An Overview of Data Protection in Kenyan Health Sector

Strathmore University

Centre for Intellectual Property and Information Technology Law

1.0 Introduction

The use of big data analytics and new technologies in the health sector has considerably changed how health data is being used, accessed, analyzed, and shared between health professionals and individuals. Organizations that handle health data and embrace these new techniques and practices have to maintain a high standard of security and privacy.[1] Privacy and confidentiality of health data is not a new concept within the health sector, as its existence and practice are grounded on creating and maintaining trust. This concept dates back to the creation of the Hippocratic oath.[2] The obligation of privacy and confidentiality prohibits the unintended sharing of health data. Rapid technological advancements in the health sector have made privacy and confidentiality now more than ever important. Thus, data protection plays a significant role in protecting the processing of health data and binds healthcare providers not only by oath but also by law.

> "Privacy and confidentiality of health data is not a new concept within the health sector, as its existence and practice are grounded on creating and maintaining trust."

Privacy in healthcare is rooted in the ethical obligation of health providers who communicate with patients or have access to their medical records to hold that information in confidence. Given the sensitivity of the information that medical practitioners are privy to, professional-patient confidentiality can promote trust and thus effective communication between physicians and patients for the provision of quality healthcare services.[3] It also ensures that the health information is not used against them by third parties, which can lead to economic harm, embarrassment, or discrimination.[4] Beyond ensuring that health information is not disclosed, the duty of confidentiality requires that health records be kept securely. Health records consist of data entered by healthcare professionals, either paper or electronically, to support clinical decision-making.[5] To protect the privacy of health records and support professionals in holding them in confidence, health facilities adopt security measures that generally ensure that only authorized persons have access to information. These include reinforcing the obligation of confidentiality with a confidentiality clause in contracts with health workers.

The right to privacy is a constitutional right established under the Constitution of Kenya 2010.[6] The introduction of the Data Protection Act 2019 (DPA) gives effect to the right to privacy under Articles 31(c) and (d). The DPA categorizes health data under a special category of data, sensitive personal data. In the health sector, data is a fundamental element in the promotion of the right to the highest attainable standard of healthcare. It informs the decisions of players in the health sector in service delivery,

[1] https://globaldatahub.taylorwessing.com/article/health-data-and-data-privacy-challenges-for-data-processors-under-the-gdpr

2

[3] https://www.ncbi.nlm.nih.gov/books/NBK9579/#:~:text=Ensuring%20privacy%20can%20promote%20more,1999%3B%20Pritts%2C%202002

4 https://www.ncbi.nlm.nih.gov/books/NBK9579/#:~:text=Ensuring%20privacy%20can%20promote%20more,1999%3B%20Pritts%2C%202002

[5] 'Confidentiality and Privacy of Personal Data.' (National Center for Biotechnology Information) https://www.ncbi.nlm.nih.gov/books/NBK236546/

[6] Article 31

health research, health education, financing, human resources development, policy development and implementation, and governance and regulation.[7] The purpose data serve is dependent on whether data is collected from an individual, facility, or population level. Still, it ultimately eases the identification of problems and needs and the optimal allocation of scarce resources and enables the making of evidence-based decisions in health policy.[8]

With the ongoing shift towards the use of information technology in data management, understanding data protection in the context of the health sector becomes imperative in ensuring the right to privacy is maintained in addition to the already existing norms of confidentiality. 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 (HIS).[9] Further, the Cabinet Secretary is obligated to come up with legislation within three years of enacting the Act providing for the protection of privacy and the management, collection, use, and disclosure of personal health information as well as m-Health, e-learning, and telemedicine.[10] The Health Act also introduced and recognized eHealth as a form of health service. Consequently, there has been an increase in the development and adoption of eHealth, mhealth, and telemedicine platforms, and the adoption of AI technologies in the health sector to detect, predict and diagnose diseases for which data has become a commodity. This has further propelled the generation and use of health data. It is in this context that we analyze the policy structures relating to health data in light of the DPA which introduces new standards in the processing of personal data. This is also necessary for understanding the policy gaps that exist to enable the development of data protection guidelines specific to the health sector.

2.0 Existing laws and Policies.

The laws and policies reflected below, in one form or another, demonstrate how health data is perceived in the adoption of new technology in the health sector and give insights as to the extent to which data protection has been considered in the implementation and use of new technologies that process health data.

