December 2016

Regulating mHealth in South Africa

What is mHealth?

The delivery of health-related services via information and communications technologies (ICT) is referred to as eHealth. The South African mHealth strategy (2015–2019) defines mobile health—or mHealth—as a subset of eHealth, which involves the use of mobile computing, medical sensors, or other communication technology in the delivery of health services. mHealth has the potential to empower clients with information to inform their healthcare decisions and link them to health services.

Why regulate mHealth?

Many types of mHealth projects and applications can compromise client privacy or confidentiality. For example, an application may store sensitive client data without any controls on who is allowed to access it. Or clients may be negatively affected by incorrect medical advice from information applications, or misdiagnosed through remote conversations with health providers. To avoid these and other negative scenarios, it is essential that regulations to protect clients be in place and enforced.

Aside from the client perspective—in which privacy, confidentiality, and security are typically the chief concerns—healthcare providers also should have protections, beginning with an understanding of what mHealth applications and services are allowed. Similarly, mHealth application providers, service providers, mobile network operators, and wireless application service providers need to understand the regulatory environment, in order to avoid legal challenges and incorrect practices.

Policy and legislation for health and for ICTs converge to govern eHealth. These two fields each have regulators for specific aspects. For example, the health sector often has a regulator for health providers or medicines, and the ICT sector often has a regulator for telecommunication companies. Because mHealth is a subset of eHealth, the legislation that applies to eHealth can be adopted for mHealth.

What existing regulation affects mHealth in South Africa?

The Protection of Personal Information (POPI) Act of 2013 is important legislation for any mHealth project to consider. The act specifies minimum requirements for the processing of personal information—defined as information on any identifiable living person (or, in South African terms, any juristic person, which includes companies).

The personal information covered includes all demographic information, such as age, gender, and race, as well as religion, culture, and language. All health information—whether it be mental health or physical health—is explicitly covered. Biometric data, and the views and opinions of the person, are also covered. The POPI Act gives a person rights that should not be violated by any mHealth project or application.

The POPI Act also created an "information regulator," a person whose responsibility will be to enforce the POPI regulations and to create new regulations. The regulator can fine organisations that do not comply. When the regulator position is established, all e-information officers of public and private organisations will be required to register with this office.

Another key piece of legislation is the National Health Act No. 61 of 2003. Section 14 of this act states:

> *All information concerning a user, including information relating to his or her health status, treatment, or stay in a health establishment, is confidential.*

This section also specifies rules concerning when a provider must secure client consent to disclose information (unless there is a court order or a serious threat to public health).

Section 15 covers access to health records by healthcare workers, and section 17 covers the protection of health records.

In 2014, the National Health Act was amended to add requirements from the National Health Normative Standards Framework for Interoperability in eHealth. These requirements, which apply to mHealth projects and applications that handle client information, are as follows:

> *(a) any Patient Information System which is used and/or intended for use in the health sector in South Africa should comply with National Health Normative Standards for Interoperability in eHealth;*
>
> *(b) any Patient Information System which is used and/or intended for use in the health sector in South Africa must be subjected to conformity assessment to ascertain its level of compliance with National Health Normative Standards for Interoperability in eHealth;*
>
> *(c) conformity assessments must be carried out independently;*
>
> *(d) certificates of conformity in compliance with National Health Normative Standards for Interoperability in eHealth must be issued:*
>
> *(e) the National Department of Health must allocate a budget to establish and maintain the foundational national shared eHealth infrastructure (e.g., health information exchange, demographic registries, shared clinical repositories, and security and audit services)*
>
> *(f) the National Department of Health must allocate a budget to establish and maintain a "connectathon" which will be used for compliance assessment;*
>
> *(g) the National Department of Health must establish a National eHealth Standards Board to govern and maintain the implementation of the National Health Normative Standards Framework for Interoperability in eHealth, as well as the standards referenced in the Framework; and*
>
> *(h) the National Department of Health must publish and update, when necessary, the Health Normative Standards Framework for Interoperability in eHealth. Including amendments on eHealth and the health normative standards framework.*

Although the mandates described are clear, they do not mention how these eHealth standards will be regulated and enforced. The **eHealth Standards Board**, when established, could be the appropriate regulating body with the power to fine organisations that fail to comply. Another option could be to increase the powers of the **Office of Health Standards Compliance** beyond that office's current mandate (to enforce standards at health establishments) to also enforce eHealth standards.

