GSMA

Mobile for Development mHealth

Mobile SIM-based Medical Applications

Michael J. Kleeman, Martin Harris and James Erasmus

February 2015

Author: Michael J. Kleeman, Senior Fellow, University of California San Diego (UCSD), mkleeman@ucsd.edu

Co-Authors: Martin Harris, GSMA
James Erasmus, GSMA

Table of Contents

Executive summary

This white paper will explore the potential of enhanced mobile technologies provided or enabled by the Subscriber Identity Module (SIM) in the evolution of mobile-based health services (mHealth). This paper is intended to start and frame the discussion. Potential and specific solutions will involve further research.

As mobile technology becomes more affordable and widespread across the world, the application of mobile-enabled technology to the delivery of healthcare services has great promise in contributing to improving the health of millions. Nowhere is this more true than in developing markets where access to even basic healthcare services can have a significant impact in improving quality of life, and no area of healthcare can have as great an impact as delivery of maternal and early childhood health and nutrition related services.

While there have been numerous programmes over the past decade aimed at improving care to this target population they have been characterised by a bespoke approach with limited integration across network and health systems, leading to an uncertain impact of the value of using mobile technology compared to other methods of ICT based service delivery. These have largely been solutions of a limited life span and scale which, along with the data collected, mostly disappeared when the project funding ended.

This white paper has found that:

- Very few, if any, mHealth solutions to date have leveraged the technical capabilities of the SIM card located in all GSM phones (which accounts for over 85% of the global mobile market and is higher in developing markets) such as identity, security, core network system access and application environment.
- There is a clear need for the use of secure identity for users/patients and health workers in their interactions with health providers and supporting systems, which will increase tailored and meaningful services with a higher level of assurance and privacy. This is an area where, as the name suggests, the SIM has a lot to offer. It already supports identity on the mobile network along with mobile financial services, which now enable over 250

million people globally with low cost, portable and secure financial and national identity.

- In order for SIM-supported mHealth services to be effective they will need to leverage and drive standardised protocols and data ontologies used or planned for in eHealth services. Further, properly implemented with provisions for identify security, a SIM-based approach could address the technical requirements for data sovereignty by enabling the disaggregation of identity from health records, which could allow the data to be stored offshore.
- The storage and application facilities on the SIM, whilst limited, have the capacity to aid health providers in providing support for critical medical and nutritional information and interactions with the patient through a robust and reliable mechanism.
- A SIM-supported mHealth identity system can provide increased levels of security for personal information and enable the integration of data from across multiple mHealth applications.

Alongside Government, health providers and NGOs the mobile network operators (MNOs) will have a key role in providing mHealth services based on SIM technology. However this will have to be standardised on a nationwide basis and enable interoperability for the fostering of universal services and ensuring reach for the potential of SIM-supported mHealth services. Being nationally based and regulated, MNOs are well placed to provide the basis for these services.

The benefits of a SIM-supported approach are realised by the citizens/patients, healthcare providers and the government ministries overseeing maternal and child health and nutrition, along with related services.

This table summarises the benefits of the SIM-supported approach

Benefit	Citizen/ patient	Care provider	Government
Secure access	X	X	X
Security and privacy of data	X	X	X
Access to informa-tion in emergency	X	X	
Portability	X	X	
Open access		X	X
Ability to network enabled capabilities	X		X

There are also potentially major benefits for mobile operators with this approach. Since it leverages the inherent security of the SIM and network-based services, it enables mobile operators to partner with the government in providing a nationwide mHealth service and one that can integrate across any and all mHealth service applications, providing a logical single system. With unified, secure and network-enabled and stored identity, the approach helps protect the privacy of citizens and their medical data while avoiding the situation common today with multiple third-party mHealth systems and data that cannot be integrated or centrally managed.

This white paper provides background on this approach, examines other alternatives for mHealth service delivery and provides use cases and example high-level architectures for potential SIM-supported mHealth services, together with recommendations for potential deployments.

A SIM-based approach for medical applications

This white paper discusses the use of a SIM-based approach for medical applications, principally mHealth applications. While there are technical elements of this approach, discussed in detail in later sections, put simply a SIM-based approach uses the SIM card in a mobile phone coupled with network-based authentication services, to provide secure access to medical information for healthcare providers approved by the patient, with a centralised record of who accessed the information and when.

Using this approach, all users, patients and providers need to have their identity verified by a trusted agent of the government before they can use the system. In contrast to virtually all existing mHealth systems in which there is often no formal verification of identity before accessing medical information or access logging, the SIM-based approach also permits the same verified identity to be used for any number of conforming mHealth systems or applications.

A SIM-based approach could also store a limited set of 'in case of emergency' medical data (such as blood type, allergies, etc.) locally on the phone/SIM, available to authorised users at any time, even when there is no network connectivity. Because it uses the same types of interfaces and interactions that users access daily on their phones it can be easily learned and used. All of this is detailed in later sections of this paper.

During a medical crisis such as an epidemic (the recent EBOLA epidemic is a prime example) there are often multiple mHealth systems deployed to assist in the response, often leading to duplicate or incompatible data and complications for healthcare providers accessing the necessary patient medical information. The approach discussed in this white paper could help to provide a common identity registry, allowing authorised health providers to access patient information quickly and in a secure manner and permit the government to integrate medical information from across multiple systems. It could further help to protect patient medical data and enable health providers in remote locations with limited network coverage to access critical information from the SIM on the patient's phone.

This capability, combined with the mobile operator's ability to track phone connections through CDRs and network data, could help to speed-up the contact tracing so critical to controlling the spread of a disease such as Ebola.

The benefits of SIM-based medical applications

For the purposes of this paper we will be focusing on three SIM-based medical applications. In the last section we will review additional use cases, but the main document focuses on the following three:

Registration – The verification of identity of the individual and the secure establishment of that identity in the SIM for accessing mobile health-related information. This registration and associated authentication can be used for general health-related information access as well as mHealth data. The registration certifies the identity of the individual (patient and provider), which can then be used to authenticate access to medical information via any online connected application. A SIM-based approach can allow the separate storage of personal identification (in the SIM and network) from medical information (in the mHealth application database) while enabling the joining of these when needed for the provision of health services. In this manner it can also enable the individual patient data from multiple online applications to be more easily integrated.

Authentication – The use of the SIM and security codes (PIN) to let the user of the phone prove their identity for medical purposes and allow access to data stored under that account; both locally on the user's phone and, because these are network-based applications, permit access on the health provider's device for reading and updating. The authentication can be strengthened by using differing Levels of Assurance (LoA) from a simple 'OK' confirmation through PIN codes and non-repudiation signing (PKI support)[1]. This also enables the use of the phone to validate other activities, such as payment for services with higher security. However there are trade-offs between complexity and security (remembering and then accurately entering one security PIN as opposed to two or three) and these will need to be explored by the implementing organisations[2].

Health records/registers – SIM cards come in varying capacities and processing power. They are capable of storing key medical data, some of which could be made accessible in the clear and some with password/PIN access. This ability could allow for emergency access to key information (such as blood type) as long as the phone with the medical information storing SIM (or the SIM alone) is present.

> "Portability lets the user carry limited medical information with them at all times"

In order to better understand the value proposition of utilising SIM-based capabilities in medical applications it is best to quickly examine the special nature of medical information. Medical information is highly personal, sensitive and considered private by individuals. Medical information can be life-critical and thus real-time access is important. Medical information is generated and used by multiple parties, often using different applications and devices. Managing personal authentication and access control to an individual's medical information is of real value to healthcare systems in developing markets.

Taken against this background one can see that while similar in nature to mobile money, mobile health applications have special characteristics that increase the benefits of utilising SIM-based solutions. The basic attributes of SIM-based solutions: reach, secure access, physical portability, networked capabilities (e.g. remote backup), and ease of use all lead to the generation of benefits to the different user constituencies.

For **patients/citizens** each of these attributes is important:

- Secure access and data protection provide the individual with confidence that their medical information is secure and that only authorised users can see it. This security could be further enhanced by the separation of personal identity from the central medical record, storing such personally identifiable information only in the database created at registration and linking it with the health information only when the information is presented to the health provider after authentication by the SIM mHealth system. The SIM mHealth concepts proposed here can support either implementation approach.
- Portability can let the user carry some limited medical information with them at all times, since mobile phones are almost always carried by their users. The ability to access them even at times without network connectivity means availability of the limited emergency level information stored locally in the SIM.[3]
- The connected nature of the SIM allows for capabilities such as remote backup and allows users to access data stored in a central secure location, permitting a deeper set of data than that which might be stored locally in the SIM, and protection against loss or corruption of the data on the SIM either by technical failure or loss of the device or SIM, plus the ability to restore data when SIMs are renewed/swapped. Such a capability also permits data to be drawn from multiple sources for presentation to the provider and lets different mHealth applications use the same authentication tools.

Care providers can realise similar benefits if adequate compliance is obtained and security guaranteed:

- Secure access and data protection allow authorised users to access the current user/patient data on their connected device and help insure that the medical information they are seeing and updating is specific to that SIM-carrying patient.
- Portability means that some data is locally stored and if the patient has their phone then the provider can authenticate directly and provide access to the emergency data stored locally on the SIM.
- Network capabilities allow providers to access data stored in a central secure location through remote authentication with the user, permitting a deeper set of data than that locally stored, plus the ability to interact with the medical record via web or other interfaces and then update the central database and the appropriate SIM data.

For **government** the benefits are parallel:

- Secure access and data protection creates a level of trust and protection for the medical information associated with the SIM, which is likely to be part of a national programme. And since the SIM-based approach enables personal identity and identifying information to be stored separately from medical data, this can insure greater security for the medical information while enabling appropriate parties to access the data in an identified manner once they are authenticated to the SIM-based.
- Open access enables the government to authorise different mHealth platforms to access the medical records of their citizens, as long as they comply with the ontology and APIs (read-only access can also be provided but this is much less valuable) for access and authentication. Properly implemented with provisions for identity security, a SIM-based approach can also help to address the technical requirements for data sovereignty, enabling the offshore storage of de-identified medical data.
- Portability means the phone can be used for authenticating and accessing information in a central hospital, regional clinic or by community health workers in the field.
- Network capabilities can permit the government to select a secure central location for the medical records but allow multiple points of remote access: by phone, PC, tablet, etc., while maintaining data integrity.

Benefits of SIM-based mHealth

Benefit	Citizen/ patient	Care provider	Government
Secure access	X	X	X
Security and privacy of data	X	X	X
Access to information in emergency	X	X	
Portability	X	X	
Open access		X	X
Ability to network enabled capabilities	X		X

For **MNOs** there are also benefits:

- Creation of sustainable mHealth services, closely linked to the key capabilities of the network. The generation of sufficient returns for sustainability will depend on the generation of low margin revenue (to appeal to the majority of users) at scale.
- Leverage of MNO identity solutions and Know Your Customer (KYC) processes from mobile money. SIM registration can create a more attractive relationship with the customer base. Depending on the nature of the services adopted, there will be costs related to STK and SIM distribution, particularly for more advanced functionality (e.g. KPI encryption support, larger memory capacity), some of which could be planned into existing SIM distribution mechanisms and amortised across different services requiring similar functionality.
- Cement MNO reputation with both the customer base and investors, through the provision of impactful life enhancing and secure services.
- A good relationship with the relevant government authorities, by supporting national health capabilities.
- Opportunities to extend to other service areas, such as agriculture.