2.1 Health Act 2017.

The Health Act was enacted in June 2017 to establish a unified health system, to coordinate the inter-relationship between the national government and county government health systems, to provide for the regulation of health care service and health care service providers, health products, and health technologies, and for connected purposes.[11]

The Act recognizes the right to privacy is recognized in the context of standards of health. The Act recognizes the right to be treated with dignity and respect and have their privacy respected in accordance with the provisions of the constitution and the Act. [12] The Act also recognizes eHealth, a

[7] 'Health Information Systems: Tool kit on monitoring Health Systems Strengthening.' (World Health Organization, 2008) https://www.who.int/healthinfo/statistics/toolkit_hss/EN_PDF_Toolkit_HSS_InformationSystems.pdf
[8] 'Health Information Systems: Tool kit on monitoring Health Systems Strengthening.' (World Health Organization, 2008) https://www.who.int/healthinfo/statistics/toolkit_hss/EN_PDF_Toolkit_HSS_InformationSystems.pdf
[9] Section 105
[10] Section 104, Health Act
[11] Health Act, 2017. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/HealthActNo.21of2017.pdf
[12] Section 5(2)

combined use of electronic communication and information technology in the health sector including telemedicine, as a mode of health service. In recognizing eHealth as a mode of health service, the act required the cabinet secretary for the Ministry of Health among other things to develop within three years of operation of the Act to develop legislation that provides for the protection of privacy.[13]

The technical working group tasked with developing guidelines for the regulation of eHealth in the country developed a report in 2019[14] and was expected to submit a comprehensive regulatory framework to the Cabinet Secretary by September 20, 2019.[15] The status of the availability of the framework is unknown. The report identified important areas that were to be considered in the creation of an eHealth regulatory framework, with data protection and confidentiality being one of them.[16]

2.2 Health Sector ICT Standards and Guidelines.

The Standards and Guidelines were developed in 2013 by the Ministry of Health in recognition of the value of using ICT to enhance efficiency and delivery of service in the health sector. The standards are applicable to those in the health sector using ICTs in offering services or information to the public, further, the standards were developed to provide guidance and a consistent approach in the health sector in establishing, acquiring, and maintaining current and future information systems and ICT infrastructure.

The Standards and Guidelines addressing the operation of ICT systems include references to data protection, privacy, and confidentiality. Privacy is perceived in the context of the users who use the MOH ICT systems. Confidentiality is also perceived in the context of keeping the users' documented account information confidential, information security requirements that must be adhered to by staff using information systems also include confidentiality. In discussing Data access, however, the standards require the systems in use to ensure that electronic records are safeguarded against unauthorized access and that access to patient-level data is limited only to authorized persons per existing regulations.

The Standards and Guidelines are primarily focused more on the protection of the systems in terms of implementation and use, and less on the actual processing of health data through the systems in use.

2.3 Kenya Standards and Guidelines for mhealth Systems.[17]

The Standards and Guidelines on mHealth systems were developed in 2017 with the intention of ensuring that all mHealth-based systems are correctly implemented, with the implementation of the

[13]Section 104(d)
[14]The working group was composed of members from the Medical Practitioners and Dentist Board and the Ministry of Health.
[15]'Report of Technical Working Group to Develop Guidelines And Checklists For Report On The Regulation Of Electronic Health Practice In The Country.' < http://medicalboard.co.ke/resources/4.%20Draft%200%20-%20Electronic%20Health%20Regulation.pdf>
[16]Report of Technical Working Group to Develop Guidelines and Checklists For Report On The Regulation Of Electronic Health Practice In The Country.' < http://medicalboard.co.ke/resources/4.%20Draft%200%20-%20Electronic%20Health%20Regulation.pdf>
[17]'Kenya Standards and Guidelines for mhealth Systems' (Ministry of Health, 2017)https://www.health.go.ke/wp-content/uploads/2020/02/Revised-Guidelines-For-Mhealth-Systems-May-Version.pdf

Standards reducing duplication of efforts in promoting data and information sharing among systems and harnessing the proper use of mobile technology.

The Standards and Guidelines apply to the health sector at all levels of health care and health management levels and provide guidance in establishing, acquiring, and maintaining mobile-based health information systems that foster data and information sharing across multiple systems. The Standards and Guidelines reflect numerous considerations on data protection in the context of privacy and confidentiality:

