KICTANet
The Power of Communities

MEMORANDUM ON:

A. **THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT) REGULATIONS, 2024;**
B. **THE DIGITAL HEALTH (DATA EXCHANGE) REGULATIONS, 2024; AND**
C. **THE DIGITAL HEALTH (USE OF E-HEALTH APPLICATIONS AND TECHNOLOGIES) REGULATIONS, 2024**

Submitted to:

Office of the Principal Secretary, State Department for Medical Services, Nairobi; Nairobi; or emailed to dharegulations@dha.go.ke

Submitted By:

Kenya ICT Action Network (KICTANet)

19 December 2024

19 December 2024,

Office of the Principal Secretary,
State Department for Medical Services
P.O. Box:30016–00100, Nairobi.
Afya House 6th Floor, Cathedral Road
+254-20-2717077
Nairobi

Submitted via email to dharegulations@dha.go.ke

Dear Sir/Madam

Re: Memorandum on: The Digital Health (Health Information Management) Regulations, 2024 b) The Digital Health (Data Exchange) Regulations, 2024 c) The Digital Health (Use of e-Health Applications and Technologies) Regulations, 2024

Greetings from KICTANet!

We submit this memorandum with expertise on human rights and Information and Communication (ICTs) and in response to the call for input on:

a) The Digital Health (Health Information Management) Regulations, 2024
b) The Digital Health (Data Exchange) Regulations, 2024
c) The Digital Health (Use of e-Health Applications and Technologies) Regulations, 2024

We have included herein a matrix presentation that captures the key issues and concerns, and highlights our proposals on relevant provisions of each of the Bills for your review and consideration.

We are available to provide further input and perspectives on the Bills, as and when required.

We look forward to your response.

Regards,

Kenya ICT Action Network (KICTANet)

a) The Digital Health (Health Information Management) Regulations, 2024

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
4 (Kenya Health Data Governance Framework)	Establishes the framework for data collection, access, sharing, and use.	Lack of clarity on enforcement mechanisms for compliance by health data controllers and processors.	Introduce clear sanctions for non-compliance and define a compliance monitoring body to conduct regular audits of health data controllers and processors.	a) **Article 31** of the Constitution guarantees the right to privacy, requiring effective enforcement of data protection standards. b) Additionally, under the **Data Protection Act, 2019**, **Section 23** mandates the Office of the Data Protection Commissioner to ensure compliance through audits.
7 (Notification of Health Data Breaches)	Mandates health data controllers to notify the Agency and the Data Protection Commissioner within 24 hours of a breach and take corrective measures.	The 24-hour notification period may be impractical for detecting complex breaches and implementing immediate containment measures.	a. Extend the notification period to 72 hours, aligning with international standards such as the EU GDPR[1]. b. Include a preliminary notification option within 24 hours to report suspected breaches, with full details to follow within 72 hours.	a) Extending the notification period ensures thorough breach analysis and proper reporting. b) **Section 43** of the **Data Protection Act No. 24 of 2019** allows a 72-hour window of notifying the Data Commissioner in case of a data breach. c) The EU GDPR also allows for a 72-hour notification period (**Article 33**), and aligning with international best practices will enhance Kenya's global standing in data governance.
10 (Health Data Privacy	Prohibits unauthorized access to health	a) The regulation states that the Agency will	a) Define clear and specific **privacy standards**, aligning	a) **Section 41** of the ***Data Protection Act, 2019*** requires data controllers to implement appropriate technical and organizational

[1] Understanding the GDPR breach notification timeline: A step-by-step guide - Thoropass.

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
	data and mandates deletion of data by controllers who lose access rights.	implement "privacy standards" but does not define what these standards entail or reference specific frameworks or guidelines. b) While the regulation restricts access to health data without authorization, it does not specify how client consent must be obtained (e.g., *explicit, written, digital*) or managed over time. There is also no mention of situations where the client cannot give consent, such as medical emergencies or incapacitation. c) When a health data controller loses access, they are required to notify	with the **Data Protection Act, 2019**. b) Establish guidelines for obtaining and managing **client consent**, including exceptions for emergencies. c) Specify timelines and methods for notifying clients and processors when access to health data is revoked. d) Provide technical guidelines or tools for secure **permanent data deletion** and introduce a verification process. e) Include secure **data transmission protocols** to protect data during transfer to the Agency. f) Establish clear **monitoring and**	measures to protect personal data. Clearly defined privacy standards ensure alignment with the Data Protection Act b) **Section 25** of the ***Data Protection Act*** mandates that data processing be based on freely given, informed, and specific consent. Providing clear consent guidelines upholds **data subject rights**. c) Including exceptions for emergencies ensures timely access to critical health data without violating privacy rights, balancing legal compliance with healthcare needs. d) Defined timelines (e.g., 14 days) and notification methods (e.g., SMS, email, or registered post) ensure that affected parties are promptly informed of changes in access to their health data. e) Timelines prevent delays while methods ensure consistency and traceability in communications. This aligns with **Article 47** of the Constitution of Kenya on fair administrative action. f) **Section 40** of the ***Data Protection Act*** requires data controllers to securely delete personal data when no longer needed. Providing **technical tools** (e.g.,