[1] FICAM has defined a model for Level of Assurance which pertains to the level of trust which can be put in both the vetting procedure which supports the identity of the individual and the mechanism used to establish identity. This ranges from level 1 (Little or no confidence in the asserted identity's validity) to level 4 (Very high confidence in the asserted identity's validity). http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf

[2] It is also possible to use a single passcode (PIN) for multiple applications. The Mobile Connect project is moving to standardise such use for single secure sign-on to many applications.

[3] As discussed below, SIM cards come in different sizes, with different storage and processing capabilities, although with the same standardised interface. In many markets a significant number of SIMs are more basic in nature, with limited storage and processing, and the SIM mHealth system needs to be designed to function with even the most basic SIMs in order to be a universal offering. This places constraints on the amount of data that can be accessed off-line.

Other related applications of SIM technology and current mHealth approaches

In its preparation, our research covered how mobile phones are being used in medically related settings with a special focus on those applications that could beneficially utilise SIM-based features. What was discovered in this research is that while such applications are being explored at this time, none have been released into full service (as far as it could be ascertained).

One application that utilises the same SIM-based features discussed here is the broadly deployed and well known mobile money service (e.g. M-Pesa by Safaricom). In many ways it parallels the core possibilities of mHealth SIM applications discussed above:

- **Registration** – The verification of identity of the individual through KYC processes and the association of that identity with the SIM for financial transactions.
- **Authentication** – The use of the SIM and security codes to let the user of the phone prove their identity for cash in/out, transfer funds, bill payments, etc.
- **Local storage with network-based data** – Information locally stored in a combination of network and mobile money information from the operator. This enhances security and interoperability and permits restoration in the case of a damaged or lost phone or SIM.

Depending on what credentials are required, the registration for mHealth services could be combined with other services. More generally the ability of a secure registration process to provide an authenticated digital identity is a major trend. Practically, the concept for registration and authentication provided for mHealth where a trusted agent uses national identification ID and personal document verification, enables a digital KYC capability which can be used across

> **“The numerous applications deployed for mHealth in developing markets, while covering a wide range of functionality, typically do not utilise SIM-based features.”**

multiple application domains. Since medical information is among the most sensitive data we have, meeting the security requirements for mHealth should provide a basis for other domains as well, such as mobile money and national digital identity (voting, benefits, etc.). This move to what is called an authenticated single-sign-on is a basis for the mobile industries Mobile Connect initiative as well [4] [5].

These same attributes of security, portability and network connectivity that can enable SIM-based mHealth applications are used to support mobile money capability. This parallel capability, and the wealth of experience developed in deploying mobile money systems, could be of immediate benefit to the design, development and deployment of SIM-based mHealth applications. These will be explored in the following sections;

Comparison of existing mHealth applications

There are numerous applications deployed for mHealth in developing markets[6]. While these cover a wide range of functionality and have yielded benefits for patients and providers they typically do not utilise the SIM-based features we have been discussing. Generally these mobile applications fall into three categories:

- SMS-based applications with centralized servers for message generation. By creating smart back-end applications that can execute on the basis of different parameters, including time, end-user response, user profiles (e.g. requiring certain compliance in taking medication), etc., SMS-based applications have found wide adoption. Additionally, because of the inherent interoperability of SMS they also allow national deployments across multiple MNOs and permit initiation of the application activity from a central server. An example of this class of application is discussed below for vitals registration.
- USSD-based applications. Since these typically require a direct relationship with the MNO(s) to implement, they are harder for external providers to deploy. Additionally, in order to provide uniform service across providers they would require all providers in a market to coordinate on the USSD application. As USSD applications are based on a real-time session protocol and are resource-intensive on the network, operators prefer to limit access.
- Third party applications on either smartphones or feature phones. These applications utilise the MNO’s data network to interact with application servers at the MNO, Ministry of Health, local data centre or via the cloud internationally.

This requires the installation of client software (applications) on the smartphone platform (e.g. Android, iOS, Java, etc.) which can be done over-the-air, side loading or by preinstallation. These applications can make use of the smartphones assets in respect of advanced visual and audio capabilities along with wider bandwidth data access to present more sophisticated user interfaces and functionality to users. It should be noted that third party applications have limited (if any) access to SIM features and secure personal data on the phone, which will limit some of the features described here.

The following table summarises the current mHealth application types and compares them to the SIM-based approach covered in this paper.

Comparative Mobile Communication Channels

Deployment model	Benefits	Constraints	Comparison to SIM-based applications
SMS-based	• Easy to develop • Inherent interoperability • Familiar user interface	• Limited interaction (line by line transactions) • Limited security • No network data backup, local data storage (Inbox) is unstructured. • Constrained user interface	• Lower security • No data backup from device to network • Less flexible application design and interface • No authentication capability • Unstructured and not persistent local data
USSD-based	• Structured user interface • Easy interaction • Data stored in the network • National level control over data	• Requires MNO involvement • Nationwide service requires multi-MNO cooperation • Limited interaction (line by line transactions) • No data persistence on the device	• Lower security • No data backup from device to network • No on-device functionality when out of coverage • Limited authentication capabilities • No local data • Session length constraints
IP Data-based	• Flexible design, integral Internet access • Does not typically require MNO relationship • Choice of development tools • Does not require GSM network knowledge for offline capabilities	• Only works where there is mobile data coverage. • Device cost. • Data plan required. • No national level control over data • Service fees can be expensive • No inherent data security or multiple-system interoperability	• Less secure • Single mHealth system • Limited or no data sovereignty control • No data backup from device to MNO network • No integrated authentication capability. • Stand-alone customer support
SIM-based	• Network Level Security, Data Portability • Local emergency data access • Single sign-on/authentication for multiple mHealth Applications, • Network-based data backup and recovery • Nationwide service with MNO interoperability • Can utilise messaging channel (SMS, USSD) as a data bearer. • Familiar user interface • SIM Toolkit SDK • Works with almost all phones. • National level control over data	• Requires MNO involvement • Nationwide service requires MNO cooperation • Application distribution and updates can be limited (OTA or SIM Swap)	

[4] *http://gsmamobileeconomy.com/gsmamc/*
[5] *http://www.mobileworldlive.com/mhealth-tracker*
[6] *For a current compendium see Gayle Mendoza, Lungi Okoko, Sarah Konopka and Edna Jonas. November 2013. mHealth Compendium, Volume Three. Arlington, VA: African Strategies for Health project, Management Sciences for Health*

The majority of mHealth applications are deployed in local situations and to relatively small populations (with some exceptions). There is a move by some National Ministries of Health to standardise on one application or application type in their countries. However, these applications all have significant limitations to broad applicability and value generation:

- Few are targeted at or are available to the average citizen/patient. Most are designed for use by community health workers (CHWs) or medical professionals. A SIM-based authentication/registration/data store provides greater involvement of the patient and allows them access to their own medical data.
- Differing levels of security, with some having no security (SMS applications have limited security), and few if any can leverage SIM security capabilities.
- No common data ontology limits interoperability across systems or comparison of data gathered. Except in nations with national standards, such as Rwanda, there is virtually no common approach to data, platform selection or interoperability.
- Very little, if any, service consolidation limits the value proposition for the end-user and MNO, resulting in low uptake or adoption of the service and an inability to attain critical economies of scale required for sustainability of the individual service.

The GSMA Personal Data Initiative did document case studies utilising mobiles to register births in rural Uganda[7]. Neither of the approaches utilised SIM-based capabilities. In fact, the two MNOs involved chose different platforms (SMS and USSD) to provide the functionality. There are however key attributes of this work which are relevant to the issue of medical information applications utilising SIMs:

- The systems all use central data repositories and web-based applications coupled with mobile-based data entry. The Ministry of Health (MoH) is involved with both deployments and there is effectively a common ontology.
- The systems both address the issue of authorised agents to provide the registration information. In the rural settings targeted by this work, these agents are the village elders who used to utilise paper-based approaches for such registration.
- The service providers understood the importance of standardising on platforms and in each case mobiles were provided to the agents.

The most directly relevant comparison, however, is still in the mobile money arena. The most broadly deployed mobile money application, M-Pesa (Safaricom in Kenya), utilises the SIM toolkit and authentication together with central systems, in some instances, with third parties offering additional financial services. Trusted agents are involved in the registration of users and there is a degree of data standards, along with emerging interoperability acrossmobile money providers. There are customer care elements to address phone loss and/or damage to the SIM. In short there is a working system with wide deployment which parallels many of the elements required for SIM-supported mHealth applications. It is interesting that, to date, no large scale mHealth application has leveraged mobile money like SIM-based approaches; however it is notable that, as discussed above, the vast majority of mHealth applications are point solutions and are not part of a comprehensive national system.

Roles of the various actors

As described above, the proposed SIM-supported mHealth application approach is envisioned as a system for the delivery of mHealth information leveraging the unique capabilities of mobile network infrastructures to ensure reach, high security and ease of use. Additionally the approach is designed to be standardised at a national level

[7] *Mobile Birth Registration in a case study of Orange Senegal and Uganda Sub-Saharan Africa, GSMA Mobile Identity Team, 2012*

(or perhaps even international in terms of infrastructure elements) to enable users to seamlessly and uniformly interact with the system no matter which operator services their mobile needs.

In order for this concept to be realised it will require the participation of all of the stakeholders involved in this system, starting with the government and MNOs but also including the health system providers and ultimately the patients/citizens. The roles differ but the integrated participation is central to the successful deployment of a national SIM-supported mHealth solution. Below are some participants' potential roles.

