February 2016

Privacy and Security for mHealth Projects in South Africa

According to a 2011 World Health Organization report, governments cite issues related to data privacy, data security, and the protection of individual health information as two of the top barriers to the expansion of mHealth.

Protecting personal health information that is collected and transmitted over mobile devices is essential to bringing any mHealth project to scale and ensuring that mHealth platforms can be built upon in the future, while safeguarding the rights of people using the healthcare system.

Current Legal Framework in South Africa

In South Africa, the current legal framework protects the confidentiality of patients' health records. The most important sections in the National Health Act (61 of 2003) regarding privacy are sections 14, 15, 17 and 74(1). Section 14 states that

"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 gives rules concerning when you need a patient's consent to disclose their information (unless there is a court order or a serious threat to public health). Section 15 covers access to health records by health care workers, and section 17 covers the protection of health records. Section 74(1) states that:

"The national department must facilitate and coordinate the establishment, implementation, and maintenance by provincial departments, district health councils, municipalities, and the private health sector of health information systems at national, provincial, and local levels in order to create a comprehensive national health information system."

Relative to health systems, the Minister of Health adopted in April 2014, the Health Normative Standards for Interoperability in eHealth (HNSF). All patient information systems used in the health system now need to conform to these standards.

The right to privacy is also considered to be a fundamental right and is listed in the Bill of Rights of the Constitution in Section 14. The other relevant piece of legislation is the *Protection of Personal Information* (POPI) Act of 2013. It should be noted that when legislation overlaps, the one that offers the most protection to patient data will apply.

POPI Act

The POPI Act of 2013 is an important piece of legislation for any mHealth project to consider.

The act aims to give minimum requirements for the processing of personal information, which is defined as information on any identifiable living person (or juristic person in South African terms, which includes companies). The personal information covered is wide-ranging. It 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, which any project should ensure it does not contravene. The following should be kept in mind when handling personal data:

- Content, justification, and objection to data collection and storage
- Collection directly from the data subject
- Collection for a specific purpose

CONTENTS

- Retention and restriction of records
- Information quality
- Access to personal information
- Correction of personal information
- Security safeguards
- Automated decision making
- Direct electronic marketing
- Trans-border information flows

Content, justification and objection

The responsible party must be able to justify why they are processing a person's personal information.

Consent from the person (or a competent responsible person in the case of a child) is one justification, but there are many others. For example, if the data is necessary to execute a contract with the data subject or it is for the legitimate interests of the data subject (like to prevent their death).

The person can withdraw their consent at any time. They can also object to the collection and storage of their personal data at any time, and then the responsible party may no longer process the information.

Collection directly from the data subject

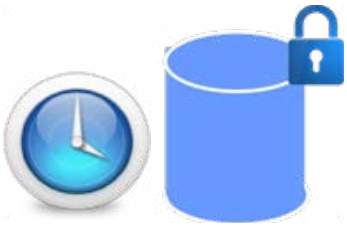
The collection of data must be directly from the person except in a few cases. Valid exceptions include instances in which the data are from a public record that has already been made available by the person, or if they have already given consent. In practice, this means that when getting consent from the person, they should be informed who will be processing the data.

Collection for a specific purpose

The purpose of the data collection needs to be specified and communicated to the data subject before collection.

Retention and restriction of records

Records should be kept only for as long as they are necessary to achieve the purpose for which the data has been collected. For example, if a third party is collecting the information to transfer to another responsible person, then the third party must delete the personal information after it has been sent. Likewise, an mHealth project should only hold the records as long as necessary. However, if safeguards are in place, specific data can be held for historical, statistical, or research purposes.



Information quality

The responsible party must try to ensure that the data is complete, accurate, not misleading, and up to date where necessary. For mHealth projects, this may be an issue when the data are only collected once. For example, how can the project ensure that a person's mobile phone number is up to date or that the information held about a health condition is current?

Access to personal information

A data subject can request that the responsible person inform them if they hold data about them or not. The data subject will need to provide proof of identity.