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		clients and processors. However: ● There is no specified timeline for this notification, which may delay informing affected parties and hinder their ability to take appropriate action. ● Practically, contacting all clients may prove difficult for controllers with large datasets, especially where client contact details are incomplete or outdated. ● Additionally, there is no clarity on how this notification should be issued (e.g., email, SMS, registered post),	**enforcement mechanisms**, including penalties for non-compliance.	encryption-based deletion software) ensures compliance and mitigates risks of residual data remaining vulnerable to breaches. g) A formal verification process increases accountability and ensures deletion is **irreversible** and complete. h) Section 41 of the *Data Protection Act* emphasizes data security during processing and transfer. Mandating secure protocols (e.g., encryption methods like TLS, SFTP) protects data integrity and confidentiality during transmission. i) Monitoring ensures health data controllers and processors adhere to privacy, deletion, and transmission requirements. Penalties deter non-compliance and enforce adherence to the regulation. j) Strong oversight mechanisms, aligns with **Section 58** of the *Data Protection Act*, assures data subjects that violations will be addressed promptly and fairly. k) Enforcement strengthens the Agency's role as an effective data steward, ensuring the regulation's implementation is meaningful.

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		which could lead to inconsistencies. d) The requirement for health data controllers to **"permanently delete all copies of the data"** raises operational concerns: ● Some controllers may not have the **technical capacity** to ensure complete and irreversible deletion of health data, particularly if it is stored in multiple systems or backups. ● Permanent deletion without proper oversight may result in **data loss** if the deletion occurs		

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		before transmission or validation by the Agency. ● The regulation does not specify a mechanism to **verify permanent deletion**, raising accountability concerns and potential non-compliance risks. e) The regulation requires controllers to transmit a copy of their data to the Agency when their access is revoked. However: ● There is no clarity on **how the data**		

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		should be transmitted securely to prevent breaches during transfer. ● This step increases the risk of data duplication, as copies of the data would exist both with the Agency and previously authorized processors, increasing potential vulnerabilities.		
12 (Migration of Legacy Data)	Requires migration of legacy data to compliant systems or the National Health Data Bank within specific timelines.	a) The 24-month timeline for transferring legacy data may be unrealistic for institutions, particularly small facilities or those using outdated	a) Extend the timeline to **36 months** to allow institutions adequate time to prepare and comply. Provide technical and financial assistance for under-resourced facilities to ensure	a) Many health facilities, especially in rural or underfunded counties, lack the infrastructure or expertise for immediate data migration. Phasing implementation over 36 months ensures compliance without disruptions to healthcare services. b) **Section 41** of the **Data Protection Act,** provides that data controllers must ensure

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		systems. b) The regulation does not specify the **protocols and formats** for migrating legacy data, creating ambiguity and the risk of inconsistencies in migration processes. c) The **one-year deadline** for migrating legacy data to compliant systems may be impractical for smaller health providers with limited technical or financial capacity.	smooth migration. b) Develop and publish **clear protocols, formats, and technical tools** for migrating legacy data. c) Extend the migration deadline to **24 months** for smaller health data controllers and processors. Introduce a phased migration approach based on institutional size and capacity	the integrity, accuracy, and completeness of migrated data. Clear protocols prevent errors and inconsistencies during migration. c) Providing tools and guidelines reduces ambiguity and ensures uniform standards, enhancing the efficiency and accuracy of migration processes. d) Small health providers may face financial and technical barriers that prevent compliance within one year. Extending the deadline ensures inclusivity and minimizes service disruptions.
16 (Secondary Use of Health Data)	Allows secondary use of de-identified health data for public health purposes upon	a) The regulation specifies that sensitive personal health data shall be used in **de-identified form**,	a) Define clear **de-identification standards** aligned with international best practices, such as **HIPAA Safe Harbor**	a) **Section 41** of the Data Protection Act requires data controllers to implement measures ensuring data security and integrity. Clear de-identification standards reduce the risk of re-identification, protecting data subjects' privacy.