The government

Privacy, security and data sovereignty issues are largely personal ones, but the national government is responsible and has ultimate authority. Therefore the government, most likely the Ministry of Health, will take a lead role in specifying how the medical information of their citizens needs to be managed and protected. Since the solution being proposed is one which can be nationwide in scope, the government will need to develop standards (most likely together with MNOs and healthcare providers) for key elements of the system, including:

- Authorisation of MNOs to manage, transact and potentially store mHealth information
- Interfacing with accredited regional and national eHealth database or EHR system
- Criteria for registering patients and providers to the mHealth system including APIs to national ID registers and KYC services.
- Authorisation of agents to register patients or providers
- Standards for the language use in the UI
- Standards for emergency data elements
- Security and audit requirements
- Selection of the central data repository location and operations
- Approval of which other mHealth applications and systems can access the data and authorisation capabilities of the system
- Determination of payment structure for the SIM-based mHealth application

The mobile network operator(s)

The MNO is central to the operation of the SIM-supported mHealth application environment. The architecture requires interaction with core network elements and aids the development of applications that touch network services and SIM interfaces. In addition to the networkbased interfaces the operator can be an initial interface with the citizen/patient (and potentially healthcare provider) for registration and SIM replacement. In addition to the basics of providing elements of KYC, authentication mechanism and provision of a SIM toolkit-enabled application, the proposed solution adds several further requirements to be met by the operators:

- They will have to standardise their solution with other MNOs and the government to provide a base uniform offering to clients. This is perhaps the major difference between this solution and other SIM-based functions which tend to be orientated to the individual network
- They will have to provide an authentication mechanism to third parties (such as the operator of the mHealth application core servers) which will work across a multioperator environment
- They will potentially have to interface with national health records systems
- They will have to enable training for their direct sales and agent network in authorising and registering mHealth clients
- They will have to provide co-operation in cases of fraud with the relevant authorities
- They will need to operate servers and services to provision both the SIM application and to backup/restore data with the SIM in case of replacement
- They will need to work with the stakeholders in the provision of key network resources, e.g. short codes, CSR, etc. in support of sustainable services

Health system players (including NGOs)

The providers will benefit from the mHealth solution, but in order to do so will need to accept a national standard. This need not be the exclusive means of their accessing their patients' data, but it will be one way and could become a primary means of authenticating them to national data. The real benefit will be uniformity for, at the very least, emergency patient information, coupled with the ability to interact with the medical information of patients who provide permission for such access. However this solution may cause concern for some providers for a few reasons:

- The patient is in control of their access to the medical information, which may be a change from their way of doing things
- The provider will be able to have access to emergency medical information even if the patient is unconscious
- For CHWs and other field medical personnel (as well as clinic or hospital personnel) the SIM-based solution may become a standard for confirming service delivery and thus linked to payments for that service delivery
- There will be a system tracking which patient data they see, thus increasing transparency and accountability

Despite the fact that providers may have to give up some of the independence they have often had, the SIM-supported mHealth solution will enable them to provide better medical care to their patients, better referral capability (since they can link other providers to the medical record) and have an additional channel to use when communicating with their patients. They may also have to pay additional network fees (depending on government funding or requirements).

Patients

The citizen or patient is ultimately the main beneficiary of the mHealth application. They should receive better healthcare, be able to control who has access to their electronic health records and improved care in case of emergency. They will be able to insure that CHWs actually deliver the services they are supposed to deliver to them (through payment verification). Patients will have to register to receive these benefits and also learn how to use the application. They may also have to pay additional network fees (depending on government funding or requirements).

Key requirements and issues in deployment

A SIM-based approach is elegant in its operational simplicity. However underlying this simplicity are a number of business and operational issues which need to be understood, agreed to by the different parties (government, operators, mHealth platform providers) and then properly implemented to insure a successful deployment.

Data to be stored[8]

There are three places in which information can be stored in a SIM-supported mHealth solution:

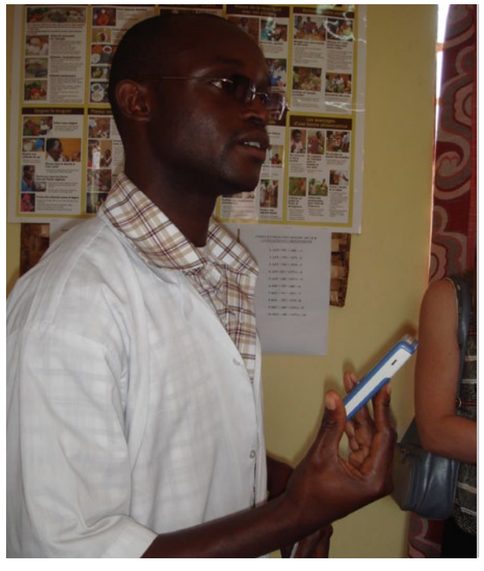
- The first is in the SIM, where it is secure and can be backed up in the network. In the applications we are describing, some data will always be stored this way. However, storage capacity of SIMs can vary and the majority of SIMs have little storage, which can create a limitation on the amount of data that can be stored on the phone. Also most SIMs only support limited data record structures which may not be suitable for some more complex EHR requirements.
- The second is on a separate memory card in the phone, but this data may not be fully secure, and many phones either do not have a secondary storage capability or, even if the phone can support one, the user may not have the separate memory card installed. Thus this option is not always available, and is not as secure as the SIM data.
- Lastly, the data can be stored in the network, both replicating what is on the SIM but also potentially expanding on what can be locally stored on the SIM/phone. This is the case with mobile money, where only essential data is stored locally on the SIM, along with the SIM-based application, and the majority of the data is stored in the network and mobile money systems. This distributed approach eliminates the capacity constraints on smaller memory SIMs, and can address other issues such as authorised third party devices accessing the information, but requires reliable network connection channels.

This data issue is one of the key issues that SIM-supported applications will have to address. One of the issues is what data should be stored, and where. The basic personal registration and authentication information has to be part of the record, but what other medical information is essential? And what information has to be available at all times and what information can be centrally or network stored and therefore only available when the phone is able to get reliable mobile coverage (sometimes an issue in rural areas)? In answering this question it is perhaps useful to examine the different types of medically related information.

Medically-related information can be classified into three general types:

1. **Life-critical** – information that can make a difference between immediate life and death. Examples of this are blood type (in case of transfusion), allergies, and medications being taken. Also diagnoses of life threatening illnesses, or highly infectious ones, such as HIV. This is key information that a care provider needs to have access to, to avoid mistreating the patient or harming them or putting the provider at heightened risk. Also included in this category is the identity and authentication information of the individual/patient. This ID process can be used to link or connect to other information, such as that in 2 and 3 below.
2. **General medical information** such as age, weight, other diagnoses, current treatments, vaccinations, nutritional interventions, etc. Also general medical history, care providers, etc., provide effectively what is now referred to as an electronic health record (EHR). All of this is important information, but can be voluminous, and is not life critical if unavailable at the time of care.
3. **Medically related but non-medical**. Insurance or other financially-related information, general demographics (address, etc.). Important in the overall health system but not medically-critical for care.

Broadly considered, type 1 data above should be locally stored on the SIM. Fortunately there are standard ways of coding this data (more on this below) and it does not require a lot of storage and so it should be possible to have this on the smallest of SIMs. Type 2 data and type 3 data can be stored in the network (or Ministry of Health data centre) and accessed through the identity process from the SIM. The principal difference between type 2 and type 3 data is the level of encryption and security required for personal medical or financial information.



[8] *See also Data Standards and Ontology discussion*

Device dependency

One of the attractive attributes of a SIM-based mHealth application is the near universality of its use. The majority of GSM phones (and in developing markets virtually all operators utilise the GSM standard) and especially at the low end, are capable of supporting SIM-based applications. Complications may arise with SIM form factor issues, dual SIM phones and virtual SIM technologies[9].

SIM cards come in four different sizes, in the case of removable SIMs (there are also 'embedded' SIMs, which are not used in mobile phones), all with the same general functionality but increasingly with a smaller form factor. Part of the reason for this is the increased density of solid state memory (same memory in smaller physical space) and also the desire on the part of handset manufacturers to save more space and utilise it for other components.

SIM card sizes

Since the majority of use of SIM-supported mHealth applications happens when the device is in the phone, the size of the SIM is not relevant for primary use. In the case of preprogrammed SIMs, the different sizes mean that agents should stock different size SIMs (as most do already). Where the correct size SIM has to be provided, as the actual smart chip is the same size, it is often found that agents will trim a SIM to the required size from standardsized SIM stock. While SIMs are provided in different sizes, a full size SIM can also be cut down to the other sizes using special tools, to simplify stocking.

However, should the subscriber not be able to use their phone either because it is damaged or the subscriber is unconscious then there is the use case (described below) of removing the SIM from the phone and placing it in either a dual SIM phone (one that can read from different SIMs and under user control select the one being used) or a stand-alone SIM reader. In these cases the SIM form factor may become an issue.

Another dimension of device dependency or constraint is the display, and how much information can easily be accessed through the user's phone, or may be better accessed on a different device such as smartphone, tablet or PC. As more information is stored and needs to be accessed, the display limitations of most basic and feature phones can become a constraint. This factor supports the use case of the subscriber authenticating, using their device (and SIM), access to their information by a health provider using a different device.

The use of different devices, and potentially applications, to read and update a wide range of medical data requires the standardisation of the data. Not only will the SIM-based application need to be standardised across providers but to enable multiple applications to utilise the data the underlying ontology and data standards need to be complied with. This issue is described in more detail below.

SIM card sizes

CSIM card	Introduced	Standard Reference	Length (mm)	Width (mm)
Full-size (1FF)	1991	ISO/IEC 7810:2003, ID-1	85.6	53.98
Mini-SIM (2FF)	1996	ISO/IEC 7810:2003, ID-000	25	15
Micro-SIM (3FF)	2003	ETSI TS 102 221 V9.0.0, Mini-UICC	15	12
Nano-SIM (4FF)	2012	ETSI TS 102 221 V11.0.0	12.3	8.8

[9] *Companies such as Movirtu along with MNO are offering a virtual SIM capability where users can share a single SIM and still be individually identified to the network, see http://www.movirtu.com/#!share/coeo*

Multiple records on a SIM

This is one of the more interesting issues with regard to mHealth, especially in maternal and early childhood healthcare. Unlike mobile money, where the subscriber and the mobile money account are related one-to-one, it is possible that with mHealth, a SIM-supported solution may be used by a mother or father with multiple children, resulting in a one-to-many relationship. This creates a unique situation for SIM-based applications, one that can be addressed in several ways:

- The SIM can be designed to support separate records for multiple children. However this can be a problem, as SIMs typically have a limited ability to process and store all of the desired information.
- The SIM can store the principal information about the parent and life-critical information about the children (such as HIV infection).
- The SIM can store the principal information about the parent and information about the immediate needs of the children (such as vaccinations due) which can be updated from the network on a periodic basis.
- The SIM can store the basic information about the parent plus the number of children and the identification key can permit access to the complete information on the children from the central data repository held in the network. This avoids the SIM limitation issue but requires network connectivity and coverage to work reliably.
- The SIM-supported solution can be engineered to support multiple users for authentication, either where there is a single authenticating authority, e.g. the parent, or where multiple users can have authentication through different keys on the SIM.
- As many of the key beneficiaries of these services may not have direct access to a phone and have to make use of a shared device, supporting multiple identities off a single SIM will be key to making such services affordable and accessible.

In practice, a mix of local and network storage will probably be the preferred approach, since it will be used as a general element of any SIM-based solution. The principal question to be addressed is: which information should be stored and processed on the SIM and which to store centrally but accessed using the SIM authentication?

Network availability

As suggested above the availability of reliable mobile network connections is a factor in overall system design and operation. No matter how well most mobile networks are designed and operated, there can still be equipment failures or geographic issues which prevent 100% coverage and reliability. Thus any solution needs to be technically designed with local storage to complement any network-based (see Central Storage Location below) repository. As suggested elsewhere in this section there is real value in central information storage, both for capacity and backup reasons. However local storage on the SIM would be essential for vital data that needs to be available at all times. Thus most mHealth solutions opt for a hybrid local/central information storage approach, and this is recommended here as well.

Device/SIM loss

In a SIM-supported mHealth solution the applications and their data, as the name suggests, reside in part on the SIM, which is usually in the user's handset and accessible. However there are numerous circumstances where this might not be the case. In many markets, users often have multiple SIMs, usually to take advantage of promotions from the different mobile providers. In some cases a phone is shared by multiple users, either with their own SIM, a shared SIM, or in some places a virtual SIM. Occasionally the SIM will get lost. Phones get lost or stolen and when that happens the SIM is lost or stolen with the phone.