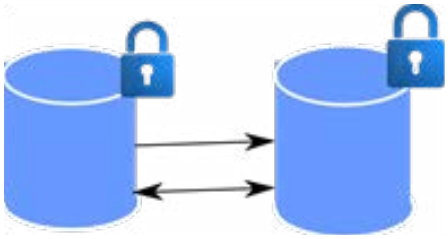
If the responsible party does hold data, they must provide that information in an understandable format on request. However, the responsible party can charge a fee for this.

Correction of personal information

A data subject may ask the responsible party to correct or delete information held about them. This right extends to instances in which the information is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully. It also covers situations in which the data retention period has been longer than reasonable. The responsible party must act upon such a request as soon as possible and provide credible evidence that information has been corrected or deleted.

Security Safeguards

The responsible party must try to secure the integrity and confidentiality of personal information by taking appropriate measures to prevent loss, damage, or unlawful access to data.



For example, failing to keep HIV status confidential can cause significant damage. The responsible party must identify all internal and external risks to confidentiality, and establish appropriate reasonable safeguards. The risk register and the safeguards must be continually reviewed and updated.

If third parties are used for collecting or processing data, there must be a written contract in place that ensures appropriate security measures are in place.

Automated Decision Making

The law prohibits computers from making decisions about patients without appropriate measures in place to protect a patient's legitimate interests. For example, if a computer model determines who gets treatment, the patient must be able to ask a human being to check the decision.

Direct Marketing

The responsible party can only directly market to a data subject electronically (for example, by email or SMS) if they are their customer or they have consented. Direct marketing includes offering any good or services, or asking for a donation (like blood or organs). A customer is someone whose details the responsible party has obtained in the context of a sale of a product or service.

Data Security Standards

Health specific security standards are detailed in the Health Normative Standards Framework for Interoperability in eHealth in South Africa.

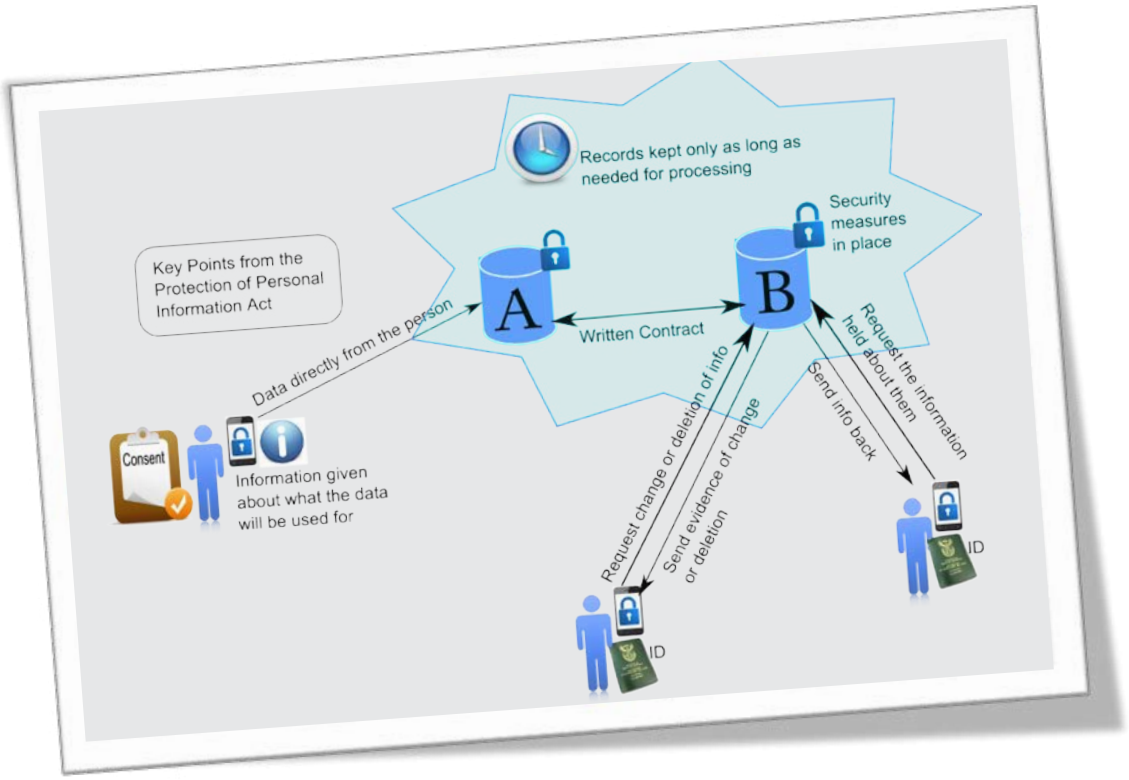
The ISO/TS 22600-1:2006 standard is identified. This covers Privilege Management and Access Control. The standard includes specification of requirements for sharing healthcare information. It also contains specification of the technical architecture models and the implementation model.