The National Department of Health's **District Health Management Information Systems (DHMIS) Policy** provides an official regulatory framework for the DHMIS under the National Health Act of 2003, which empowers the minister to establish the legal framework for health information systems. This policy details who should control access to DHMIS data. The policy also states that the functions of the **National Health Information Systems Committee of South Africa (NHISSA)** shall include the "development of policies and regulations to govern information management in the health sector."

The Independent Communications Authority of South Africa Act No. 13 of 2000 (ICASA Act) established a regulator to oversee broadcasting, telecommunications, and postal services. **ICASA** licenses broadcasters, signal distributors, and providers of telecommunication services—including mobile network operators—and issues the frequency spectrum on which they operate. ICASA has the power to create new regulations.

The **Wireless Service Providers Association (WASPA)** was formed in 2004 as a voluntary self-regulatory body. Its remit is to represent and support self-regulation by mobile network service providers. It has a code of conduct and can fine members.

In December 2015, the **Medicines and Related Substances Amendment Act (Act No. 14 of 2015)** was passed. This law changed the regulatory environment for medical products and devices and established a new regulatory agency called the **South African Health Products Regulatory Agency (SAHPRA).**

SAHPRA will have final authority over the approval of new products and medical devices, determine which medical devices should be subject to registration, and impose conditions on the registration and sale of these items. However, SAHPRA's control over mHealth applications and services is unclear.

The **Health Professions Council of South Africa (HPCSA)** is a statutory body established under the **Health Professions Act, 1974 (Act No. 56 of 1974)** to serve and protect the public and to provide guidance to registered healthcare practitioners.

The HPCSA regulates health professionals in South Africa and registers professionals who meet specific standards. This regulator has the power to institute disciplinary proceedings regarding any complaint, charge, or allegation of unprofessional conduct against any person registered with the council. The HPCSA can also prosecute those who pretend to be registered.

The HPCSA has the final say over how health professionals should interact with clients, which means that the council should assess challenges arising from communications through mobile channels and offer guidance.

The **South African Nursing Council (SANC)** sets and maintains standards of nursing education and practice in South Africa. The SANC was established by the **Nursing Act, 1944 (Act No. 45 of 1944)**, and currently operates under the **Nursing Act, 2005 (Act No. 33 of 2005)**. Part of the SANC's mandate is to uphold and maintain professional and ethical standards within nursing by controlling and exercising authority over practices pursued by registered nurses, midwives, enrolled nurses, and enrolled nursing auxiliaries. Because nurses are the biggest workforce sector in public health facilities, the SANC should also provide guidance on how nurses should engage with mHealth initiatives.

The following table summarises the regulatory bodies that will play a role in regulating mHealth.

Regulator	What they regulate	Status
Information regulator	Processing and storage of personal information	To be established
Office of Health Standards Compliance (OHSC)	Health establishments with respect to adherence to standards	Established. Powers would need to be extended to cover eHealth/mHealth
South African Health Products Regulatory Agency (SAHPRA)	Medical products and devices	To be established
Health Professions Council of South Africa (HPCSA)	Healthcare professionals	Established
South African Nursing Council (SANC)	Nurses and midwives	Established
Wireless Application Service Providers Association (WASPA)	Mobile network service providers	Voluntary association (Self-regulating)

South Africa's legislation and regulatory bodies protect clients and provide baseline guidance for health providers and the private sector. However, in a number of areas, it is unclear what regulation exists. New mHealth technologies, such as mobile devices and applications, can present challenges when regulation fails to keep pace with change. There may be specific challenges affecting privacy, confidentiality, and security, as well as issues arising from the technological limitations of some communication methods, such as SMS.