- Privacy is described in the Standards and Guidelines to refer to aspects of the information systems that deal with the ability of an organization or individual to determine what data or information is to be shared with third parties.
- Confidentiality is the degree to which access and disclosure of the information is limited to authorized users. mhealth systems must put in place measures to ensure client data is protected against unintended or unauthorized access through providing security services which must include, anonymization and pseudonyms for client data before it can be shared, aggregating client data before sharing to reduce possibilities of tracking, data minimization so that access is only available to the dataset required for a particular use.
- Guidelines on minimal mhealth non –functional requirements require the development of the process of mhealth applications to conform to requirements of security which must ensure that the client's data is handled in a secure manner by putting in place mechanisms that will guarantee privacy, security, and confidentiality and the security of data at transmission and when it is archived.
- mHealth systems are required to conform to guidelines that require consideration of the right to privacy when collecting information.
- Where mHealth relies on digital messaging or e-prescription appropriate safeguards must be put in place to safeguard against potential privacy and confidentiality violation.
- The Standards also give guidance on the risks of texting personal health information and guidelines to help secure patient health information
- Where the mhealth systems provide technology-based patient interactions, healthcare providers and practitioners who give advice or treatment through the system are required to apply the principles of obtaining the patient's informed consent in order to protect the patient's privacy and their right to confidentiality
- Guidance is also given on authentication of prescriptions where it is required that, when receiving e-prescriptions, the process must maintain privacy and security. Receipts must be in a secure area and only handled by staff to protect the confidentiality of patient information.

The Standards and Guidelines discuss data governance in terms of security, validation, accountability, and ownership. Under security, appropriate measures ensuring data security must be put in place ensuring data confidentiality, integrity, availability, and nonrepudiation of users are enforced for client data. Validation ensures the accuracy of the data held in the mhealth system by enforcing validation measures at the points of data collection and storage. Accountability, on the other hand, requires the implementation of assurance processes, which can be achieved through audit trails, quality assurance, and robust credential-

"The Standards and Guidelines discuss data governance in terms of security, validation, accountability, and ownership."

based access. The government owns and maintains the data collected from a client through a mhealth system or application; however, the client has the right to access the data.

2.4 Kenya National eHealth Policy 2016-2030[18]

The national eHealth policy was formulated in 2016 and is intended to be applicable till 2030 the policy document was developed to develop long-term strategies, policy guidelines, and standards govern the adoption, deployment, and utilization of eHealth products and services in Kenya.[19] Data protection in this policy is also viewed in the context of privacy and confidentiality and is identified in guidance that provides for

- Standardization of eHealth solutions: i.e. standardization in the procurement of eHealth solutions to ensure quality, confidentiality, privacy, and security of eHealth data.
- Policy goals and objectives: the aim of the eHealth policy is to provide direction on the adoption and utilization of technologies for the collection, storage, retrieval analysis, and exchange of patient health information in an ethical, effective and secure manner.
- Employing a patient-centric approach to the management and use of electronic data in a way that guarantees the confidentiality, integrity, and privacy of patients at all times.
- Secure transfer of eHealth information: in ensuring the secure transfer of health information confidentiality of information must be maintained during transmission, and policy guidelines on the management of health data must be provided without compromising patient's privacy and safety.
- Digital access to health care: in ensuring accessibility of electronic health services interventions that must be implemented among others include the promotion of cross border sharing of health information without compromising the patient's privacy.
- Health information research: in promoting health informatics research, data used must be anonymized to protect the identity and privacy of the subject.
- Management of health data: maintaining security, privacy, and confidentiality in the adoption and utilization of eHealth products and services. Security through protecting health information networks software, and hardware from unauthorized access. Privacy through informed consent enables patients to determine when, how, and to what extent their information is communicated to other parties and confidentiality through ensuring non – disclosure of private information
- Managing privacy, confidentiality, and integrity: through implementing interventions that develop standards and guidelines on privacy, confidentiality, and integrity of health data and information, ensuring sensitive health data information is stored in anonymized or encrypted formats and ensuring appropriate security measures are put in place to maintain the integrity of electronic health records.
- Data acquisition: to ensure eHealth systems capture quality data, the safe use of Electronic Data Capture systems and other standard clinical equipment must be promoted in protecting the privacy and confidentiality of patients.

[18]Kenya National eHealth Policy 2016-2030 (Ministry of Health , 2016) <https://health.eac.int/file-download/download/public/86>

[19] Kenya National eHealth Policy 2016-2030 (Ministry of Health , 2016) <https://health.eac.int/file-download/download/public/86>

2.5 The Kenya National Patients' Rights Charter[20]

The Patient's Rights Charter was issued by the Ministry of Health in 2013, in recognition of health as a constitutional right. The charter is meant to inform clients and patients of their rights and responsibilities and provides guidelines for the resolution of conflicts where conflict arises between parties. The first chapter covers patients' rights, under these rights those that can be directly linked to data protection is the right to confidentiality, the right to give informed consent to treatment, and the right to information. The second chapter covers responsibilities, linked to data protection is the responsibility to give health care providers relevant, accurate information.

