MATRIX OF COMMENTS ON THE DIGITAL HEALTH (DATA EXCHANGE COMPONENT) REGULATIONS, 2025

REGULATION	STAKEHOLDER	STAKEHOLDER COMMENT	TWG RECOMMENDATION	JUSTIFICATION
2	Gitahi Ng'ang'a Living Goods	We need a clear definition of **digital health solutions** with considerations of the various nuances around system development and enhancements.	**Adopted**	The definition to be amended to include technologies(software) "...Technologies, infrastructure"
2	AKU	Clarification on the meaning of health data controller (Data Exchange - Regulation 2)	**Not adopted**	The Data Protection Act provides for the definition of health data controller

2		DHA section 2 defines "consent" as the meaning assigned to it by the Data Protection Act. Section 2 of the Data protection Act defines consent not " informed consent". The two are not the same. This creates conflicts of laws. Let us retain the same requirement for Health Care, which is "informed consent".		
2	Fran Africa Alliance for Pop Research	Provide a definition for the term "Telemedicine".	**Not adopted**	This is sufficiently defined in the Digital Health Act

2	KMLTTB	Definition of "Telemedicine" **Recommendation:** Addition of telemedicine application diagnostics involving medical laboratory diagnostics and radiology services. **Justification:** This is to avoid criminalizing telemedicine in diagnostics	**Not adopted**	This is sufficiently defined in the Digital Health Act
2	APHRC	There is need for clarification of terms in the data exchange regulations e.g. data controller	**Noted**	The provisions of these Regulations are aligned to the Data Protection Act.
2	MoH	On Data Exchange Can the data controller be the same as the data controller of data protection commission?	**Noted**	The terms have the same meaning as provided in the Digital Health Act

4(6)	David Chiaji	Smaller healthcare providers lack the resources to meet onboarding requirements within the specified six-month period. Kindly consider extending onboarding deadlines for entities demonstrating legitimate constraints and also provide technical and financial assistance to small providers.	**Noted**	The recommendations are administrative and operational in nature.
4	Council of Governors (COG)	Regulation 4(3) provides that the Agency shall grant access to the system to authorized persons from the Ministry of Health and the county department of health for conduct of analysis of data for purposes of—	**Not Adopted**	The proposed terms of planning, budgeting and reporting have been covered in these Regulations

		This regulation should be amended in clause (c.) to read as follows: (c.) **planning, budgeting and** policy formulation. (a) reporting in compliance with subnational, national, regional and global reporting requirements; (b) decision making; and (c) policy formulation Justification The proposal is necessary since data is critical in planning and budgeting for health.		

4	Helium Health Limited	Regulation 4 (3) of the Draft Regulations provides that the Agency may grant access to the System to a person from the Ministry responsible for matters relating to health or to the respective county department responsible for matters relating to health for the purposes of reporting, decision making and policy formulation. We propose that the Agency should put in place adequate measures to ensure that the designated person, who is granted access to the System, does not utilize the access for ulterior purposes (e.g. for their personal business/any other business, profiting from the access they	**Noted**	The recommendations are administrative and operational in nature.

		have). As such, adequate penalties for such infractions should be provided for in the event of default by any person so appointed. Also, such designated person should only be granted access to anonymized data to safeguard the privacy of data subjects' personal data.		
4(6)	Mohamed Ibrahim Hassan TURBO	Is onboarding compulsory/voluntary?	**Noted**	Yes. This is described in regulation 4(6).
4	The Kenya National Public Health Institute	The current framework grants the Agency significant autonomy over data systems. This Regulation assigns the Digital Health Agency the responsibility to authorize data access, inadvertently excluding NPHI as a key stakeholder for data	**Noted**	Regulation 4(4) provides that the national and county government shall be onboarded. NPHI, being a national entity, is provided for in this regulation.

		access and analysis. This omission risks sidelining NPHI in decision-making processes, undermining its data-driven mandate for disease surveillance and outbreak response. Recommendation: Amend Regulation 4 to include key public health institutions, such as the NPHI, as designated entities for data analysis with authorized access to data system.		
4	Tech Hive Advisory Africa	The regulation (4(4) allows for the Cabinet Secretary or a County Executive Committee Member to designate a party who will be granted access to the System. However, this provision does not require a person claiming to have	**Noted**	The recommendations are administrative and operational in nature.

		been designated to provide any proof of such designation. This could potentially open the system to unauthorised disclosure An additional paragraph should be added as follows: "The Cabinet Secretary and a County Executive Member shall issue a letter of authorisation to a person designated in line with paragraph 4 above. The Agency shall not grant a person access to the System without first receiving the letter of authorisation from such person and the Cabinet Secretary or the County Executive Committee Member."		
4(6)	Tech Hive Advisory Africa	Regulation 4(6) provides a six month timeline for onboarding	**Adopted**	The onboarding process will be extended to one year as proposed

		health data controllers into the comprehensive integrated health information system, which could strain resources and affect the compliance abilities of smaller and medium-scale health data controllers. We recommend an extended onboarding timeline to ensure all data controllers are equipped for a smooth integration process, to a minimum of one (1) year. Additionally, it is essential to provide technical assistance and training programs for controllers who may struggle to integrate seamlessly into the system. This support will help them meet the necessary requirements		

		effectively without compromise to data integrity.		
4	KICTANet	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	a)**Noted** b)**Noted** c)**Noted**	The recommendations are administrative and operational in nature. The Health Act provides that the Director General for Health will define the minimum requirements The Regulations sufficiently provide for this.

		with 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.	d)**Noted** e)**Noted** f)**Adopted**	The recommendations are administrative and operational in nature. The recommendations are administrative and operational in nature. The onboarding process will be extended to one year as proposed

		Recommendations 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 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.		

		Justification 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 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 timeline ensures compliance without disrupting healthcare services		
4	Council of Governors (COG)	Regulation 4(4) should be amended in clause (c) to read as follows: 4.(4) A person to be granted access	**Not Adopted**	The Regulations sufficiently provide for this.

		under sub regulation (3) shall be designated by the Cabinet Secretary Or the County Executive Committee Member. **Justification** The proposal is necessary as an important editorial that introduces a missing word.		
4(1)	Sky-Rock Health	There is a lack of explicit requirements for compliance with international privacy standards. Mandate encryption standards, audit protocols, and patient consent processes to be as per HIPAA norms	**Noted**	The privacy requirement is in compliance with the Data Protection Act requirements The encryption requirement is an operational issue since the IT industry is dynamic.
4(1)		Health data breaches are a	**Noted**	The encryption requirement is an operational issue since the IT

		growing concern globally. Clear requirements for encryption, audit trails, and secure storage enhance trust in digital health systems. Specify minimum standards for encryption (e.g., AES-256 encryption)		industry is dynamic.
4	Festus/kisumu	How will we compel all vendors to be on boarded onto the system?	**Noted**	The Digital Health Act has outlined the onboarding as a requirement. The encryption requirement is an operational issue since the IT industry is dynamic.
4(1)		There is a need for Kenyan alignment with global standards of healthcare best practices.	**Noted**	The encryption requirement is an operational issue since the IT industry is dynamic.

		International standards like HIPAA mandate secure storage and transmission of health data to protect patient confidentiality Kindly Specify minimum certifications such as ISO 27001, which is standard for information security management systems (ISMS) for cloud-based health data.		
4(6)	Alexander Wanyama Kakamega Private Health Sector Organizations (KPHSO) Kakamega	The six-month probation period needs to be adjusted	**Adopted**	The onboarding process will be extended to one year as proposed

4(6)	CSO	What happens to systems already online before coming into force of the Act.	**Noted**	This has been provided in the Digital Health (Use of e-health applications and technologies) regulations
Regulation 5	Smart Applications International Ltd	Part III - The Enterprise Service Bus: The regulations lack details on expectations, reliability, and accountability of the National Health Information highway/system. Without statutory guidelines, the government cannot hold service providers accountable for maintaining system efficiency. **Recommendation**: The regulations should define system reliability, availability, and accountability.	**Not Adopted**	The recommendations are administrative and operational in nature.

5(2)	Arnold Ndukuyu	Typo Part 3, Regulation 5(2) is incorrectly repeated	**Adopted**	The regulation has been amended
5(3)	Arnold Ndukuyu	Interoperability should go beyond the local borders and reference industry best practices.	**Noted**	The recommendations are administrative and operational in nature.
5	Dr. Okeyo Kenya Nutritionists & Dieticians Institute	Why is it a bus? Is this the best terminology?	**Noted**	This is the term used in the Act
5(1)(e)	Tech Hive Advisory Africa	This regulation provides that the Enterprise Service Bus should monitor and eliminate redundant services. However, the regulation does not define a redundant service, nor does it specify what	**Not Adopted**	The recommendations are administrative and operational in nature since the IT industry is dynamic.

		will render a service redundant and the metrics upon which a service may be deemed redundant. We recommend that an additional definition should be added on what will constitute redundancy and the metrics for determining what will qualify as redundancy.		
5	Joshua Nairobi	Explain further on the ESB.	**Noted**	The explanation was offered to the stakeholder
5	KICTANet	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 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. **Recommendations** 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.	**Noted**	a)The Regulations sufficiently address matters relating to data protection and security

		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 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.	**Noted** **Noted** **Noted**	b)The technical guidelines will be developed c)The recommendations are administrative and operational in nature. d)The recommendations are administrative and operational in

		e) Assign the Agency the responsibility to conduct periodic audits of compliance with interoperability standards and establish penalties or remedial actions for non-compliance **Justification** 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	**Not Adopted**	nature. e)The responsibility has already been assigned under the Act

		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 eectively in the Health Information Exchange. d) Tailored support for resource-constrained facilities prevents exclusion from Kenyas 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 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.		
5	Joshua Adem Hope Hospice Kajiado	Requesting for the omission of the term "the bus". I further propose for the reduction of the process at the exchange	**Not adopted** **Not adopted**	This is the term used under the Act This is the object of the regulations

		system by enforcing some to be under one roof.		
5		Is the ESB a "Broker" between the patient and facilities ?	**Noted**	The 'bus' is the facilitative system between the patients and facilities.
5		ESB - what informed this, were there test trials.	**Noted**	This is the term used in the Act
5	Nzisa Liku CDC	Provide clear definitions of the ESB	**Noted**	The term is already defined under the Act
5(2)	Living Goods	Why does the ESB include telemedicine platforms and supply chain management?	**Noted**	They are components of the Digital Health ecosystem
5(2)(b)	Occupational Therapy Council of Kenya	**Telemedicine**	**Adopted**	Regulation amended to add "care" before the word "treatment"

		Inclusion of rehabilitation in Digital Data Exchange PART III 5(2)(b): Consider including rehabilitation as a specific domain in the digital data exchange to support comprehensive care, particularly for persons with disabilities and chronic conditions		
6	Smart Applications International Ltd	Part III - The Enterprise Service Bus - Clause 6: The Enterprise Service Bus has significant responsibilities, yet no minimum requirements or accountability measures are specified. **Recommendation**: Data Processors should have the option to apply for onboarding onto the	**Not Adopted**	The data controller oversees the processor.

		National Health Information System on behalf of Data Controllers.		
6	Technical University of Mombasa Health Services	How are the systems that are used by private hospitals going to be integrated with the National Health system?	**Noted**	This is provided for in the onboarding application
6	AKU	Private institutions - what mechanisms have been placed to ensure/support private institutions to onboard onto the system?	**Noted**	The recommendations are administrative and operational in nature.

6	John Daktari online	The onboarding process is unclear	**Noted**	Regulation 6 sufficiently provides for the onboarding process
6	Tech Hive Advisory Africa	This regulation limits the onboarding on the enterprise service bus to data controllers. However, data processors may also benefit from the interoperability standards developed under the Act and the other benefits of the enterprise service bus. We recommend extending onboarding on the enterprise service bus to include data processors. This will ensure that all digital health solutions align with the interoperability standards to be developed under the Act.	**Noted**	This is defined in the Act

6	KICTANet	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 training will be provided to data controllers during the process. Recommendations a) Define clear onboarding criteria for health data controllers, including technical capabilities, compliance with security	**a) Not Adopted** **b)Not Adopted**	a)The regulations provides for the onboarding process b)The recommendations are administrative and operational in nature.

