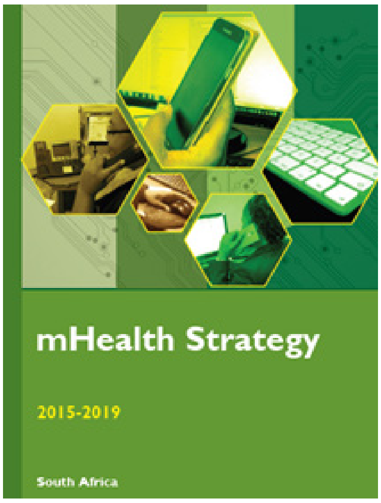
September 2015

Good Practices in Issuing Mobile Devices to Healthcare Workers

Mobile health, or mHealth, is defined as the use of mobile computing, medical sensors, or other communication technology in the delivery of health-related services.[1] mHealth has the potential to empower patients with information to inform their healthcare decisions and link them to health services. Providers and health managers can use mHealth to access data for decision making and for the improvement of health systems performance.

Despite this potential, some mHealth initiatives have struggled to deliver benefits, in part due to a lack of coordination and a duplication of effort between programs implementing mHealth initiatives. This is further exacerbated by the complications of distributing mobile devices to healthcare workers. If devices are assigned in an uncoordinated manner by multiple projects, then each project will face a similar set of challenges and health workers could potentially be given many different mobile devices, resulting in duplication of cost and effort.



The South African mHealth Strategy 2015–2019 provides some tangible ways to address these coordination and duplication challenges. It states that the Department of Health should "provide guidelines for mHealth projects providing tablets/smartphones to healthcare workers [which]… all face common problems around SIM recharge methods, broken/lost devices, training and security."

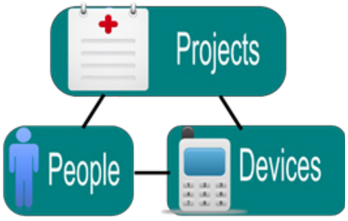
This technical brief describes an approach focused on the One Device Principle for mobile health and shows how it can be used to promote greater coordination among projects. It will also detail the major issues that need to be addressed when distributing devices to healthcare workers.

> The One Device Principle is "the principle that any national, or regional, healthcare system should strive for the situation whereby, at any given time, a healthcare worker will have a maximum of one mobile device allocated to them that they use for the implementation of various mobile health projects."

Establishing the One Device Principle

If a healthcare system applies the One Device Principle, there are a number of things that will naturally follow as good practice. These are detailed below:

1. All mHealth projects that plan to issue health workers with mobile devices will need to utilise a standardised platform or operating system. This will allow devices to be reused by several projects. To allow for flexibility, mobile applications should also be platform-independent.
2. There should be centralized storage for all the information about mobile health projects and who is responsible for which device. It's important to have a central database that holds information on the projects, the people, and the devices.
3. Before new mHealth projects start, it is necessary to assess what equipment has already been deployed and can be reused, using the central database outlined above.
4. The method of financing mobile devices, and other associated costs, should be defined so that projects can budget effectively for the costs they will incur. In general, there will be a capital cost for new devices and an ongoing cost for monthly fees, replacements,



[1] South Africa mHealth Strategy 2015-2019; National Department of Health; August 2015.

and support. Reusing devices may introduce cost savings for all projects, but financial obligations of each project should be clear from the outset.

5. Support and maintenance will need to be centralised and there should be policies and standard operating procedures for the following:
    a. Procurement of devices
    b. Initial set-up of devices
    c. Management of airtime, data costs, and contracts
    d. Issuing devices to healthcare workers
    e. Training of users by projects
    f. Loss, breakage, or theft of devices
    g. Loading new applications onto existing devices.

Procurement of devices

To allow for standardisation, the procurement of new devices should follow a set procedure. This should include the feature set of the device — for example, it should be determined whether a device should be multi-SIM or have a specific resolution camera attached. Some degree of consideration for future project requirements should also be a factor. If an operating system platform has been specified, this should also be a requirement for the device. The total cost of the device should also be a consideration.

The central database will contain information linking a healthcare worker to a specific device, together with its capabilities. This should be used to determine the outstanding device requirements for the project.

Initial set-up of the device

The standard operating procedures for setting up a device will include methods of installing specific applications and SIM cards. At this stage, the status of the device, and what has been installed on it, should be recorded in the central database.