2.6 Health Information Policy 2014-2030

First issued in 2014 by the Ministry of Health, the Health Information Policy was developed to provide guidance on the management of health information. This was due to the introduction of the Health Information System (HIS) and the continued adoption of ICT in the health sector. The policy identifies weaknesses in the HIS to include, including the lack of policy and guidelines, inadequate capacities of HIS staff, unskilled personnel handling the data, lack of integration, and many parallel data collection systems. The policy acknowledges the challenges brought about by the use of IT including the right to privacy of individuals and the protection of their rights in relation to the HIS. The policy addresses data collection and information sharing, guidelines on data processing, data warehousing, mandatory reporting by healthcare providers,and quality data management in the health sector. Aspects of data protection are discussed in the following contexts,

"First issued in 2014 by the Ministry of Health, the Health Information Policy was developed to provide guidance on the management of health information."

- Priority actions: The policy highlights specific policy actions in meeting the objectives of the policy which are data protection through, developing guidelines and legal framework for health data and information reporting and feedback, promoting standardization harmonization, management and coordination of data collection tool systems, defining data management processes and addressing challenges regarding storage and security of health data and information.
- Application and use of ICT: the policy notes the use of ICT in data processing and the need to address the constraints the use of ICT presents in the lack of legislation to protect privacy while permitting the use of health data, the lack of uniform multipurpose data standards that meet the needs of the diverse groups that record and use health information and the lack of understanding of health informatics by the workforce. A further note is made on the need for the protection of personal health information and consideration of how the privacy principles will apply to the health sector.
- Data Management (Recording and Analysis), Dissemination, and use: In acknowledging that data processing varies from one system to another depending on the data collection tools,

[20]'The Kenya National Patients' Rights Charter.' (Ministry of Health , 2013) http://medicalboard.co.ke/resources/PATIENTS_CHARTER_2013.pdf

priority must be given when handling patients' records. For instance, data collected by the alt sector ought to be non-patient identifiable.

- Access to Health and Health-related Data and Information: Where the transfer of records is required, health workers who have authorized access to patients' records will be required to maintain the highest level of confidentiality and ensure that shared confidentiality is only practiced in the interest of the patient.
- Storage, Confidentiality, and Security of Health Data and Information: The policy notes that appropriate standards are needed in relation to how data is maintained. It also notes the sensitive nature of the data captured and the need for appropriate security against unauthorized access and modification and compliance with privacy standards and any existing or proposed health law. Further, the storage of collected data must be handled with confidentiality and privacy.
- Data transfer to third parties: the duty of confidentiality applies to data that health care professionals collect, the policy implies that the duty does not extend to third parties and must therefore be regarded as unavailable to third parties. This however is only in the absence of clear and authoritative reason. For instance, where an insurance company requests patient information for the purposes of advertising. In the case of referrals, care must be taken to ensure only relevant parts of the patient's information are shared.

"The Act recognizes the sensitive nature of information relating to HIV tests and related medical assessments and makes specific provisions on privacy and confidentiality"

2.7 HIV and AIDS Prevention and Control Act

Enacted in 2006, the HIV and AIDS Prevention Control Act came into force in 2009 and provides for, measures for the prevention, management, and control of HIV and AIDS, the protection and promotion of public health and for the appropriate treatment, counselling, support and care of persons infected or at risk of HIV and AIDS infection, and for connected purposes.[21] The Act recognizes the sensitive nature of information relating to HIV tests and related medical assessments and makes specific provisions on privacy and confidentiality. Part V of the Act gives power to the cabinet secretary of health to prescribe privacy regulations or guidelines relating to the recording, collecting, storing, and security of information, records, or forms used in respect of HIV tests and related medical assessments.[22]

All data and records that relate to HIV testing and any related medical examination should not directly or indirectly identify the person to whom the HIV test or medical examination relates. This provision specifically applies to, [23]

- A request for an HIV test by persons in respect of themselves
- An instruction from a medical practitioner to a laboratory for an HIV test to be conducted
- The laboratory testing of IV or IV antibodies
- The notification to the medical practitioner of the result of the HIV test.

[21]HIV and AIDS Prevention and Control Act, 14 of 2006, Laws of Kenya. http://guidelines.health.go.ke:8000/media/HIV_and_AIDS_Prevention_and_Control_Act.pdf
[22] Section 20
[23]Section 21

Data processing of information or forms in respect of HIV tests or related medical assessments is to be conducted in accordance with the privacy guidelines to be prescribed by the Ministry of Health.

2.8 Standard Operating Procedures in handling Health Records and Information Management during the COVID-19 Pandemic[24]

The guidelines and protocols were developed in response to the COVID-19 pandemic. The guidelines are intended to educate health records and information management practitioners, clinicians, nurses, and other healthcare workers about the importance of adhering to these standards in order to provide quality and accurate health and health-related data, diagnosis, and medical certification of cause of death. According to the guidelines, patient privacy includes personal space, personal data, personal choices, cultural and religious affiliations, and personal relationships with family members and others. The privacy and confidentiality of health records and patient information should be maintained throughout their processing and management lifecycle.