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
	authorization and payment of fees.	but it does not define the **standards** for de-identification. b) The regulation states that only authorized persons can access data, but it does not specify who qualifies as an authorized person or what criteria must be met. c) The regulation requires health data controllers to facilitate access but does not clarify their **responsibilities** in ensuring data is de-identified before sharing. d) The Agency is tasked with granting rights for secondary use, but there are no clear	**Guidelines** or **ISO/IEC 20889**. Include mechanisms to verify de-identification processes. b) Provide clear guidelines on who constitutes an **authorized person** (e.g., public health researchers, policymakers) and include vetting processes to ensure only qualified entities access the data. c) Specify that health data controllers must verify and document the **de-identification process** before granting access for secondary use. Provide technical guidelines for ensuring data security during facilitation. d) Develop and publish **criteria and procedures** for	b) Global Standards such as **GDPR** - Article 89 emphasize secure anonymization for secondary data uses. c) Defining "authorized persons" ensures fairness, prevents misuse, and aligns with **Section 25** of the Data Protection Act No. 24 of 2019, which mandates lawful and transparent processing. d) Clearly identifying access qualifications enhances public confidence that sensitive health data is only used for legitimate purposes. e) Section 40 of the DPA mandates data controllers to process personal data securely. Ensuring de-identification aligns with privacy principles under **Article 31** of the Constitution. f) Without clear guidelines, poorly anonymized data may risk exposing sensitive personal information, violating privacy rights. g) Section 25 of the DPA emphasizes fair and transparent data processing. Clearly defined criteria ensure consistent, fair, and accountable decision-making processes.

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		criteria for approval or rejection of access requests. e) The regulation requires payment of **applicable fees** to access health data but does not consider waivers for **public interest research** or institutions with limited funding. f) While the fourteen-day response period is reasonable, the regulation does not provide a mechanism for appealing a **rejected request** or addressing delays in decision-making.	granting secondary data access, including considerations such as purpose, data security, and the credentials of requesting entities. e) Introduce fee waivers or reduced fees for public interest projects, students, and research institutions conducting studies for national public health benefit. f) Introduce an **appeals process** for rejected data access requests, with clear timelines for review and resolution. Include penalties for unjustified delays in responding to valid requests.	h) Published procedures increase confidence that health data access requests are reviewed fairly and responsibly, balancing public health benefits with privacy protection. i) **Section 36** of the **Data Protection Act No. 24 of 2019** allows proportional access fees. Waiving or reducing fees for public interest projects promotes health research and aligns with Kenya's Vision 2030 to foster innovation. j) Fees must not create barriers for research that could benefit underserved communities or public health systems. This ensures data access supports national health priorities without excluding stakeholders due to financial constraints.
17 (Access to Health Data	Enables data subjects to access and share their	a) (Reg 17 (1)) The regulation assumes all data subjects	a) Provide **alternative access options** for data subjects, such as access	a) Article 43 of the Constitution guarantees the right to health, which includes equitable access to health information. Addressing the

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
by Data Subject)	health records securely.	have access to digital infrastructure (e.g., smartphones, internet) to use the patient portal. This excludes individuals in underserved areas. b) (Reg 17(2))The regulation lacks details on the **technical safeguards** for secure sharing, such as encryption, multi-factor authentication (MFA), or access logs to monitor usage. c) (Reg 17(3)) The proposed limitations are appropriate but may be impractical for **less technologically literate users** or those with limited	through healthcare facilities, public kiosks, or assisted access programs for underserved communities. b) Mandate the use of **end-to-end encryption** for data sharing and implement multi-factor authentication (MFA) for secure access. Provide access logs so users can track who has accessed their records. c) Include **user-friendly guidance tools**, such as step-by-step instructions, visual aids, and helplines, to assist users in managing secure access limitations. d) Revise the provision to state that **both the data subject and the Agency** share responsibility for	digital divide ensures no individual is excluded from accessing their Shared Health Record. b) Ensuring alternative access mechanisms accommodates the socio-economic disparities in Kenya's healthcare landscape. c) **Section 41** of the **Data Protection Act** requires data controllers to implement appropriate technical measures to safeguard personal data. d) Robust security measures reduce the risk of data breaches, enhancing trust in the patient portal and ensuring compliance with Kenya's data protection laws. e) Ensuring accessible guidance tools promotes user adoption and compliance with access limitations. Further, Article 35 of the Constitution of Kenya ensures the right to access information, which includes designing systems that are understandable and usable by all, regardless of technical expertise. f) **Section 40** of the **Data Protection Act** places security obligations on data controllers. While users should take precautions, the Agency must also ensure systems are secure

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		experience managing access codes or passwords. d) (Reg 17(4)) Holding the **data subject solely responsible** for preventing unauthorized access is impractical and burdensome. Data security should also be the responsibility of the Agency. e) (Reg 17(5)) Expecting clients to update their records after treatment abroad may be unrealistic, as many may lack the knowledge, resources, or guidance to do so effectively.	securing Shared Health Records, with the Agency providing guidance on precautionary measures. e) Require healthcare providers to offer **assistance or automated systems** for updating records when patients return from treatment abroad, ensuring accurate and complete health records. f) Develop clear guidelines for monitoring and tracking, including specific protocols for securing sensitive data during cross-border transfer, and ensure compliance with the Data Protection Act.	and educate users on best practices. g) Ensuring that providers, not just patients, are responsible for updates improves the accuracy of medical records, which is critical for continuity of care. This also aligns with the principle of data protection on accuracy and completeness. Also, Many patients may not understand how to update records or possess the relevant documentation, making provider involvement essential. h) **Section 48** of the **Data Protection Act** prohibits cross-border data transfer without sufficient safeguards. Transparent tracking protocols ensure compliance and protect the privacy of data subjects. i) Ensuring data and biological material are securely tracked and stored aligns with Kenya's sovereignty and international best practices for health data governance.