		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 resources to ensure inclusivity across counties. Justification 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.		
6		Provide for reimbursement of onboarding fees after blocking or suspension from the ESB.	**Noted**	The fee is utilized for the maintenance of the system
6	Nelson Kakamega	What happens when a government facility procures a system that cannot be onboarded?	**Noted**	The procurement procedures need to include certification requirements. For existing system, the transition provisions have been provided in the Digital Health (Use of E-health Applications and Technologies) Regulations

6	Justus Mughoshi	What are the penalties for facilities not onboarding to the system? (6	**Noted**	The Regulations provide for the penalties
6	Calvine Lwaka	How will onboarding be conducted where a user has multiple systems?	**Noted**	The recommendations are administrative and operational in nature
7(1)(g)	Calvine Lwaka	How much will the cost of onboarding be?	**Noted**	This has been provided in Schedule 2 of the regulations
7	CSO	Where a person applying to be onboarded to the Bus doesn't possess the requisite documents, how will they get into the system?	**Noted**	This is provided for in the Regulations.
7	Boniface Igumba /APHRC.	What happens to controllers who are unable to pay the onboarding fees, and what is the impact of this on service delivery?	**Noted**	They will not get onboarded

7	Prof. Bulimo KEMRI	This is a government system, why should there be an onboarding fee?	**Noted**	The fee is utilized for the maintenance of the system
7	Council of Governors (COG)	7.(5) An applicant who dissatisfied by 2 decision of the Agency in relation to onboarding to the enterprise service bus may apply to the Complaints Committee for a review of the decision in accordance with the Digital Health (Health Information Management) Regulations, 2024. This regulation is amended by inserting	**Adopted**	The Regulation is to be amended

		the word "is) between the words "who" and "dissatisfied" to read as follows: 7.(5) An applicant who is dissatisfied by a decision of the Agency in relation to onboarding to the enterprise service bus may apply to the Complaints Committee for a review of the decision in accordance with the Digital Health (Health Information Management) Regulations, 2024. **Justification** The proposal is necessary as an important editorial that introduces a missing word		
7(3)		There's duplication of licensing for the same issues i.e. Data	**Noted**	The licence prescribed in the regulations is for purposes of

		controller licensing by ODPC and DHA		accessing the national health information system and not for handling data as an ODPC requirement.
7(3)(b)	Mwirigi Kiula	7(3)(b) on an application programming service endpoints leaves out the shared implementation element – replace with "an application programming interface endpoints and integration service."	**Adopted**	The Regulation is to be amended as proposed
7(4)	Helium Health Limited	By the provisions of Regulation 7 (4) of the Draft Regulations, an Enterprise Service Bus licence issued under the Draft Regulations is valid for a period of one year from the date of issue. We advise that in order to avoid the risk of being onerous which	**Not adopted**	Annual renewal is necessary for ensuring that the users maintain certification and the proper monitoring of the system

		may discourage compliance and consequently slow down innovation, the validity period of the licence should be longer, ranging from a two to three year period.		
7(5)	Tech Hive Advisory Africa	This regulation allows an applicant who is dissatisfied with the decision of the Agency to apply for a review of the decision. However, it does not specify a timeline within which the applicant should initiate the review process. Consequently, this regulation innately opens the period within which a review can be initiated. We recommend a redraft of the regulation as follows: "(5) An	**Not Adopted**	The matters of complaints have been addressed in the Digital Health (Health Information Management) Regulations.

		applicant who dissatisfied by a decision of the Agency in relation to onboarding to the enterprise service bus may apply to the Complaints Committee for a review of the decision in accordance with the Digital Health (Health Information Management) Regulations, 2024, provided that such review may be initiated within fourteen (14) days of receiving the Agency's decision."		
8	KICTANet	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	**Not adopted**	The recommendations are administrative and operational in nature.

		how often the inventory will be updated, which could lead to outdated or inaccurate records. Recommendation 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 Justification		

		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		
8	Office of the Data	The Digital Health (Data Exchange) Regulations, 2024;	**Noted**	The recommendations are administrative and operational in

	Protection Commissioner.	Regulation 8(1) on the Inventory of the Health Data Controllers, duplicates the register kept by the ODPC under Section 8(1), 18-21 of the Data Protection Act,2019 The inventory should reflect the register maintained by the ODPC. Further, the regulations should specify which register would supersede the other in the case of a conflict.		nature.
9(1)	Rebecca Kiptui MOH	Suspension of data controllers: How long is the suspension? And is it varied depending on the breach?	**Noted**	The period is dependent on the breach
9	Helium Health Limited	Regulation 9 (1) of the Draft Regulations outlines the circumstances in which a health	**Adopted**	The Regulation is to be amended to insert a clause on the criteria for permanent blocking

		data controller may be suspended from the Enterprise Service Bus, while Regulation 9 (2) provides that a party who is suspended from the Enterprise Service Bus shall be blocked from access thereto. However, confusion arises in Regulation 9 (4) where reference is made to the fact that a health data controller, who is permanently blocked from accessing the Enterprise Service Bus, shall migrate health data. This is because there is no provision of the Draft Regulations which states the circumstances under which a health data controller may be permanently blocked or which rules could be infringed to bring about this		

		penalty. We recommend a revision of Regulation 9 of the Draft Regulations to address the above omission, with an introduction of specific actions by a health data controller that may cause such health data controllers to be permanently blocked from accessing the Enterprise Service Bus. Additionally, prior to any suspension or blocking of access to the Enterprise Service Bus, the health data controller should be given prior notice of the alleged infraction and adequate time to remedy it. The controller should only be suspended or blocked if		

		they fail to remedy the alleged violation(s).		
9	Tech Hive Advisory Africa	This regulation outlines the instances where the digital health solution of a party will be suspended on the enterprise bus service. It specifies where "the digital health solution of the health data controller is not valid;" as one of such instances. However, this provision is vague as it does not specify what constitutes a valid digital health solution, nor does it reference any other regulation that provides the assessment metrics that may be used to determine the validity of a digital health provider.	**a)Not adopted** **b)Adopted**	a) The recommendations are administrative and operational in nature. b) The Regulations to be amended to include a sub-regulation (h) as proposed

		In addition to the grounds specified for the suspension of a certification, we reckon that misrepresentation of any fact presented during the application process should also be a ground for suspending a digital health service provider from the enterprise service bus. We recommend that an additional provision specifying the assessment that will be conducted to determine the validity of a digital health solution be included in the regulation. Additionally, a sub-paragraph should be added as follows: "(h) where the health data controller misrepresents any information		

		submitted during the application for onboarding on the enterprise service bus."		
9	Physicians for Human Rights	Suspension from Enterprise Service Bus disrupts critical services. We suggest temporary access during investigations.	**Not Adopted**	The recommendations are administrative and operational in nature.
9	Tech Hive Advisory Africa	It is acknowledged that an underlying essence of this Regulation is to promote accountability. However, there are instances that may require a health data controller to take remedial action if they are duly noted of the Agency's decision to block their access on the enterprise service bus platform. Therefore, we recommend that the data controller should be duly notified of the	**Adopted**	The Regulation is to be amended to insert a clause on the criteria for permanent blocking.

		Agency's decision to block access to the enterprise service. We recommend that this regulation be redrafted as follows: "(3) a. The Agency shall notify the health data controller of the blocked access to the enterprise service bus within three days before the proposed date of blocking such access. However, this notice will not be necessary where access is to be blocked due to a data breach. 3b. where the Agency notifies a data controller of its intention to block the controller's access, the controller shall have the opportunity to take such remedial action and notify the Agency		

		before the 3-day period elapses. "		
9	KICTANet	a) (Reg 9(1)a): The regulation does not define what constitutes a serious data breach or provide criteria for 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.	a)**Adopted** b)**Not Adopted** c)**Adopted** d)**Not Adopted** e)**Not Adopted**	a)Regulation 9(1)(a) amended to delete the word "serious" appearing before the words "digital health solution of the health data controller has a" b) The recommendations are administrative and operational in nature. c) he regulations is to be amended to reduce the timeline notification to twenty-four hours d) The recommendations are administrative and operational in nature.

		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 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. **Recommendations** a) Clearly define serious data breaches (e.g., breaches exposing sensitive health data). Include thresholds or examples to standardize enforcement.		e) The recommendations are administrative and operational in nature.

		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 timeline (e.g., 14 days) for the Agency to		

		review and process re-onboarding applications after compliance issues are resolved. **Justification** a) Clear definitions ensure uniform application of the rule, avoiding subjective or arbitrary suspensions. Aligns with Section 41 of the Data Protection Act, 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 resource-intensive, and without Agency support, blocked controllers may fail to comply, leaving critical health data inaccessible. Supporting migration aligns with the 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.		
9(4)	KEMRI	What happens to patients who need treatment at a facility in case the facility is suspended from the bus?	**Noted**	The recommendations are administrative and operational in nature.
10	The Kenya National Public Health Institute	The health data banks are critical repositories of both aggregate and case-based data. NPHI requires access to these data sets for monitoring health security threats. The Regulations do not guarantee NPHI access to these data banks, potentially hindering its ability to	**Not Adopted**	The Kenya National Public Health Institute, being a national entity, is provided for in Regulation 10(1)

		respond to public health emergencies. Recommendation: Designate NPHI as a co-custodian of the health data banks with access to case-based data for public health purposes.		
10	Eric Angula Medtronic Labs	IT competencies to manage county data banks is lacking. How will counties be supported in this?	**Noted**	The recommendations are administrative and operational in nature.
10	Dr. Lishenga RUPHA	For functions allocated to the counties mainly county data banks, the administrative structures should clearly be defined in the regulations to ensure transparency and stakeholder involvement. Have a policy guidance to the counties to support this.	**Noted**	The recommendations are administrative and operational in nature.

10	John Daktari online	County-National Data bank - the flow of data between the county and national data banks is unclear.	**Noted**	The Digital Health Act provides for the flow of data between the county and national data banks. The recommendations are administrative and operational in nature.
10	Steve Health X Africa	The process of data movement between the county and national data banks is unclear	**Noted**	The Digital Health Act provides for the flow of data between the county and national data banks. The recommendations are administrative and operational in nature.
10	Association Private Hospitals	Who is the custodian of the county data banks and does it integrate with the National Data Bank?	**Noted**	The Digital Health Act provides for the flow of data between the county and national data banks. The recommendations are administrative and operational in

				nature.
10	Council of Governors (COG)	10.(2) Any health data transmitted to the national health data bank or the county health data bank shall be stored, reviewed, audited, updated and secured in accordance with the Act and the relevant laws including – This regulation is amended by deleting one set of the words "issued by" that come immediately after the word "policies' to read as follows: (a) the security and cybersecurity standards and policies issued by the issued by the Cabinet Secretary for the time	**Adopted**	The Regulations are to be amended to delete the repeated word "issued by"

		being responsible for matters relating to information and communication technology and digital economy; and 10.(2) Any health data transmitted to the national health data bank or the county health data bank shall be stored reviewed, audited, updated and secured in accordance with the Act and the relevant laws including - (a) the security and cybersecurity standards and policies issued by the Cabinet Secretary for the time being responsible for matters relating to information and communication technology and digital economy; and		

		Justification The proposal is necessary as an important editorial that removes repeated words in the clause.		
10	Living Goods	Is there a timeline for operationalizing data banks?	**Noted**	The recommendations are administrative and operational in nature.
11	Living Goods	Is there a timeline for operationalizing shared services?	**Noted**	The recommendations are administrative and operational in nature.
11(2)	CUEA	The users and consumers of the shared resources in the system shall pay a service fee for use of the system. Will this be out of pocket user fees? Recommendation: Explicitly state	**Not Adopted**	The users are the health information systems who are to pay the prescribed fees.

		who pays the user fees.		
11	Helium Health Limited	While Regulation 11 (2) of the Draft Regulations provides that users and consumers of the shared resources in the System shall pay a service fee, there is no indication as to whether this fee(s) shall be one-off or recurring. In order to avoid ambiguity, we recommend that clarification should be provided within the Draft Regulations as to the frequency of payment of the service fee.	**Not Adopted**	The users are the health information systems who are to pay the prescribed fees as per the Second Schedule.
12(1)	NCI-K	Coding for cancer (ICD-0)	**Noted**	This is provided for in the Digital health solution certification framework
13	Council of	13.(6) A certified digital health	**Adopted**	The Regulations amended to

	Governors (COG)	solution shall, upon the payment of the applicable fee by the responsible digital healthcare provider, be granted access to the client registry to identify clients and patients and to verify their identity information. This regulation is amended by deleting the words "to" that comes immediately after the words "upon" to read as follows: 13.(6) A certified digital health solution shall, upon the payment of the applicable fee by the responsible digital healthcare provider, be granted access to the client registry to identify clients and patients and to verify their identity information.		delete the word "to" that comes immediately after the words "upon"

		Justification The proposal is necessary as an important editorial that removes an unnecessary word in the clause.		
13	Curtis Clinton Okinyi Yaitaa representative Ngara UHIEF office Starehe Ngara	How will street families be registered in the Client Registry?	**Noted**	The recommendations are administrative and operational in nature.
13	Hadija Kipoin Chief's office Kahawa West	Provide more options on documents required for foster children e.g. forster certificate.	**Noted**	The recommendations are administrative and operational in nature.
13	Daisy Korir Kericho	How will clients without identification cards and seeking services in health facilities be	**Noted**	The recommendations are administrative and operational in nature.

		catered for?		
13	Emmanuel Kayere Nakuru	Consider introducing QR Codes for scanning of patients data and health records for efficiency in service delivery especially for in-patients.	**Noted**	The recommendations are administrative and operational in nature.
13	Veronica Musyoka Nakuru	Can Alien children use Kenyan Birth certificates for registration in the Client Registry?	**Noted**	The recommendations are administrative and operational in nature.
13	Denis	What are the limitations to data access for private facilities tapping into the client registry?	**Noted**	The recommendations are administrative and operational in nature.
14	KMLTTB	Regulatory details to include registration and licensure by relevant respective professional regulatory body. **Justification**: This is to prevent mischief in the meaning of	**Noted**	This is beyond the scope of the Regulations

		regulatory details		
14(4)	KMLTTB	Delete the requirement to master facility code correctly issued by the Kenya Medical Practitioners and Dentist Council but only include hospitals mostly in government. **Justification**: To ensure all health facilities such as medical laboratories, pharmacies, physiotherapy clinics, etc. inclusion of all facilities	**Noted**	The Kenya Health Master Facility Code is used for the purpose of uniquely identifying healthcare providing entities
14	Duncan Mutua	Is there need to have another registry, yet the regulators (KMPDC) have robust systems handling the desired information.	**Noted**	The Kenya Health Master Facility Code is used for the purpose of uniquely identifying healthcare providing entities
14	KMLTTB	**Recommendation:** Include the role of the Health Professionals	**Noted**	This is beyond the scope of the regulations

		regulatory body in determining the payments **Justification:** Health Professionals regulatory body understands the services they offer and hence should assist in rationalizing any charges		
14(2)(e)	NCI-K	Disease-specific registries by government agencies. How does DHA encourage or discourage the same; citing the fact that the act provides casing example cancer registries	**Noted**	All disease registry will be consumers of the shared resources
14(2)(e)	NCI-K	How do facilities running disease-specific registries pay to be onboarded to the ESB? Example; They collect patient-level data across facilities	**Noted**	The regulations sufficiently provide for onboarding procedures..

		providing oncology.		
14	Mohammed Hassan	For facilities, is it only one person who is supposed to register on behalf of the rest?	**Noted**	The regulations clearly define who is to register healthcare facilities
15	Steve Health X Africa	What happens to telemedicine platforms that are a component of the facility HMIS? Telemedicine should not be separated from healthcare delivery.	**Noted**	The recommendations are administrative and operational in nature.
15	KICTANet	a) (Reg 15(1)): Potential exclusivity may create monopolistic tendencies, restricting competition among telemedicine providers. b) (Reg 15(3)e): The requirement	**a)Not Adopted** **b)Not Adopted**	This has been provided for in the Act This is a legal requirement under the Data Protection Act

		could delay service delivery due to lengthy registration processes. c) (Reg 15(5)a : Stringent certification requirements may exclude innovative but uncertified providers, 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. Recommendations a) Ensure that alternative, verified sources of reference are also allowed for telemedicine providers. b) Specify the minimum necessary	**c) Not Adopted** **d) Noted** **c)Not Adopted** **d)Not Adopted**	This has been provided for in the Act The recommendations are administrative and operational in nature. The recommendations are administrative and operational in nature. The recommendations are

