Declaration of Helsinki, has since 1981 applied 'the Common Rule' as an ethical standard governing biomedical and behavioral research involving human subjects. The Common Rule governs oversight of federally funded human research and is incorporated in the 1991 revision to the U.S. Department of Health and Human Services Title 45 CFR 46 (Public Welfare). It includes requirements for researchers' obtaining and documenting informed consent and Institutional Review Boards with additional safeguards for certain vulnerable research subjects namely pregnant women, foetuses, prisoners and children. Many academic journals require Common Rule compliance for all research, including where privately funded, and there are several state laws on human subject research74. The Council of Europe in 1997 adopted the Convention on Human Rights and Biomedicine ("the Oviedo Convention") which stressed that the human being has primacy over the sole interest of society or science75. It states that research on a person can be performed only subject to conditions such as the lack of an alternative of comparable effectiveness, the approval of the research project by the competent body after independent examination of its scientific merit, and ensuring the person undergoing research has been informed of the safeguards and her rights.

According to (Yamamoto,2016) Japan was once progressive in the digitalization of healthcare fields but unfortunately has fallen behind in terms of the secondary use of data for public interest. There has recently been a trend to establish large-scale health databases in the nation, and a conflict between data use for public interest and privacy protection has surfaced as this trend has progressed. Databases for health insurance claims or for specific health checkups and guidance services were created according to the law that aims to ensure healthcare for the elderly; however, there is no mention in the act about using these databases for public interest in general. Thus, an initiative for such use must proceed carefully and attentively.

Health policy and systems research focuses on what works, for whom and under what conditions. Such research is valuable in the development and analysis of health policy, but also in contextualizing policy solutions. Furthermore, what policy-makers value and subsequently prioritize is shaped by many factors, including population needs, resource availability, historical priorities and many others(Campbell & Mills, 2022). We need to address the scarcity of health policy and systems research relevant to data protection, confidentiality and security.

Health information is regulated by different federal and state laws, depending on the source of the information and the entity entrusted with the information. The Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are two examples of federal laws that regulate privacy and the exchange of specific types of information (CDC,2022). The work of healthcare providers, school personnel, and others interacts with FERPA and HIPAA frequently, which is why it is important to understand these laws and know when they apply. The (Pharmaceuticals and Medical Devices Agency) PMDA projects that collect a large amount of medical record information from large hospitals and the health database development project that the Ministry of Health, Labor and Welfare (MHLW) is working on will soon begin to operate according to a general consensus; however, the validity of this consensus can be questioned if issues of anonymity arise. The likelihood that researchers conducting a study for public interest would intentionally invade the privacy of their subjects is slim. However, patients could develop a sense of distrust about their data being used since legal requirements are ambiguous. Nevertheless, without using patients' medical records for public interest, progress in medicine will grind to a halt. Proper legislation that is clear for both researchers and patients will therefore be highly desirable.(WHO, 2020).

A revision of the Act on the Protection of Personal Information is currently in progress. In reality, however, privacy is not something that laws alone can protect; it will also require guidelines and self-discipline. We now live in an information capitalization age. The problem, however, is that all this information often disappears altogether, or it is somewhere that the individual does not know and thus has no way of accessing. In essence, a large amount of information is produced but completely disappears. Thus, deciding policies relating to research, medical care, and health in this situation is quite a challenge. So, it is a process of trial and error for any country to make a progress. Reports suggest that although rules are made, they have proven to be rather ineffective. Moreover, the use of data has become extremely difficult even when it is for fair use and there is no intention of infringing on anyone's privacy. This is true for all countries, but privacy protection laws prioritize the protection of data and tend to be insensitive about the consequences of the decision to not use data. An epitome of this is, if no data were allowed to be used for writing or research purposes, progress of medicine would grind to a halt (Sejpal, 2022).

Data Governance related to the governance of healthcare data should be the initial step in managing healthcare data. It is due to the need of moving the healthcare industry towards a value-based business model. It demands common data representation that encircles different security standards (e.g., ICD, CPT, and LOINC). Currently, data generated in the healthcare industry is diverse and would demand a proper governance model (Nishat, 2021). There are no policies for healthcare data standardization and normalization for proper data governance. Privacy-preserving analytics in

the healthcare industry is grasping IoT devices to monitor and transmit vitals to healthcare clouds. Therefore, it needs to process and analyze data in an ad-hoc decentralized manner. However, the execution of resource-exhausting operations with privacy preservation is becoming a challenge. As new healthcare data analytics are becoming popular, healthcare data privacy laws need revision, and new laws should be drafted to illustrate all processes involved in the usage of patients' private data.

Identification of the Relevant Privacy Violation privacy in IoT-based devices can be violated at many stages. Firstly, it is violated by collecting data by third parties. Secondly, the usage and distribution of private data, and thirdly, the data is combined with other data. The third possibility is not known by the users who are using IoT-based medical devices to process and generate data. By combining newly generated information with existing data about a patient or health activity, it raises the high commercial value for many data-hungry organizations and commercial firms. Most of the data is often generated by automated medical devices, therefore, a higher trust level should be maintained for this data than on manually entered human data. This is important because medical insurance companies are monitoring the health conditions of their customers with the help of medical devices to ascertain the specific risks associated with their customer's health. These devices are also tracking users' geo-locations and such data must be protected through adequate device safety measures as well as legislative limitations on data usage (Nishat, 2021).

Data and context quality are mostly overlooked issues even if these facts play a significant role in the privacy debates in the context of IoT. The quality of data highly depends on the environment in which it is collected. The quality of context may be unknown where there is no or incomplete information about the context. It may also be ambivalent as there is a chance of contradictory information from different context sources. Context quality generates new problems of confidentiality that have not been addressed by current research. Context quality is related to the information that is not to be processed by hardware components that likely provide the information. It is better to protect context quality as it is sensitive information. Change in context quality is also sensitive information. IoT devices generate data based on context and do not allow users to shut down the system or to easily disconnect from it (CIPIT, 2022).To enhance transparency of the healthcare systems, not only healthcare data that is propagated from different devices need to be controlled, but also the data generated automatically by the healthcare devices need to be managed. Despite this important issue, no law has been made in this regard. There is a need to develop a combined approach with technical standards and existing regulatory frameworks to ensure data transparency.