2.9 The Data Protection Act vis - a- vis the existing laws and policies.

The existing laws and policies regulating health information/data all came into force prior to the enactment of the DPA. Having established that specific aspects of data protection i.e. privacy and confidentiality are not new to the health sector, a Comparison of the DPA with the existing guidelines makes the following observations,

- The regulations and guidelines in various aspects provide for privacy, security, and confidentiality and in some cases the storage of health data, these similarities are distinct.
- The DPA introduces principles applicable in the processing of personal data – for which health data holds a special category, sensitive personal data. Some of the principles and provisions noted in the DPA are not clear or provided for in the guidelines.

The identified similarities in comparison with the principles of data protection and the provisions of the data protection act are as follows,

- **Integrity and Confidentiality(security):** the principle requires the processing of data in a manner that ensures appropriate security, including protection against unlawful, unauthorized, or accidental loss. This requires appropriate technical and organizational measures e to ensure the security of the data. The laws highlighted, save for the Health Act capture this principle in regard to data access. (gap- clarity with respect to both organizational and technical safeguards/ implementation of both organizational and technical safeguards).

- **Purpose limitation:** this refers to the collection and processing of data for specified, explicit, and legitimate purposes with no further processing contrary to the original purpose for the collection. For example, where health data is collected for purposes of medical examination and treatment, the same data cannot then be used for research unless consent has been given and the same properly communicated prior to the collection of the data. Only the Kenya Standards and Guidelines for mHealth systems identify this principle.

[24] https://www.health.go.ke/wp-content/uploads/2020/05/Guidelines_HRIO-Management-COVID-19-final-28.04.2020-1-1.pdf

- **Data minimization:** this refers to the collection of data that is adequate, relevant, and necessary for the intended purpose. This principle is outlined in the Kenya National eHealth policy.

- **Consent:** Consent under the DPA refers to the manifestation of express, unequivocal, free, specific, and informed indication of the data subject's wishes by a statement or by 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 concept of consent can be identified in the Kenya National Patients' Rights Charter and the Kenya Standards and guidelines for mhealth systems.

- **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 grants the data subject the right to be informed on the use of their personal data, the right to access their personal data, the right to object to the processing of their personal data, the right to correct inaccurate or misleading data, and the right to have inaccurate or misleading data deleted.[25] These rights can be identified in the Kenya National Patients' Rights Charter and the Kenya National eHealth Policy.

- **Data Transfer:** Data transfer is provided for in the Act in the context of cross-border data transfer – 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 also contemplated under the Kenya National eHealth policy with respect to digital access to health care in promoting accessibility to electronic health services.

In line with the observations made above the following gaps are noted,

- **Data protection principles:** The data protection principles guide the lawful processing of personal data. They equally apply to the processing of health data and must therefore be provided for and implemented across all existing laws and policies. The principles of lawfulness, fairness, transparency, accuracy, data minimization, purpose limitation, storage limitation, security, and accountability though present in a few of the policies have not been provided for or adequately incorporated in discussing the processing of health data.
- **Rights of the data subject:** the rights of the data subject are relevant to the processing of health data. The principle of accuracy for instance requires that data collected is accurate and, where necessary, kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. This principle is only enforceable where data subjects (patients) can exercise these rights. Consequently, these rights must be provided for in all the policies that relate to the processing of health data.

- **Data Transfer and Sharing:** Health care involves a diverse set of public and private data collection systems,[26] the existing laws and policies attempt to provide the necessary standards and

[25] Section 26

[26] 'Improving Data Collection across the Health Care System.' (Agency for Health Care Research and Quality)https://www.

guidelines for the processing of health data across these systems. It is notable however that the laws and policies fall short in adequately providing for data transfer not only in the context of cross-border data transfer where the circumstances would merit but also the transfer of data across the data collection systems which would occur for instance in the case of referrals.

- **Third-Party data sharing:** Health data is not only relevant to healthcare professionals in carrying out their respective duties. This information can be shared with third-party entities within the healthcare system, for example, insurance companies and government agencies like NHIF. The laws and policies note in different contexts the duty of privacy and confidentiality for those who directly process health data but fail to give provisions and guidance where third parties are likely to be involved. This is not only necessary for data sharing with insurance companies – private or governmental; it is especially relevant with the recognition of mhealth services and the use of eHealth systems.