		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 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		administrative and operational in nature.

		mechanisms for the telemedicine health provider registry. Justification 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 and processors. A transitional		

		framework would ensure the 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 oversight ensures the agency adheres to best practices.		
16	Dr. Okeyo Kenya Nutritionists & Dieticians Institute	Clearly define the scope of the professionals that are to be in the registry	**Noted**	The Health Act provides for the definition of a health worker. Regulation 16 sufficiently provides for the scope of the professionals.
16	KMLTTB	**Recommendation:** Delete the health data controller at the end of the sentence	**Adopted**	The regulations to be amended to delete the words "health data controller" in regulation 16(1)(c)

		Justification: The health data controller should never be allowed to register a health professional without necessary qualifications employed by health professional regulatory bodies. This may be abused and a window for corrupt entries.		
16	Duncan Mutua	The regulators have systems that manage all aspects of their respective health workers. API's would be ideal instead of having parallel systems.	**Noted**	The recommendations are administrative and operational in nature.
16	Simon Mbai	Is a community health promoter recognized as a health worker?	**Noted**	The community health promoters are described in the Primary Health Care Act 2023.
16	Fredrick	How will CHPs be onboarded if they aren't under any regulatory	**Noted**	The Community Health Promoters are not health workers

		bodies		and thus will not be onboarded.
16	Mwirigi Kiula	The definition of the Health Care professional is limited in scope and reality – the health care professional in the digital health ecosystem is far beyond the medical, nursing, billing and health records. What is the real full set of health workers? The regulated and non-regulated cadres e.g., ambulance drivers, porters, customer service, ICT experts in the health facilities?	**Noted**	The Digital Health Act and the Health Act defines a healthcare professional.
16	Helium Health Limited	We note that neither the Draft Regulations nor the Digital Health Act, 2023 pursuant to which the Draft Regulations are to be issued	**Adopted**	The term used in the regulations is "healthcare provider" Amend the regulations to replace

		define the term "health worker". This creates room for ambiguity in defining who falls under the category of persons to be captured by the health worker registry. However, the Digital Health Act 2023 defines a "healthcare professional" as including any person who has obtained health professional qualifications and licensed by the relevant regulatory body. In order to ensure consistency of terms and avoid ambiguities, we recommend that all references to "health worker" in paragraph 16 should be amended to read "health care professional".		the term "healthcare worker" with "healthcare provider"

16	Medic	Is a CHP considered as a healthcare worker and therefore part of the health worker registry?	**Noted**	The Community Health Promoters are not health workers and thus will not be onboarded.
16	KMPDC	Is the health worker registry a duplication of KMPDC's registry?	**Noted**	The scope of the health worker registry goes beyond the professionals regulated by KMPDC
17	Mwirigi Kiula	17(4)(d) on prevailing industry practices is open to abuse – the industry practices must be adopted/adapted through a proper framework - replace with "Adopted industry best practices."	**Not Adopted**	It is implied that the best practices will be applied in making recommendations on review of the the Kenya Health Enterprise Architecture
18	KMLTTB	**Recommendation:** Delete "issued by Pharmacy and Poisons Board through the system". **Justification:** The health products and technologies bill is currently	**Adopted**	The regulations to be amended as proposed

		in parliament as envisaged by the Health Act. Also, medical laboratory reagents and equipment don't fall under competencies available under PPB as they require scientific validation and verification in certified medical laboratories.		
18	Martha Ministry of Health	Inclusion of Braille enablement in HPTs. The regulations should work to enhance disability inclusivity in health by promoting access to disability-friendly health services.	**Not Adopted**	This is beyond the scope of the regulations
19(1)	Kenya National Blood	The regulations fail to include blood, organs, and tissues.	**Not Adopted**	The definition is implied

	Transfusion Services	Expand the scope of these regulations to include biological organs as health products and technologies.		
19	KMLTTB	**Recommendation:** Delete " Pharmacy and Poisons Board" and replace it with competent professional bodies. **Justification:** This is to allow the regulatory bodies to practice their competencies in assessing the suitability of the said product. This may include KMLTTB, KEBS, and the proposed HPT authority.	**Adopted**	The regulations are to be amended to as proposed
19	KMLTTB	**Recommendation:** Delete "Pharmacy and Poisons Board pursuant to section 3B(2)(b) and (d) of the Pharmacy and Poisons	**Adopted**	The regulations are to be amended to as proposed

		Act "and replace with competent professional regulatory bodies with competencies to ascertain quality. **Justification**: This is to avoid criminalizing telemedicine in diagnostics.		
19(4)	KMLTTB	**Recommendations:** delete the provisions of payment. **Justification:** Payments for these services is a double tragedy as it will increase the cost of health care. It is important to note that validation and verification is a scientific process that will cost money in terms of samples for evaluation and procurement of laboratory services and more	**Not Adopted**	The fee is necessary for the maintenance of the system

		importantly in this particular provision		
19	Helium Health Limited	We note that this Regulation contains two separate paragraph 19 (3). We recommend that this should be rectified to prevent confusion. Secondly, regarding the second Article 19 (3), which requires that suppliers of a health product or technology shall apply for registration into the National Logistics Management Information Services Platform, it is our considered view that such additional registration may be onerous. The registration stated in paragraph 7 (1) should cover any other required registrations under	**Adopted**	The regulations are to be amended as proposed

		the Draft Regulations.		
19	Gitahi Ng'ang'a Living Goods	The NLMIS is misplaced in the shared/common resources	**Not Adopted**	The Digital Health Act has provided for the NLMIS as a component of the shared ehealth records.
19	KEMRI Wellcome Trust Programme	What are the opportunity costs of the NLMIS and how does it promote/inhibit the availability of HPT in the country?	**Noted**	Response offered on the advantages of NLMIS
19	KICTANet	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)	**a) Noted** **b) Noted** **c) Noted**	a) The recommendations are administrative and operational in nature. b) The recommendations are administrative and operational in nature. c) The recommendations are administrative and operational in

		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 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,	**d) Noted** **e) Not Adopted** **f) Noted** **g) Noted**	nature. d) The recommendations are administrative and operational in nature. e) The regulation provides for the minimum subsidised amount that is required to onboard into the NLMIS f) The recommendations are administrative and operational in nature. g) The recommendations are administrative and operational in nature.

		discouraging participation in the health product supply chain. **Recommendations** 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 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 online reporting options for regions with limited internet connectivity. g) Introduce a sliding scale for		

		annual retention fees based on the suppliers turnover or financial capacity. Consider exemptions or subsidies for nonprofit and public health suppliers. h) Develop contingency measures, such as backup systems and decentralized reporting options, to maintain supply chain functionality during platform downtime or breaches **Justification** 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 inefficiencies. 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.		
20 & 21	Helium Health Limited	We note that paragraphs 20 (7) (b), 21 (5), etc, prescribe that offenders of the varying provisions of the Draft Regulations will face	**Not Adopted**	The regulation as drafted is in order

		penalties under Section 59 of the Digital Health Act, which among other penalties, prescribes imprisonment for certain periods. We propose that in line with international standards, punishment for infringements of the Draft Regulations should be effective, proportionate and dissuasive, and not resort to prison terms unless for serious violations, especially those that involve criminal activity.		
20	The Kenya National Public Health Institute	The Shared Health Record is designated to provide a single reference for patient medical history, essential for continuity of care and disease tracking.	**Not Adopted**	The Kenya National Public Health Institute, being a national entity, is provided for in the Regulations

		NPHI's mandate to access and analyze case-based data is not articulated, which could impede its surveillance efforts. NPHI requires access to case-based data, such as patient-level information from the Shared Health Record and other registries for real-time disease surveillance; monitoring and response to public health emergencies; and analyzing trends to inform health security policies. Aggregate data alone is insufficient for the depths of analysis required to predict and mitigate health risks. Recommendation: Amend Regulation 20 to explicitly grant NPHI access to case based data for surveillance, outbreak response		

		and research.		
20	Steve Health X Africa	Provide an opt-out option for the Shared Health Record	**Not Adopted**	
20	Director Gregory Ganda	Are there fees for updating the Shared Health Record (Post op)?	**Noted**	Response offered that there is no fees for updating the SHR
20	Micheal ICTA/Eldoret.	Are facilities charged for updating records? Facilities don't raise claims for updating of records, will they be charged to access the system for this purpose?	**Noted**	Response offered that there is no fees for updating the SHR
20		Where will the updating of the Shared Health Record be done; is it service provider level/ national level?	**Noted**	Response offered that updating of the Shared Health Record will be done at the service provider level

20	KICTANet	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 security vulnerabilities. d) (Reg 20(7)): The regulation references Section 59 of the Act but does not clarify whether penalties are administrative fines,	a) **Noted** b) **Noted** **c) Noted** **d) Noted**	a) The recommendations are administrative and operational in nature. b) The recommendations have already been [provided for in the regulations c) The recommendations are administrative and operational in nature. d) The penalties have already been defined and the mitigation circumstances will be decided on a case-to-case basis

		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 regulation does not address audit mechanisms for tracking cross-entity requests, which could lead to misuse or unauthorized sharing	**e) Noted** **f) Noted**	e) This has already been implied in the regulations subject to privacy rights f) The recommendations are administrative and operational in nature.

		of health data **Recommendations** 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 (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 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. **Justification** 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 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 eective 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 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.		
20(9)	Tech Hive Advisory Africa	The regulation mandates that data controllers must respond to any requests for additional information, beyond what is stored in the shared folder, within seventy-two hours. However, meeting this timeline may be challenging for data controllers if they are experiencing a high volume of requests or encountering technical difficulties.	**Not Adopted**	The seventy-two hour timeline is sufficient for data controllers to provide the necessary data.

		We recommend extending the timeline and requiring detailed justification if the timeline is not met. This provision may be revised to allow for a "thirty day" timeframe. If the required information is not provided within thirty days, the data controller should immediately notify the client with reasons for the delay.		
21	The Kenya National Public Health Institute	The Regulation proposes the maintenance of a Health Management Information Services (HMIS) Platform giving the Agency authority to provide a minimum data set for reporting including, electronic integrated	**Not Adopted**	The Kenya National Public Health Institute, being a national entity, is provided for in the Regulations

		disease surveillance and response; public health events as well as disease or events of international concern. The NPHI is mandated to spearhead the public health component of the national disaster response framework. This entails providing leadership, regulation, and coordination in all areas related to national public health priorities including the management of critical public health data for emergency preparedness and response. This regulation, as it stands, will limit the role of NPHI in effectively carrying out its mandate.		

		Recommendation: Designate the NPHI as a central repository and a co-custodian for the synthesis and dissemination of the disease burden and public health trends in line with global health security principles. This will leverage NPHI's mandate to ensure timely dissemination of critical data related to disease outbreaks and health events in a format suitable for public consumption. Real-time access to data reported to the HMIS platform will enhance coordination of responses to public health events.		

21(2(a)	KEMRI WT	Define the "data of public health interest" that will be publicly available.	**Not Adopted**	The term has been used in its ordinary meaning
First Schedule Form 4	KMLTTB	**Recommendations:** Delete blood and blood products **Justification:** Blood and blood products are donated by non-remunerated healthy blood donors and inclusion in this list will commercialize the process thereby introducing unethical practices. Safe blood for transfusion must be tested for transfusion transmissible infections (TTI) such as~~as such~~ HIV, syphilis, Hepatitis B and C, and other infectious diseases which are part and parcel of medical laboratory services the world over.	**Not Adopted**	The details in the form are for guiding the registration

Second Schedule	KMLTTB	Consider reducing all applicable charges by 90% Justification: This is to ensure that there is Universal Health Coverage devoid of exorbitant costs that limit access to quality health services.	**Not Adopted**	The fees are utilized for the maintenance of the system
Second schedule	Fredric Omondi	Onboarding fees for Telemedicine platforms are too high.	**Not Adopted**	The fees are utilized for the maintenance of the system
Second schedule	AFIDEP	Telemedicine costs - the accumulative fees for telemedicine providers are prohibitive increasing the barriers to the access of health services especially in hard-to-reach areas.	**Not Adopted**	The fees are utilized for the maintenance of the system
Second schedule		Insurance providers; Clarify on the difference between	**Not Adopted**	The response provided cuts across all service providers

		the fees and whether it cuts across all insurance providers. If they do then the common *mwananchi* will be affected as they are too high (premium may be increased)		
Second Schedule	Eveline Koskei Kericho	Can the fee for Services offered to clients through the Enterprise Service Bus be waived for government facilities?	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system
Second Schedule	Jilo B Said Isiolo	Consider the following adjusted fees for Onboarding to the Enterprise Service Bus: Level 2 & 3 – (500) Level 4 – (1000) Level 5 – (2000)	**Not Adopted**	The fees are utilized for the maintenance of the system

		Level 6 – (5000)		
Second Schedule	David Machari Lang'ata CPU	You must lower the licensing cost. This sounds to be for the rich so the poor will not get the service.	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system
Second Schedule	Mohamed Ibrahim Hassan TURBO	The onboarding fees is too high	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system
Second Schedule	Michael Litu Indiazi ICTA CC Office	Requesting for waiver of fees for updating of records.	**Not Adopted**	There are no fees for updating records in the system. Further, the fees are already subsidised.
Second Schedule	Hellen Koech Kapsoya	I support the digitalisation of health data but the fee for onboarding is high. How did you come up with the fees?		The fees are utilized for the maintenance of the system Health data is a strategic national asset and the country ought to benefit from the use of its health

				data.
Second Schedule	Jilo B Said Isiolo	Telemedicine platform onboarding X annual license should be capped at 10,000	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system
Second Schedule	Jilo B Said Isiolo	Health Insurance Providers onboarding into the Enterprise Service Bus should be capped at 25,000	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system
Second schedule	Peter Sirimia Nyalenda	Licensing fees are very high	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system
Second Schedule	Patrick Kericho	Onboarding fees needs to be clear especially on HMIS/PALs and HIMs		

Second schedule	Michael Ngiri Kericho	Can onboarding fees be waived for public facilities to KMPDC fees?	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system. Further, the fees are already subsidised.
Second schedule	Philip Chule	The payments are not clear to us; do you mean that when I visit a hospital I am mandated to pay the fees shown to us? What are the costs being passed on to the patients?	**Noted**	The fees will be borne by the health providers not the patients.
Second Schedule	MNTRH	MNTRH intends to establish telepsychiatry services to enhance access to mental health services, which will be non-chargeable with the fees charged in onboarding to the telemedicine platform. We are	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system. Further, the fees are already subsidised.

		worried about who will bear the costs for the onboarding and licensing.		
Second Schedule	KHPOA	Fees on onboarding facilities is likely to make the cost of doing business hard. There is need to have a one stop license. The cost can be on the use of data for research	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system.
Second Schedule	Living Goods	The fees for Onboarding Level 1 providers (Community Health) are not indicated.	**Adopted**	The schedule is amended to include level 1 at the cost of ksh 1000 onboarding and kshs 500 annual license.