Data governance is the remedy for such data problems. Data governance in simple words is the process of controlling patients' data by identifying who is the data governor, what are the data rules, how to enforce these rules, and how to monitor compliance improvement(Alofaysan et al., 2014).

The development and expanding accessibility of large-scale medical databases have supported the rapid increase in clinical epidemiological studies based on such databases in Japan. Examples of these databases include the nationwide Diagnostic Procedure Combination (DPC) databases, commercial and regional claims databases, nationwide patient-, disease-, and procedural-registries, and electronic medical record (EMR) databases. Two common types of databases currently used for observational clinical research are administrative claims databases and EMR databases. Administrative claims databases are archives of medical insurance bills generated by medical facilities, including hospitals, clinics, and pharmacies. Hospitals and clinics prepare medical insur- ance claims and send them to the corresponding insurers through Health Insurance Claims Review & Reimburse- ment Services. Pharmacies also prepare prescription insurance claims. Since 2003, Japan has adopted a diagnosis-related group-based payment system for acute inpatient care, known as the DPC payment system, and majority of acute-care hospitals currently prepare DPC claims (Kumamaru et al., 2020).

The validity of the evidence generated from database studies is highly dependent on the quality of the data, which must be assessed and validated. When discussing the quality of data, especially data from registry databases, two important characteristics are their completeness and their accuracy. The importance of legal or ethical considerations in data- base research was recently noted. For example, the Taipei Declaration adopted by the World Medical Association in 2016 (WMA, 2016) clearly stipulates the ethics of database research. Some public databases, such as the NDB, have a legal basis for research use, but there is no general regulation of database research in Japan (Yamamoto,2014). Japan's new Clinical Research Act, enforced in April 2018, does not include observational studies among its targets. The Protection of Personal Information Act (PPI Act), which regulates the handling of personal information, excepts research in general. Only the National Research Ethics Guidelines set such rules, and based on these guide- lines, only research approved by an Ethics Review Board can be conducted. These guidelines basically impose strict rules that override the PPI Act. In observational research using databases, opt-in is required in principle, as specified by the PPI Act. A new law enacted in 2018, usually referred to as the Next-Generation Medical Infrastructure Act, allows the use of anonymized medical data in an opt-out basis((Kumamaru et al., 2020)).

Privacy violating interactions and presentation in IoT-based healthcare applications like heartbeat monitors, geo-tracking devices, automated insulin pumps, and other healthcare devices envisage and require strong interaction with the patient. In such devices, the information will be provided through sensors or other recorded medical device readings. This information goes through different devices to reach its ultimate destination and becomes a threat to privacy when this sensitive information is exchanged through different systems. In smart cities, for instance, an individual could make a query for the way to a specific health clinic. Such a query should not be answered, for instance, by showing the way to a health clinic nearby, visible to any passerby, another example of such medical devices that do not encrypt data while transmitting to the remote server. Any adversary intending to sniff that data could easily use this information for a malicious purpose. Due to the close interaction and presentation techniques, the threat of privacy-violating interaction and presentation is a major challenge in healthcare laws (CIPIT, 2021).

Life cycle transition privacy is compromised when private information is disclosed by IoT devices during the life cycle transition. These devices hold information like vital sign readings, drug dosage, and actuator functions. Healthcare data is highly sensitive, but also the collection of simple usage data (e.g., location, duration, frequency) could disclose a lot about the life cycle of people. Despite evident problems with healthcare devices, the life cycle transition problem has never been addressed. The life cycle of healthcare devices is still modeled as buy-once-own-forever and solutions have not evolved beyond a total memory wipe (e.g., before selling a wearable) or physical destruction. There is a need to identify the requirements for flexible solutions to implement convenient privacy life cycle management mechanisms (Nishat, 2021).

In Japan, there is no special law for the comprehensive utilization of personal data in the medical field, and a comprehensive legal system has been lacking for decades. This paper examines the background and issues of the cancer registration law specific to cancer and the legal structure of medical information in Japan and points out that one of the problems that has become clear in dealing with COVID-19 is the difficulty of handling the complicated system of anonymously processed information and the difficulty of using it for the purpose. The report also points out that the Medical Big Data Law, which is also based on the premise of anonymous use, has a complex mechanism in addition to that of the Personal Information Protection Law (JLT, 2019). A system to certify certification bodies and other protection measures will be introduced yesterday, but before examining the specifics of anonymization, it is necessary to establish a fundamental system that enables the use of more basic information in a way that can be easily understood by healthcare professionals (IFIPAICT, 2022).

Linkage refers to the linkage of different previously separated systems like combining forms of revealed data sources. When data is gathered from different sources with different permissions and contexts it causes loss of context and poor judgment. Threats of linking different systems and data sources are not novel. Online social networks and integrated third-party applications are facing the same problems. However, IoT networks and services rely on the interaction and collaboration of many coequal systems. Managing the numerous devices in IoHT systems and their connectivity with other systems will raise more challenges in linkage threats. The threat of linkage will cause problems in the IoT evolution process. There are mainly two reasons for it. First, the horizontal linkage of different companies and manufacturers systems to create a heterogeneous distributed system-of-systems delivering new services that no single system can provide. Successful linkage will make data exchange more agile and controllable between different parties. However, horizontal linkage also causes more local data flows than vertical linkage that could improve privacy. These problems should be properly addressed in IoT healthcare laws to prevent passive monitoring and intrusive data collection by IoT devices(Flash,2018).

As indicated by (CIPIT, 2022), From 14 July 2022 in Kenya, the provisions of the Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021 (the Regulations) will come into force and the process of registration with the Office of the Data Protection Commissioner (the ODPC) will also begin for data controllers and data processors. All civil registration entities (such as the Office of the Registrar of Persons which issues national identity cards) specified in the Data Protection (Civil Registration) Regulations, 2020 are exempt from the Regulations. Aside from this exemption, the Registration Regulations also exclude the following data controllers and data processors from mandatory registration: those with an annual turnover or annual revenue of below KES 5 million (approx. USD 42,000) and those with less than 10 employees.

However, it is worth noting that the Regulation also appears to contradict the above exemption, providing that the above entities are still required to undertake mandatory registration. It is not clear how the two provisions will be reconciled. Following the commencement of the registration process, we anticipate that the position will become clearer. For some entities, registration will be considered mandatory. These include entities processing personal data for activities such as gambling, health administration, financial services, telecommunication services, and transport services, regardless of whether they have an annual turnover or annual revenue of below KES 5 million (approx. USD 42,000) or have less than 10 employees (CIPIT, 2022).