The mHealth applications discussed here all consider having a central storage capability which can provide backup and recovery in case of loss. Due to the SIM's inherent security (see SIM basics section) it cannot be easily accessed by the thief or person who might find it, and once notified, the network operator will be able to disable the SIM (and thus the phone it is in) from accessing any network services, plus potentially wiping any sensitive information from the SIM. Key here, for the mHealth application, is the availability of customer support and a network of connected authorised agents who can validate the user's identify and issue a replacement SIM. In many ways, authenticating identity for a replacement SIM is even more critical than the initial issuing of a medical SIM since the replacement SIM will enable access to an individual's medical information, whereas the initially authenticated SIM only has access to allow such information to be collected. Thus while device and SIM loss are not uncommon in any market, special care from both the customer support team and the re-issuing agent will be needed to ensure that adequate user security protection is in place.

Trusted agents

The issuance of a SIM designed to support mHealth applications is an activity that requires appropriate levels of security; and the issuance of a replacement SIM, as discussed above, requires even more security. There are currently different levels of trusted agents involved with mobile applications.

- **Basic registration** - Agents who issue SIMs (and thus mobile service accounts) are contracted by and in some markets licensed by the MNO. In many (and an increasing number of) markets the government requires identification in the form of a national ID card or passport to issue a SIM, and these transactions are recorded electronically and stored on a central database.
- **Mobile money** – Since mobile money requires a financial relationship with or via the MNO, customers who obtain these accounts typically have to provide information such as a national ID and any replacement SIMs have to be validated by the MNO or mobile money service provider's customer service personnel.
- **Vital records** – In Uganda the birth records provided to the government through the MNOs are originated by a restricted set of users, typically the village elders, who are historically authorised to record births. They are authenticated to the network via their phone and SIM. In the case of Uganda, MNOs provide the approved SIMs directly to the elders, thus using what can be considered a valid chain of custody. A comparable system of digitally validated identify for both issuers of SIMs and those that are authorised to update the information on the SIM.

> **"No matter how well most mobile networks are designed and operated, there can still be equipment failures or geographic issues which prevent 100% coverage and reliability."**

- **Medical information access and update** – As discussed earlier mHealth differs in several ways from mobile financial services. One of the key differences is that health information needs to be accessed and updated by many people, not just the user/phone owner (see below for description of other users).

Trusted users other than owner

The need for healthcare providers to access and update a third party's (user/patient) information, combined with the sensitive nature of medical information, places a special requirement on the mHealth system design and operations to ensure that all the parties involved have the appropriate credentials and are properly authorised. These personnel can include community health workers or hospital or medical clinic personnel (and in some countries Ministry of Health personnel) and anonymous information may be requested by researchers. The fact that so many people and systems may be accessing and updating personal medical information, even if the user/patient is providing authenticated access approval, suggests that a complete audit log of all transactions will be critical for trusted mHealth applications (as it is for financial services).

Central data repository location

Because of the need to store more data than most SIMs could hold or process, plus the requirement for backup and recovery and multi-party access, a central data repository is a requirement of the SIM-supported application system. This is a common feature in several application areas and the STK and architecture is designed to permit data to be distributed and moved securely to and from the SIM/phone. However, for medical applications there is a requirement for universal access within a country, independent of the MNO serving the client. And it will not be uncommon for the user/patient and provider to be on different mobile networks. The next section addresses this in greater detail, but the location of the data repository must support access independent of network. In practice, this can mean the data base system is at a third party site such as a secure private or government data centre, or at the Ministry of Health. It can also be housed at one of the mobile operators, but would have to be available transparently to the systems of all operators to support universal access (see data sovereignty below).

The requirements for data centre location will depend on government regulations (see data sovereignty below for one dimension of this issue) on the management of their citizens' personal information, government preference (several MoHs in Africa prefer mHealth data to be stored at their sites), terrestrial connecting network capacity and reliability, operations quality and personnel qualifications. Whatever the location, it is critical that the central data stores be operated in a highly reliable manner with suitable redundant systems (computer, power, and network) to insure that all operators can access the information stored there.

Interoperability across MNOs

In typical mobile environments interoperability refers to technical interoperability and the GSM/3GPP standards for the interchange of voice, message and data traffic to support this seamlessly. However, for SIM-based applications, interoperability will require that all operators deploy an application supporting required functional, protocol and data standards, so that the data is freely accessible to authorised users independent of which network they are on. The central repository addresses some of these issues and application standards can be imposed on the way that the SIM toolkit APIs and structures are used.

There are, however, interoperability issues which are not technical and need to be addressed to ensure successful mHealth SIM applications:

1. Standardised agent and user authentication and identity management.

2. Centralised or at least coordinated customer care in the case of access problems or lost or stolen SIMs.
3. Centralised or at least coordinated customer care for user issues in accessing and using the applications. This is especially important where multiple parties are involved (as in the case of a medical service provider accessing patient information via the SIM application, followed by the user/patient validating that services were provided and triggering payments) when the parties are on different mobile networks.

These operational issues are important to address in the design phases of a SIM-supported application project as they can often take more time and effort to address than technical issues.

Data standards and ontology

One of the principal issues in mHealth is the lack of standardisation of data across the numerous systems that have been deployed. With no common ontology (an ontology provides explicit definitions of terms and relationships between terms within a specific domain, in this case, health), data from one system is virtually meaningless when used with another. The sharing of data or even the interpretation of data can be impossible without translation tables. One system might even code for gender differently than another, or use a different term to label gender. Adding to this generic issue of lack of standards is the complexity of health terms across cultures, in which the same term can mean different things (fever in one country refers to malaria, and in another an elevated temperature).

Given this complexity and the need for interoperability across operators, and for epidemiological and research purposes across geographies, the standardisation of the data will be critical. Without standards it will complicate the ability of different systems to utilise the data in a SIM-based system. With standards and well defined APIs, the SIMbased capabilities can create a wide array of new capabilities in eHealth, and save significant costs for all electronic and mHealth applications. Done properly, and with the cooperation of organisations such as the World Health Organization (WHO), these standards can create the core for a broader set of inclusive eHealth data standards, benefiting the entire health community.

Encryption and security

The protection of personal data is an important part of creating a trusted system. This is especially true in the case of medical/health information. Thus individual data needs to be both secure and perceived as secure by the parties involved with the system. The recommended SIM-supported mHealth applications have three elements and each has its own parameters and issues to be addressed:

1. The SIM-based data and transmission to/from phone: These are secure by nature, even if the SIM is lost or stolen. The data is protected by the architecture of the SIM (see tech section) which allows access to stored data, plus it can provide the means for encrypting data during transmission. However, as the data moves between the phone and the central database these need to be explicitly encrypted. There is a trade-off between the robustness of the encryption and the processor and power use on the phone. However the volume of data is relatively small and thus this data can be encrypted for transmission.
2. Central data repository: This data presents the greatest data security risk, as this is the aggregated data from all the citizens in the system, plus information on the healthcare providers. This needs to be fully encrypted and access control rigorously applied to its use. This encryption can be stronger and more secure than the over-the-air transmissions (encryption and decryption take power and time to process and the central site will have computers and power to perform the calculations needed for the en/decryption, while the mobile devices have limited processing capacity and power in comparison). Also any applications that permit access to the data (especially in an aggregate manner) need to have high security for access control.
3. Healthcare provider devices: Similar to the subscriber/patient phone, these devices (which can be phones, tablets or even computers) need to have the proper authentication for access (SIM-based devices like phones and some tablets can use the same authentication as the citizen/patient phone) and appropriate audit trails for use.

The issue of an audit trail is important for security. Any system used for operations and management of health data (like financial data) should have an immutable audit file (one that even the system manager cannot tamper with) to identify all reads and writes to the data files.

[8] *In the US NSTIC is in the process of piloting the standardisation and use of a common easy-to-use mobile identity solution for citizens to access online services whilst improving security and privacy. (http://www.nist.gov/itl/nstic-091714.cfm)*

Data sovereignty

Data sovereignty refers to the regulation of data collected about or created by citizens of a nation by the national authorities. In practice it usually means that some classes of data (and medical data is one common class) are by law required to be stored in the nation of origin, and not in another jurisdiction. What this means for mHealth is a constraint on international cloud storage of the data. In most cases the central data store will be with a national MNO, Ministry or local secure data centre, and comply with any national sovereignty requirements. Data that is anonymous (identity removed as supported by the SIM-based approach discussed here, and/or aggregated data) can usually be accessed internationally and stored, but many Ministries of Health would prefer to certify any data removed from the sovereign data storage location.

Building the base

The SIM-supported model could be designed to provide universal national secure and audited access to individual health information. In order for this to work, the platform capabilities need to be broadly adopted and straightforward to implement. In practice this will mean that MNOs make the use of the system, by patients, providers and other mHealth platforms, as intuitive as possible. In order to help this, the following are recommended:

- SIMs pre-configured with any required applications and security enhancements (e.g. PKI). Once the application is developed and certified by the MoH and the MNO, then the MNO should insure that all relevant SIMs are pre-loaded with the application and support the capability for remote update.
- Network-downloadable application support (OTA). This will help deal with the installed base of SIMs that are not pre-loaded with the application and to keep all users' applications current.
- Standardised APIs to allow other platforms to access the authentication and access capabilities of the SIM supported solution. However user organisations should also agree to subscribe to the open data standards and audit trail capabilities of the mHealth platform. This also allows the logical integration of data across multiple mHealth systems using the same SIM-based authentication and ID approach since they share a common secure patient identifier.

Regulatory constraints

The national health and communications regulatory authorities can impose restrictions on mHealth applications, data and use. Most of the Health Ministry issues are discussed above. The communications regulatory issues can include interoperability issues, CSR obligations for free or discounted service, and numbering (for speed dial, SMS or USSD purposes or even national mHealth phone numbers with reverse charging). All of these can create obligations and costs for MNOs. It is recommended that, as part of any initiative, the mobile operators work together to create uniform approaches to addressing these issues and present an effective proposal to the regulators in advance of regulatory initiatives. This can often simplify the obligations while still addressing the needs of the government, its people and the operators. However, care must be taken to ensure the long-term sustainability of any critical service such as SIM-based mHealth and while the operator can work with the government in making these services economical there need to be cost offsets (such as tax or fee reductions) in addition to appropriate incremental revenue streams for the provisioning of the range of mHealth service capabilities and systems described here.

Use cases

Background

The research in the area of mHealth identified no major systems utilising the specific SIM-enabled or supported approach. Additionally, in the field, the mHealth applications differ significantly between developing and developed markets.

In developing markets there have historically been two basic types of mHealth solutions:

1. Third party using 2G or 3G data where the users are the healthcare workers and data is stored locally for patient transactions and centrally for major persistent data store. There are no devices which are specific to the citizen/patient in these systems as they tend to be provided directly to the healthcare providers (such as community health workers). This approach has limitations in rural areas where data services are sometimes unavailable even when voice and SMS are available.
2. Trusted agent approaches like the vitals registration systems described above where there is a trusted agent with a dedicated phone. Again, the patient is not involved in the technical chain or authentication.