Second Schedule	APHRC	Will insurance providers not take advantage and misuse patients data by determining charges & premiums based on health risks of a patient?	**Not Adopted**	The Digital Health Act provides for penalties in case of breach The recommendations are administrative and operational in nature.
Second Schedule	Joshua Hope Hospice	The fees are prohibitive and should be renewed.	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system.
Second Schedule	David	The fees are too high	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system.
Second Schedule	KEMRI	Why charge for onboarding yet this is a government initiative that	**Not Adopted**	The fees are necessary for the operationalization and

		must be complied with?		maintenance of the system.
Second schedule	AFIDEP	Telemedicine costs - the accumulative fees for telemedicine providers are prohibitive increasing the barriers to the access of health services especially in hard-to-reach areas.	**Not Adopted**	The fees have been subsidised for proper functioning of the system.
Second schedule	AKU	This is a government initiative so why do even public institutions have to pay to be onboarded onto the ESB?	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system.
Second Schedule	KEMRI WT	Lower-level facilities are already struggling to conduct normal service delivery, what	**Noted**	The fees have been subsidised for proper functioning of the system.

		mechanisms have been laid out to ensure they can afford to be onboarded onto the ESB?		
Second Schedule		Are all the facilities required to pay the fees?	**Noted**	The healthcare facilities will be required to pay the onboarding fees.
Second schedule	APHRC	The onboarding fee threatens to interrupt normal service delivery	**Noted**	The fees have been subsidised for proper functioning of the system.
Second schedule	Association of Private Hospitals	The payer and mode of payment for the health facility bill fees are unclear	**Noted**	The recommendations are administrative and operational in nature.
Second Schedule	John Daktari online	Telemedicine providers already pay to another regulator. Where is the convergence between the agency and the other regulator?	**Noted**	There is no conflict between the agency and the regulators

Second schedule	Gitahi Ng'ang'a Living Goods	Level 1 (community health) solutions are not included in the fees.	**Noted**	The schedule was amended to include level 1 at the cost of ksh 100.
Second Schedule	Justus Mughoshi	The facility onboarding fees are too high to incentivize facilities to join the system. (Second schedule)	**Noted**	The fees have been subsidised for proper functioning of the system.
Second Schedule	Association of Private Universities	The health facility bill fees - Who will bear the cost of this? Is it the facility or the patient?	**Noted**	The fees have been subsidised for proper functioning of the system.
Data exchange - Second schedule	Abel MTRH	The fees for onboarding/maintaining telemedicine solutions onto the ESB are too high and the costs are likely to be pushed to the patients.	**Noted**	The fees have been subsidised for proper functioning of the system.

		They should be categorized/differentiated between govt not for profit and private for-profit fees		
General	Ben Roberts	The sector is unable to efficiently evaluate the regulations without reference documents/ information on the Comprehensive Integrated HIS (KHEA, ESB) Recommendation - sufficient sensitization of the sector	**Noted**	Responses provided on where to access the documents.
General	Ben Roberts	The unique identifier, a key component of a health digital health architecture is missing	**Noted**	Unique identification is included as a component in the implementation of the Digital Health Architecture.

MATRIX OF COMMENTS RAISED ON THE DIGITAL HEALTH (HEALTH INFORMATION MANAGEMENT PROCEDURES) REGULATIONS, 2025

REGULATION	NAME/ ORGANIZATION	COMMENT	TWG RECOMMENDATION	JUSTIFICATION
2	Living Goods	How do we define a digital health solution? Is it the platform or specific flavors/implementations?	**Adopted**	The definition to be amended to include technologies(software) "...Technologies, infrastructure"
2	Ministry of Health	Migration is the data processor the same as the controller. The processor was not mentioned in the presentation.	**Noted**	Data migration is the responsibility of the health data controller as they decide on the manner of processing health data
3	Council of Governors (COG)	The object of these Regulations is to give effect to the provisions of the Act by ensuring the safe management of health information. The regulation should be amended to read as follows: "The object of these	**Not Adopted**	The Regulation as drafted is in order

		Regulations is to give effect to the provisions of the Act by **providing for policies and procedures that ensure** the safe management of health information." The amendment is necessary to make the object respond to the specifics set out by section 60(a) of the Digital Health Act		
4	Council of Governors (COG)	The regulation should be amended as follows: 4(1) The Kenya Health Data Governance Framework established pursuant to section 21(1) of the Act **and is included in these regulations as the First Schedule,** shall be the reference document for the management of health data and shall govern the collection, access, sharing, and use of health data.	**Not Adopted**	The framework will be provided for separately

		Justification The proposed amendment is necessary because section 21(1) of the Act requires the cabinet secretary to, in consultation with the Director-General, establish a health data governance framework. The amendment will enable any person reviewing the proposed regulations to read them together with the proposed Kenya Health Governance Framework to see whether they make sense. Furthermore, it will not be possible to fully personalize the Act and the regulations without the Kenya Health Data Governance Framework. The Cabinet Secretary should ensure that regulations are made with the necessary completeness that will		

		enable the users to start using the Act. There is no reason why the Cabinet Secretary should propose regulations contemplated under section 60 of the Act without proposing the Kenya Health Data Governance Framework Contemplated under section 21(1) of the Act. Finally, matters relating to Health Data Governance Framework are of great interest to the COG and county governments which would like to know whether they have been given any role in the framework		
HIM - 4	Civil Society Organisation	What liability stands and when will DHA avail the health data governance framework?	**Noted**	The response provided to the stakeholder that the draft document is available.
4(2)	KICTANet	Lack of clarity on enforcement	**Not Adopted**	The enforcement mechanism is

		mechanisms for compliance by health data controllers and processors. Recommendation: Introduce clear sanctions for non-compliance and define a compliance monitoring body to conduct regular audits of health data controllers and processors. Justification 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		already provided for in the Digital Health Act No. 15 of 2023

4(5)		Include provisions for controlled access to anonymised health data for public and research purposes.		
5	Smart Applications International Ltd	Part III - The Enterprise Service Bus: The regulations lack details on expectations, reliability, and accountability of the National Health Information highway/system. Without statutory guidelines, the government cannot hold service providers accountable for maintaining system efficiency. **Recommendation**: The regulations should define system reliability, availability, and accountability.	**Not Adopted**	The recommendations are administrative and operational in nature.
5(c)	Helium Health Limited	The provisions of Regulation 5 of the Draft Regulations outline the role of the Digital Health Agency ("the Agency")	**Not Adopted**	The recommendations are administrative and operational in nature.

		with respect to the management of health information in Kenya. We note that paragraph 5 (c) requires the Agency to ensure that health data controllers submit health data to the Agency in the applicable format. However, without a proper description as to what circumstances the Agency may mandate health data controllers to submit data, the risk of abuse exists.		
6	Cleophas Kisumu	Mitigation How do we mitigate breach of data?	**Noted**	The Regulations sufficiently addresses matters relating to breach of data
6(1)/9	KEMRI	How will we ensure that we safeguard the data so that we do not have the "Wanacry" situation where the government will be asked for ransom?	**Noted**	The Regulations sufficiently addresses matters relating to breach of data

6	Gitahi Ng'ang'a Living Goods	The regulations should also be consistent with general data collection systems that may collect patient data and how they're to be handled	**Noted**	The Kenya Health Data Governance provides for data protection and management across the entire data processing life cycle
6 (General comment)	Pauus Oriema Sanitation Officer	We need to have automatic generator for control of power to avoid theft of data	**Noted**	The recommendations are administrative and operational in nature.
HIM **6(1)**	Kennedy Radio Citizen	What measures are in place to hold the data & keep it successfully especially given the challenges of transferring data for NHIF	**Noted**	The Regulations provide for the methods of storing data, transfer of data and migration of data. This has further been enhanced in the health data governance framework
6	Fredrick Omolo MOH- Kisumu County Wealth	Does the regulation or Act cover for data protection eg. firewalls	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
6	APHRC	Can we ensure availability, quality,	**Noted**	The Regulations sufficiently

		integrity and security of health data?		address matters relating to data quality and security. This is further enhanced in the health data governance framework
7(2)	Mr. Koech	What happens when someone hacks the information and causes a threat to the person's data?	**Noted**	These Regulations adequately provide for data breach situations
7(2)(i)	KICTANet	The 24-hour notification period may be impractical for detecting complex breaches and implementing immediate containment measures. Recommendations a. Extend the notification period to 72 hours, aligning with international standards such as the EU GDPR 1 .	**Adopted**	Amend the notification form to reduce the information required to be submitted within 24 hrs. Amend regulation 4(2)(b) to include the words "within seventy two hours from the identification of the breach, provide a report to the Agency of the -"

		b. Include a preliminary notification option within 24 hours to report suspected breaches, with full details to follow within 72 hours. Justification 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.		

7	Bii – Mathari National Hospital	Data Protection on Private Sector ie KRA eTIMS cannot be offered on the basis of vendor certificates	**Noted**	This is provided for in the Digital Health (Use of E-health applications and technologies)
7	Helium Health Limited	There is a requirement that the health data controller of a digital health solution should, within forty-eight hours of the notification of an event of breach to the Agency, notify the Agency of the i) corrective measure taken; (ii) the mitigation action adopted; and (iii) the timelines for the rectification of the breach. The provided timeline of forty-eight hours may not be practical because in certain circumstances, it may not be possible to understand the scope/extent of the breach until much later. Thus, it may not be possible to provide the required information on breach	**Adopted**	Amend the notification form to reduce the information required to be submitted within 24 hrs. Amend regulation 4(2)(b) to include the words "within seventy two hours from the identification of the breach, provide a report to the Agency of the -"

		mitigation and rectification within that timeline. In the circumstance, we recommend that a longer timeline of between 10-15 working days should be applicable in this paragraph.		
7	APHRC	Regulation requires the Data health Controller or Processor to notify the DHA of a data breach, when the Data Protection Act, 2019 requires the same to be reported to the Data Commissioner. Add the requirement that the notification of breach made to DHA should be copied to the ODPC. The timelines for reporting breaches should, to the extent possible, align to those in Section 43 of the Data Protection Act.	**Adopted**	Amend the notification form to reduce the information required to be submitted within 24 hrs. Amend regulation 4(2)(b) to include the words "within seventy two hours from the identification of the breach, provide a report to the Agency of the -"
7	Fredrick Omolo	How is the regulation going to	**Noted**	These Regulations adequately

	MOH-Kisumu County Wealth	cooperate in the event there is a breach How do you charge the one who breaches the regulations Act		provide for data breach situations
7	Veronica Musyoka Nakuru	Need for more different and punitive sanctions for breaches No provision for compensation for victims of data breaches - may result in litigation	**Noted**	These Regulations adequately provide for data breach situations The Data Protection Act provides for incidences where compensation of the victim is deemed
7 (2)(i)	Tech Hive Advisory Africa	This regulation (7 (2)(a)(i)) states that in the event of a breach, the affected party must notify the Agency within twenty-four hours of becoming aware of the breach. If the health data controller of a digital health solution fails to comply with this regulation, they commit an offense and, upon conviction, may face penalties as outlined in the Digital Health Act.	**Adopted**	Amend the notification form to reduce the information required to be submitted within 24 hrs. Amend regulation 4(2)(b) to include the words "within seventy two hours from the identification of the breach, provide a report to the Agency of the -"

		However, there may be certain circumstances where this notification cannot be made within the twenty-four hour timeline. We suggest adding the following sub-paragraph: "Where the notification to the Agency is not made within 24 hours, the notification shall be made within 48 hours and shall be accompanied by an explanation of the delay." This addition aims to minimise the risk of unjustly revoking the certification of a digital health solution and imposing penalties.		
7(2)(a)(i)	Janice Njoroge M-TIBA	The form provided for the notification requires a lot of information that cannot be availed in 24 hrs Reconsider the 24 hrs	**Adopted**	Amend the notification form to reduce the information required to be submitted within 24 hrs.