Densely populated countries such as the US, UK, and China have streamlined their healthcare systems, national

telemedicine infrastructure, and self-triage options to enhance access to healthcare among the citizenry. Self-triage or symptoms checkers were embraced to reduce over- reliance on medical professionals, reduce medical visits, and reduce the cost of healthcare (Montenegro, da Costa, & da Rosa Righi, 2019). Unlike telemedicine, the adoption of AI-led conversational agents triage systems has proved cost-effective as they leverage mobile applications accessible to all citizens. Since devolution, the healthcare industry in Kenya has seen a reduction in funds, thus affecting resourcing of existing healthcare facilities and the construction new facilities to meet healthcare demands (Masaba et al, 2020). Underfunding has also contributed to the scarcity of medical supplies forcing patients to procure the medicine from private facilities. Furthermore, due to poor remuneration, healthcare workers have continually been on a go-slow or strikes, leading to the closure of healthcare facilities. The WHO has stipulated that globally, the recommended ratio between skilled health workers and the population is 1.74 per 1000 population. This is equivalent to 17.4 per 10,000 in Kenya (Organization, 2019). In his study (Isabai, 2020), highlighted that the decline in the health worker-to-population ratio in Kenya has been attributed to neglect of healthcare system development, brain drain, deplorable working.

Kenya's name is a household among the countries leading in technology. Following the launch of M-Pesa in 2007, Kenya has emerged as a global leader in the development of mobile money and in increasing rates of financial inclusion. Kenya leads the world in mobile payment services and platforms and has reached exceptionally high levels of financial inclusion. It could be noted that, unlike many other countries, Kenya also has a comprehensive and reasonably functional system to provide unique identification to its population, which is extensively used for know-your-customer (KYC) purposes and citizen- government interactions. It should also be recognized that as early as 2002 the government had begun to develop an e-governance strategy. The mobile financial services revolution that began in 2007 allowed this strategy to be implemented more intensively, as well as dynamizing the private sector. The combination of Kenya's digital payments platform and its identification system opens the way to leverage digital technology in many ways to better provide a range of services, and opportunities to beneficiaries of public programs, business, and taxpayers and investors. Digitization has played, and continues to play, a critical role in strengthening the relationship between government policies, regulatory institutions, and the desired economic, political, and social outcomes. More importantly, it has become an enabler of market development. It can, however, also be constrained by the capacity of regulatory institutions and regulatory technology(Ndung'u, 2019).

With the Registration Regulations in force, it is incumbent on all data controllers and data processors to register with the ODPC to avoid penalties for non-compliance. Further, failure to comply with the requirement to register may have other repercussions such as denial of operating licenses. For example, the Central Bank of Kenya Act (Chapter 491 of the Laws of Kenya) was amended to require digital credit providers to be registered with the OPDC, failing which they would be denied the necessary licenses for their business from the Central Bank. With the myriad of amendments made to various legislation following the enactment of the Data Protection Act, 2019 (the DPA), such as amendments to the Capital Markets Act (Chapter 485A of the Laws of Kenya) and the Kenya Information and Communications Act (No 2 of 1998), to name a few, it is likely that the effects of registration of data controllers and data processors under the DPA will have far-reaching implications on how organizations operate in Kenya. These implications would primarily relate to the processing of personal data by organizations established in Kenya and the processing of personal data relating to natural persons located in Kenya (Makulilo & Boshe 2016).

According to (CDC, 2022), Health Insurance Portability and Accountability Act (HIPAA) was enacted by the US government to implement the security and privacy of healthcare data for American citizens. It has separate rule sets for security and privacy. The privacy rules enable the privacy of the health data to protect the data from disclosure. The security rules provide security of the individuals' health information by adopting advanced technologies to acquire more efficient means of patient care. The HIPAA security and privacy rules are implemented to healthcare and non-healthcare organizations that store, transmit, and process healthcare data of US citizens by any means. In May 2018, a new General Data Protection Regulation (GDPR) replaced directive 95/46 consolidating and innovating data protection rules. The introduced GDPR is considerably more comprehensive and establishes requirements for internal compliance mechanisms that did not exist in the legislation. It applies to all sectors of the economy, all broadly defined personal data, and every sector that controls or processes data. Moreover, it applies protective standards throughout the lifespan of the data. GDPR is designed to enable people to better control their data. Although the EU already established its data protection directive in 1995, it was not completely reasonable for all the member states of the EU. To remove all the reservations, the GDPR has been established and is applicable throughout the EU.

The Privacy Act (Australia) entails the set of principles of Australian legislation to protect the personal information of Australian citizens. These principles refer to the usage, storage, and disclosure of personal information. Moreover, individuals have the right to the access and correction of their personal information. This law also includes data security, data quality, and cross-border data flow policies (Semantha et al., 2020).

As stated by (Semantha et al., 2020), Saudi Health Information Exchange Policies (SHIEP) main objective is to present the permissible usage of the KSA (Kingdom of Saudi Arabia) health information exchange like patient care, public health, and quality. This policy applies to all individuals and organizations who have access to the Saudi Health Information Exchange managed records such as participating healthcare subscribers, business associates, health information services providers, and subcontractors. Personal Health Information (PHI) will be available for treatment, healthcare operations, and public health, but it may be permitted for research and education. This policy shall not permit the usage of healthcare information for market studies and legal investigation or inquiry. The purpose of this policy is to ensure that the information security is conducted in a manner that protects personal health information and supports the availability, confidentiality, integrity, and accountability of the Saudi Health Information Exchange shared clinical information. Saudi Arabia's Ministry of Health has published a suite of policies relating to the Saudi Health Information Exchange ("SHIE") initiative (may also be referred to as Saudi eHealth Exchange ("SeHE")), which is broadly aimed at the use of health information, including patient data, in the context of the increased adoption of technology and digitalization in the health system. While the exact legal status of the policies and the programme is not entirely clear, the policies provide a good indication of what the Ministry of Health expects in terms of the use of data in a healthcare context (Semantha et al., 2020). Healthcare technology providers seeking to introduce their solutions to the Saudi market need to familiarize themselves with the legal and regulatory framework relating to the use of patient data. It is not permitted to disclose patient health information held in the SHIE system other than for the treatment, patient use, operational and public health purposes specified in the policies. The patient care rights section of the SHIE policies provides for a mechanism for patient complaints, including in respect of data breach incidents (in respect of which there is an obligation to notify affected persons), as well as a mechanism by which patients may seek a report of any disclosure of information about them via the SHIE system (Semantha et al., 2020).