b) **The Digital Health (Data Exchange) Regulations, 2024**

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
4 (Administration of the System)	Grants the Agency authority to manage the system, including onboarding all digital health solutions within six months.	a) (Reg 4(1)): The regulation relies on **future-issued standards**, creating potential delays and ambiguity if these standards are not published in a timely or detailed manner. b) (Reg 4(2)): The regulation does not specify the **content or scope** of the reports, nor does it require the Agency to make parts of the reports publicly available for accountability purposes. c) (Reg 4(3)): The regulation allows access for various purposes but does not specify **data privacy safeguards** to ensure compliance with	a) Mandate the **publication of specific digital health and ICT standards** within six months of the regulation coming into force. Require periodic updates to reflect technological advancements. b) Define the minimum content requirements for the reports (e.g., data usage, access logs, compliance status) and mandate the **publication of non-sensitive findings** for transparency. c) Require that data shared for analysis is **de-identified and aggregated** where possible, in compliance with data minimization and privacy principles	a) Specifying timelines for issuing standards ensures that the Agency has a clear framework for administering the System. Section 41 of the *Data Protection Act* emphasizes the need for clear data security and governance measures, which require well-defined standards. b) Publishing non-sensitive parts of the reports aligns with Article 10 of the Constitution (accountability and openness). Public availability of certain metrics, such as data breaches or policy impacts, fosters public trust and demonstrates compliance with the **Digital Health Act.** c) **Section 25(c)** of the **Data Protection Act** mandates that data processing, including sharing, be lawful, necessary, and limited to the intended purpose. De-identification

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		de-identification and data minimization principles. d) (Reg 4(4): The provision lacks details on **vetting or eligibility criteria** for persons granted access, which may lead to misuse or unauthorized access to sensitive health data. e) (Reg 4(5)): The regulation does not specify how **access levels** will be enforced or monitored to prevent misuse or unauthorized escalation of access rights. f) (Reg 4(6)): he **six-month onboarding deadline** may be impractical for smaller health data controllers with limited resources or for those using incompatible legacy systems.	outlined in the **Data Protection Act.** d) Establish clear **eligibility criteria and a vetting process** for designating authorized persons, including confidentiality agreements and training on data handling and compliance. e) Require the implementation of **role-based access control (RBAC)** and periodic audits of access rights to ensure compliance with data classification and security requirements. f) Extend the onboarding deadline to **12 months** for smaller controllers and provide technical assistance or funding to facilitate migration to the System.	ensures that individual privacy is maintained, even when data is accessed for reporting or policy-making. d) Vetting ensures that only qualified individuals with legitimate purposes are granted access to sensitive health data. **Section 40** of the **Data Protection Act** obligates data controllers to ensure the security of personal data at all stages, including when accessed by authorized personnel. e) Role-based access control aligns with **Section 41** of the **Data Protection Act**, which mandates technical and organizational measures to secure personal data. Auditing access rights prevents misuse and ensures that sensitive health data is only accessed by individuals with proper authorization. f) Smaller controllers often face financial and technical challenges that delay onboarding. Extending the

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
				timeline ensures compliance without disrupting healthcare services.
5 (Enterprise Service Bus)	Establishes the Enterprise Service Bus for routing, monitoring, and secure exchange of health data among certified digital health solutions.	a) (Reg 5(1)): The regulation outlines the roles of the ESB but does not specify how the **monitoring and control of message routing** will address issues like data security breaches or system conflicts. b) (Reg 5(2)a): The regulation does not detail **how standardization and interoperability** between digital health solutions will be achieved, particularly for legacy systems and smaller providers. c) (Reg 5(2)b): The regulation assumes the telemedicine platform will support **remote healthcare**, but it does not address the	a) Establish clear protocols for **real-time monitoring**, secure logging, and alert systems to detect and address anomalies, conflicts, or unauthorized access during message routing. b) Develop **technical guidelines** for integrating legacy systems and ensuring interoperability, including specific data exchange standards, APIs, and compliance frameworks for all stakeholders. c) Establish a **capacity-building program** to support the adoption of telemedicine infrastructure in	a) **Section 41** of the **Data Protection Act** requires robust technical measures for data security. Monitoring and logging ensure that unauthorized activity can be detected and resolved quickly. b) Proactive conflict resolution and anomaly detection improve the reliability and security of message exchanges across the ESB. c) **Section 19** of the **Digital Health Act requires the use of** standardized data exchange protocols. Providing clear integration guidelines supports compliance and ensures smaller providers can participate effectively in the Health Information Exchange. d) Tailored support for resource-constrained facilities prevents exclusion from Kenya's