3.0 Developing Data Protection Guidelines for the Health Sector.

When developing data protection guidelines for the health sector, "domestic laws must afford appropriate safeguards to prevent any such communication and disclosure of personal health data."[27] There are several jurisdictions that have demonstrated this in their guidelines namely: the United States (US), the United Kingdom (UK), and the European Union (EU). The health guidelines and standards in these jurisdictions clearly distinguish between privacy and security, as well as explain consent, the right to be forgotten, privacy by design, and how to conduct a risk assessment. Effective data protection systems recognize and safeguard all types of patient data, including emails, documents, and scans, while also enabling healthcare providers to securely share data in order to provide the best possible patient care.

3.1 Data Protection Guidelines from other Jurisdictions

3.1.1 US

Enacted in 1996, the Health Insurance Portability and Accountability Act (HIPAA) established a set of national standards to ensure that patient's sensitive health information remains private and is never disclosed without their explicit consent. Protected health information (PHI) is any information that can be used to identify a patient, such as a patient's name, address, date of birth, bank or credit card information, social security number, photographs, and insurance information. Entities that handle PHI are required to implement and maintain physical, network, and process security measures to ensure HIPAA compliance. Covered entities are required to be HIPAA compliant, particularly those that provide treatment, payment, and operations in healthcare, as well as business associates, defined as anyone who has access to patient information and assists with treatment, payment, or

"Entities that handle PHI are required to implement and maintain physical, network, and process security measures to ensure HIPAA compliance."

ahrq.gov/research/findings/final-reports/iomracereport/reldata5.html

[27] European Court of Human Rights. *Case of Z v. Finland:* Application No. 22009/93 ECHR 10; European Court of Human Rights: Strasbourg, France, 1997.

operations.[28] Other entities, such as subcontractors and other business associates, must also adhere to the rules. These rules are key in ensuring data protection of health data:

- The HIPAA privacy rule determines how and with whom personal health data may be shared. It confers certain rights on individuals with respect to their health information, including the right to access and correct their records. Additionally, it enables efficient use of those records during diagnostic or therapeutic procedures. Patients, for example, may expressly consent to their records being viewed by their primary care physician and any necessary specialists, but not by anyone else. The privacy rule is applicable to health plans, healthcare clearinghouses, and healthcare providers who engage in certain electronic healthcare transactions.

- The HIPAA security rule requires health organizations to anticipate potential cyber threats or data breaches by implementing administrative, physical, and technical safeguards to protect the confidentiality, integrity, and security of electronically stored, protected health information (ePHI). The security rule applies only to electronic transmissions of patient information, not to oral or written transmissions. All covered entities, including those that use certified EHR technology, must assess their security risks, implement safeguards to ensure compliance with the security rule, and document each security compliance measure. A risk assessment should cover the entity's circumstances and environment, taking into account the covered entity's size, complexity, and capabilities, as well as its technical infrastructure, hardware, and software security capabilities, the likelihood and criticality of potential risks to ePHI, and the cost of security measures.

HIPAA permits the disclosure of certain PHI for treatment purposes, without an individual's consent.[29] All uses and disclosures of PHI that is not expressly permitted by the rule require authorization. Where the privacy rule requires patient authorization, voluntary consent alone does not constitute a valid authorization for the use or disclosure of protected health information unless it also meets the requirements for a valid authorization. An authorization is a detailed document that grants covered entities the authority to use protected health information for specified purposes other than treatment, payment, or healthcare operations, or to disclose protected health information to a third party specified by the individual.[30] HIPAA makes a clear distinction between consent and authorization. While this is commendable, it creates ambiguity, particularly when it allows for disclosure of PHI for 'treatment purposes.' There is a requirement to spell out precisely what treatment purposes entail.

"HIPAA is aimed at organizations that handle protected health information, such as covered entities and business associated."

HIPAA is aimed at organizations that handle protected health information, such as covered entities and business associates. The privacy rule, which further restricts the disclosure of PHI, gives patients the right to view and correct their health information and medical records. While HIPAA does not provide for the right to be forgotten and only applies to PHI, the key takeaway is that processes and systems are essential in ensuring security in the healthcare industry.

[28] 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e).
[29] 45 CFR 164.506.
[30] 45 CFR 160, 164.