Following recent guidance by the ODPC, we understand that an entity that should register as a data controller and data processor needs to make two separate registration Following a seven-year effort to develop a substantive law on data protection, Kenya enacted the Data Protection Act 2019 (the Act) on 25 November 2019. Previously, data protection in Kenya was regulated under various sectoral laws and the Constitution, Articles 31(c) and (d) of which guarantee every person a right to privacy over information relating to their family or private affairs and over their communications. The sectoral laws that contained provisions on data protection included the Access to Information Act, the Kenya Information Communications Act, the Banking Act, the Public Health Act and the HIV Aids and Prevention Control Act. The Act provides a comprehensive legal framework on data protection in Kenya, giving effect to Articles 31 (c) and (d) of the Constitution. It has also amended several existing laws to include provisions on data protection, some of which shall be discussed in greater detail below. Where sectoral laws have not been amended, they continue to apply to the extent they do not conflict with the Constitution or the Act (CIPIT, 2022).

Four sets of regulations have been published to provide guidelines on some provisions of the Act.

- the Data Protection (Civil Registrations) Regulations 2020 came into force in October 2020 and regulate the processing of personal data by civil registries, including births, deaths, adoptions and marriage;
- the Data Protection (General) Regulations 2021 (the General Regulations) provide guidelines on some of the processing requirements or obligations set out under the Data Protection Act, and came into force in February 2022;
- the Data Protection (Complaints Handling and Enforcement Procedures) Regulations 2021 were published to facilitate fair, impartial and expeditious investigations and hearings of complaints lodged with the Data Commissioner, and to provide for the issuance of penalty and enforcement notices; they also came into force in February 2022; and
- the Data Protection (Registration of Data Controllers and Data Processors) Regulations 2021 provide the procedure for the registration of data controllers and data processors in Kenya, and will come into force in August 2022.

Public and private healthcare providers have incorporated eHealth and telemedicine to streamline healthcare processes, reduce cost, enhance quality, and reach out to persons with unmet healthcare needs (Isabai, 2020). Telemedicine has gained traction among providers who render specialized healthcare services, meeting patients with chronic diseases. Existing Telemedicine initiatives have been through online video conferencing and call centers. Both eHealth and telemedicine have not been effective in meeting the considerable healthcare deficit among the population due to underlying systemic challenges within the healthcare sector.

The Kenyan health sector is embracing the use of technology, e–Health, to improve healthcare services and the quality of care. This transition is characterized by the introduction of technologies such as Health Information Systems (HIS), mHealth,1 and telemedicine to provide health services. Owing to the digitization of health records, m-Health and HIS services have significantly increased the amount of health data they process. It is, therefore, critical to understand how data is managed and protected (in addition to the already existing norms of confidentiality) in these processing activities in the

health sector in order to ensure patients' right to privacy are protected. The Health Act, enacted in 2017, gives powers to the Cabinet Secretary for the Ministry of Health to establish and maintain a comprehensive integrated Health Information System. Further, the Cabinet Secretary is obligated to develop legislation within three years of the Act providing provisions for the protection, management, collection, use, and disclosure of personal health data. The Health Act introduced and recognized eHealth The Kenya Standards and Guidelines on m-health Systems describes mobile health (m-health) as the use of portable devices such as cellphones to provide health services and information and or, interventions and programs designed to support health service provision through mobile technology and devices. as a form of health service. The increase in the development and adoption of eHealth, m-Health and telemedicine platforms, and emerging technologies such as Artificial Intelligence (AI) to detect, predict and diagnose disease has made health data a commodity. It is in this environment that we analyze the policy structures relating to health data in light of the DPA. It is necessary to understand the legislative gaps that currently exist in health acts and policies enacted prior to the DPA to enable the development of data protection guidelines, specific to the health sector, that ensure compliance with the act.

Technology is not enough to achieve these goals. Therefore, changes should be made not only at the technological level but also in the management and design of complete healthcare processes and what is more, they should affect the business models of service providers. The use of Big Data Analytics is becoming more and more common in enterprises. However, medical enterprises still cannot keep up with the information needs of patients, clinicians, administrators and the creator's policy. The adoption of a Big Data approach would allow the implementation of personalized and precise medicine based on personalized information, delivered in real time and tailored to individual patients. As noted by (Batko and Slezak, 2022), to achieve this goal, it is necessary to implement systems that will be able to learn quickly about the data generated by people within clinical care and everyday life. This will enable data-driven decision making, receiving better personalized predictions about prognosis and responses to treatments; a deeper understanding of the complex factors and their interactions that influence health at the patient level, the health system and society, enhanced approaches to detecting safety problems with drugs and devices, as well as more effective methods of comparing prevention, diagnostic, and treatment options.

Approach to fully assess which health-specific data protection guidelines are needed, we examined the existing laws and policies that relate to the processing of health data. The assessment identified the areas in the laws and policies that comply with the provisions in the Data Protection Act and areas where there are gaps. The laws and policies analyzed included: i. The Health Act, 2017. ii. Health Sector ICT Standards and Guidelines for m-Health Systems. iii. Standards and Guidelines for Electronic Medical Record Systems in Kenya iv. Kenya National eHealth Policy 2016-2030. v. Health Information Systems Policy 2014-2030. vi. HIV/AIDS Prevention and Control Act. vii. Standard Operating Procedures in Handling Health Records and Information Management During the COVID-19 Pandemic (Anjarwalla & Khanna, 2022).

Effective HISs are dependent on an understanding of the aim of integration and its desired benefits. Activities that lead to better integration address the interest in getting more and better information, e.g. on health needs or the outcome of health services. The latter can be measured by assessing the effectiveness of surgical procedures, quality of life, and similar outcomes. Other activities that lead to better integration include better opportunities for linking data between different registries, integration of relevant data sources in a central database or platform, integration of information on health and social care, and opportunities to integrate data at the personal level. These provide better insights into improving the management of care pathways, service delivery and quality, and the impact of social. The objectives of national HISs, and integration projects and their challenges differ between decentralized and centralized political structures, systems based on national health services and (social) health insurance, and the size of the population. These structures have an impact on governance, cooperation and coordination, and are of fundamental relevance for the successful development and implementation of integrated HISs. Optimism has been created for better integration by new technologies, such as information and communication technology (ICT), and secondary use of data from e-health applications, even though there are considerable challenges that need to be overcome before these technologies can be harnessed(Michelsen et al., 2015).