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		infrastructure gaps that may limit its adoption in underserved areas. d) (Reg 5(2)c): There is no mention of **how data security and accuracy** will be maintained when managing sensitive supply chain data, including procurement and inventory information for health commodities. e) (Reg 5(2) (should be 5(3); there is a typo): The regulation references **interoperability standards**, but does not specify who will monitor compliance or address non-compliance during implementation.	underserved counties, including funding for hardware, training, and reliable internet connectivity. d) Require implementation of **real-time auditing systems** for data integrity and security. Ensure that all supply chain data is encrypted during storage and transmission to prevent breaches or manipulation. e) Assign the Agency the responsibility to conduct **periodic audits** of compliance with interoperability standards and establish penalties or remedial actions for non-compliance.	digital health ecosystem. e) **Article 43** of the **Constitution of Kenya** guarantees the right to health, which includes equitable access to telemedicine services. f) Many counties lack the infrastructure necessary for telemedicine. A capacity-building program aligns with Vision 2030 goals for expanding healthcare services to underserved regions. g) **Section 41** of the **Data Protection Act** requires security measures for personal and sensitive data, which extends to logistics and supply chain information. h) Real-time auditing ensures that errors or anomalies in the supply chain system are quickly detected and corrected, preventing disruption in healthcare service delivery. i) **Section 58** of the **Digital Health Act** gives the Agency oversight

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
				authority for compliance. Regular audits ensure adherence to standards, improving interoperability and system performance. j) Without enforcement mechanisms, non-compliance with interoperability standards could lead to inefficiencies and data silos, undermining the ESB's goals of seamless integration.
6 (Onboarding to the Enterprise Service Bus)	Requires health data controllers to apply for onboarding with proof of registration, a data protection impact assessment report, and onboarding fees.	a) (Reg 6(1)): The regulation does not specify the **requirements or criteria** for onboarding health data controllers, which could lead to inconsistencies or exclusions of smaller institutions. b) The regulation does not provide details on **how the onboarding portal will function**, what resources will be available, or whether	a) Define clear **onboarding criteria** for health data controllers, including technical capabilities, compliance with security standards, and submission of necessary documentation (e.g., certifications). b) Provide a **user-friendly onboarding process** with detailed guidance, training sessions, and technical support through the portal. Include multilingual	a) **Section 41** of the **Data Protection Act** requires technical and organizational safeguards for data controllers. Onboarding criteria ensure compliance and uniformity. b) A well-designed portal with training ensures that health data controllers, regardless of size or location, can onboard successfully. **Article 43** of the **Constitution** (right to health) supports accessible systems for health service providers.

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		training will be provided to data controllers during the process.	resources to ensure inclusivity across counties.	
8 (Inventory of Health Data Controllers)	Requires the Agency to maintain an inventory of health data controllers with detailed information on their operations and digital health solutions.	a) **Lack of clarity on access and use of the inventory**: The regulation does not specify whether the inventory will be publicly accessible or restricted to authorized personnel only. b) The regulation does not address **how often the inventory will be updated**, which could lead to outdated or inaccurate records.	a) Define **access controls** for the inventory. For transparency, make non-sensitive information (e.g., number of onboarded entities) publicly accessible while restricting sensitive details to authorized personnel. b) Mandate periodic updates (e.g., every six months) to ensure that the inventory reflects accurate and up-to-date information about health data controllers and digital health solution	a) Article 10 of the Constitution promotes accountability and openness in public institutions. Publicly available aggregate statistics foster public trust, while restricted access to sensitive details ensures compliance with **Section 41** of the *Data Protection Act* on data security. b) **Section 40** of the *Data Protection Act* requires data controllers to maintain accurate and complete data. Periodic updates ensure operational integrity and accurate records for effective oversight of the enterprise service bus.
9 (Suspension from the Enterprise Service Bus)	Allows the Agency to suspend health data controllers for various compliance failures, such as data breaches	a) (Reg 9(1)a): The regulation does not define what constitutes a **serious data breach** or provide criteria for	a) Clearly define **serious data breaches** (e.g., breaches exposing sensitive health data or affecting a large number	a) Clear definitions ensure uniform application of the rule, avoiding subjective or arbitrary suspensions. Aligns with Section 41 of the *Data Protection Act*,