3.1.2 UK

The General Data Protection Regulations (GDPR) appears to be a far more adequate response to the challenges of protecting personal health data in the digital health era.[31] It strengthens patients' rights and empowers them to control and own their health data, while also attempting to clarify the rights and protections associated with personal health data exchanges in the digital healthcare era.[32] Additionally, the GDPR establishes new data protection standards for health and strengthens data controllers' and processors' obligations in the health sector regarding informed consent.[33] The GDPR further states that patients must be informed of the potential risks associated with data collection "in an intelligible and easily accessible form, using clear and plain language."[34]

GDPR requires data controllers to conduct a data protection impact assessment (DPIA) prior to processing sensitive health information in order to identify potential risks associated with data processing and devise solutions. Certain provisions[35] clarify to patients the decisions made through automated processing, including profiling, the logic involved in data processing, as well as the consequences. Thus, patients are informed of the risks associated with the use of decision-making algorithms, allowing them to participate in the decision-making process. Additionally, the GDPR incorporates cybersecurity provisions to increase transparency. These include safeguards against unauthorized and unlawful access, loss or damage,[36] data protection by design and default,[37] and steps taken to protect against external threats[38] and data abuse.[39]

Privacy by design is considered the most important provision of the GDPR's health data protection provisions, particularly for health data collected via wearable devices. The GDPR[40] requires healthcare organizations to safeguard patient data from the start. Additionally, privacy by default should be applied to any new health service or product. The GDPR strengthens the protection of personal health data through the established standards ranging from informed consent, data access, DPIA, transparency, automated decision-making, data portability, and privacy by design and default.

The GDPR has been lauded for its emphasis on consent and for setting compliance standards for all entities that fall within its scope. Consent is required for the processing of personal health data, which is classified as sensitive data. However, if a legal basis exists and the data meets one of the processing conditions, the data may be processed without consent. Among these conditions are the following:

- the data subject has expressly consented to the processing of their personal data for one or more specified purposes,
- processing is necessary to carry out the controller's or the data subject's obligations and

[31]Malgieri G & Comandé G, 'Sensitive-by-distance: Quasi-health data in the algorithmic era' 26 (3) *Information and Communications Technology Law*, 2017, 229–249, <https://doi.org/10.1080/13600834.2017.1335468>.
[32]Haug, C J, 'Turning the Tables - The New European General Data Protection Regulation' 379 (3) *The New England Journal of Medicine*, 2018, 207-209, < https://doi.org/10.1056/NEJMp1806637>.
[33]Sousa M, Ferreira D, Santos-Pereira C, et al. 'openEHR Based Systems and the General Data Protection Regulation (GDPR)' *Studies in health technology and informatics*, 2018, 91-95, <https://ebooks.iospress.nl/publication/48760>
[34]Article 7.
[35]Articles 12, 13, 22 and 29.
[36]Article 5.
[37]Article 24.
[38]Article 32 (2).
[39]Article 32 (4).
[40]Article 25.

exercise specific rights under employment and social security and social protection law,
- processing is necessary to safeguard the data subject's or another natural person's vital interests where the data subject is physically or legally incapable of doing so,
- processing is necessary for the purposes of preventive or occupational medicine, for assessing an employee's working capacity, for medical diagnosis,
- processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or for the purpose of ensuring the high quality and safety of health care and medicinal products or medical devices,
- processing is necessary for public interest archiving, scientific or historical research, or statistical purposes in accordance with Article 89(1).[41]

Most organizations that are subject to GDPR must appoint a Data Protection Officer (DPO). A DPO is in charge of:
- informing the controller or processor, as well as their employees, about data protection laws
- staff training and compliance monitoring
- assisting with data protection impact assessments
- engaging with relevant authorities.[42]

The DPO must have a thorough understanding of data security, privacy, and data subject rights.

In addition, the Health Service (Control of Patient Information) Regulations 2002 establish a legal framework in England and Wales for the disclosure of data without patient consent for public health purposes. The Regulations provide for lawful processing in the following circumstances: communicable diseases and other risks to public health,[43] as well as medical research.[44]

In the United Kingdom, health regulations grant data subjects rights and focus on protecting both data subjects' rights and personal data. They also cover sensitive personal data, consent, data privacy risk assessments, the right to be forgotten, and the appointment of a data protection officer (DPO). All of these considerations are critical for ensuring data protection in the delivery of healthcare services.

3.1.3 EU

The Council of Europe issued a set of guidelines[45] to its member states in 2019 urging them to ensure that health-related data processing is conducted in accordance with human rights, particularly the right to privacy and data protection.[46] The Council urged governments to communicate these guidelines, better known as the Protection of health-related data-Recommendation CM/Rec(2019) 2, to healthcare systems and entities that process health-related data, including healthcare professionals and data protection officers. The Recommendation is applicable to both public and private sector organizations that utilize health-related data in innovative ways, such as developing digital health solutions based on genetic data, scientific research, data sharing, or mobile health applications.[47]