				Amend regulation 4(2)(b) to include the words "within seventy two hours from the identification of the breach, provide a report to the Agency of the -"
7(2)(a)(i)	Carepay (M-Tiba)	Notification of Data breach Consider additional time for notification of breach. If notification of breach is to be done under Schedule 1. The agency risks either not receiving a completed form. In the alternative, introduce a simple form of notification of breach and the form under Schedule 1 to be submitted within 4hrs post breach. Compliance is important on notification.	**Adopted**	Amend the notification form to reduce the information required to be submitted within 24 hrs. Amend regulation 4(2)(b) to include the words "within seventy two hours from the identification of the breach, provide a report to the Agency of the -"

7(2)(a)(ii)	Carepay (M-Tiba)	The process of notification in corporate requires the DPO is notified with all the details of the breach then the DPO notifies the Agency/ODPC. Reporting to the Agency doesn't mean the ODPC shouldn't be notified	**Noted**	These Regulations adequately provide for data breach situations in line with the Data Protection Act
7(2)	Arnold Ndukuyu	Crisis response structure to deal with cybersecurity issues - The notification of data breaches to the DHA should be accompanied by the notification of data subjects	**Noted**	These Regulations adequately provide for data breach situations in line with the Data Protection Act
7(2)(a)(ii)	Mwirigi Kiula	The 24-hour notification period is unrealistic on account of: o Operational infeasibility. o The time required to conduct root cause analysis – retain the 72-hour	**Adopted**	Amend the notification form to reduce the information required to be submitted within 24 hrs. Amend regulation 4(2)(b) to

		notification as per the DPA.		include the words "within seventy two hours from the identification of the breach, provide a report to the Agency of the -"
7(4)	Helium Health Limited	Paragraph 7 (4) of the Draft Regulations state that the Agency shall revoke the certification of a health digital solution which fails to comply with the provisions of the Draft Regulations, while paragraph 7 (5) requires all healthcare providers and health facilities to use a digital health solution that has been certified by the Agency in line with the Digital Health (Use of e-Health Applications and Technologies) Regulations 2024, which is currently in development and paragraph 7 (6) outlines what constitutes a health data breach.	**Adopted**	Amend the Regulations to read "... the Agency **may** revoke the certification of a health digital solution..." The certification framework provides for the process of revocation Harmonise with the Certification Framework and the Digital Health (use of E-health Applications and Technologies) Regulations

		We suggest that rather than an absolute revocation of the certification upon any breach of the Draft Regulations, a more measured approach should be explored, with offending entities facing various penalties depending on severity, from fines to suspension of certification. Similarly, we recommend that prior to any such revocation, prior warning and ample time for rectification of wrongdoing should be given to any offending entity. Additionally, we recommend that in line with International best practices, the Draft Regulations should only resort to an imprisonment penalty, as outlined in Section 35 (2) of the Digital Health Act, 2023 referenced in paragraph 7 (3), in extreme circumstances.		

8	Helium Health Limited	We note that paragraph 8, which deals with the requirement on health data controllers to maintain an inventory of health data processors that they engage, is a repetition of paragraph 7.1. We recommend that one of the two clauses be deleted.	**Adopted**	Delete regulation 7(1) to avoid duplication
8	APHRC	Recommendation: Protection of data at rest through the provision of synthetic data to promote and ensure data sovereignty	**Not Adopted**	Data protection is adequately covered by data security measures such as encryption
9	Cephas Joseph	The regulations should include the provisions for annual systems and data protection audits by data controllers in alignment to the Data Protection Act .	**Not Adopted**	The provisions of these Regulations are aligned to the Data Protection Act
9	Fredville	How do we ensure data is fully protected?	**Noted**	The Regulations sufficiently address matters relating to data

				protection and security. This is further enhanced in the health data governance framework
9		How do we ensure that there is a proper firewall that won't be hacked?	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
9	Omondi	How do we ensure security of hardware?	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
HIM - Regulation 9		There is a need for enhanced guidance on data security measures in e-health technologies. Adherence to HIPAA-compliant safeguards ensures data integrity and	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework

		protects against unauthorised access. Require e-health developers to implement multi-factor authentication, secure APIs, and real-time monitoring systems		
HIM - 9		E-health platforms are frequent targets for cyberattacks. Implementing robust security measures, such as two-factor authentication (2FA) and secure APIs. Risk mitigation in alignment with standards like the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework.		
9	Prof. Bulimo KEMRI	The centralization of health data exposes Kenyans' health data to severe security and data breaches.	**Noted**	Regulation 9 sufficiently addresses matters relating to data protection and security of personal data.

		What mechanisms have been laid out to secure health data, including the devices to be used in processing health data?		
9/10	APHRC	Data protection and security issues should be greatly considered to avoid profiling.	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
9/10	George Khamisi	On the matter of fake doctors , how will the system sort out this and the penalties to unlicensed professionals trying to access data.	**Noted**	The Digital Health (Data Exchange) Regulations provides for the verification of health providers who will access the system through the health worker registry. The Digital Health Act further provides for penalties on unauthorised access to health data.

9	Peter K. Kakai Nakuru	How do we ensure Security of data?	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
10	APHRC	There's need for a perspective shift from data privacy to an expanded perspective of data solidarity that tracks the use of health data	**Not Adopted**	The concept of data solidarity is implied throughout the Regulations
10/9	Association of Private Universities	Potential data protection and security risks should be assessed and sufficiently addressed.	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
10	Gideon Kuria Ruaraka	How will I be assured that my health record in my phone is only made for me not any other person	**Noted**	These Regulations adequately provide for data breach situations in line with the Data Protection Act

10	Sylla Too Nakuru	Assurance of the safety and privacy of the data	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
10	Dorothy Matelong Ministry of Interior Turbo	Those who are vulnerable in terms of illiteracy levels, how safe is their data?	**Noted**	These Regulations adequately provide for data breach situations in line with the Data Protection Act
10	Eliud kiptoo	How sure are we that the information in the website is private?	**Noted**	The Regulations sufficiently address matters relating to data privacy, protection and security. This is further enhanced in the health data governance framework
10	Peter K. Kakai Nakuru	Paragraph 10 (2) of the Draft Regulations provides that no person or entity shall access health data unless authorized by the client or the health data controller to whom the data relates	**Not Adopted**	This is provided for in the Health Data Governance Framework

		to. We recommend that the Draft Regulations be revised to provide clarification about what form of health data this provision applies to. Ideally, the provision should only apply to non-anonymized health data as saying otherwise might stifle the advancement of the health-tech sector and healthcare in Kenya. This is because the processing of anonymized health data for clinical research and other purposes plays a significant role in enhancing the quality of healthcare provision all over the world.		
10	Eliud Kiptoo/ Eldoret.	How do we ensure health information is private? What are the privacy/data protection	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data

		measures for deaf persons considering the current lack of privacy for deaf persons on Health Facilities.		governance framework
10	Lydia Awuor Eldoret	Data should be discrete for patients privacy	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
10	Idriss Beiresa Kakamega	This looks good but for privacy to remain intact only the patient should be allowed to open using the thumb at any institution	**Noted**	This is provided for in regulation 9(1)(a)
10	KICTANet	The regulation states that the Agency will implement "privacy standards" but does not define what these standards entail or reference specific frameworks or guidelines. b) While the regulation restricts access	**Noted** **Noted**	(a)The privacy standards are integrated throughout the text of the Regulations. (b)The Data Protection Act sufficiently provides guidelines for

		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 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.	**Adopted** **Noted**	consent in provision of healthcare. Additionally, regulation 19 provides for the exemption in medical emergencies (c) 1 - Add "within 7 working days of the loss of access" (c) 2 - This is provided for in the Data Protection Act, 2019 (c) 3 -Means of notification will be determined administratively (d) The recommendations are administrative and operational in nature. Interchange regulation 10 (c) & (d) Amend regulation 10(3)(d) to

		• Additionally, there is no clarity on how this notification should be issued (e.g., email, SMS, registered post) 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 before transmission or validation by the Agency. • The regulation does not specify a	**Noted**	delete the word "permanently" (e) The recommendations are administrative and operational in nature. The Agency will determine the applicable format to be submitted.

		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 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. **Recommendations** Define clear and specific privacy		

		standards, aligning with the Data Protection Act, 2019. b) Establish guidelines for obtaining and managing client consent, including emergency exceptions. 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 enforcement mechanisms, including penalties for non-compliance		

		Justification a) Section 41 of the Data Protection Act, 2019 requires data controllers to implement appropriate technical and organizational 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 aected 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., 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 elective data steward, ensuring the regulations implementation is meaningful.		
10(2)	KEMRI Wellcome Trust	Health Information Management Regulations in totality- To what extent will this limit access to public data for improvement of health outcomes? This data ultimately belongs to the people and should be used to improve people's health	**Noted**	This is provided for in the Digital Health (Data Exchange) Regulation 21(2)
10(2)	APHRC	What about the privacy of patients who	**Noted**	The Regulations sufficiently address matters relating to data

		happen to be data subjects?		protection and security. This is further enhanced in the health data governance framework
10(2)	Kenya Private University of Kenya	How will we ensure privacy of the patients/ persons considering the fact that the data will be available to both private & public facilities including insurance?	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework
10 (2)	Nelly Rotich	Have you considered including the Data Protection Act or health data governance framework to regulations 4(1) and 10(2) considering the large volumes of data handled and transmitted through the system and with third parties?	**Noted**	The provisions of these Regulations are aligned to the Data Protection Act
10	John Njue	Data privacy and confidentiality concerns over data collection done by CHPs.	**Noted**	The Regulations sufficiently address matters relating to data protection and security. This is

				further enhanced in the health data governance framework
10		Deletion: Not provided under any govt. Platform. Protocol for deletion ie a patient can selectively delete some data	**Noted**	This is provided for in the Data Protection Act
10		Right to deletion (Is it provided)	**Noted**	This is provided for in the Data Protection Act
11(1)(b)	Tech Hive Advisory Africa	This regulation allows data retention for at least twenty years, with the possibility of indefinite storage. We recommend that the retention period for data be capped to a maximum of twenty years or a reasonable timeframe as may be specified by law. The addition of a maximum storage period reduces unnecessary exposure to risks associated with prolonged storage and	Not Adopted	Section 25 of the Digital Health Act provides for the retention period. The Regulations cannot amend the Act.

		upholds the principles of storage limitation and data minimisation.		
11(1)	UoN	Part II (1) leaves the agency with too much leeway for archiving data		Section 25 of the Digital Health Act provides for the retention period. The Regulations cannot amend the Act.
11(1)(b)	Tech Hive Advisory Africa	This regulation allows for the retention of data for a minimum of twenty years. However, this blanket retention period applies to all types of health data and may not take into account the varying needs of different categories of health data. For instance, clinical trial data, medical records, and administrative data may each have distinct retention requirements. We recommend classifying data based on its category and defining different	**Not Adopted**	Section 25 of the Digital Health Act provides for the retention period. The Regulations cannot amend the Act. The Health data governance framework provides for retention of data based on its categories.

		retention periods for various types of health data according to their purpose. For instance, medical records should be retained for up to 20 years when needed for continuity of patient care or legal reasons, while administrative health data can be kept for shorter periods.		
11	Tech Hive Advisory Africa	The regulation does not outline how the Agency should identify data that is nearing the end of its retention period. This lack of guidance could result in data being kept longer than necessary, thus increasing security risks. We recommend including a provision for using data lifecycle management tools to track data as it nears the end of its retention period.	**Not Adopted**	The recommendations are administrative and operational in nature.
11(6)		What are the identifiable data sets for de-identified health data in archiving	**Noted**	The recommendations are administrative and operational in

		maturity		nature.
11	Tech Hive Advisory Africa	The regulation(11(4)) framing may be misleading since it refers to "death subjects" instead of "data subjects," as intended by the provision. We recommend the following revision for clarity: "The data of the deceased data subject shall, on confirmation of the death of a data subject be archived after the lapse of a period of eight years from the date of confirmation of the death of that data subject"	**Adopted**	Amend the regulations to read " The data of the deceased data subject shall…"
11	Ministry of Health	An elaborate system. Thank you. However on the archival area is health data not permanent?	**Noted**	Archived data will still be available when needed.

12(1)	Rebecca Kiptui MOH	Data Migration - For the purposes of the regulation, are data controllers and processors the same?	**Noted**	No. The terms are defined in the Data Protection Act Cap. 411C
12(1)	Dr. Lishenga RUPHA	Define the mandatory datasets that should be migrated to the county health data banks under the migration of data regulations Data migration should be done by the agency not left to the facilities which lack capacity.	**Noted**	The recommendations are administrative and operational in nature.
12	Eric Angula Medtronic Labs	The country currently lacks the framework for data migration.	**Noted**	The recommendations are administrative and operational in nature.
12	KICTANet	a) The 24-month timeline for	**Not Adopted**	The concerns highlighted are

		transferring legacy data may be unrealistic for institutions, particularly small facilities or those using outdated 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. **Recommendations** a) Extend the timeline to 36 months to allow institutions adequate time to prepare and comply. Provide technical		administrative and operational and will be considered as the Agency implements its mandate

		and financial assistance for under-resourced facilities to ensure 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 **Justification** 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 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.		
12		The timeline for migrating legacy data	**Noted**	The recommendations are

		does not account for the technical and financial constraints faced by providers. Kindly provide standardized migration tools and financial incentives to assist healthcare providers in transitioning legacy data.		administrative and operational in nature.
12	Allan Mandera	What initiatives are there to reach out to remote areas regarding digital data migration?	**Not Adopted**	The concerns highlighted are administrative and operational will consider them as it implements their mandate
12	John Daktari online	Data migration beyond Kenya has not been covered	**Noted**	Regulation 17 adequately provides for data migration and ownership in the patient portal
12	Gitahi Ng'ang'a Living Goods	Consent should be included in data migration	**Not Adopted**	The Data Protection Act sufficiently provides guidelines for consent in provision of healthcare. Additionally, regulation 19

				provides for the exemption in medical emergencies
12	Eric Angula Medtronic Labs	The country currently lacks the framework for data migration	**Not Adopted**	The recommendations are administrative and operational in nature.
12(2)	Penda Health	Better define 'Migration of legacy data' under the above said regulations.	**Noted**	The recommendations are administrative and operational in nature.
12	Medtronic Labs	Please provide more clarity on data migration both to the National and County Data banks. What is the framework?	**Noted**	The recommendations are administrative and operational in nature.
HIM - 12	Rabal Dispensary	Are institutions managing health data using solutions to transfer this data to county data banks within 24 months of their operationalization?	**Noted**	The recommendations are administrative and operational in nature.