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
	or misuse of access rights.	assessing the severity of a breach. b) (Reg 9(1)f): Suspending access for failure to pay fees may disproportionately impact small or underfunded health data controllers who may struggle with financial constraints. c) (Reg 9(3)): The three-day notification timeline may be too long, especially for active health data controllers whose operations could be significantly disrupted by blocked access. d) (Reg 9(4)): The regulation requires permanently blocked controllers to migrate health data but does not clarify how migration will be funded or managed for	of records). Include thresholds or examples to standardize enforcement. b) Introduce a **grace period** for fee payment and provide a mechanism for fee waivers or subsidies for resource-constrained health data controllers. c) Reduce the notification period to **one day** to minimize disruptions and allow health data controllers to address compliance issues more quickly. d) Specify that the **Agency shall provide technical and financial support** for data migration to ensure that permanently blocked controllers can comply with the migration requirement. e) Introduce a specific	which emphasizes securing personal data and addressing breaches proportionately. b) Article 43 of the Constitution guarantees the right to health, which may be undermined if small healthcare providers lose access to the system due to financial constraints. Fee waivers ensure equitable participation while maintaining the integrity of the enterprise service bus. c) A shorter notification period ensures that health data controllers can promptly address issues, minimizing disruptions in service delivery. This aligns with Article 47 of the Constitution, which ensures fair administrative action that is timely and efficient. d) Migration is often resource-intensive, and without Agency support, blocked controllers may fail to comply, leaving critical health data inaccessible. Supporting migration aligns with the

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		resource-limited entities. e) (Reg 9(5): The regulation does not specify **timelines** for the Agency to review re-onboarding applications, which may cause unnecessary delays for compliant controllers.	timeline (e.g., **14 days**) for the Agency to review and process re-onboarding applications after compliance issues are resolved.	principle of equitable access to health systems under Article 43 of the Constitution. e) Clear timelines ensure fairness and accountability in administrative processes, aligning with Article 47 of the Constitution, which mandates fair and timely decision-making.
15 (Telemedicine Health Provider Registry)	Requires telemedicine providers to use certified digital health solutions and submit reports on e-health services.	a) (Reg 15(1)): Potential exclusivity may create monopolistic tendencies, restricting competition among telemedicine providers. b) (Reg 15(3)e): The requirement could delay service delivery due to lengthy registration processes. c) (Reg 15(5)a : Stringent certification requirements may exclude innovative but uncertified providers,	a) Ensure that alternative, verified sources of reference are also allowed for telemedicine providers. b) Specify the minimum necessary information required for the registry and enforce stricter access control measures to sensitive data. c) Implement a temporary conditional approval for providers awaiting registration by the Office of the Data Protection	a) **Article 227 of the Constitution** mandates fair competition in public procurement and practice. Allowing multiple verified sources ensures accessibility while preventing monopolistic practices. b) **Section 25 of the DPA** outlines data protection principles, including data minimization, which ensures that only essential data is collected and retained. c) **Section 18 of the DPA** establishes the process for registration of data controllers

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		potentially hindering technological advancement. d) (Reg 15(6)): The centralization of management under the Agency may lack sufficient oversight mechanisms, increasing risks of abuse or inefficiency. e)	Commissioner (ODPC). d) Develop clear, published guidelines for issuing telemedicine provider codes, including timelines and an appeals process for rejected applications. e) Provide a phased certification plan to allow innovative providers to comply while still operating under strict interim safeguards. f) Establish independent oversight mechanisms for the telemedicine health provider registry.	and processors. A transitional framework would ensure continuity of telemedicine services while awaiting compliance. d) Transparency in issuing codes will prevent discrimination and uphold fairness. e) **Articles 10 and 232** of the Constitution emphasize innovation and public service inclusivity. Balancing innovation with compliance will foster technological growth while protecting patient data. f) Article 43 of the Constitution guarantees the right to the highest attainable health standards. Dynamic frameworks ensure timely access to cutting-edge telemedicine solutions while aligning with international best practices. g) Article 201 of the Constitution requires accountability and transparency in public financial management. Independent

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
				oversight ensures the agency adheres to best practices.
19 (National Logistics Management Information Services Platform)	Serves as a central point for tracking health products and technologies, with suppliers required to pay onboarding and annual fees.	a) Reg 19(1): Exclusivity of the platform as the sole reference point may stifle innovation by excluding other effective logistics systems. b) (Reg 19(2): The extensive data requirements (e.g., batch details, location, condition, and usage) raise privacy and security concerns, particularly if improperly accessed or used. c) (Reg 19(3)b: The Agency's dual roles (administration and regulatory enforcement) could lead to inefficiencies or conflicts of interest, affecting timely oversight and resolution	a) Allow interoperability with other verified platforms or systems to enhance flexibility and competition. b) Implement strict access controls, encryption protocols, and data minimization practices for sensitive information to reduce security vulnerabilities. c) Introduce independent oversight mechanisms to ensure separation of administrative and regulatory functions, including a clear appeals process for aggrieved stakeholders. d) Establish transparent guidelines for granting access to the platform, including published criteria, timelines, and a	a) Encouraging interoperability ensures operational efficiency while safeguarding the rights of stakeholders. b) **Section 25 of the DPA** mandates adherence to data protection principles, including minimizing data collection and ensuring data security. c) Article 201 of the Constitution emphasizes accountability and transparency in public service. Separation of roles ensures checks and balances, reducing risks of inefficiency. d) Section 31 of the DPA emphasizes data security and resilience. Redundancy in systems protects against disruptions, ensuring continued operations in critical health supply chains.