In developed markets there are also two basic models [10]:

1. Stand-alone applications, some with centralised data storage and reporting but all largely patient-centric. These typically use a user ID/password pair for access.
2. Electronic health records systems where there are patients and providers where each accesses the systems with a user ID/password pair, sometimes with multi-factorial authentication including the Universally Unique Identifier (UUID) of the phone or biometric. The patient phone is not part of the access control for the provider activity.

The suggested use case scenarios and design for developing markets put the citizen/patient more in the centre of most transactions, authenticating and validating access by the provider and also permitting them to access their own basic medical information (especially in an emergency).

In developing markets the assumption would be that most patients have a basic personal phone or access to a 'family' or shared phone. Some may have what is described as a feature phone and a few possibly a low end smartphone (Android, Nokia Asha, etc.). This will make services provided over voice, SMS, USSD and STK more relevant to their situation.

Health workers, in comparison, will often have access to more capable feature phones, smartphones and tablet devices, either through personal investment or by supply from health providers and government agencies. This opens up the possibility of more sophisticated web-based services.

Therefore, we assume that, in the majority of cases, patients/citizens have basic/feature phones and in a few cases smartphones and that the service[11] can be delivered via USSD, SMS or smartphone applications. Providers will have either feature phones (CHWs), tablets or smartphones (clinic providers and hospital staff) or access the system through a web-based interface.

1. Service provisioning – for a user with no current mobile account with the MNO or service provider

In the case where a potential service user does not have either a mHealth account or a mobile account with the MNO providing the services, the user will need to acquire access to both the network and the mHealth service. In most developing markets this is usually done through a local MNO-approved agent, but in the mHealth context others, such as CHWs or medical facility workers could also be authorised to provide this service.

In this case when the SIM is issued by an agent, the agent can supply a SIM pre-loaded and configured with any relevant SIM mHealth applications and linked tariff plans. There then needs to be a process to allow the user to subscribe to the health service and create any required accounts.

A key part of the registration process will be for the user to establish identity, comparable to Know Your Customer (KYC) processes used in SIM registration and mobile Money account setup. As with the mentioned processes this will need to be linked with government identity (register) schemes and in particular Ministry of Health processes and an API to any appropriate government database that will speed up this process.

[10] In the US NSTIC is in the process of piloting the standardisation and use of a common easy-to-use mobile identity solution for citizens to access online services whilst improving security and privacy. (http://www.nist.gov/itl/nstic-091714.cfm)
[11] The user interface should be capable of being tailored to the language preference of the user.

This process will need to be carefully thought through, so that identity can be established from existing documentation and/or by any relevant attestation by trusted sources. The level of assurance which can be provided by any mobile-based service will be linked to the level of identity which this process can provide.

As part of this process it may also be required to capture some basic user details such as birth date, gender, number of children and for example, priority nutrition interventions, which would form the basis of the health details within the system. This setup should also be reflected in any linked centralised system where the relevant data and links to the user's mobile account are kept, so that any interactions such as authentication can be provisioned.

Careful thought will need to be applied to how the user can best be trained in the use of such services through agents, CHWs, etc., along with how authentication can be handled in a scalable and user-friendly way. e.g. PIN, how it can be set, memorised and reset.

The system will also need to deal with other scenarios, such as users who already have a mobile account but need to register for and access the mHealth service, and how users interact with health professionals and/or service agents in both the registration to the service and in day-to-day use.

As part of this service the SIM should be able to provide;

- Support for a service registration process e.g. through a SIM-based application.
- Authentication process for users.
- Local storage and access of key medical data and access codes, etc. for the relevant services.

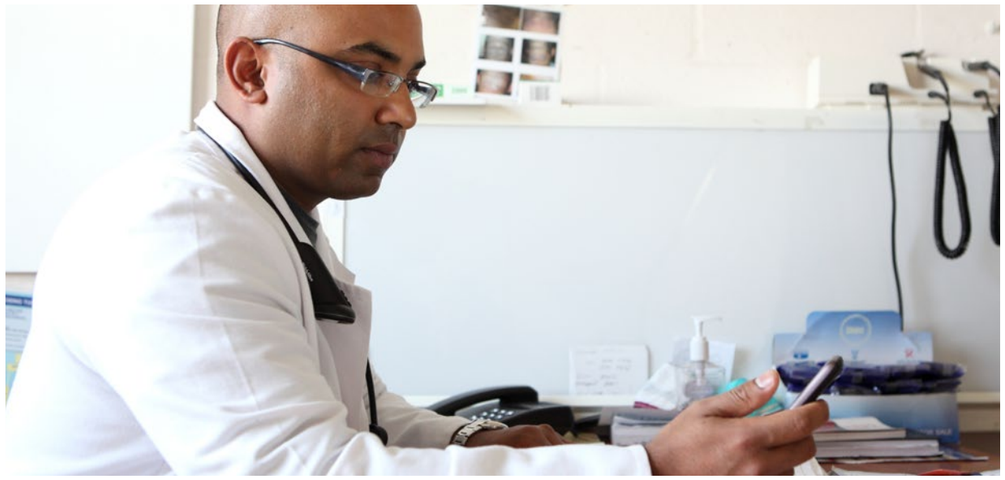
At the end of the process the user should be clear about the use of the service and the interactions required through the mobile phone in order to facilitate the service and linked services with health workers and facilities. The system has also created an account for the user and a medical record associated with that user. In the case where the data is de-identified there is a unique numbered key generated to link the medical information in the central database with the user/patient identification.

Use Case 1

> **"A basic design principle behind the SIM-enabled mHealth application is that the user/ patient is in control of their medical information and can grant access to their healthcare provider to read/update as appropriate."**

As many potential users in the areas where these services will be focused, pregnant mothers may not be enrolled in any national, regional or health related identity schemes and consequently often lack the required documentation for an identity verification process. In this situation often the "trusted agent" for the MNO and the health provider is also a village elder (or similar) who can attest to the identity of the pregnant mother wanting to register. In this case the elder could be issued with a SIM and authentication application, which would carry a higher level of identity assurance and allow them to attest to the identity of the pregnant mother in a non-repudiable way (similar to electronic signatures).

[9] *The user interface should be capable of being tailored to the language preference of the user.*



2. Service provisioning – for a user with a mobile account wanting to add the mHealth application

In the case where a potential service user does have a mobile account with the MNO providing the services but wants to add the mHealth application they will need to either obtain a new SIM with the application pre-loaded or have the application downloaded over the air (OTA) to their phone/SIM. In either case this will require the user to authenticate to the trusted agent (MNO agent, CHWs or medical healthcare facility worker) their identity with the necessary documentation. There then needs to be a process to allow the user to consent and subscribe to the health service and create any required accounts and/or profile.

The Know Your Customer (KYC) processes, as well as the SIM capabilities described in the first use case, are the same for this case.

At the end of the process the user should be clear about the use of the service and the interactions required through the mobile phone in order to facilitate the service and linked services with health workers and facilities. The system has also created an account for the user and a medical record associated with them. In the case where the data are de-identified then there is a unique numbered key generated to link the medical information in the central database with the user/patient identification.

Use Case 2

In this instance there may well be a case when a mother enrols (or has previously enrolled) and wants to register her child on the service. As the application and authentication is already set up for the mother, the child could be associated with the same SIM and also have the autonomy of their own account, while still having their identity linked to the mother's. This would allow the mother to authenticate on behalf of the child but the records would be specific to the child e.g. nutritional interventions could be recorded for the child and as the mother authenticates these she would receive any linked incentives.

3. Service provisioning – for a healthcare provider with a mobile account wanting to add the mHealth application

Healthcare providers register in a similar way to patients as described above in use cases 1 and 2, with the addition of a prior approval from the Ministry of Health. Specifically it can be expected that the Ministry of Health will have a list of approved providers permitted to access the mHealth information. Either by the use of an API or hard copy this can be made available to healthcare facilities or NGOs which can then register the healthcare providers associated with their organisations. There will need to be a separate process to permit unaffiliated providers to register for the service, either directly with the MoH or with an authorised agent.

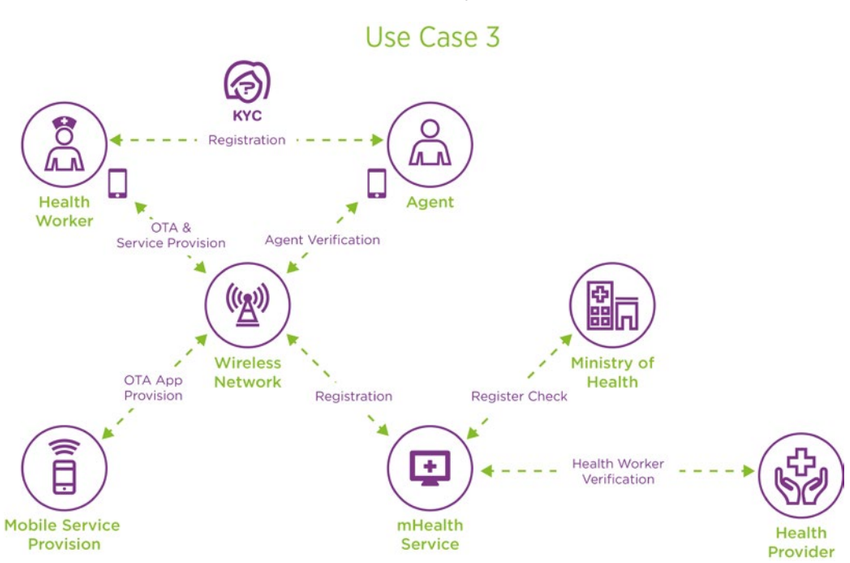
The healthcare provider may be accessing the mHealth information via a computer and web access. To be consistent in the security and authentication process (and to permit the separation of identity and medical information) they will still need to authenticate via the SIM-based application (this will need to be built into the SIM and web-based applications with appropriate APIs). This will require that any user have a mobile attached device with SIM (phone or tablet).

Careful thought will need to be applied as to how authentication can be handled in a usable way for the user e.g. PIN, how it can be set, memorised and reset.

As part of this service the SIM should be able to provide;

- Support for a service registration process e.g. through a SIM based application.
- Authentication process for users either on the SIM enabled device or via web access.
- Authentication link to permit provider to see the patient information stored in the mHealth system.

At the end of the process the provider should be clear about the use of the service and the interactions required through the mobile phone in order to access patient medical information. The system has also created an account for the provider and an access log to document and time stamp the patient data they have accessed or referred on to another provider.



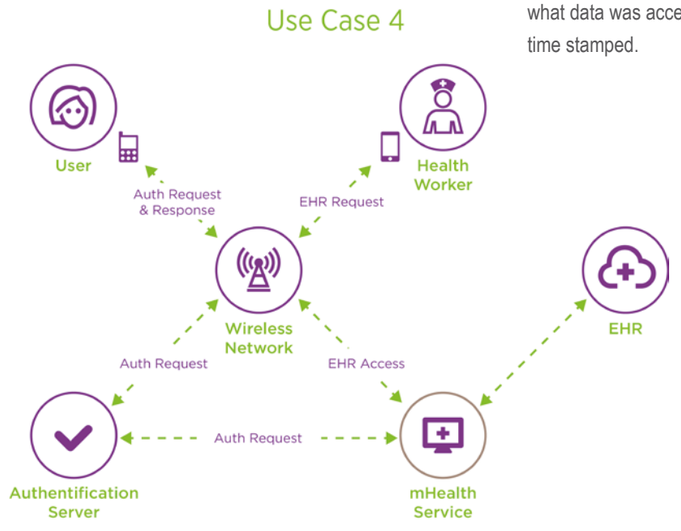
With CHWs given identity and applications specific to their role in the service, it is conceivable that the process would help to reduce the lag in digital payments due to them, as well as provide an audit trail of their work. In one scenario a CHW who distributes nutritional supplements for children can have the intervention authenticated by the mother on behalf of each child, confirming when and where the intervention occurred and helping the CHW incentive targets to be accurately recorded and provide a higher level of assurance that distribution is reaching the required individuals.