		Considering the work that goes into this process, the timeline is too short		
HIM - 12	Brian/ICT solutions Engineer.	What is the progress in establishing the county data banks?	**Noted**	The recommendations are administrative and operational in nature. It is provided for in section 26 of the Digital Health Act
13 (1) (b)	KEMRI Wellcome Trust	Who is a duly recognized working group? Doesn't this limit the constitutional requirement for transparency since data is de-identified?	**Adopted**	Amended to delete 13(1)(b)
HIM - 13	KEMRI WT	Data Sharing - data sharing should be made easier to support evidence generation for patient support and decision-making	**Noted**	The recommendations are administrative and operational in nature.
13	Noah	On the disclosure of health records to	**Noted**	Transfer of health data shall only

	Kiptoo/MTRH	NSSF for the calculations of the benefits for their clients? Does the data controller have the capacity to disclose the records?		happen as legally permitted
13	Ronald Kipkemboi Eldoret	Data is being shared, what are the privacy provisions for personal health status?	**Noted**	The Regulations sufficiently address matters relating to data privacy, protection and security. This is further enhanced in the health data governance framework
13	KEMRI WT	Data Sharing - data sharing should be made easier to support evidence generation for patient support and decision-making	**Not Adopted**	The concerns highlighted are administrative and operational will consider them as it implements their mandate
13	Philip Chule	How are you sure that our data will not be shared with unauthorized persons? Stringent data protection measures are necessary.	**Noted**	The Regulations sufficiently address matters relating to data privacy, protection and security. This is further enhanced in the health data governance framework

13	Augustine Choge KAPSERET	If the data is being shared, those accessing should be discrete to prevent leakage of a patient's information	**Noted**	The Regulations sufficiently address matters relating to data privacy, protection and security. This is further enhanced in the health data governance framework
13.	Noah Kemei MTRH	The disclosure of patient records to NSSF for the process of the validation of benefits for the clients who are retired on medical grounds. Does the data controller have the capacity to disclose to the concerned party?	**Noted**	Transfer of health data shall only happen as legally permitted
13		On the Data transfer what happens to the system sending the data?	**Noted**	The system is secure. The Digital Health (Data Exchange) Regulations provides for this.
14	Secretary General	How can the health status of a patient	**Noted**	The Regulations sufficiently

	Association of Public Health Officers Kenya	be safeguarded from sharing without their consent?		address matters relating to data privacy, protection and security. This is further enhanced in the health data governance framework
14	MTRH	The definition/threshold of consent should be consistent between the Health Act and the regulations. The definitions should be aligned to promote informed consent		The Data Protection Act sufficiently provides guidelines for consent in provision of healthcare. Additionally, regulation 19 provides for the exemption in medical emergencies
14	Sylla Too Nakuru	How can children access digital health data?	**Noted**	The children will access data through their guardians'/parents' consent in provision of healthcare. Where the parent/guardian is not available the provisions of the Health Act (section 9) will apply.
14	Zadoin/kisumu	How does the client access the data?	**Noted**	Through the patient portal as set out in regulation 20(2)(c) of the

				Digital Health (Data Exchange) Regulations.
14	Helium Health Limited	Paragraph 14 (4) of the Draft Regulations provides that any request for health data containing personally identifiable information shall be accompanied by the execution of a data sharing agreement between the requesting party and the health data controller. We note that no sample or template data sharing agreement is annexed to the Draft Regulations. In the absence of a template data sharing agreement, we recommend that a list of minimum requirements for data sharing agreements to qualify to accompany a health data request should be provided in the Draft Regulations.	**Noted**	The provisions of these Regulations are aligned to the Data Protection Act. Further, the data sharing is an administrative and operational issue and has been provided for in the Kenya Health Data Governance Framework

		Furthermore, for added protection on such sensitive personal data, we suggest that an additional requirement be added in paragraph 14 (4) for a data protection impact assessment be conducted by a party requesting such data.		
14	Caleb Rono MTRH	Disclosure of health records; body that requires disclosure of data for validity (Are clients involved in making the decisions)	Noted	Section 24(2) of the Digital Heal;th Act provides for instances when data can be disclosed to third parties
14	Tech Hive Advisory Africa	This regulation allows for requests to access data within the system containing personally identifiable information, provided the request is accompanied by a data-sharing agreement between the health data controller and the requester, along with the data subject's consent. However, the provision does not address other	**Noted**	The provisions of these Regulations are aligned to the Data Protection Act

		lawful bases for processing outlined in Section 45 of the Data Protection Act. In order to align the regulation with the existing legal framework, we recommend this regulation should incorporate other lawful bases for processing sensitive data, as outlined in Section 45 of the Data Protection Act.		
14	Joran Abieno Kisumu Central	How does the regulation make data accessible to the patient?	**Noted**	Through the patient portal as set out in regulation 20(2)(c) of the Digital Health (Data Exchange) Regulations.
14	NSDCC	Does it mean for us to access the data, we need to pay for it so as to comply?	**Noted**	This has been provided for in regulation 4(3) of the Digital Health (Data Exchange) Regulations
14	AFIDEP	Data availability and use for counties-	**Noted**	This has been provided for in regulation 4(3) of the Digital

		The regulations should promote data access and use especially to counties to support decision making		Health (Data Exchange) Regulations
14(5)	AKU	How assured are researchers of the completeness of the data they're requesting? Value for money, what is the risk of paying for data that is not in the system? The determination of fees should be on a case-to-case basis.	**Noted** **Not adopted**	The Digital Health Agency shall have measures to ensure all data in the system adheres to all data quality dimensions. Uniformity of fees is necessary for transparency and accountability.
14(5)	AKU	How will the regulations support the regulation of independent researchers?	**Not Adopted**	The regulation of researchers falls beyond the scope of the regulations.

				This is under the scope of NACOSTI
14(5)	Dennis Ngeny SHA Eldoret Office	Please properly vet the masters, PhD and independent researchers before giving them access.	**Noted**	The regulation of researchers falls beyond the scope of the regulations. This falls under the scope of NACOSTI
14(5)	Noah Kiptoo/ MTRH	When one is doing research on a challenge or an outbreak for the benefits of Kenyas; will you charge ?	**Noted**	Yes. Fees are necessary for the efficient running of the system
14(5)	Rev Nyaure	What consideration has been given for researchers seeking to solve a problem within the community/for the benefit of the country? Consider scrapping the fees for researchers researching public health relevant studies	**Not adopted**	Fees are necessary for the efficient running of the system

14(5)	Orade/kisumu	Can researchers access data for free?	**Not Adopted**	No. Fees are necessary for the efficient running of the system
15		Regulation 15(1) protects the right to correction of personal data, which is a duplication of Section 26(d) and (e), of the Data Protection Act, 2019. Cross-reference Section 26(d), (e) of the Data Protection Act,2019 to this regulation	**Noted**	the provisionsT of these Regulations are aligned to the Data Protection Act.
15	Omondi	How do we ensure quick correction of personal health data?	**Noted**	Regulation 15 sufficiently provides for the correction of personal health data
16	KICTANet	a) The regulation specifies that sensitive personal health data shall be used in de-identified form,but it does not define the standards for de-identification.	Noted	(a)-(c)The recommendations are administrative and operational in nature. (d) This has been provided for in the health data governance framework

		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 **Recommendations** a) Define clear de-identification standards aligned with international best practices, such as HIPAA Safe Harbor Guidelines or ISO/IEC 20889.		(e)The recommendations are administrative and operational in nature. (f) This has been provided for in Regulation 23(1)(d)

		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 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. **Justification** 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.		

		b) Global Standards such as GDPR - Article 89 emphasizes 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. 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.		
16	CUEA	Secondary use of health data: (Will a fee be charged for all researchers, including undergraduate) Recommendation: If a fee is charged, exemptions should be considered for students.	**Not Adopted**	Fees are necessary for the efficient running of the system
16(4)	Daniel Mwanga APHRC	Fees on data access- This limits research and innovation; undermining UHC.	**Not Adopted**	Fees are necessary for the efficient running of the system

16	Daniel Mtai	Clarification on the regulation of health data collected for research purposes	**Noted**	This has been provided for in the health data governance framework
17	KICTANet	a) (Reg 17 (1)) The regulation assumes all data subjects 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 experience managing access codes or	**Noted**	(a)The recommendations are administrative and operational in nature (b)This has been provided for in Regulation 9(2) (c)The Digital Health Agency is responsible for ensuring digital health literacy (d) The regulation has provided for prevention of unauthorized access sharing appropriately the responsibility between the Agency in Regulation 9(2) and the data subject.

		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. **Recommendations** a) Provide alternative access options for data subjects, such as access through healthcare facilities, public kiosks, or assisted access programs for underserved communities. b) Mandate the use of end-to-end		(e) The updating of records is under the guidance of the referring healthcare provider under Regulation 17(5) (f) The recommendations are administrative and operational in nature.

		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 securing Shared Health Records, with the Agency providing guidance on precautionary measures. e) Require healthcare providers to get 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 **Justification** a) Article 43 of the Constitution guarantees the right to health, which includes equitable access to health information. Addressing the 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 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.		
17(1)	Aga Khan University /BMI	How sure are we that we will get the data? Can we have a balance on monetizing data for the digital agency and the use of data?	**Noted**	This is provided for by the Digital Health Act and this Regulations
17	Daktari Online	Any clarification on patient data being shared outside Kenya	**Noted**	This is sufficiently provided for in section 46 of the Digital Health Act and Regulation 17

17	Zadoin	What happens to information being shared outside the country	**Noted**	This is sufficiently provided for in section 46 of the Digital Health Act and Regulation 17
17	NSDCC	What happens to data outside the country?	**Noted**	This is sufficiently provided for in section 46 of the Digital Health Act and Regulation 17
17	Ministry of Health	How about disabled people. Will they know about the digital health data. How will they be helped?	**Noted**	The Digital Health Agency is responsible for ensuring digital health literacy
20	Helium Health Limited	Similarly, reference to imprisonment in paragraph 20 for disclosure of personal health data for market research should be substituted for other forms of penalty. This is because penalties should be effective, proportionate and dissuasive; prison terms should be limited to serious violations, especially those that involve criminal activity.	**Noted**	The penalty provided for in the Digital Health Act is sufficient.

21		Sensitive personal data on health should at all times only be processed or shared with the express permission of the data subject An instant alert via SMS and/or email should be sent to the data subject when their sensitive personal data is processed. The OTP text message can be used to authorize the processing.	**Noted**	The Data Protection Act sufficiently provides guidelines for consent in provision of healthcare.
22	Kiptoo Kemei/ Eldoret MTRH.	Disclosure processes - How will the disclosure of health information be managed for legal processes e.g. production of records in Courts	**Noted**	Section 24 of the Digital Health Act provides for instances in which personal data can be shared with third parties.
22	Arawa Hospital - Prisca Okeyo	Data Confidentiality: Using OTP/ biometrics- Incase of emergency the information can be gotten through hospital authentification. How safe is the patient's data?	**Noted**	The Data Protection Act sufficiently provides guidelines for consent in provision of healthcare. Additionally, regulation 19 provides for the exemption in medical emergencies

22		Conflict of Powers: There are situations where the powers of the Agency and the Office of Data Protection Commissioner may overlap, particularly because sensitive personal data is also considered health data. We recommend that the regulations explicitly outline what is applicable in these cases to prevent confusion and provide clarity for health data controllers and processors.	**Not Adopted**	The provisions of these Regulations are aligned to the Data Protection Act
22	Likoni Catholic Hospital- Faith Mwende	Health Information Management- How secure is the patient's information where you find the guardian or principal are the ones to authenticate?	**Noted**	Section 24 of the Digital Health Act provides for instances in which personal data can be shared with third parties.
23(1)		Regulation 23(1)	**Not Adopted**	The provisions of these Regulations are aligned to the Data

		defines the nature of disputes that can be resolved by the Complaints Committee including: (b) unauthorized sharing, access and use of data; (d) access to data or denial of access to data. Remove Regulation 23(b) and (d) as part of the disputes under the Complaints Committee under the Regulation. These disputes fall within the jurisdiction of the Data Commissioner under Section 9(a) of the Data Protection Act,2019		Protection Act
23(1)	Council of Governors (COG)	The draft regulations provide for a Complaints handling mechanism and empower the Board to establish a	**Noted**	The recommendations are administrative and operational in nature.

		Complaints Committee. However, it is unclear how the Committee is appointed and whether it is an internal mechanism or if members are drawn externally. Given the sensitivity of the matters involved, it is crucial to shorten the timelines. Additionally, complaints should be received by the Agency and then referred to a Committee to ensure that the Agency retains responsibility for any decisions made by the Committee.		
23	National Gender and Equality	We appreciate the provision on lodging of complaints by aggrieved persons. We are however concerned that various special interest groups may not be aware that their data has been breached or shared/ accessed in an unauthorized way.	Not Adopted	The Digital Health Agency is responsible for ensuring digital health literacy

		One proposal would be for the agency to provide in the Regulations a provision on continuous sensitization of the beneficiaries on their rights to privacy data.		
23(2)(b)	National Gender and Equality	i. Proposed to amend Regulation 23(b) by substituting the phrase "through virtual complaints desk" with the following; b. Through electronic means including email, web posting or any other electronic means approved by the Agency from time to time. Ii.propose to insert additional sub Regulations as follows c. delivery to such other place as the Agency may, from time to time designate; d. By registered post to the designated postal address of the Commission;	**Adopted**	Amend to include "electronic or print means"

		e. Through a duly registered courier service.		
23(2)(a)	Mwirigi Kiula	Use of a designated officer would be a bit outdated in the era of 24/7, 365-day citizen support: o Level 1: Provide for 24/7, 365-day citizen experience/contact/support center. o Level 2: Respective departmental heads. o Level 3: Designated Officer. Integrate the citizen experience/contact/support center with a knowledge management system.	**Noted**	The designation is necessary for the purposes of accountability in complaints management
24	National Gender and Equality	a. Propose to amend Regulation 24 by inserting a new sub regulation (1) to	**Not Adopted**	Regulation 23 uses the word "person" which covers the

		replace the existing (1) as follows-; (1) Any person aggrieved by a matter may lodge a complaint with the Agency- (a) acting in their own interest; (b) acting on behalf of another person who cannot lodge in their own name including children, persons with various forms of disabilities, and older members of society; (c) acting as a member of, or in the interest of, a group or class of persons; (d) acting in the public interest; or (e) an association acting in the interest of one or more of its members, in		suggested classes of persons. The Regulations do not contain any fee in relation to filing of complaints.

		accordance with these Regulations b. Amend by renumbering the existing sub - regulations accordingly c. Amend further by inserting a new sub Regulation (5) as follows (5) The agency shall not charge any fees for the lodging of a complaint with it under these Regulations. d. Amend form 3 to include complaints lodged on behalf of a third party as per our proposals above		
24	Mwirigi Kiula	Apply data minimization and protection of subjects in the complaint form.	**Noted**	The Regulations as drafted is sufficient for purposes of ensuring fair handling of complaints
26	Orade/kisumu	Beyond the complaints committee, where do we go?	**Noted**	Regulation 26(6) provides for application of review to the Board

26	Nicholas Kiptoo	Composition of the complaints committee should be inclusive to ensure comprehensive representation	**Noted**	It is an administrative committee appointed by the Board
26	National Gender and Equality	Could you consider reducing the number of days from seven to three in 26 (1) and from thirty to ten in 26 (2) accordingly.	**Not Adopted**	The time provided is sufficient for fair administrative action
37	Occupational Therapy Council of Kenya	Are health care providers/professionals going to be certified by the agency? If Yes, will they be required to pay a separate fee from what the facility does?	**Noted**	No The Agency will collaborate with the regulators to ensure the health worker registry is updated for purposes of accessing the system.
37	Simon Mbai	Are community systems covered in the scope of certification and what considerations will be made for systems such as e-CHIS. (4(3)(a))	**Noted**	All systems are covered in the ecosystem

37	Steve Health X Africa	What happens to the current telemedicine-regulation structures under KMPDC?	**Noted**	The Digital Health Act is the primary law on matters relating to telemedicine and all other laws need to align to the standards set by the Act.
37	Smart Applications International Ltd	The requirement for certification of e-health applications and digital health technologies will stifle innovation and go against the government's agenda to grow the economy and create jobs. Small to medium-sized enterprises will be locked out of the industry. **Recommendation**: Delete the mandatory certification requirement or make certification voluntary.	**Not Adopted**	Certification is mandatory in the Digital Health Act. Certification requirements are necessary to ensure data security, protection and sovereignty.