Over the past few years, the legal situation for integration of personal data has become more restrictive in some countries and less restrictive in others (Michelsen et al., 2015).In some countries, discussion to make linkages easier is ongoing. In others, there is no political will to integrate data, such as those from the mortality database with data from patient records. When experts were asked how the integration of their national HISs could be improved, some answered explicitly that they would like changes in the legislative environment to overcome the limitations of data protection by implementing pseudonyms and finding an answer to how to prevent re-identification. They agreed that this would have to be implemented without compromising the privacy of citizens and patients.

The Data Protection Act introduced principles that elevated the standard of health data processing. Primarily, the DPA defines health data as a special

category of data and establishes data protection principles that must be applied when processing data. Health authorities are now required to ensure that personal data is used fairly, lawfully, and transparently, and only to the extent necessary to pursue health-related public interests, in accordance with the applicable data protection principles under the Data Protection Act (Anjarwalla & Khanna, 2022).

A study by (Isabai, 2020) regarding Kenya stipulated that the realization of AI-led self-triage systems is a possibility. Digital penetration and literacy in Kenya have been on the rise, meaning the public has access to digital technical technology and better understands their operation. Telemedicine initiatives have proved to be costly, as it requires the deployment of ICT infrastructure within the country. Leveraging digital penetration and literacy among citizens in delivering AI-Led conversational self-triage systems will enhance access to primary healthcare. Accessible to all citizenry on the web or smartphone, the AI-self-diagnostic conversation agents will provide medical consultation to the citizenry and make referrals.

The health sector has enacted laws and policies that require and recognize data protection when health data is processed. While these identified laws and policies address distinct issues and acknowledge certain data protection principles, they are, in specific instances, inconsistent with the Data Protection Act. As a result, it is necessary to amend these laws and policies to ensure full compliance with the DPA. Specifically, the Health Act, Health Sector ICT Standards and Guidelines for m-Health Systems, Standards and Guidelines for Electronic Medical Record Systems in Kenya, Kenya's National eHealth Policy 2016-2030, Kenya's National eHealth Policy 2014-2030, and Kenya's Health Information Policy 2014-2030 must be amended (Anjarwalla & Khanna, 2022).

Data Protection Act principles relating to health data Health laws and policies relating to health data, specifically, to processing health data Integrity and Confidentiality (security): the principle requires the processing of data in a manner that ensures the security of the personal data including protection against unlawful, unauthorized or accidental loss. These data are provided not only by patients but also by organizations and institutions, as well as by various types of monitoring devices, sensors or instruments. Data that has been generated so far in the healthcare sector is stored in both paper and digital form. Thus, the essence and the specificity of the process of Big Data analyses means that organizations need to face new technological and organizational challenges. The healthcare sector has always generated huge amounts of data and this is connected, among others, with the need to store medical records of patients. However, the problem with Big Data in healthcare is not limited to an overwhelming volume but also an unprecedented diversity in terms of types, data formats and speed with which it should be analyzed in order to provide the necessary information on an ongoing basis. It is also difficult to apply traditional tools and methods for management of unstructured data. Due to the diversity and quantity of data sources that are growing all the time, advanced analytical tools and technologies, as well as Big Data analysis methods which can meet and exceed the possibilities of managing healthcare data, are needed (Batko and Slezak, 2022). As (Ndungu, 2019) noted, even as it can help to strengthen government capacity, digitization raises new demands on that capacity for effective regulation. To reap the full range of potential benefits, Kenya will need to ensure a competitive ecosystem and infrastructure that facilitates entry. An enabling regulatory environment and robust consumer protections will also be critical.

This requires the implementation of appropriate technical and organization measures to ensure security of the data with the exception of the Health Act, the laws and policies listed in the 'Approach' section fully capture the integrity and confidentiality principle outlined in the DPA, particularly in relation to data access. The Health Act, however, makes no reference to the security provision. It does recognize the right to privacy and provides that an individual has the right to be treated with dignity and respect and to have their privacy respected in accordance with the Constitution and the Act. Purpose limitation: this refers to the collection and processing of data for specified, explicit and legitimate purposes with no further processing that is inconsistent with the original purpose for which the data was collected. For example, where health data is collected for the purpose of medical examination and treatment, it cannot be used for research purposes unless consent is obtained and the consent is properly communicated prior to the data collection (CIPIT, 2022).

The purpose limitation principle is present only in the Kenya Standards and Guidelines for m-Health Systems. All the other acts examined make no mention of it. Data minimization: this refers to the collection of data that is adequate, relevant and necessary in relation to the purpose for which it is collected. The data minimization principle is only found in the Kenya National eHealth policy. All the other laws and policies examined) make no mention of it Consent: consent refers to manifestation of express, unequivocal, free, specific and informed indication of the data subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of personal data relating to the data subject. Consent often forms the legal basis for the lawful collection and processing of personal data and in this context health data. The DPA gives provisions on the conditions for consent. The principle of consent is addressed in the Health Act (Section 9), the Kenya Standards and Guidelines for m-Health Systems, and the Kenya National Patients' Rights Charter. The first chapter of the Patients' Right Charter discusses patient rights; among these rights, the right to confidentiality,

the right to give informed consent to treatment, and the right to information while the second chapter discusses responsibilities, particularly the obligation to provide relevant, accurate information to health care providers (CIPIT, 2022). Rights of a Data subject: in this context these are the rights of a patient exercisable with respect to the processing of their data. The Act provides for the rights of a data subject to include: the right to be informed on the use of their personal data; the right to access their personal data; the right to object processing of their personal data; the right to correct false or misleading data, and the right of deletion of false or misleading data. This principle is present in the Kenya National Patients' Rights Charter and the Kenya National eHealth Policy. Patient rights are discussed in the Charter, including the right to confidentiality, the right to give informed consent to treatment, and the right to information. The Kenya National eHealth Policy discusses the importance of taking a patient-centered approach to managing and utilizing electronic data in a manner that ensures the confidentiality, integrity, and privacy of patients at all times. All the other acts examined (listed in the Approach section) make no mention of it. Data Transfer: The Act provides for data transfer in the context of cross border data transfer – that is, the transfer of data outside the Kenyan jurisdiction. Data can only be transferred outside of Kenya in accordance with the provisions prescribed under Section 48 and the establishment of appropriate safeguards under Section 49 This is part of the Kenya National eHealth Policy's goal of increasing access to electronic health services. Among the interventions that must be implemented to ensure electronic health service accessibility are the promotion of cross-border sharing of health information without compromising patient privacy. All the other acts examined (listed in the Approach section) do not address this principle (Anjarwalla & Khanna, 2022).