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		of disputes. d) (Reg 19(3)e): Granting access to certified digital health solutions without specific criteria for approval risks arbitrary decisions or exclusions. e) The registration requirement could impose undue administrative and financial burdens on smaller suppliers, discouraging participation in the health product supply chain.	grievance redress mechanism for rejected applicants. e) Introduce a tiered fee structure based on supplier size or capacity, with waivers for small-scale suppliers or nonprofit organizations. f) Provide training and financial support for suppliers to build capacity for digital reporting. Allow offline reporting options for regions with limited internet connectivity. g) Introduce a sliding scale for annual retention fees based on the supplier's turnover or financial capacity. Consider exemptions or subsidies for nonprofit and public health suppliers. h) Develop contingency measures, such as	

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
			backup systems and decentralized reporting options, to maintain supply chain functionality during platform downtime or breaches.	
20 (Shared Health Record)	Establishes a single source for patients' medical history, requiring updates within 24 hours after encounters.	a) (Reg 20(2)c): The regulation does not specify the **security standards** for the patient portal, increasing the risk of unauthorized access to sensitive data. b) (Reg 20(2)d): The regulation does not specify the **frequency of audits** or actions to be taken upon detecting unauthorized access. c) (Reg 20(5)a): The regulation does not define the **encryption standards** for data transmission, creating potential inconsistencies and	a) Specify **security protocols** for the portal, such as end-to-end encryption, multi-factor authentication (MFA), and periodic security testing to safeguard access. b) Mandate audits on a **quarterly basis** and require the Agency to take corrective actions, including notifying affected clients and imposing penalties on data controllers responsible for breaches. c) Specify **encryption protocols** aligned with global best practices	a) **Section 53(2) of the DPA** requires data controllers to implement technical safeguards (e.g., encryption) to ensure data protection by design and default. Enhanced portal security aligns with this provision. b) MFA and encryption are global best practices for securing sensitive online systems, especially in healthcare. c) Regular audits fulfill the obligation under **Section 43 of the DPA**, which mandates timely reporting of data breaches and ensures accountability in managing health data systems. d) Regular audits build trust in the system by ensuring that unauthorized access is detected

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		security vulnerabilities. d) (Reg 20(7)): The regulation references **Section 59** of the Act but does not clarify whether penalties are administrative fines, criminal charges, or other sanctions. e) (Reg 20(8)): Restricting access to a specific encounter may hinder **continuity of care**, particularly when healthcare providers require a broader medical history for effective treatment. f) (Reg 20(9)): The regulation does not specify the **format or security standards** for sharing requested information, potentially leading to insecure data sharing practices. g) (Reg 20(10)): The	(e.g., AES-256 encryption) to ensure uniform security measures across all health data controllers. d) Clarify the **nature and extent** of penalties (e.g., specific fines or imprisonment) and provide guidance on mitigating circumstances that may affect enforcement. e) Allow limited **conditional access** to a patient's broader medical history (e.g., past treatments and chronic conditions) based on client consent or approval from the Agency. f) Require information to be shared in a **secure format** (e.g., encrypted files or secure online access) and include a verification process to	and addressed promptly. e) Frequent audits allow early detection of anomalies, preventing data misuse or breaches that could undermine the healthcare system's credibility. f) **Article 43 of the Constitution** guarantees the right to health, which includes access to adequate medical care. Balancing privacy with conditional access ensures effective treatment for chronic or complex cases. g) Limiting access solely to a specific encounter may force providers to operate without critical patient history, compromising care quality. h) **Article 35 of the Constitution of Kenya)**: Clients must access their information in a way that protects their privacy. Secure formats and identity verification ensure compliance while mitigating risks of unauthorized

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
		regulation does not address **audit mechanisms** for tracking cross-entity requests, which could lead to misuse or unauthorized sharing of health data.	confirm the recipient's identity. g) Introduce mandatory **audit logs** for all inter-entity data requests, specifying who accessed the data, when, and for what purpose, to ensure accountability and transparency.	access. i) Audit logs enhance traceability and prevent misuse, fostering confidence in Kenya's healthcare system. j) Log tracking ensures that inter-entity sharing is restricted to authorized and documented purposes, minimizing data breaches or misuse in Kenya's expanding digital health ecosystem.

c) **The Digital Health (Use of e-Health Applications and Technologies) Regulations, 2024**