4. Service authentication and access: the process of a patient authenticating to the SIM-supported mHealth application and permitting a healthcare provider to access their medical information. This assumes that the patient is present and conscious and there is network connectivity

A basic design principal behind the SIM-enabled mHealth application is that the user/patient is in control of their medical information that is securely stored and can grant access to their healthcare provider to read/update and add this information as appropriate.

The user/patient accesses the SIM mHealth application on their phone and then authenticates via their PIN code. The healthcare provider, who has already authenticated to the system in a similar manner, provides the user/patient with their mobile number to enter into their phone.

This action then can either permit the provider access to the medical information for a period of time (this time needs to be determined by the national authorities, balancing ease of use with security needs, and will differ depending on if there is an outpatient or CHW visit or hospitalisation) or in the case of the separate data and identification files it can cause the linking of these data and delivery of them to their user device.



The healthcare provider may be accessing the mHealth information via a computer and web access, which can trigger authentication over the same mechanism, but when they authenticate to the system it is informed what the access device is.

The healthcare provider can then read or update information in the patient's record or request permission to refer the information to another provider. In this case the user/patient receives an authentication request (via their SIM) with this they can approve or deny the request.
At the end of the session if there needs to be a confirmation of service (or associated payment of service as in the case of a CHW) the provider can request such confirmation through the SIM-based application and an authentication request will be sent to the user/patient for their approval.

As part of this service the supporting SIM services should be able to provide;

- Local authentication with network-based application confirmation
- Menu support for the needed transactions
- Authentication process to permit provider to see the patient information stored in the mHealth system and to confirm service delivery.

At the end of the transaction the user/patient will have their local data updated as required (e.g. vaccination records, nutritional interventions etc.), plus any central EHR updates, and an entry will be made in the audit log, documenting what data was accessed/changed by what provider, and time stamped.

In the scenario where a mother and her children are interlinked against her SIM, this (potentially) remote authentication capability also has a benefit when she is separated from her child e.g. when the child is admitted to a care facility but the mother still needs to care for her other children and/or work. She can still receive authentication requests on behalf of her child without being present, thus reducing treatment cycles as well as keeping her informed.

5. Emergency service authentication and access. This assumes that the patient is unconscious and there is network connectivity

In order for providers to access key medical information in an emergency there needs to be provision for access without patient approval. This can be supported under certain limited conditions:

a. The patient is in an approved facility.

b. The providers are pre-approved for emergency access.

c. There is proper oversight to avoid abuse.

When the user is not in a position to actively take part in an active authentication of access to their medical details (for instance when they are unconscious) an override process can be enacted by approved authorities which will enable access to key medical information for the patient according to the nature of the request and the healthcare provider making the request. Such emergency information, such as blood type, can be essential in providing emergency life-saving services.

For security reasons emergency access triggers three special actions in addition to making the medical record available:

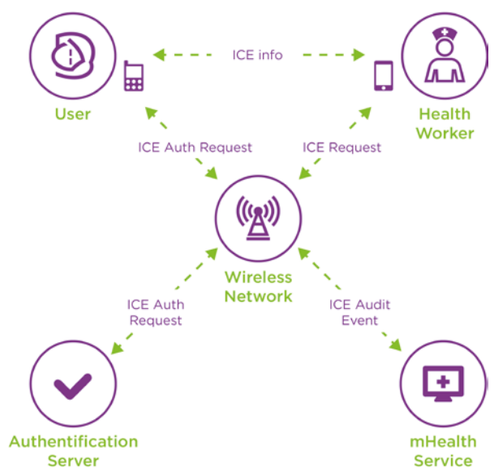
1. A special entry is made in the audit log.
2. The provider's supervisor and MoH are notified.
3. The patient's significant other person is notified by SMS of the access and location of the patient.

As part of this service the SIM service should be able to provide;

- Emergency access with special codes.
- Menu support for the needed transactions.
- Interface with the central application to trigger the special security measures above.

At the end of the transaction the user/patient will have their local and remote data updated (e.g. vaccination records, nutritional interventions etc.) and an entry will be made in the audit log documenting what data was accessed/ changed by what provider and time stamped, in addition to the special security transactions.

Use Case 5



Being able to query critical medical information for a child could be beneficial in making sure any nutritional supplements supplied are not going to trigger a reaction e.g. a nut allergy flagged when distributing a peanut-based nutritional supplement. It is also foreseeable that linking the distribution service to the authentication procedure could create an automatic alert to the agent distributing the supplement.

6. Emergency service authentication and access. This assumes that the patient is unconscious and there is no network connectivity

This case is the same as case 5 except for the lack of immediate network connectivity. In the case when there is no network access, the amount of data that can be accessed is limited to what is on the SIM, thus the need for In Case of Emergency information. This can be supported under certain limited conditions:

a. The patient is in an approved facility.

b. The providers are pre-approved for emergency access.

c. There is proper oversight to avoid abuse.

When a patient presents with an emergency and there is no network connectivity, their phone must still be available. The mHealth application is then launched by the provider or their assistant and an emergency code, pre-approved by the MoH and included in the application, is entered. The provider can then view the In Case of Emergency information. The same sequence can be followed if the SIM is removed from the patient's phone and placed in the provider's phone or tablet to provide easier reading of the data.

For security reasons, emergency access triggers three special actions in addition to making the medical record available when the phone with the SIM reconnects to the network:

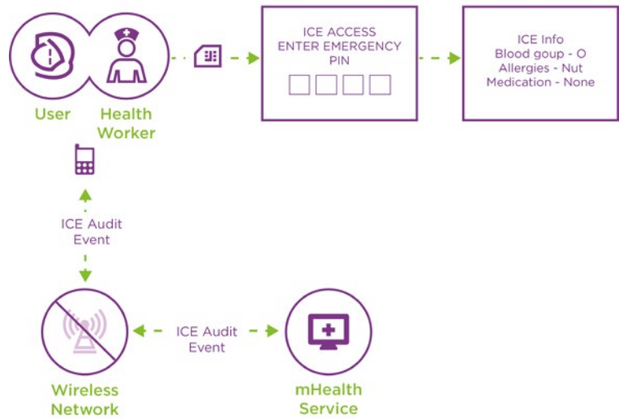
1. A special entry is made in the audit log.
2. The provider's supervisor and MoH are notified.
3. The patient's significant other person is notified by SMS of the access and location of the patient.

In addition to the capabilities of the service under use case 5, in this case the SIM service should be able to provide;

- Emergency access with special codes to the In Case of Emergency Information when there is no network connectivity.
- Menu support for the needed transactions.
- Interface with the central application to trigger the special security measures above, which can be delayed until the phone is connected to the network.

At the end of the transaction the provider will have accessed the In Case of Emergency data and the other notification measures described above stored until the phone reconnects to the network.

Use Case 6



In emergency situations where the speed of access and the accuracy of the information has a significant effect on the outcome, for a pregnant mother this might be when an attending midwife is not known to the mother, the midwife will have an immediate starting point (assuming a standardised system) for that information, especially where the mother-to-be in question is unlikely to be coherent or in a position to provide a medical history.

7. Support for patient or provider when their device or SIM is lost/damaged

Device loss and damage is not uncommon, especially in markets where SIMs are removed frequently. The process for providing support in these cases includes a centralised customer care facility which can be accessed over a different phone/SIM. The person needing the support calls the support number (which would be provided on their registration documentation) and authenticates to the customer care person (such as the MNO call centre) who will:

1. De-activate their mHealth service and if required deactivate network access and wipe their SIM (according to MNO policy).
2. If the new SIM has the mHealth application installed, ask the customer to authenticate and the new SIM will be linked to their health record.

a. If the new SIM does not have the application installed but the application can be installed Over The Air, download the application to the SIM.

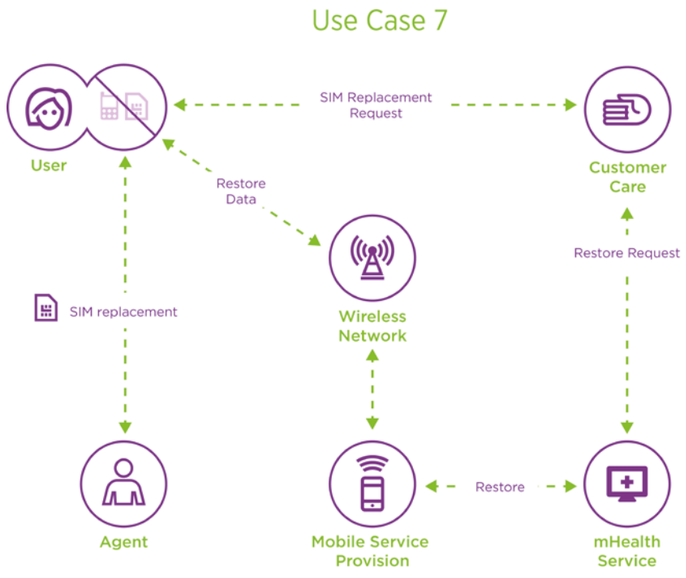
3. Download the In Case of Emergency data to the SIM from a central backup.

If the customer cannot provide sufficient information over the phone they are directed to an authorised agent to begin the process again. After they are re-authorised to the system their new SIM is linked to their medical record and the In Case of Emergency data will be downloaded to the SIM.

At the end of the transaction the provider will have been re-established on the network and mHealth application and the transaction logged in the audit file.

> **“Device loss and damage are not uncommon, especially in markets where SIMS are removed frequently. The process for providing support includes a centralised customer care facility which can be accessed over a different phone/SIM.”**

Use Case 7



8. Remote system integration

The SIM-supported mHealth application provides authentication of identity and approval to access medical information stored on a remote server. It can then link personally identifying information to that medical data if that file does not contain the personal identification. A key attribute of the system is it is open nature, that is, it can interface with different mHealth systems, including national governmental databases.