Howbeit, Kenya is not at a comparison level in healthcare technology and data privacy and protection levels as is the case with their financial technological prowess. If and when the same focus can be meted out on healthcare matters as it deserves the storyline will most definitely change. The Cabinet Secretary for Health (MOH), the Office of the Data Protection Commissioner (ODPC), and the Medical Practitioner Board should collaborate to develop standardized data protection guidelines for the health sector. The guidelines should provide guidance on the implementation of the data protection principles in the health sector, consent, exercise of data subjects rights, responsibilities of healthcare institutions in data processing, the responsibilities of health care practitioners in the processing of data, data transfer, and data sharing (CIPIT, 2022). A country may or may not have a law for user data protection, but the healthcare system should follow the laws of the country from which the user belongs. The same thing applies to the social and cultural norms, which should be applied according to the laws of the state to which the user belongs. In the case of data residing on cloud servers, again, the privacy laws will be applied according to the region of the patients (CDC, 2020).

For digitization to be sustainable, the areas of concern will need to be addressed. First, challenges on the market side include connectivity, transparency, interoperability and the problem of market dominance, market segmentation, and associated regulatory challenges. Second, better institutions to protect the market, such as consumer protection laws and competition regulations, are essential. This may not require the creation of new regulatory institutions; existing laws can be amended and enhanced, and existing institutions strengthened in terms of capacity, as well as legal frameworks to support their regulatory 37 capabilities. There are already significant overlaps in regulatory agencies and creating additional ones will create room for diffusion of responsibility problems leading to regulatory failure. Third, market infrastructure issues will require attention, from improving connectivity to reducing unit costs. Finally, the identification system needs to be upgraded to provide the inclusive, privacy-protecting, e-ID that Kenyans will need as the country transitions further towards a digital economy and society (Ndungu, 2019).

As indicated by (CIPIT, 2022) The Health Act should include a provision addressing the integrity and confidentiality of data access (security). While it recognizes the right to privacy and states that an individual has the right to be treated with dignity and respect and to have their privacy respected in accordance with the Constitution and the Act, it should be revised to include this principle and to require the implementation of appropriate technical and organizational measures to ensure data security. II. The Standards and Guidelines for EMR Systems should incorporate minimum implementation requirements that are consistent with the data protection principles in the Data Protection Act. These include: lawfulness, fairness, and transparency, accuracy, data minimization, purpose limitation, storage limitation, security, data retention, and accountability, as outlined in Section 25 of the Data Protection Act. Policy Recommendations. The Cabinet Secretary for Health (MOH), the Office of the Data Protection Commissioner (ODPC), and the Medical Practitioner Board should collaborate to develop standardized data protection guidelines for the health sector.

Healthcare providers must ensure that they properly manage patient data to create a culture of trust and transparency with patients while meeting strict data privacy and legal regulations. Data privacy in healthcare is constantly evolving with continuously updated laws and regulations. In this way, patients get the data privacy they deserve and expect.

CONCLUSION AND FUTURE PERSPECTIVES

After a widely reviewed analysis, this study produced several observations, primarily on the challenges and opportunities on data protection and privacy in healthcare. There are numerous benefits to improving how health data is processed especially, in regards to improving the delivery of healthcare services. These benefits are only possible if data is collected and processed in a manner that protects and preserves the data subject's rights, particularly as it relates to their personal health information. It is important, therefore, to ensure that the systems in use adhere to the data protection standards mandated in the Data Protection Acts, and to revise the existing laws and policies, and develop sector-specific guidelines, to guide the processing of health data to ensure compliance with the act. This review paper discussed the key contexts of data privacy and protection in different environments while comparing and contrasting the challenges and opportunities. The healthcare system should be designed in such a way that it provides the controls in a user-friendly manner. Authorized personnel for example an end-user must have full control over his/her collected data at any moment and can be traced to identify the end user for accountability i.e., to whom it can be or cannot be shared. At any moment, the user should be given the possibility to know and control who has his data, what data have been collected, and for what purposes they will be used for the legitimate initial purpose.

Healthcare data is a subset of personal information and needs extra security policies and protection. All organizations that provide a health service and hold health information (other than an employee record) are covered by the Privacy Act, whether or not they are small businesses. In certain circumstances, the Privacy Act permits the handling of health information and personal information for health and medical research purposes, where it is impracticable for researchers to obtain individuals' consent. Because of the key role of the IoT in disease prevention, real- time tele- monitoring of patient's functions, testing of treatments, health management, and health research, considering the risks relating to Health care and patient data is essential. Moreover, health policymakers should be aware of the ethical commitment to using IoT technology.

In developed countries, there are data privacy and protection laws implemented to securely process citizens' personal data. American, European, Japan, Australia and other leading countries' law enforcement organizations are working to find a common ground for solving healthcare data privacy problems while also making a more effective existing legal framework. An effective legal framework should ensure the user's awareness and their control over the IoT healthcare products with their services. Compliance with other international data privacy frameworks makes it more adequate with HIPAA in full force and costs of potential data breaches skyrocketing, the importance of reliable security is greater than ever. Monitoring software provides the first level of defense against insider threats and will help healthcare organizations stay on top of their security and compliance needs.

We believe this research will help the industrial and governing bodies to design and implement IoT-enabled healthcare systems while protecting the security and privacy of individuals. As future work, we plan to explore cybersecurity risk assessment approaches with respect to IoHT to aid organizations and governments in better protecting themselves against pertinent risks. Sharing health-care data is needed, achievable and worthwhile. Digital identity is required to make this happen. Consumers will be able to see and donate their data, allowing them to become health-care heroes every day. Modern medicine best practice holds that the health-care system empowers the patient by putting them in the center of their own health-care story; each individual creates their own circle of care. We do not yet have the tools to allow patients to do this but a suggestion on having a universal healthcare Data Protection Act should be envisaged. This will hasten data awareness and warrant healthcare data the importance and value it deserves.