Management of airtime, data costs, and contracts

Purchasing the actual device is often not the largest cost associated with issuing healthcare workers with mobile devices. Airtime and data can be a considerable expenditure and can also be a significant logistical problem. Where possible, projects should work cooperatively to address the logistical issues. For example, if one project utilises a particular method of giving healthcare workers airtime, then other projects should identify whether this approach would also work for them and what the implications would be. By centralising and standardising the management of airtime, data, and contracts, the implementing health system will save costs and reduce logistical work. All of this coordination must be done in conjunction with an established agreement that details which project will pay for which costs.

Projects could also consider making use of toll-free numbers, short codes, and closed user groups. In these cases, the different projects should coordinate so that one solution — such as a single toll-free number — can work for all their needs.

Where possible, it might be appropriate for remote monitoring software to be installed on devices. This will allow the central database to report how much data is being used and when recharges may be required.

Issuing devices to healthcare workers

The logistics of delivering devices should be handled by a support team. Before a device is issued it should be tested to ensure that it will work as expected in its assigned location.

The mHealth project must also provide clarity as to what the healthcare workers' roles and responsibilities will be with respect to the care and use of their mobile device. One challenge associated with issuing mobile devices is the concept of personal use versus work use, therefore acceptable usage terms should be made clear to all involved. The healthcare worker will need to sign for the device and agree to the terms and conditions stipulated.

User training by projects

A good practical approach would be for a support team to conduct training when new applications are loaded onto devices. This training should include information on what to do when there is a problem with the application or device that cannot be resolved by the user. Users should be informed of the details of a central helpdesk/support team that can be contacted when problems are detected.

What happens when a device is lost, broken, or stolen?

There are many scenarios in which a device may be rendered unusable. To cover these scenarios there should be policies and procedures that describe what staff should do in each specific case. Estimates for device failure for mobile phones is up to 20 percent in the first year of ownership,[2] so it is important to have clear procedures

[2] Mobile Device TCO Models for Line of Business Solutions, Volume 1, Track 7: Enterprise Mobility Mobile Device TCO; https://www.motioncomputing.com/downloads/Proven_Results_Construction/WP_VDC_Mobile_Device_TCO.pdf, page 5.

for replacing a device that fails or is damaged in order to prevent interruption of work. Limits on health worker liability for lost, broken, or stolen phones should also be clearly stated. Cases when devices are stolen require particular attention and a procedure for filing a report with the authorities and claiming insurance.

The theft scenario should also be considered from a data protection perspective. Security measures, such as device and application passwords, can help prevent data loss in the event of a device being stolen. In the event of theft, it may be possible to implement security features such as remote wiping of data, encryption, and geofencing, which is the ability to set up triggers when a device enters or exits certain boundaries.

To reduce the risks associated with theft, it may be appropriate to add tracking capabilities to the device. There are many applications available for tracking. For example the open source Prey Project (https://preyproject.com) has software for many different platforms that allows devices to be GPS-tracked and locked remotely. It might also be possible to set off an alarm remotely, display a message on the locked screen, and disable the power button.

Although anti-theft software can be useful, it should be noted that it is not able to cover situations where the power source is disconnected or where the device has been reset to defaults.

Loading new applications onto the device

When a new project begins that will be reusing devices, a new application will need to be loaded onto an existing device. There should be a defined method for installing the new application or link. There should also be checks to identify that all the existing applications still work after installation.

What happens when a healthcare worker changes roles or leaves their position?

For the most part, a device will be issued to a healthcare worker who has a specific set of tasks to perform. There should be a standard procedure for what happens to a mobile device when a healthcare worker changes roles or leaves the employment of the healthcare system.

When a healthcare worker leaves employment, the device should generally be returned to his or her manager and then placed in a central device storage area. However, in some cases (for example when a person will directly take over a role from a departing employee), it may be appropriate to assign the device to the person taking over the position, with details of the changes recorded in the central database.

Similarly, when a healthcare worker changes roles within the system, it may be possible for them to retain their current device, reconfigured with the new suite of applications applicable to their new role. Unnecessary applications should also be removed.

Limitations of the One Device Principle

The One Device Principle is a simplification of the scenarios faced by healthcare managers and mHealth implementers. Some devices may have a very specific set of sensors or functionality that are not generally available on standard devices. An example of this may be a blood pressure checker that connects to another mobile device. It would not make sense for the blood pressure checker to be considered as the healthcare worker's one device, but the device that it links to could be considered such.

There may also be cases where there is one device that is shared amongst staff carrying out similar specific functions. These shared devices would not count as the healthcare worker's one device but would be considered as a shared device. That said, issues related to financing, standard operating procedures, data security, and monitoring will still need to be considered for that shared device.
Due to scenarios such as the above, there will always need to be a degree of flexibility in the application of the One Device Principle.