In order to allow for remote system integration there are administrative and technical requirements. Administratively the following needs to occur:

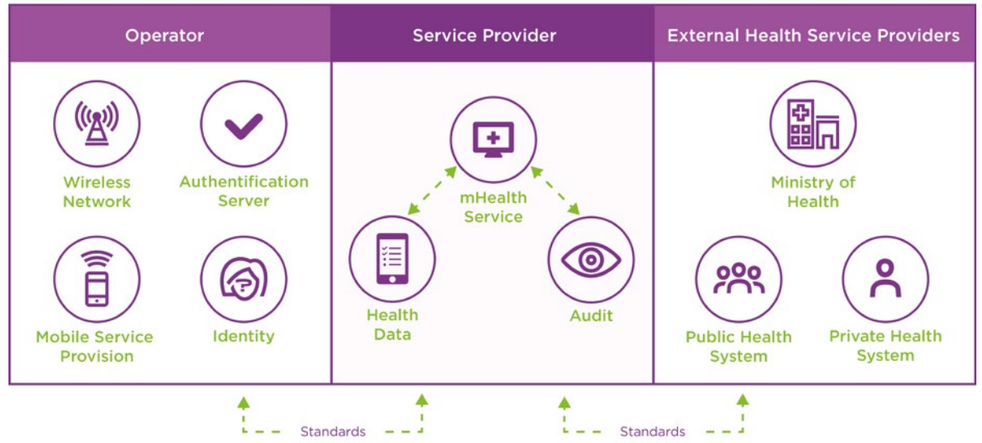
1. Before interconnecting systems, permission needs to be granted by the MoH and certain key standards agreed to. These include:
   a. Data ontology and conventions.
   b. The approved level of encryption and security.
   c. Compliance with national data sovereignty rules.
   d. Inviolable transaction audit.
2. The MoH can then provide information to the managers of the other system, including access credentials and technical documentation on APIs and other interface standards.

Technically the activities are:

1. The interconnecting system needs be technically capable of interconnecting.
2. The core SIM mHealth application will securely exchange data between it and the interconnecting system.
3. There needs to be a test process which the interconnecting system is required to pass before production begins.
4. The transaction, like all in the system, is logged in the audit file.

At the end of the process the MoH will have a list of interconnected systems and all transactions logged in the audit file.

Use Case 8



The provision of interconnected systems could only help improve the quality of care and outcomes for undernourished children, especially when treatment of disease is improved by the quality of the nutrition and key supplements that are needed on a regular basis. By interconnecting systems handling both treatment management and nutritional distribution services through a common SIM based authentication approach, it will help provide a more holistic and beneficial approach to the patient.
These systems will also provide key data and analytics which could help pinpoint failures in the overall process and recommend improvements to rectify the process(es).

Expanded use cases made possible by mHealth registries

The focus in this white paper is on the core applications and capabilities enabled through the use of SIM-supported mHealth authentication and data access. However the establishment of a national SIM-based mHealth system will permit the deployment of several other capabilities for government, MNOs, academics and other private sector players. Key among them are the use of data generated to enable improved epidemiological studies of disease spread, the use of the data and the transactional metadata, allowing the Ministry and other health officials to generate improved disease management and healthcare practices.

This can be critical in case of an epidemic because the network connection can help identify and track patients who may spread disease or help identify disease hot spots. The metadata can be used for routing service delivery tracking, but with the benefits of immediate reporting and a granularity on geography, provider type, treatment (or vaccination), etc. – all hard to collect with manual systems.

The ability to look at a nationwide database showing what services were provided to citizens, in what settings and by what kind of providers can identify best practices (and service gaps). By understanding the patterns of illness (and wellness) government and researchers can respond more quickly to epidemic outbreaks and even see if any prior treatments mitigated the disease spread. The kinds of analyses are limited only by the creativity of the researcher, and with the inherent security and privacy designed into the SIM-based mHealth platform, these kinds of research analyses can be performed quickly while still respecting the rights of citizens to privacy.

The mHealth platform can be linked to mobile financial transaction services to provide payment to community health and other health workers after confirmation that services were delivered (and when and where).

Thus the establishment of a secure, nationwide, SIM-based platform for mHealth can provide a wide range of capabilities and benefits to the country as well as to all the participants in the system. It is an enabler, rather than a limiter, in the use of a mix of technologies for mHealth, providing a standardised authentication and data ontological approach to mHealth services.

Feedback to providers on geographic basis (e.g. epidemic)

In the case of an epidemic the mHealth application's access to network information can help identify and track patients who may spread disease or help identify disease hot spots. Tied together with the personal information links, the MoH can also determine demographic trends or impacts (e.g. woman or older men more impacted, etc.) In addition, if the patient has a medical record, with any prior treatments or medications, this information can assist in helping to understand other factors that may also be relevant. Also it can help citizens/patients self-report for hot spot identification.

Reference architectures for deployment

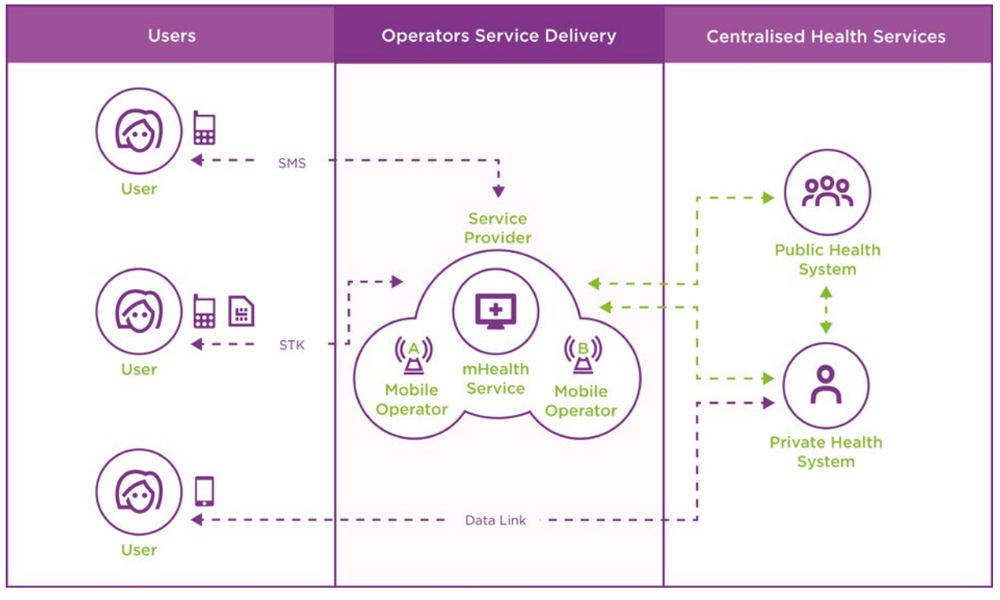
Technical

There are three major elements of the SIM mHealth platform:

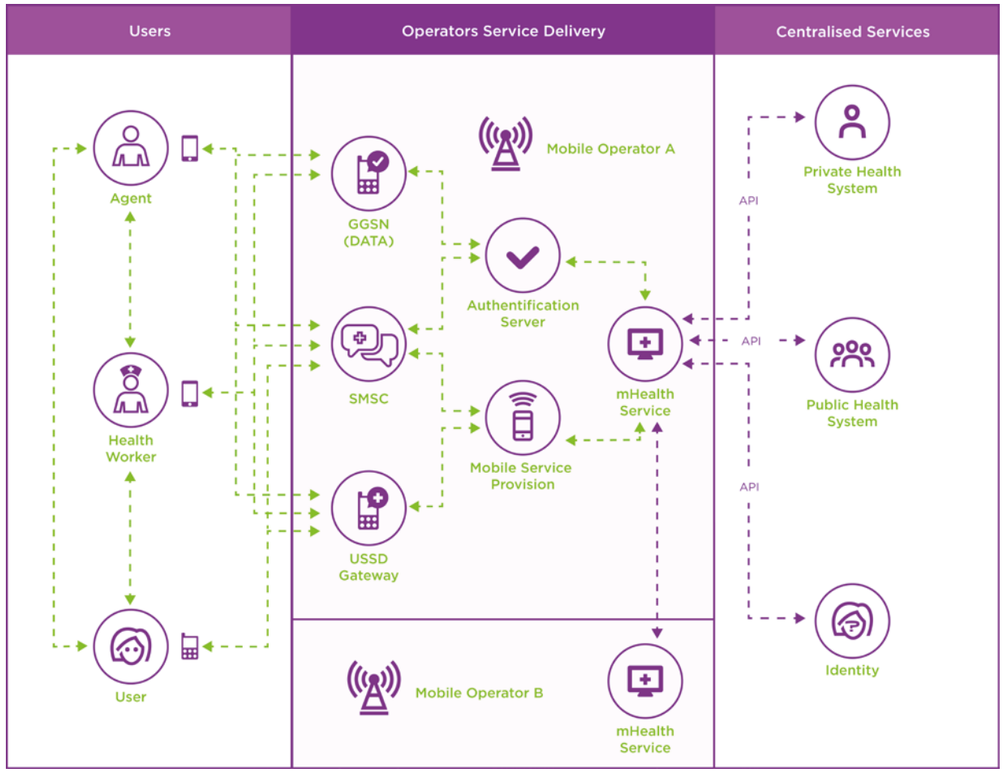
- The SIM-based application and associated UI (together with OTA download support).
- The network based authentication server and registration applications (these include linked healthcare service provider access authorization).
- The mHealth database and associated server with access and audit applications.

Each of these elements can be operated in a different environment or hosting location or they can be co-located. If they are co-located then the authentication server and mHealth database must be accessible by multiple operators (or each operator can operate a separate authentication server but these must be in sync in order to allow centralised customer support). It is assumed that the communications links between different back-end elements (authentication and database servers) will be encrypted and robust.

Base architecture



Multi MNO architecture



The SIM-based application with standardized UI could contain the following functions:

- Menu presentation (we are assuming that the MNO will select transport option when online and standalone when offline) for basic data access of locally stored information with language preference.
- Local data store of critical medical information.
- Network based interaction with application which will permit any required authentication and functional access.
- Access locking when too many invalid access attempts are made with central network notification including location data (GPS or Cell Site ID).
- Network transfer interface depending on transport provided by MNO.

> **“The system as a whole operates as a loosely-coupled one, permitting the distribution of the different elements and different physical and logical configurations.”**

The network-based server and applications support the following functions:

- Validation of SIM or server-initiated credential transaction
- Network linked applications and associated UI with language preference (see below for operational details) including menu presentation, third party authorisation, authorisation approval for mHealth database access, audit log, fraud detection and notification, lock-out function and customer care access
- Network and SIM server interfaces (APIs)
- Interface to mHealth database server and applications passing authentication data and access permit lifetimes

The mHealth database server and applications support the following:

- Authentication time control and interface with network based authentication mechanism
- Creation, reading and update of medical information
- Audit logging
- Web-based access and presentation
- Special device use (e.g. tablet or smart-application APIs)
- Fraud detection algorithms
- Third-party (e.g. National Health System) interfaces with APIs and authentication management

The system as a whole operates as a loosely coupled one, permitting the distribution of the different elements (the mobile device needing to be distributed by definition) permitting different physical and logical configurations. This means the system can have all elements centralised at one MNO (although this is unlikely) or have separate authentication servers but one mHealth database server which can be at the MoH, one of the MNOs or even a third-party data centre.

[12] *Ironically one mobile platform which doesn't support STK as standard is Android (although many vendors add STK support for continuity) which as the smartphone OS of choice in many developing markets, which could see upgrading users see a loss of key mobile services such as mobile money, although third party apps for STK are available.*

SIM basics

The SIM is essentially a small standardised 'smart' card, which is designed and built to be inserted into GSM (or UMTS) mobile phones. As the name suggests, this module identifies the user to the mobile network. It is issued by the mobile operator to a subscriber when they purchase a pre, post or blended payment plan and associated mobile phone number.