37	Medtronic Labs	Will level 1 digital health solutions be certified as well? It is missing from the draft regulations	**Noted**	The regulations amended to include level 1 providers
37	Ministry of Health	E-health Application Will there be assurance that the application is not harmful?	**Noted**	Yes The certification framework will provide the assurance of the application.
37		The certification framework under Part III of the Regulations lacks explicit integration of Data Protection Impact Assessments (DPIAs) Include mandatory DPIAs before certifying digital health solutions. The DPIAs should be submitted to the ODPC in accordance with Section 31 of the Data Protection Act. (DPIAs mitigate risks to personal data and ensure compliance with Section 31	**Noted**	The provisions of these Regulations are aligned to the Data Protection Act.

		of the Data Protection Act).		
27	Rebecca Kiptui Ministry of Health	Will the agency look into infringements by digital health solution providers e.g. world coin?	**Noted**	Yes The Regulations sufficiently address matters relating to data protection and security. This is further enhanced in the health data governance framework These Regulations adequately provide for data breach situations in line with the Data Protection Act
37	Kamau Mwangi	Kindly consider involvement of the solution vendors as key stakeholders in the development and validation of the certification framework. If the vendor gets the solutions certified, I believe the facility that deploys the certified solution does not	**Not Adopted** **Noted**	Any document, guideline or policy to be prepared by the Digital Health Agency shall be developed in accordance with Article 10 of the Constitution on public participation. Only the digital health solutions will have to be certified

		require to do anything else. Please confirm that this is the case.		
37(2)(d)	KICTANet	The standards are referenced but not explicitly outlined, leaving room for ambiguity and inconsistent implementation Recommendations Publish the specific digital health standards (e.g., interoperability, data security) to provide clarity for digital health solution providers and ensure uniform compliance Justification Clearly defined standards streamline compliance and reduce ambiguities, ensuring alignment with Kenya's Health Data Governance Framework and	**Adopting**	The regulations amended as recommended

		promoting transparency in certification requirements		
37	ians for Human	Certification framework lacks transparency. We suggest publishing standards, timelines, and compliance criteria before enforcement.	**Adopted**	The regulations amended as recommended
37	Zadoin Kisumu	How does DHA integrate with counties on the certification framework?	**Noted**	As the owners and users of the county facilities, they have the responsibility of ensuring the solutions used in their facilities are certified.
37		How are the different levels of digital health of different counties being taken into consideration? Certification should be made easier for	**Noted**	The Agency has the responsibility to provide technical support and capacity building to counties based on their unique needs.

		remote areas/ counties		
37	Joseph	What is the linkage between the National system and individual systems; Will facilities be using two systems? eg. How will elephant be linked with the national system?	**Noted**	All the systems will be certified as provided for in the regulations. Any other certified system that is not owned by the government will be onboarded to the Health Information Exchange at a fee.
37	Smart Applications International Ltd	The regulations focus on certification costs rather than establishing accountability for the Digital Health Agency. **Recommendation**: The regulations should prioritize value addition and quality assurance rather than being an administrative and financial burden. Consider making certification	**Not Adopted**	The certification process provides for security of digital health systems, ensures compliance with the set standards on interoperability, reporting and data protection and confidentiality. The fee is utilized for the maintenance of the system.

		voluntary or reducing fees.		
38	Smart Applications International Ltd	Part III - Certification: The value addition of certification is unclear. The process should be governed by defined quality checks and accredited auditors with expertise in digital health. Certification should not be a mere revenue collection tool. **Recommendation**: The regulations should specify the certification criteria and qualifications of officers.	**Not Adopted**	The certification process is defined in the regulations. The recommendations are administrative and operational in nature.
39	Eric Angula Medtronic Labs	Certification process - the process is unclear	**Noted**	The certification process is defined in the regulations and the Agency will communicate regularly to support compliance.

39	John Daktari online	The certification process is unclear	**Noted**	The certification process is defined in the regulations and the Digital Health Agency will communicate regularly to support compliance.
39	Teresa Awuor Dolts- Mombasa	How is the flow of certification of the digital systems in the counties? Will counties also have the Digital Health Agency to assist through the process?	**Noted**	Certification is a function of the Digital Health Agency however the Agency has the responsibility to provide technical support and capacity building to counties based on their unique needs.
39	Alex Wanyama	How will the agency support private facilities to understand and comply with the certification process? Including technical assistance and capacity building for the DH Standards and certification.	**Noted**	The Digital Health Agency will provide technical support to private facilities

39		The certification process may disadvantage local innovators due to stringent requirements that favor well-established vendors.	**Noted**	The certification process id to ensure the set standards are complied with and the fees are spread across different levels.
39	KICTANet	The regulation mandates certification but does not consider smaller healthcare providers that may lack resources for certification fees or technical capacity. Recommendation Introduce fee waivers or subsidies for resource-constrained providers, especially in underserved regions, to ensure equitable access to digital health certification. Justification	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system. Further, the fees are already rationalised and are spread across different levels.

		Article 43 of the Constitution guarantees the right to health. Ensuring all providers, including small facilities, can comply promotes equitable healthcare delivery. - Kenyas Vision 2030 advocates for inclusivity in healthcare innovation		
39	Dr. Fiona Asonga Technology Service Providers Association of Kenya	Developers are being charged by the Communications Authority of Kenya whilst these regulations are proposing to charge the same space.	**Noted**	
39(3)(a)	Tech Hive Advisory Africa	These Regulations state that digital health providers are required to complete a self-attestation and submit a self-attesting report.	**Noted**	The Certification framework provides for the contents of the self attestation report.

		However, the regulations do not specify what content should be included in this self-attestation report. As a result, digital health service providers may be unclear about the expectations of the Agency in this regard. Additionally, regulation 8(3)(i) mandates a Cybersecurity Assessment Report. However, the lack of a standard for this report may hinder the evaluation of the effectiveness of cybersecurity measures across different digital health solution providers and hinder effective risk management. We recommend adding an additional sub-paragraph under this regulation to address this issue.		

		Alternatively, the Certification Framework, should specify the details to be included in the self-attestation report and the cybersecurity standards required for the assessment report.		
39(2)	KICTANet	Self-attestation may lead to insufficient scrutiny of digital health solutions, increasing risks of non-compliance or data breaches. **Recommendation**: Mandate independent third-party audits or verification of critical elements (e.g., cybersecurity) to complement self-attestation and enhance credibility. **Justification**: a) Third-party audits are widely	**Not Adopted**	The recommendations are administrative and operational in nature. Self attestation is cost effective, it ensures compliance and allows freedom to the innovator to improve their solution

		recognized for ensuring rigorous evaluation of compliance and security standards. b) Strengthening the evaluation process reduces risks of vulnerabilities in certified solutions		
39(3)(f)	Kamau Mwangi	Does the vendor require to register with ODPC as a data controller/Data processor, taking into consideration that the vendor is just providing a tool (the solution) to the health facility that will use it to process personal data? The facility should therefore, being the data controller, be the only one required to register with ODPC, rather than the vendor	**Noted**	Any vendor who is developing a system that will handle sensitive personal data should comply with the Data Protection Act.

41(6)		Where the application for verification is rejected, following payment of the certification fees, what support will be given to the digital health solution provider in such a scenario?	**Noted**	The recommendations are administrative and operational in nature.
41	Smart Applications International Ltd	Part IV - Certification Process: Lack of clear guidelines on certification timelines and processes may create inefficiencies. Without a defined charter, the Digital Health Agency will not be held accountable, potentially causing delays that hinder innovation and business operations. **Recommendation**: The regulations should specify fixed timelines for processing applications.	**Not Adopted**	Regulation 10(1) sufficiently provides for this.

41(4)	Tech Hive Advisory Africa	The regulation permits a digital health provider to submit further evidence of compliance after receiving a testing report. However, it does not specify a timeline for submitting this further evidence to the Agency. This lack of a timeline could result in extended periods of non-compliance, potentially jeopardising the validity of the initial evaluation conducted by the Agency. We recommend including a reasonable timeline for submitting further evidence to the Agency to preserve the integrity of the initial evaluation conducted.	**Not Adopted**	The recommendations are administrative and operational in nature.

41(4)	Tech Hive Advisory Africa	• The provision does not provide a timeframe within which the Agency will notify the digital health service provider of its decision after assessing the further evidence submitted by the service provider. We recommend including a determined timeline for notifying the service provider after assessing the further evidence to maintain structure in the Agency's activities.	**Not Adopted**	The recommendations are administrative and operational in nature.
41(7)	Tech Hive Advisory Africa	This regulation allows a digital service provider to apply for a review of the Agency's decision in relation to the Certification Process. However, it does not provide a timeframe within which the service	**Adopted**	The Regulations amended to include a timeline of thirty days for purposes of compliance with the Fair Administrative Actions Act.

		provider may initiate the review of the Agency's decision. We recommend including a determined timeline for the service provider to initiate a review of the Agency's decision in order to help conclude the testing and evaluation process effectively		
41(2)	KICTANet	While the five-day timeline is reasonable, the regulation does not specify recourse mechanisms for providers dissatisfied with test results **Recommendation**: Provide a formal appeals process for providers to contest unfavorable outcomes, with clear timelines for review and resolution. **Justification**: (Article 47 of the	**Adopted**	The Regulations amended to include a timeline of thirty days for purposes of compliance with the Fair Administrative Actions Act.

		Constitution): Establishing an appeals process ensures transparency and accountability, giving providers confidence in the certification process.		
41(1)	CDC	Consider adding the timeline for testing the system in the regulations and not only in the certification framework	**Not Adopted**	Testing is dependent on factors which include; the type of solution and expertise required
41	Nzisa Liku CDC	The timeline for testing in the certification process is missing. This should be defined in the regulations The inclusion of the timelines is positive and they enable the creation of an enabling environment	**Not Adopted**	Testing is dependent on factors which include; the type of solution and expertise required
41	Smart Applications International Ltd	Part IV - Certification Process: Lack of clear guidelines on certification	**Not Adopted**	Testing is dependent on several factors which include; the type of

		timelines and processes may create inefficiencies. Without a defined charter, the Digital Health Agency will not be held accountable, potentially causing delays that hinder innovation and business operations. **Recommendation**: The regulations should specify fixed timelines for processing applications.		solution and expertise required The timelines for testing are administrative and operational in nature
41	Tony Nairobi	The certification process is too long.	**Noted**	Certification is mandatory in the Digital Health Act. The certification process is necessary to ensure data security, protection and sovereignty.
41	Physicians for Human Rights	There is no clear timeline for application processing. We therefore suggest a maximum	**Not Adopted**	Testing is dependent on several factors which include; the type of solution and expertise required

		processing time of 30-45 days.		The timelines for testing are administrative and operational in nature
42	Physicians for Human Rights	Certification validity of only two years is burdensome. We suggest extending it to 4-5 years.	**Not Adopted**	Technology is dynamic and comes with various changes in the sector. These changes happen within a short time and hence a longer period would endanger the system. Further, certification is mandatory in the Digital Health Act.
42	Nzisa Liku CDC	Period of certification - the rationale for the 1 year is unclear.	**Noted**	Technology is dynamic and comes with various changes in the sector. These changes happen within a short time and hence a longer period would endanger the system. Further, certification is mandatory in the Digital Health Act.