ACKNOWLEDGEMENT

We would like to acknowledge Nagasaki University in Japan, KEMRI Graduate School/Jomo Kenyatta University of Agriculture in Kenya and Kenya Medical Training college for the moral support.

Contributors: Salim Omambia Matagi and Satoshi Kaneko are the sole authors and responsible for ideation, writing, images and submission.

Funding: The authors have not declared a specific grant for this research from any funding agency in the public, commercial or not- for- profit sectors.

Competing interests None declared.

Patient consent for publication Not applicable.

Ethics approval This study does not involve human participants.

Provenance and peer review Not commissioned; externally peer reviewed.

Data availability statement: Data sharing not applicable as no datasets generated and/or analyzed for this study.

ORCID Salim Omambia Matagi-
https://orcid.org/0000-0002-8795-4987

REFERENCES

1. Abouelmehdi, K., Beni-Hessane, A. and Khaloufi, H. (2018) *Big Healthcare data: Preserving Security and Privacy - Journal of Big Data*, *SpringerOpen*. Springer International Publishing. Available at: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-017-0110-7 (Accessed: October 29, 2022).
2. Ahmed Elngar, Ambika Pawar and Prathamesh Churi.(2021) Data Protection and Privacy in Healthcare Publisher: CRC Press City: Boca Raton, FL : CRC Press, 2021.Year:2021Edition:1 http://dx.doi.org/10.1201/9781003048848
3. Alofaysan, S., Alhaqbani, B., Alseghayyir, R., & Omar, M. (2014). The significance of data governance in healthcare: A case study in a tertiary care hospital. HEALTHINF 2014 - 7th International Conference on Health Informatics, Proceedings; Part of 7th International Joint Conference on Biomedical Engineering Systems and Technologies, BIOSTEC, 2014; 178–187. https://doi.org/10.5220/0004738101780187.
4. Anjarwalla & Khanna(2022) Data Protection Registration Law Comes Into Force On 14 July 2022 - Data Protection - Kenyahttps://www.mondaq.com/data-protection/1216300/data-protection-registration-law-comes-into-force-on-14-july-2022.
5. Batko, K., & Ślęzak, A. (2022). The use of Big Data Analytics in healthcare. *Journal of Big Data*, *9*(1). https://doi.org/10.1186/s40537-021-00553-4
6. Boysen, A. (2022) *The Need for a National Digital Identity Infrastructure, Centre for Intellectual Property and Information Technology law*. Available at: https://cipit.strathmore.edu/developing-data-protection-guidelines-for-the-health-sector-in-kenya/ (Accessed: October 24, 2022).
7. Campbell, J., & Mills, J. A. (2022). Health systems and policy research needed to strengthen the rehabilitation workforce. Bulletin of the World Health Organization, 100(11): 747–748. https://doi.org/10.2471/BLT.22.289032
8. Centers for Disease Control and Prevention *(2022).Health Information & Privacy: Ferpa and HIPAA. Centers for Disease Control and Prevention*. Centers for Disease Control and Prevention. Available at: https://www.cdc.gov/phlp/publications/topic/healthinformationprivacy.html (Accessed: October 23, 2022).
9. Chiolero, A. (2022). How infodemic intoxicates public health surveillance: from a big to a slow data culture. Journal of Epidemiology and Community Health, 76(6): 623–625. https://doi.org/10.1136/jech-2021-216584
10. CIPIT (2021). Centre for Intellectual Property and Information Technology. Privacy and Data Protection Practices of Digital Lending Apps in Kenya. *Journal of Intellectual Property and Information Technology Law (JIPIT): 1*(1): 131–169. https://doi.org/10.52907/jipit.v1i1.68
11. *Developing data protection guidelines for the health sector in Kenya* (2022) *Centre for Intellectual Property and Information Technology law*. Available at: https://cipit.strathmore.edu/developing-data-protection-guidelines-for-the-health-sector-in-kenya/ (Accessed: October 24, 2022).
12. Ekran Systems (2019) Healthcare Data Security: How to protect patient health information?, Ekran System - Insider Threat Protection Software. Available at: https://www.ekransystem.com/en/blog/healthcare-data-protection-solutions-monitor-and-audit-your-software (Accessed: October 30, 2022).
13. Enrico D'Ambrogio (2020) Japan's ageing society: Think tank: European parliament, Think Tank | European Parliament. European Union, 2020. Available at: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2020)659419 (Accessed: October 29, 2022).
14. Fernandes L, O'Connor M and Weaver V (2022) Big Data in health care: Challenges and opportunities. Available at: http://infokara.com/gallery/5-jan.pdf (Accessed: October 27, 2022).
15. Flash, K. (2018). The Data Librarian's Handbook. *DttP: Documents to the People*, *45*(4): 32. https://doi.org/10.5860/dttp.v45i4.6571
16. Folio3 (2022) What is the importance of data quality in healthcare in 2022?, Folio3 Digital Health. Available at: https://digitalhealth.folio3.com/blog/importance-of-data-quality-in-healthcare/ (Accessed: October 30, 2022).
17. *Health Information Privacy Law and policy* (2022) *HealthIT.gov*. Available at: https://www.healthit.gov/topic/health-information-privacy-law-and-policy (Accessed: October 23, 2022).
18. *Healthcare Data Security: How to protect patient health information?* (2022) *Ekran System - Insider Threat Protection Software*. Available at: https://www.ekransystem.com/en/blog/healthcare-data-protection-solutions-monitor-and-audit-your-software (Accessed: October 23, 2022).
19. IFIPAICT. (2022). Possible utilization of personal data and medical care in Japan ... IFIP International Conference on Human Choice and Computers. Retrieved October 31, 2022; from https://link.springer.com/content/pdf/10.1007/978-3-031-15688-5_7.pdf