For any potential scenario, regulatory bodies should consider whether existing regulations are sufficient or whether additional guidance or regulation is required. Here are some examples of mHealth-related questions for regulators to think about:

In what cases can sensitive information be shared using SMS? For example, if a system sends SMS messages to HIV-positive clients, could receiving these messages affect the confidentiality of client health information?

What security standards and procedures should apply to mobile devices used by healthcare workers? For example, are there ways to enforce password protection and encryption of stored information?

What is the accreditation procedure for applications that deal with client data? The Health Normative Standards Framework for Interoperability in eHealth covers interoperability requirements, but does not regulate how data should be held securely on a device and how access to sensitive data should be controlled.

Can healthcare workers use mHealth applications only on devices issued by a registered healthcare organisation or can they use these applications on their personal devices? It is common for healthcare workers to bring their own devices to the workplace. If they use these devices for accessing client data, how can access be controlled?

Can informed consent be collected remotely from clients using mobile devices or applications? Informed consent is often necessary for sensitive data to be collected. May a client give informed consent using an electronic device, and, if so, what rules should apply?

What rules cover medical devices controlled by mobile devices? For example, a smartphone may be used to control a number of diagnostic devices. How will these devices and their applications be registered and subject to regulations?

What standards should be in place for clients opting out of services? Just as regulations are necessary to govern how a client is enrolled for a service, there should also be regulations on how clients can opt out of a service and provisions for what happens to the data that has been collected.

Should there be a limit on how many push messages can be sent per day or week? Many mHealth services involve the sending of push messages. If these are sent several times a day, clients may consider them intrusive.

Conclusion

Although mHealth regulations currently in place in South Africa have a number of gaps, regulatory bodies will be able to address many of them in the medium to long term.

People involved in the design and implementation of mHealth projects should keep abreast of regulatory developments to ensure they are in compliance.

Useful additional reference documents and articles

The following publications provide more insight into and examples of regulation relevant to mHealth:

Callens, S. (2010). The EU legal framework on e-health. In Mossialos, E., Permanand, G., Baeten, R., & Hervey, T.K. (Eds.), *Health systems governance in Europe: The role of European Union law and policy* (pp. 561-588). Cambridge, England: Cambridge University Press. Retrieved from http://www.euro.who.int/en/about-us/partners/observatory/publications/studies/health-systems-governance-in-europe-the-role-of-eu-law-and-policy

Greenfield Management Solutions. (2013). Satellite-enhanced telemedicine and e Health for Sub-Saharan Africa (eHSA) Programme: Study on regulatory aspect. Retrieved from http://ec.europa.eu/europeaid/blending/satellite-enhanced-telemedicine-and-e-health-sub-saharan-africa-ehsa-programme_en

United States Federal Communications Commission. (2014). Amendment of the commission's rules to provide spectrum for the operation of medical body area networks, FCC 14-124. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-124A1.pdf

United States Food and Drug Administration. (2015). Mobile medical applications: Guidance for industry and Food and Drug Administration staff. Retrieved from https://www.federalregister.gov/documents/2013/09/25/2013-23293/mobile-medical-applications-guidance-for-industry-and-food-and-drug-administration-staff

This publication has been supported by the U.S. President's Emergency Plan for AIDS Relief (PEPFAR) through the United States Agency for International Development (USAID) under the terms of MEASURE Evaluation–Strategic Information for South Africa associate award AID-674-LA-13-00005. MEASURE Evaluation-SIFSA is implemented by the Carolina Population Center at the University of North Carolina at Chapel Hill, in partnership with ICF International; John Snow, Inc.; Management Sciences for Health; Palladium; and Tulane University. Views expressed are not necessarily those of PEPFAR, USAID, or the United States government. FS-16-200