42	Physicians for Human Rights	There is no provision for continued operation during re-certification. We suggest allowing continued operation if an application is submitted before expiry.	**Not Adopted**	Just like any other certification, the application for recertification should be done before the end of the validity period of the initial certificate. Refer to the certification framework
43(b)	Nekesa Were Medic	Since certification is annual, the ad hoc audits are an inefficient use of resources and may serve to frustrate developers.	**Noted**	The certification process is necessary to ensure data security, protection and sovereignty.
43(b)	Tech Hive Advisory Africa	The regulation permits the Agency to conduct an ad hoc audit, which may include on-site visits to the digital service health provider. However, it does not require the Agency to notify the provider before initiating the ad hoc audit. This lack of notification may not allow	**Not Adopted**	The Ad Hoc audits are important for purposes of detecting and preventing fraud, ensure compliance and strengthen internal controls, that is why they are ad hoc in nature. .

		the service provider sufficient time to prepare the necessary evidence to be requested by the Agency. Furthermore, the regulation fails to include provisions for protecting any information shared during the ad hoc audit. We recommend that the regulation be redrafted as follows: "(c) where the Agency undertakes to conduct an ad hoc audit, the Agency shall notify the digital service health provider of its intention to conduct such audit at least ve (5) days before the aud it is conducted. (d) all information disclosed during the audit process shall be treated as condential and shall be used solely for assessing the digital		

		health service provider's compliance with the Certication Framework."		
43(b)		How will ad hocs audits be done? Will the DHA be outsourcing this function?	**Noted**	This is a DHA operational function.
43(b)		Why the need for the provision of ad hoc audits? Is this proper use of already limited resources? Why not just schedule the audit?	**Noted**	The Ad Hoc audits are important for purposes of detecting and preventing fraud, ensure compliance and strengthen internal controls, that is why they are ad hoc in nature.
43		I recommend that DHA plays a much more supportive role as opposed to having a gatekeeper/watchdog. Please consider adding support function such as assisting managers to meet the regulations and remain compliant	**Noted**	The Digital Health Act mandates the roles of the Agency which includes the issues raised.
43	John	Support supervision of systems beyond certification	**Noted**	The proposed function falls within the ambit of the functions espoused

	Daktari online			in the Digital Health Act
43(2)	KICTANet	A six-month compliance window may be too short for certain health data controllers and solution providers, particularly in resource-limited settings. **Recommendation**: 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 programs to facilitate compliance **Justification**: Realistic timelines are essential for ensuring compliance without disrupting service delivery, particularly in underserved areas. Article 47 of the Constitution	**Adopted**	The regulation is to be amended to extend the compliance period to twelve months

		guarantees fair administrative action, requiring the Agency to consider the operational realities of health data controllers. KICTANets advocacy for phased implementation of digital policies supports this approach.		
45	Helium Health Limited	Regulation 45 of the Draft Regulations outline the circumstances under which a digital health solution certification may be revoked, with no provision for a stepped penal process. We propose that in order to ensure justice is properly dispensed, offending parties are given sufficient opportunity to present a defence and for a more measured approach such as prior warning and ample time for rectification of wrongdoing be given to	**Not Adopted**	The conditions given for revocation are substantive and may have grave impact on the data subjects and health data.

		offenders before revocation of certification.		
45	Rebecca- MOH	E- health application- will there be assurance the application registration is not harmful	**Noted**	The certification framework provides for this
45	Office of the Attorney General	45 – Revocation of certification.	**Adopted**	Amend to cross-reference with the certification framework (review process)
45(b)	KICTANet	The regulation mandates revocation but does not consider whether breaches were caused by negligence or unavoidable circumstances (e.g., advanced cyberattacks). **Recommendation:** Allow the Agency to assess the root cause of the breach before revoking certification. Introduce corrective measures for non-negligent breaches to support recovery.	**Not Adopted**	The conditions given for revocation are substantive and may have grave impact on the data subjects and health data.

		Justification: 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.		
45(b)	Tech Hive Advisory Africa	Regulation 45(b) states that a certification can be revoked if the service provider suffers a major security breach. This provision appears to be vague, as a major breach may occur due to different reasons, some of which may be beyond the control of the digital health service provider.	**Not Adopted**	The recommendations are administrative and operational in nature.

		It may not be justified to revoke the licence unless investigation reveals that the controller failed to put adequate security measures in place. Furthermore, grounds for revocation should also include cases where the digital health service provider has misrepresented any information provided during the certification process or during an audit. We recommend that, in the event of a breach, the initial action should be to suspend the license until an investigation determines whether the breach was due to the negligence of the service provider. Where the investigation reveals that the		

		digital health service provider failed to take appropriate remedial actions following the security breach or failed to notify the Office of the Data Protection Commissioner (ODPC) as required by the Data Protection Act, the certification may be revoked. This approach ensures that providers are held accountable for addressing breaches while also acknowledging that no system is completely foolproof. "We recommend that the following draft be included: "(b) where a major system security breach has occurred, provided that an investigation into the breach reveals that it was occasioned by the negligence of the controller. (c) where, after a major security breach, and the digital health service provider		

		fails to take necessary remedial action and/or fails to notify the Office of the Data Protection Commissioner of the breach in line with the provisions of the Data Protection Act. (d) where the digital health service provider intentionally misrepresents any information provided during the application for certification or during an audit conducted by the Agency."		
45	Helium Health Limited	The Draft Regulations provides that a digital health solution provider whose application for certification as a digital health solution provider is denied shall cease to provide the digital health solution from the date of the rejection of the application. However, the Draft Regulations do not provide any remedial option for such a	**Adopted**	The regulations amended to provide a thirty day timeline for appeal after rejection of the application

		digital health solution provider, to ensure checks and balances. We recommend that this section of the Draft Regulations be revised to provide for a time-limited opportunity to appeal an initial decision of the Board on certification, including an option to present revised documentation.		
45	Abdullahi	The implementation of the certification process should allow for the continuation of services as facilities work to comply and get certified	**Adopted**	The regulation is to be amended to extend the compliance period to twelve months
45	Abdullahi	Healthcare providers already have existing systems; consider reviewing the 6 months stipulation.	**Adopted**	The regulation is to be amended to extend the compliance period to twelve months
45(2)	KICTANet	Six months may be insufficient for certain providers, especially those using legacy systems requiring	**Adopted**	The regulation is to be amended to extend the compliance period to twelve months

		significant upgrades to meet certification standards. **Recommendation**: 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. **Justification** 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.		
45(2)	Alex Wanyama	Consider an extension to the certification timelines provided in the regulations in consideration of rural facilities that may face logistical challenges.	**Adopted**	The regulation is to be amended to extend the compliance period to twelve months
45(3)	KICTANet	The regulation does not provide a grace period for providers to resolve non-compliance issues before ceasing operations, potentially disrupting critical services. **Recommendation**: Introduce a 30-day grace period to allow providers to address non-compliance issues while maintaining limited operations under supervision.	**Adopted**	The regulation is to be amended to extend the compliance period to twelve months

		Justification: Abrupt cessation may disrupt essential healthcare services. A grace period ensures patient care continuity while compliance is addressed		
Second Schedule	Alex wanyama	The certification fees are too high. Are there exceptions to the fees?	**Noted**	No The fees are necessary for the operationalization and maintenance of the system. Further, the fees are already rationalised and are spread across different levels.
Second Schedule		High certification fees, such as the KES. 250,000 to be paid by Telemedicine vendors and KES 500,000 to be paid for Testing of the PoC, Hospital-wide HMIS, etc may discourage small enterprises and	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the system. Further, the fees are already rationalised and are spread across

		innovators from participating in the digital health ecosystem. We propose that a survey be conducted to understand the economic capacity of stakeholders and that the certification fees to be paid by startups and innovators should be reduced in order to stimulate local innovation and growth in Kenya's digital health sector.		different levels.
Second Schedule	Kamau Mwangi	These fees are too exorbitant and should be should be seriously be reconsidered if the government is serious about supporting and encouraging the digital transformation of healthcare in the country, otherwise this blocking the very thing the government is purporting to support.; 1. Application fees – KES. 20,000-/	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system. Further, the fees are already rationalised and are spread across

		This should be the only fees and scrap all the other fees. DHA is not a profit making entity, but a regulatory body and should not be viewed as an entity to generate revenue} 2. Testing of the PoC, Hospital-wide HMIS – KES. 500,000 *{ What is the justification for this that is different from the application fees?Consider scraping it}* 3. Mhealth solution – KES. 50,000 *{ What is the justification for this that is different from the application fees?Consider scraping it}* 4. Telemedicine – KES. 250,000 *{ What is the justification for this that is different from the application fees? Consider scraping it}*		different levels.

		. Innovators, Students and innovator system testing up to a maximum of KES.10,000 *{ Why should one be charged for coming up with innovation and especially students? We should be providing subsidies and support rather than penalizing innovators. Once the innovation is completed and ready to be deployed, the innovator can at that point pay the certification application fees}* These charges need to be seriously thought through and reconsidered, otherwise we risk stifling healthcare digital transformation that is really gaining traction in the continent with Kenya leading the track.		
Second Schedule	Joran Abieno	The fee on certification are Extremely	**Not Adopted**	The fees are necessary for the

		high should be reduced downwards: • Application fee from 20,000 to 5,000 • Testing of POC HMIS from 500,000 to 100,000 • M-Health solution 50,000 to 10,000 Telemedicine from 250,00 to 100,000		operationalization and maintenance of the system. Further, the fees are already rationalised and are spread across different levels.
Second Schedule	Jilo B Said Isiolo	Innovator System testing fees should be scrapped	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system.
Second Schedule	Collins Omollo	The application fees need to be reduced to 10,000, tests of the PoC Hospital wide HMIS reduced to 50,000, Mhealth solution reduced to 20,000 and telemedicine reduced to 50,000	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the

				cost of setting up and running of the system.
Second Schedule	Mary Mwami / AFIDEP	Certification fees for telemedicine digital health solution vendors (KES 250,000) – The certification fee should be reconsidered. The amount can be revised based on the level of care, with special consideration for providers improving access in rural and underserved areas.	**Noted**	The fees are necessary for the operationalization and maintenance of the system. Further, the fees are already rationalised and are spread across different levels.
Second Schedule	Smart Applications International Ltd	All e-health applications and digital health technologies require certification, restricting healthcare providers to certified solutions. This reduces competition and increases costs. Healthcare providers will have fewer choices and may pay higher fees due to certification costs.	**Noted**	Certification is mandatory in the Digital Health Act. The certification process is necessary to ensure data security, protection and sovereignty.

Second Schedule	National Spinal Injury Referral Hospital	If the HMIS is in-house and developed by the health facility do the certification fees still apply separately?	**Noted**	Yes Certification is mandatory in the Digital Health Act for all systems that handle patient data.
Second Schedule	NSDCC	For an institution to comply and be certified to have complied, must we pay the amount that has been indicated there?	**Noted**	Yes Certification is mandatory in the Digital Health Act for all systems that handle patient data. Certification is important as it considers the following factors necessary for the digital health ecosystem: a. Functionality b. Security c. Reporting Interoperability

Second Schedule	AFIDEP	The telemedicine paid for certification is too high and will be a drawback to the efficiency resulting from the technology advancement (ie the KSh. 250,000)	**Noted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system.
Second Schedule		The high cost of certification and compliance may deter smaller facilities and developers.	**Noted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system. Further, the fees are already rationalised and are spread across different levels.
Second Schedule	Dorcas Gitonga	For NGOs or non-profits developing health information systems for use by	**Noted**	The recommendations are administrative and operational in

		MOH and similar stakeholders, where do they fall in terms of obligations and fees?		nature.
Second Schedule	Physicians for Human Rights	Certification and compliance costs are high, especially for humanitarian organizations. Suggests a subsidized fee structure or waivers.	**Noted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system. Further, the fees are already rationalised and are spread across different levels.
Second Schedule	Simon Mbai	The cost of certification should be pushed to the end user, not the developer (Second schedule)	**Noted**	The regulations as drafted are sufficient
Second Schedule	Dr. Lishenga	What informed the fees for certification? The proposed fees are	**Not Adopted**	A desk review was done in comparison to other similar

	RUPHA	prohibitive to innovation in the health sector Reduce the application fee to KES. 10,000 Half the proposed fees during rollout to promote adoption.		processes. The fees are already rationalised and are spread across different levels.
Second Schedule	Dr. Lishenga RUPHA	Have a graduated model to the fees to have the reduction of re-certification fees pending on the enhancements made to the system within the certification period.	**Not Adopted**	The Agency will use resources in effort to test and verify compliance during the certification process
Second Schedule	Fran Africa Alliance for Pop Research	The fees are prohibitive and may stifle innovation.	**Noted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system.

				Further, the fees are already rationalised and are spread across different levels.
Second Schedule	Collins Omollo	Certification fees to be paid by the digital health solution vendors are too high. A waiver needs to be introduced for public health facilities that use open source digital solutions like KenyaEMR.	**Not Adopted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system. Further, the fees are already rationalised and are spread across different levels.
Second Schedule	MTRH	Certification fees for telemedicine of ksh. 250,000 is high considering that MTRH and other level 6 Hospitals are not profit-making. This fee is to be considered.	**Noted**	For HMISs with telemedicine capabilities will be charged once under POC HMIS. The telemedicine fees apply for stand alone systems

Second Schedule	Dr. Fiona Asonga Technology Service Providers Association of Kenya	The fees are punitive and inhibitive to innovation	**Noted**	The fees are necessary for the operationalization and maintenance of the systems. The fees are commensurate to the cost of setting up and running of the system. Further, the fees are already rationalised and are spread across different levels.
Second Schedule	KICTANet	High certification fees (KES 500,000 for hospital-wide systems) may exclude innovators, smaller vendors, and community-based organizations. **Recommendation** Introduce a sliding scale of certification fees based on the size and revenue of	**Noted**	The fees are commensurate to the cost of setting up and running of the system and are rationalised and spread across different levels.

		the applicant organization. Provide reduced fees or fee waivers for students, innovators, and startups to encourage participation and innovation in the sector **Justification** 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-health sector.		

General comment HIM	Association of Private Universities	What mechanisms have been laid out to improve data quality and completeness in health facilities?	**Noted**	The regulations provide measures to ensure all data in the system adheres to all data quality dimensions including data quality audits
General Comment	Tech Hive Advisory Africa	Pro-innovation - The goal of the Regulation should be to foster digital health innovations and solutions while upholding the standards set by the Agency rather than stifling innovation. Additionally, the Agency should consider establishing a feedback loop with providers to address any issues that may hinder their compliance with the Regulation, in addition to the existing complaints committee.	**Noted**	Section 3(c) the Digital Health Act provides for innovation by ensuring security of sensitive personal data.
General Comment	Tech Hive Advisory Africa	Regulatory sandbox - The Regulation may establish a regulatory sandbox, creating a controlled and supportive	**Noted**	There is a plan to have innovator sandboxes to encourage innovation.

		environment for innovative providers to test their solutions under the supervision of the Agency and the Cabinet Secretary or the County Executive Committee. This sandbox is essential to assist digital health providers in balancing innovation with compliance.		However, the recommendations are administrative and operational in nature.