20. Isabai, A. J. (2020). The Implementation of Ai Self-triage Systems as a Digital Health Solution for Primary Healthcare in Kenya: Challenges and Prospects.
21. Japanese Law Translation (2019). Act on Anonymously Processed Medical Information to Contribute to Medical Research and Development [Internet]. [cited 2019 Nov 11]. Available from: http: / / www.japaneselawtranslation.go.jp/law/detail/?id=3343&vm=04&re=01&new=1
22. *Lexology(2020). Data Privacy and protection relating to healthcare in Europe, the United States and Brazil* (2020) *Lexology*. Latin Lawyer. Available at: https://www.lexology.com/library/detail.aspx?g=99b83b76-3f2f-4b23-a5c3-30ad576af369 (Accessed: October 23, 2022).
23. Lodhia, V., Karanja, S., Lees, S., & Bastawrous, A. (2016). Acceptability, usability, and views on deployment of peek, a mobile phone mhealth intervention for eye care in Kenya: Qualitative study. *JMIR MHealth and UHealth*, *4*(2). https://doi.org/10.2196/mhealth.4746
24. Makulilo, A. B., & Boshe, P. (2016). Data Protection in Kenya. In *African Data Privacy Laws* (pp. 317–335). Springer International Publishing. https://doi.org/10.1007/978-3-319-47317-8_15
25. Masaba, B., Moturi, J., Taiswa, J., & Mmusi-Phetoe, R. (2020). Devolution of healthcare system in Kenya: progress and challenges. Public Health, 189: 135-140.
26. Ministry of Education, Culture, Sports, Science and Technology & Ministry of Heath L and W. Ethical guidelines for medical and health research involving human subjects. [Internet]. [cited 2022 Oct 31]. Available from: http://www.mhlw.go.jp/stf/seisakunitsuite/bunya/hokabunya/kenkyujigyou/i-kenkyu/
27. Montenegro, J. L. Z., da Costa, C. A., & da Rosa Righi, R. (2019). Survey of conversational agents in health. Expert systems with applications, 129: 56-67. doi:10.1016/j.eswa.2019.03.054
28. Ndung'u, N. (2019). Digital Technology and State Capacity in Kenya. Center for Global Development, August 2019, 1–43. https://www.cgdev.org/sites/default/files/digital-technology-and-state-capacity-kenya.pdf
29. Nishat, P. (2021) *Data protection in the healthcare sector, Open Access Government*. Available at: https://www.openaccessgovernment.org/data-protection-in-the-healthcare-sector/79169/ (Accessed: October 23, 2022).
30. Organization, W. H. (2019). World health statistics 2019: monitoring health for the SDGs, sustainable development goals: World Health Organization.
31. Price, W.N. II, and Cohen, I.G. (2020) Privacy in the age of Medical Big Data, Nature medicine. U.S. National Library of Medicine. Available at: https://pubmed.ncbi.nlm.nih.gov/30617331/ (Accessed: October 29, 2022).
32. Robb, D. (2021) *The internet of things (IOT) in Health Care, Datamation*. Available at: https://www.datamation.com/networks/internet-of-things-iot-health-care/ (Accessed: October 30, 2022).
33. Salim Matagi Omambia. (2021). Budgetary parameters on health human resource among healthcare workers in Samburu County referral hospital, Kenya. *Open Access Research Journal of Science and Technology*, *1*(1): 01-07. https://doi.org/10.53022/oarjst.2021.1.1.0011
34. Salisbury, H. (2021). Should GPS break the law on data privacy?, Should GPs break the law on data privacy? Available at: https://www.researchgate.net/publication/352277956_Helen_Salisbury_Should_GPs_break_the_law_on_data_privacy (Accessed: October 30, 2022).
35. Sejpal, S. (2022): *Data Protection Registration Law comes into force on 14 July 2022 - Data Protection - Kenya, Data Protection Registration Law Comes Into Force On 14 July 2022 - Data Protection - Kenya*. Anjarwalla & Khanna. Available at: https://www.mondaq.com/data-protection/1216300/data-protection-registration-law-comes-into-force-on-14-july-2022 (Accessed: October 23, 2022).
36. Semantha, F. H., Azam, S., Yeo, K. C., & Shanmugam, B. (2020). A systematic literature review on privacy by design in the healthcare sector. Electronics (Switzerland), 9(3): 1–27. https://doi.org/10.3390/electronics9030452.
37. Shah, R., & Chircu, A. (2018). Iot and Ai in Healthcare: a Systematic Literature Review. *Issues In Information Systems*, *19*(3): 33–41. https://doi.org/10.48009/3_iis_2018_33-41.
38. Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data Protection and Privacy of the Internet of Healthcare Things (IoHTs). *Applied Sciences*, *12*(4): 1927. https://doi.org/10.3390/app12041927
39. *The importance of data privacy in Healthcare* (2022). *Tiga Healthcare Technologies*. Available at: https://www.tigahealth.com/the-importance-of-data-privacy-in-healthcare/ (Accessed: October 23, 2022).
40. Wiewiorówski, W. (2020). A Preliminary Opinion on Data Protection and Scientific Research. *The European Data Protection Supervisor (EDPS): January*, 1–36. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.
41. World Health Organization (2022) *Universal Health Coverage (UHC): World Health Organization*. World Health Organization. Available at: https://www.who.int/news-room/fact-sheets/detail/universal-health-coverage-(uhc) (Accessed: October 29, 2022).

42. What is health policy and systems research (HPSR)? Geneva: Alliance for Health Policy and Systems Research; 2022. Available from: https://ahpsr .who.int/what-we-do/what-is-health-policy-and-systems-research-(hpsr) [cited 2022 Sep 19]
43. World Medical Association-Declaration of Taipei. (2016). *WMA - The World Medical Association-Declaration of Taipei*. The World Medical Association. Retrieved October 31, 2022, from https://www.wma.net/what-we-do/medical-ethics/declaration-of-taipei/.
44. Yamamoto, R. (2014). Privacy and public benefit in using large scale health databases. *YAKUGAKU ZASSHI*, *134*(5): 607–612. https://doi.org/10.1248/yakushi.13-00256-5.
45. YAMAMOTO, R. (2016). Large-scale Health Information Database and Privacy Protection. *Japan Medical Association Journal: JMAJ*, *59*(2-3): 91-109. https://doi.org/https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5333617/.
46. Yin, D. *et al.* (2022) *China's Personal Information Protection Law*, *The BMJ*. British Medical Journal Publishing Group. Available at: https://www.bmj.com/content/379/bmj-2022-072619 (Accessed: October 23, 2022).
47. Zakerabasali, S. (2022). *Internet of Things and healthcare system : A systematic review of ethical issues*. *August*.https://doi.org/10.1002/hsr2.863