Position Paper on
Data Privacy Regulations for
Digital Health Tools

INTRODUCTION

The adoption of digital health tools such as mobile health apps, wearable devices, and telemedicine platforms is rapidly increasing in Kenya. These technologies have the potential to expand access to healthcare, improve quality of care, and reduce costs. However, they also raise valid concerns around privacy and security of sensitive health data.

2

As an industry association representing healthcare providers, insurers, and technology companies, the Kenya Healthcare Federation recognizes the need for appropriate data regulations that balance innovation and privacy. This position paper outlines our perspectives on what privacy legislation for digital health should entail in the Kenyan context.

PRIVACY PRINCIPLES FOR DIGITAL HEALTH

The following core principles should guide privacy regulations for digital health tools:

1. **Transparency and Consent**: Healthcare users should have clear information on what data is collected, how it is used, with whom it is shared, and options to consent or deny consent.

2. **Data Minimization**: Only personal health data that is essential for the declared purpose should be collected. Data retention should also be minimized.

3. **Access and Correction**: Users should be able to access their health data and correct any inaccuracies. Portability between apps should also be enabled.

4. **Security**: Encryption, access controls, and audits, breach notification should safeguard unauthorized access.

5. **Accountability**: Policies, consent documents, and privacy notices should clearly lay out responsibilities around the use of data. Violations should carry penalties.

KEY RECOMMENDATIONS

1. Regulations developed should preserve privacy, ensure data subjects have control over their data, and at the same time not limit innovation.

2. Provide adequate grace period when new regulations and guidelines are published and provide forums to engage and give feedback on the success and challenges faced during implementation.

3. Implement a process that involves all stakeholders in the cycle of policy, regulation, and guidelines. This will increase ownership with the different stakeholders and improve feedback from policy, regulation, and guidelines review and implementation.

4. Establish codes of conduct for digital health companies to operationalize responsible data use and conduct that aligns with the digital health superhighway.

5. Strengthen the capacity of data regulators to provide oversight, and address grievances around violations.

6. Create a healthcare sector working committee to consult on privacy guidelines for specialized needs.

7. Support healthcare providers on best practices for managing patient health information, consent procedures, and building secure IT systems.

CONCLUSION

Appropriate data privacy regulation is key to building trust in digital health tools among patients and providers. The Kenya Healthcare Federation and its members remain committed to enabling the development of technologies that expand healthcare access while also protecting the confidentiality of health information for citizens. We aim to engage all stakeholders - government, private sector, civil society, and tech industry - to shape policy principles that balance both innovation and privacy.

5
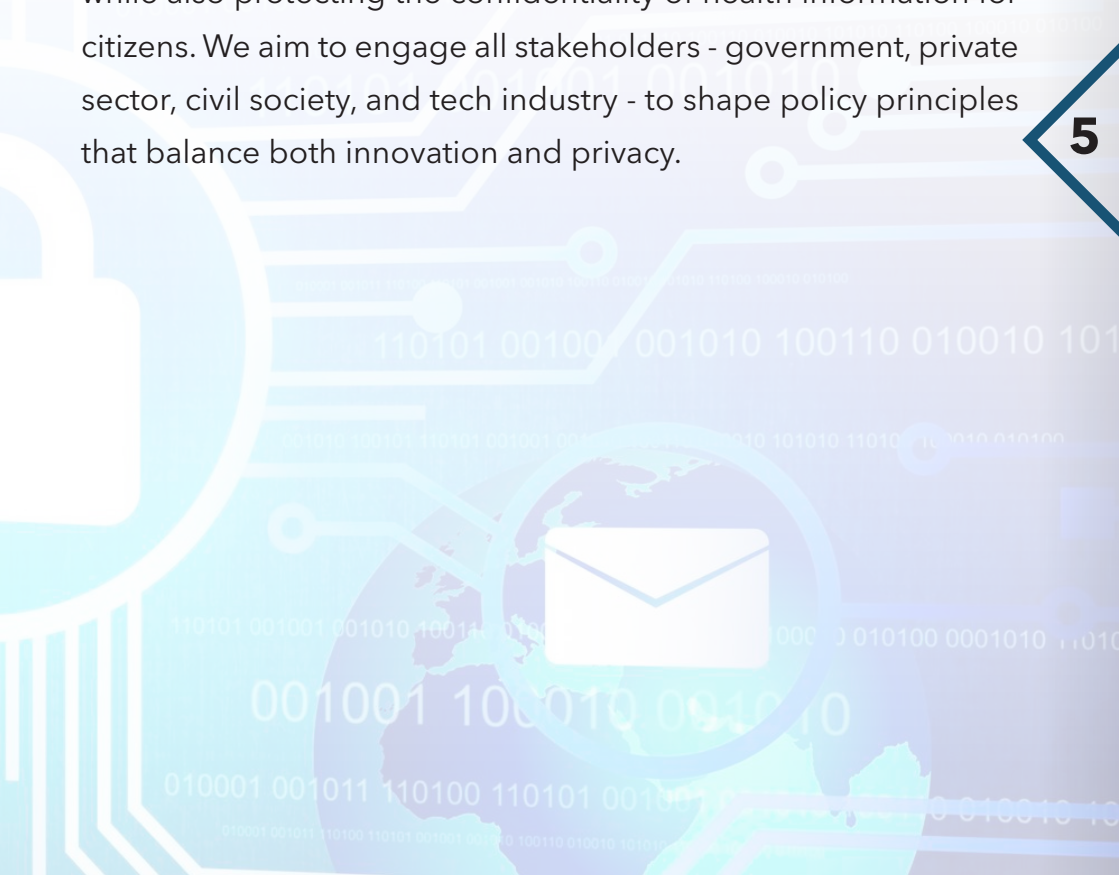
Kenya Healthcare Federation

Position Paper on
Data Privacy Regulations for
Digital Health Tools

Kenya Healthcare
Federation

The Health Sector Board of KEPSA

KHF Digital Health Committee