[41]Article 9(2).
[42]Article 39.
[43]Regulation 3.
[44]Regulation 5.
[45]Protection of health-related data-Recommendation CM/Rec(2019) 2 <https://edoc.coe.int/en/international-law/7969-protection-of-health-related-date-recommendation-cmrec20192.html>
[46]Protection of health-related data: The council of Europe issues new guidelines <https://www.coe.int/en/web/portal/-/health-related-data-council-of-europe-issues-new-guidelines>
[47]Protection of health-related data: The council of Europe issues new guidelines <https://www.coe.int/en/web/portal/-/

Several principles governing the processing of health data in the Recommendation are reiterations of GDPR provisions. However, the Recommendation provides some detailed guidance on the processing of health-related data that is more detailed than, and in some ways exceeds, the GDPR requirements, as described below:

- **Data subjects' rights:** The Recommendation states that data subjects have the right to be informed and to exercise control over their health-related and genetic data, in accordance with the GDPR.[48] There are, however, three exceptions: data subjects should have the right not to be informed of medical diagnoses or genetic test results unless they are required to be informed by law; when data subjects withdraw from a scientific research project, they should be informed that their health-related data will be processed in the context of that retraction, and data subjects have the right to be informed about the logic behind data processing involving health-related data when the results of such processing are applied to them, especially when profiling is involved.

"Several principles governing the processing of health data in the recommendation are reiterations of GDPR provisions"

- **Genetic data:** The Recommendation states that genetic data should be collected only when required by law or with consent unless such consent is expressly prohibited by law. Genetic data collected for the purposes of preventative health care, patient diagnosis or treatment, or scientific research should be used exclusively for those purposes or to enable individuals affected by the results of genetic tests to make informed choices about these matters.[49]

- **Sharing health-related data for secondary purposes:** According to the Recommendation, only recipients who are legally authorized should have access to health-related data. Additionally, recipients of health-related data must adhere to the same rules of confidentiality as a healthcare professional, unless the law provides for additional safeguards.[50]

- **Scientific research:** The need to process health-related data for scientific research should be weighed against the risks to the data subject and if genetic data is involved, to their biological family.[51] The Recommendation does not preclude scientific research from being compatible with the original purposes for which the data was collected.

- **Digital health:** Several principles in the Recommendation apply to digital health applications, especially those that incorporate artificial intelligence, machine learning and mobile devices. According to the Recommendation, systems that store health data should be "auditable", which means that any access to, modification of, or action taken on the information system should be

health-related-data-council-of-europe-issues-new-guidelines>
[48]Chapter 3 - Rights of the data subject.
[49]Recommendation 7.
[50]Recommendation 8.
[51]Recommendation 15.

traceable back to the author.[52]

4.0 Recommendations and Conclusion

Data protection in the health sector is vital due to the sensitive nature of health data. With the continued implementation and use of technology in the health sector, the weaknesses and gaps identified in regulatory frameworks must be addressed especially in light of the DPA., The following recommendations are made for the development of data protection guidelines for the health sector:

- The Cabinet Secretary for the Ministry of Health (MOH) and the Office of the Data Protection Commissioner (ODPC) together with the Medical Practitioner Board should develop standardized data protection guidelines for the health sector. The guidelines would 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 healthcare practitioners in the processing of data, data transfer, and data sharing.
- Revision of the Kenya Standards and Guidelines on mhealth systems in consideration of the provisions of the DPA to adequately provide for the data protection principles and concepts that have not been adequately incorporated into the standards and guidelines. For example privacy by default and design.
- Revision of the Health Information Policy to acknowledge the data protection legislation noting the changes it will have on the processing of health data through the HIS. In line with this, defining the roles of health institutions as data processors, identifying data controllers, and the need for trained and skilled data protection officers.
- Revision of the Standards and Guidelines for EMR Systems to reflect minimum implementation requirements that align with the data protection principles under the DPA.
- The proposed data protection guidelines should provide guidance on the criteria for conducting assessments with respect to the processing of health data and the need for internal standard operating procedures for the processing of health data which must be compliant with the provisions of the DPA.
- Developing regulations specific to the processing of patient information that would differ from the proposed guidelines. These regulations would specifically focus on the processing of patient information as far as it relates to diagnosis and treatment.

The primary reason for the proposed data protection guidelines is to address identified gaps in data protection in the health sector. The proposed guidelines, if drafted and implemented properly, will address the weaknesses in the existing policy. Further, the proposed guidelines will provide guidance on compliance with the DPA and act as a robust institutional regulatory framework in addressing issues that may arise from the adoption and implementation of technology in the health sector.

[52]Recommendation 13.5.

Authors
Florence A. Ogonjo, Rachel Achieng, and Margret Zalo

This study was made possible by a grant provided by the Hewlett Foundation.
We thank the organization for their continued support.