The SIM is not just a simple memory chip as many imagine. It is a functional microcontroller system, which has a CPU and supporting memory and storage (ROM, RAM and EEPROM) capabilities. When inserted into a mobile phone any request the phone makes is through an API to the microcontroller on the SIM. As a consequence the phone (and any supported applications on the phone) does not have direct access to the information in the SIM's storage but can only request set information from the SIM. This in part is what makes the SIM secure, along with the SIM's ability to do all relevant ciphering within the SIM and thus not expose any of its secure data (keys, etc.) outside of the SIM.

The microcontroller on the chip can also run programmes that have been installed on the SIM card. This is handled by the SIM Application Toolkit (SAT or STK) which is a standardised (3GPP) runtime environment that can be executed on all compliant SIMs and accessed by a built-in application on most (GSM) phones [12].

STK programmes can access functionalities of the host phone, e.g. user input, display output, data transmission, etc. Traditionally this was used by MNOs to provide basic content and network configuration functionality to users. In some cases this has been extended to providing financial services such as a mobile money STK application such as M-Pesa (Safaricom, Kenya). STK applications are typically limited by the size of the executable, the processing power (CPU cycles) available to them, storage they can use on the SIM and the speed of the serial interface between the SIM and the host phone.

A typical STK application size would be less than 10k, as the majority of SIMs in the market (especially in developing markets) will have a capacity of 64k (or less) both for applications and storage space. Applications are usually distributed either by pre-loading on the SIM prior to distribution or by an over-the-air (OTA) process for after-market applications. For OTA distribution the smaller the size of the application the better, but the OTA capability also allows for incremental downloads to the subscriber's SIM (and thus phone). This capability can make it possible for updated information to be made available to the subscriber and stored locally on the phone. In the case of a pregnant woman, the network could send updated messages about what to expect during different stages of their pregnancy, reminders of appointments, etc. Using the SIM and OTA capabilities such services can be included directly in a SIM-generated menu on the subscriber's phone, for quick and free access at any time.

The main purpose of the SIM is to respond to core phone and network functions, consequently the CPU cycles and RAM availability may limit the type of processing realistically possible by an STK app. Also the nature of the serial interface means that the speed with which data can be transferred between the SIM and the phone is limited to around 13k bit/sec.

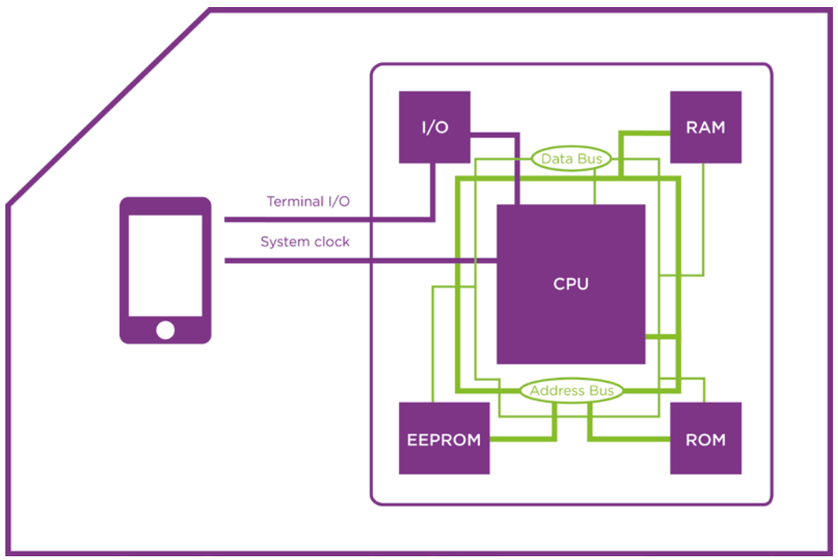
However the upside of STK applications is a near-universal reach capability, especially to basic and feature phone users, and security, both in respect of data held on the SIM and in access to security features on the SIM. Even with the constraints mentioned above, it is feasible to create quite sophisticated applications, e.g. mobile money, geo-fenced services, etc.

As an STK app is accessible on almost all mobile phones, from basic phones up to smartphones, it is easily discovered through a common MNO menu option on the phone. These services can be linked into the standard MNO service offerings to further aid discovery. As an STK app typically uses an encoded SMS (not visible to the user, other than through the STK app) as its data bearer, it inherits SMS's very effective push mechanism, which utilises the efficiency of the signalling channel on the network (hence it doesn't need to constantly poll across the network for unsolicited communications). This, combined with the STK's menu-based UI, allows for very effective and efficient push and pull mechanisms, important in delivering time-dependent information to patients, e.g. prenatal appointments, trimester information, medication reminders, etc.

The size of the SIM card has changed over the years. There are now four common sizes: standard, mini, micro and nano. Modern SIMs all use the same chip configuration irrespective of the overall size of the SIM. In most developing markets SIMs are typically supplied as the standard size and cut down to size for the phone, in effect just trimming off surplus plastic around the smart chip.

The SIM card itself holds two key pieces of information; the IMSI (International Mobile Subscriber Identity), and encryption keys used for authentication and ciphering. The IMSI is linked to the network's user identity including their MSISDN (Mobile Subscriber ISDN Number or Mobile Phone Number) and the included keys are used to authenticate the user against the network and what services they have access to. The keys also provide the means for encrypting the traffic between the phone and the network.

SIM architecture



For clarity, when phones are described as ‘SIM locked’ it is not because the SIM is locked to a particular phone but that the phone is configured so that it can only access one particular MNO’s network (this is where phones were originally subsidised by the MNO). Consequently, if you try to insert a SIM from another MNO the phone will only allow access for emergency calls.

In developing markets you will rarely see SIM-locked phones as the vast majority of phones are not subsidised, i.e. the user will purchase the phone separate from the SIM (and linked mobile plan) paying full price for the phone. This in part is why the retail cost and related taxes are important issues for Base of Pyramid (BoP) users and mobile adoption. It also explains why in these markets you see a preponderance of low cost basic/feature phones which support multiple SIMs in the same handset, allowing users to switch between MNO plans to get the benefit of cheaper tariffs for particular services (e.g. data, voice, etc.).

The use of SIM-based applications for mHealth provides a service and transport flexibility that other approaches cannot always address. While mobile data (2G/3G/4G/LTE) can be used for mHealth applications, these network resources are not always available in all areas or are adopted by users (e.g. data plan). USSD can be used wherever there is connectivity but, being a real-time protocol, can create traffic issues. Leveraging the SIM STK toolkit, developers can utilise the SMS as an effective data bearer (often in the form of binary encoded SMS) to use SMS to send and receive application data to and from the SIM, which can then process these and manage presentation to the user. Unlike human-readable SMSs, the binary encoded SMS can be addressed to a specific application on the SIM and, being binary encoded, can compact more information into a single SMS than a text message. Like human-readable SMS this transport mode is available whenever there is GSM network connectivity, and being asynchronous it can work well in both higher traffic and limited coverage environments.

It should also be mentioned that there are a variety of SIMs available for mobile phones that, while not yet widely adopted (yet), could prove useful, e.g. PKI SIM, which includes advanced encryption technologies. Another item which should be factored in is SIM cost, which is typically sub $1. This means that SIM distribution is more cost effective than upgrading phones and more often than not the cost of the SIM is absorbed by the MNO as part of their customer acquisition cost.

Bibliography

1. Federal Identity, Credential, and Access Management, Trust Framework Solutions; Trust Framework Provider Adoption Process (TFPAP) for Levels of Assurance 1, 2, 3 and 4, Version 1.1.0 , March 2013
2. Mendoza, Okoko, Konopka and Jonas, Management Sciences for Health. mHealth Compendium, Volume Three: African Strategies for Health project, November 2013
3. GSMA Mobile Identity Team, Birth Registration in Sub-Saharan Africa. A case study of Orange Senegal and Uganda Telecom solutions 2012
4. Mobile Connect - http://gsmamobileeconomy.com/gsmamc/
5. Example of SIM STK: http://developer.nokia.com/community/discussion/showthread.php/106756-SIM-Application-Toolkit-support-by-Nokiaphones

Other Readings

1. Payne, Standards and Interoperability in Mobile Health , Mobile Health Alliance, March 2013
2. BJO RKMAN JAKOB SVENSSON Bjørkman and Svensson, Power to the People: Evidence from a randomized filed experiment on community-based monitoring in Uganda, The Quarterly Journal of Economics, May 2009
3. Sax, Kohane and Mandi, Wireless Technology Infrastructures for Authentication of Patients: PKI that Rings. Journal of the American Medical Informatics Association Volume 12 Number 3 May / Jun 2005
4. GSMA Concept paper, The SIM: The Key to Better Healthcare? November 2011
5. Abu-Faraj, Barakat ,Chaleby and Zaklit ,A SIM Card-Based Ubiquitous Medical Record Bracelet/Pendant System - A Pilot Study, Proceedings from the 4th International Conference on Biomedical Engineering and Informatics, 2011

Abbreviations and terminology

API – Application Programming Interface
BoP – Base of Pyramid
CDRs – Call Data Records
CHW – Community Health Worker
CPU – Central Processing Unit
CSR – Corporate Social Responsibility
EEPROM - Electrically Erasable Programmable Read Only Memory
EHR – Electronic Health Record

IMSI – Internal Module Subscriber Identity
KYC – Know Your Customer
LoA – Levels of Assurance
mHealth – Mobile Health
MNO – Mobile Network Operator
MoH – Ministry of Health
NGO – Non-Governmental Organisation
OTA – Over-the-air
RAM – Random Access Memory

ROM – Read Only Memory
SAT – SIM Application Toolkit
SIM – Subscriber Identity Module
SMS - Short Message Service
STK – SIM Application Toolkit
UI – User Interface
USSD – Unstructured Supplementary Services Data
UUID – Universally Unique Identifier
WHO – World Health Organization

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting nearly 800 operators with more than 250 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and Internet companies, as well as organisations in adjacent industry sectors. The GSMA also produces industry-leading events such as Mobile World Congress, Mobile World Congress Shanghai and the Mobile 360 Series conferences.

For more information, please visit the GSMA corporate website at www.gsma.com.
Follow the GSMA on Twitter: @GSMA.

About GSMA Mobile for Development - Serving the underserved through mobile

GSMA Mobile for Development brings together our mobile operator members, the wider mobile industry and the development community to drive commercial mobile services for underserved people in emerging markets. We identify opportunities for social, economic impact and stimulate the development of scalable, life-enhancing mobile services.

For regular updates follow us on Twitter @GSMAm4d

About GSMA Mobile for Development mHealth

The GSMA Mobile for Development mHealth programme brings together the mobile industry and health stakeholders to improve health outcomes in emerging markets, with initial focus on Millennium Development Goals 4, 5 and 6 across Africa. The programme convenes key stakeholders using many forums including working groups and workshops, as well as providing resources and support to identify partnership opportunities to bring mHealth solutions to scale.

For more information on the GSMA's Mobile for Development mHealth programme - mhealth@gsma.com
http://www.gsma.com/mobilefordevelopment/programmes/mhealth

This document is an output from a project funded by UK Aid for the benefit of developing countries.

The views expressed are not necessarily those of UK Aid.