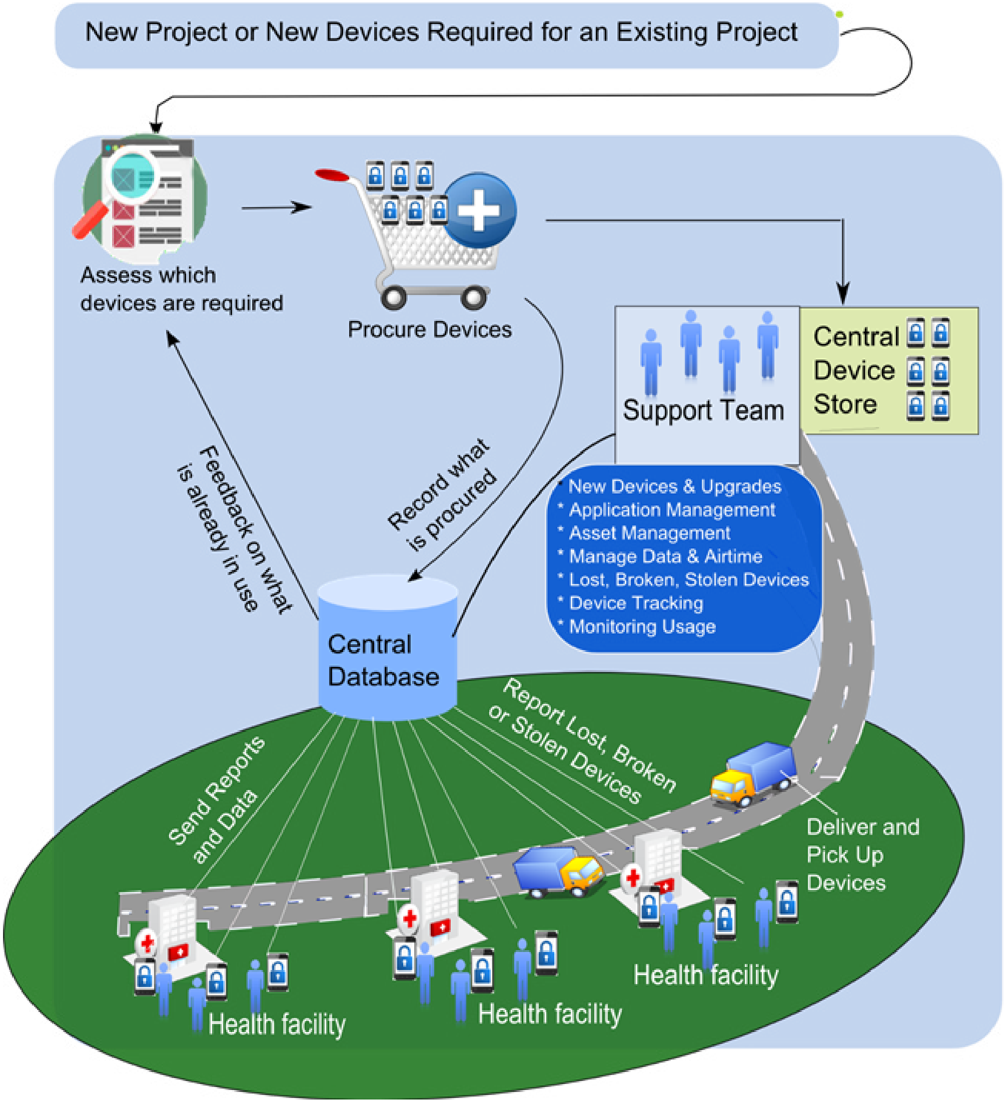
One Device Principle: Checklist

- Is a maximum of one device being used by any healthcare worker for mobile health interventions?
- Is information about mHealth projects, mobile health devices, and healthcare workers stored in a central database?
- Has a policy for shared financing of mHealth devices and operating costs been established?

- Is there a standard operating procedure for purchasing new devices?
- Is there a standard way airtime and data for devices is managed?
- Is there a standard procedure for issuing devices to healthcare workers?
- Are there standard acceptable usage terms for personal versus work use of devices for healthcare workers?
- Is there a standard operating procedure for loading new applications onto a device?
- Are there standard operating procedures for cases in which devices are lost, broken, or stolen?
- Is data held securely on devices?
- Is usage of the device monitored?

If the answer to any of these questions is "no," then there are risks that should be mitigated. These may range from issues of duplication to risks related to privacy and security.

By incorporating appropriate elements of the One Device Principle, a healthcare system will be well positioned to effectively begin to realise the benefits of mHealth projects.



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., ICF International, Management Sciences for Health, Palladium Group, 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-15-148