Other important security standards are:

- RFC 3881: Security Audit and Access Accountability Message: XML Data Definitions for Healthcare Application
- RFC 2616 (MIOS): The Transport Layer Security (TLC) protocol
- WS-I Basic Security Profile 1.1 (web services)

Trans-border data flows

Transfer of personal information outside of South Africa is lawful provided certain protections are in place. For example, the country to which the data is sent must have similar data protection legislation, the transfer must be necessary from a contractual perspective, or the person must consent to the transfer.



User account portals as part of the solution

As described, there are many issues that mHealth projects need to consider in order to be compliant with legislation. These include decisions on how consent will be recorded, and how users will be able to query the data held about them.

Some of these issues may be overcome by implementing a user account for the person when they are registered in the mHealth system. This user account should have some element of security, such as a username and password.

For mHealth projects using just SMS or USSD (menu-based simple text content for basic phones), it may be more appropriate to have a pin code associated with a cell phone number.

For this to be effectively implemented, there should be a way for users to recover their pin code or username / password in cases where details are forgotten or lost. This can potentially be done using a one-time pin sent to a cell phone number or email address. The recovery method should be set up and codes recorded when the person registers in the system.

Once a user account is in place, a web-based portal could be used to cover a number of elements of the POPI Act. The description of the purpose of the data collection and details of how it will be processed can be provided through a simple menu interface. The user account portal can also provide a way to collect user consent and, potentially, the data itself. Options can allow people to see what information is held about them and ask for it to be corrected or deleted.

Using a secure user account portal with encryption will cover some privacy and security issues. Written contracts with service providers and mobile network operators are also ways to improve security for mHealth projects. These contracts should explicitly mention the POPI Act, security measures, and retention periods.

Check list for POPI Compliance

- Full description of purpose of data collection, how the data will be processed, and who it will be transferred to
- Consent form recorded and held (where appropriate)
- Data collected directly from the user
- Risks identified regarding confidentiality and protection of records. Appropriate, reasonable security measures implemented and continuously reviewed
- Records retained only as long as necessary
- Written contract with third parties that process on your behalf to put security measures in place
- Standard process for ensuring data is up to date and correct
- Standard way for people to request data held about them
- Standard way for people to ask for data to be corrected or deleted
- Direct electronic marketing only to prospects with their opt-in consent
- Conformance to government's Health Normative Standards Framework for Interoperability in eHealth

MEASURE Evaluation SIFSA is implemented by the Carolina Population Center at the University of North Carolina at Chapel Hill in partnership with John Snow, Inc., Futures Group, ICF International, Management Sciences for Health, and Tulane University. For more information, visit https://www.cpc.unc.edu/measure/sifsa.

www.measureevaluation.org

This technical brief has been supported by 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. Views expressed are not necessarily those of USAID or the United States government. FS-15-151

USAID FROM THE AMERICAN PEOPLE PEPFAR MEASURE Evaluation SIFSA