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
4(1) (E-Health)	Requires healthcare providers and health facilities to use certified digital health solutions for service delivery.	The regulation mandates certification but does not consider smaller healthcare providers that may lack resources for certification fees or technical capacity.	Introduce **fee waivers or subsidies** for resource-constrained providers, especially in underserved regions, to ensure equitable access to digital health certification.	**Article 43 of the Constitution** guarantees the right to health. Ensuring all providers, including small facilities, can comply promotes equitable healthcare delivery. - **Kenya's Vision 2030** advocates for inclusivity in healthcare innovation
5(2)b (Certification Framework)	Mandates the Agency to establish a Certification Framework covering functionality, interoperability, security, and reporting requirements.	The standards are referenced but not explicitly outlined, leaving room for ambiguity and inconsistent implementation.	Publish the **specific digital health standards** (e.g., interoperability, data security) to provide clarity for digital health solution providers and ensure uniform compliance	Clearly defined standards streamline compliance and reduce ambiguities, ensuring alignment with Kenya's **Health Data Governance Framework** and promoting transparency in certification requirements.
7 (Certification Process)	Outlines steps for certifying digital health solutions, including self-attestation, application, testing, and re-certification.	High certification fees (KES 500,000 for hospital-wide systems) may exclude innovators, smaller vendors, and community-based organizations.	Introduce a sliding scale of certification fees based on the size and revenue of the applicant organization. Provide reduced fees or fee waivers for students, innovators, and startups to encourage participation and innovation in the sector.	High fees may stifle innovation and inclusivity, contrary to the objectives of Vision 2030 and Kenya's digital transformation agenda. KICTANet highlights the importance of affordable access to certification processes to stimulate local innovation and ensure broad adoption of certified technologies. Encouraging startup participation will also foster competitive solutions in Kenya's e-health sector.

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
8(1)	Certification application process includes self-attestation	Self-attestation may lead to insufficient scrutiny of digital health solutions, increasing risks of non-compliance or data breaches.	Mandate independent third-party audits or verification of critical elements (e.g., cybersecurity) to complement self-attestation and enhance credibility.	a) Third-party audits are widely recognized for ensuring rigorous evaluation of compliance and security standards. b) Strengthening the evaluation process reduces risks of vulnerabilities in certified solutions.
9(2)	Notification of test results within five days.	While the five-day timeline is reasonable, the regulation does not specify **recourse mechanisms** for providers dissatisfied with test results.	Provide a formal **appeals process** for providers to contest unfavorable outcomes, with clear timelines for review and resolution.	**(Article 47 of the Constitution)**: Establishing an appeals process ensures transparency and accountability, giving providers confidence in the certification process.
11(1)	Digital health solutions must notify the Agency of system breaches	The regulation requires notification but does not specify the timeline for reporting breaches, risking delays in mitigating data risks.	Require reporting of breaches within 72 hours	Rapid breach reporting allows the Agency to address risks promptly, minimizing harm to clients and the healthcare system**.**
12 (Monitoring Compliance)	Requires the Agency to conduct annual audits of certified solutions and mandates compliance with updated standards within six months.	A six-month compliance window may be too short for certain health data controllers and solution providers, particularly in resource-limited settings.	Extend the compliance window to 12 months for resource-limited facilities, while maintaining the six-month window for well-resourced organizations. Provide technical support and capacity-building	Realistic timelines are essential for ensuring compliance without disrupting service delivery, particularly in underserved areas. **Article 47 of the Constitution** guarantees fair administrative

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
			programs to facilitate compliance.	action, requiring the Agency to consider the operational realities of health data controllers. KICTANet's advocacy for phased implementation of digital policies supports this approach.
13(b) (Revocation of Certification)	Permits the Agency to revoke certification for breaches, non-compliance, or system security issues.	The regulation mandates revocation but does not consider whether breaches were caused by **negligence** or unavoidable circumstances (e.g., advanced cyberattacks).	Allow the Agency to assess the **root cause of the breach** before revoking certification. Introduce corrective measures for non-negligent breaches to support recovery.	a) Differentiating between negligent and non-negligent breaches ensures fairness and avoids punishing providers for events beyond their control. b) Providers are more likely to report breaches if they know revocation is not automatic for non-negligent incidents.
14(2)	Requires digital health solution providers operating before the regulations to apply for certification within six months.	Six months may be insufficient for certain providers, especially those using legacy systems requiring significant upgrades to meet certification standards.	Extend the transition period to 12 months, particularly for providers using legacy systems. Offer technical and financial assistance for system upgrades to support compliance during the transition period.	Transition periods must be realistic to avoid disruptions in existing services and ensure equitable adoption of certification requirements. **Article 46 of the Constitution** guarantees consumer protection, which includes ensuring health service continuity during regulatory transitions. KI

Regulation	Provision	Issue/Concern	Proposal/Recommendation	Justification for Proposal
14(3)	Digital health solutions must cease operations upon certification rejection	The regulation does not provide a grace period for providers to resolve non-compliance issues before ceasing operations, potentially disrupting critical services.	Introduce a **30-day grace period** to allow providers to address non-compliance issues while maintaining limited operations under supervision.	Abrupt cessation may disrupt essential healthcare services. A grace period ensures patient care continuity while compliance is addressed.