Mobile Health

Market Entry Toolkit

Mobile Health Technology and Architecture:

A Practical Framework for Technology Assessment for Mobile Health

Kai-Lik Foh, Mobile Health Programme Manager, GSMA – kfoh@gsm.org

September 2011

Contents

Introduction

This paper aims to help mobile industry develop a strategy around the architecture that is needed to deliver on Mobile Health strategies, including the extent to which existing infrastructure can be leveraged, which net new capabilities need to be created, considerations for integration into other systems from other partners and stakeholders. Rather than aiming to design a common technical architecture that supports all possible products and services, we list out all the different types of technical questions that would need to be considered before developing an architecture. Different mobile players will then be able to assess, depending on their own in-country technical assets and business strategy, which capabilities to develop in-house and which to partner/outsource.

This paper constitutes the first part of a larger Mobile Health Technology and Architecture workstream within the GSMA's Mobile Health Market Entry Toolkit (MET), which is being developed to provide a framework for investigating the considerations that the mobile industry needs to evaluate upon entry into the Mobile Health market.

eHealth vs mHealth Architecture

One of the debates in technical architecture in the Mobile Health space is the extent to which it is similar to (or different from) considerations in developing an eHealth architecture. eHealth architectures are typically designed by two broad groups:

a) Government national health IT bodies – which have public health and disease surveillance as the critical need and the citizen (insofar as he or she is a consumer of public health) as the critical stakeholder.

b) EMR solution providers – which typically have the automation of healthcare delivery processes as the critical need and the healthcare professional as the critical stakeholder.

Central to both is the importance of the single longitudinal health record and the different ways in which this record is used and populated.

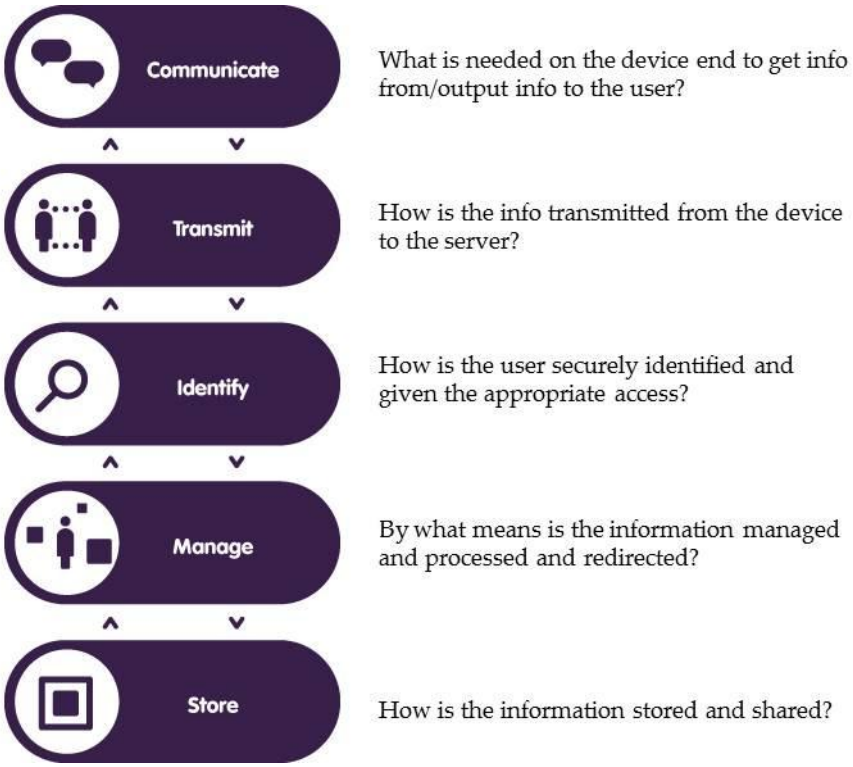
In contrast to the above, mHealth architectures have typically focused on the mobile channel of delivery and assorted ways in which health can be delivered through that channel. In addition, there is added emphasis on technical considerations on the device itself – whether it is the phone itself or the extent to which it can connect to medical devices (or even if the medical device itself is connected through the mobile network). Unsurprisingly, there are a wide variety of different ways this can be presented. The architecture that is needed to support a health tips service via text, a voice-enabled health hotline service, and a chronic disease management service enabled by remote monitoring devices all require different architecture decisions.

In designing a method that encompasses both these perspectives (bearing in mind there are MNOs that also want to pursue eHealth as a broader strategy), we start with a categorisation of technical considerations with a typical mobile operator in mind, and discuss the net new capabilities (and associated infrastructure, technologies, standards, regulations and integration requirements) that are needed to deliver on a variety of typical Mobile Health use cases as illustrated by the Product and Services workstream of the GSMA's MET.

Categorisation of Key Technical Concerns

The considerations starting from the end-user device and ending with the storage on the back-end, which we have found to be a useful framework for segregating considerations and design options for a comprehensive discussion of technical issues for any Mobile Health roll-out, are outlined in Figure 1.

Figure 1: Categorisation of Key Technical Issues for Mobile Health Roll-Out



Communication

This is the layer that faces the user. The device in question can be a mobile, a mobile-embedded device, or in the case of provider-facing health solutions, even computer terminals or other input/output devices that receive and output medical information.

The component considerations begin from the use case of the product in question, and in particular how the user will interact with the device and how it fits with his or her lifestyle. Some of the considerations to factor in are the following:

- Form factor of the device – e.g. big and easily readable keys if the end-user is an elderly consumer, rugged if it is meant to be used in dusty terrain, screen size if images/videos are a part of the product.
- On-board capabilities – e.g. GPS if location services are needed, camera (resolution) if images need to be transferred, speaker if the device is being used as an education tool.
- Operating system that determines what kind of processing capability it can handle – e.g. SIM, Java-enabled, iOS, Android, etc.

- On-board applications – e.g. the service may well rely on specialised health applications. These apps will have an impact on the way the consumer interacts with the product, which in turn depends on the type of operating system on-board and the way that applications are loaded onto the device.
- Multi-lingual capability depending on the need of the target customer group.
- Connectivity to other medical devices if remote monitoring is a part of the service – e.g. Bluetooth, etc.
- Power requirements depending on where the device will be used – e.g. long battery life may be needed for rural settings and end-users that spend extended time away from a power source.
- Device-side security – depending on the security model of the service provided, the device may be used in conjunction with additional security features like PIN passwords, voice-print recognition, biometric security to allow access and input (and corresponding output) from the device. There may also need to be encryption provided depending on prevailing regulation.
- On-SIM capabilities – e.g. if a SIM menu is used as the main user interface, or if the SIM is used to store key authentication information (or health information).

Competency in managing phone technology is taken as given, as well as the MNO's experience of rolling out other VAS. Security of information may also be an existing competency depending on other services (notably, if the MNO has rolled out a mobile money product already).

However, there will be areas where a more comprehensive strategy will need to be developed from scratch e.g embedded mobile devices (will need an in-depth look at what protocols the embedded device would need to comply with to communicate with medical devices) or rolling out a hosted eHealth service for healthcare providers (where it will have to develop/acquire capabilities on managing EMR clients).

Transmission

This refers to the component considerations that result from what type of information needs to be transmitted over the wireless network from the device to the service provider, and include the following:

- Format – voice, text, data and video, which are tied directly to the product offering in question and have an impact on the type of network requirements i.e. 2G, 3G, or even between GSM or CDMA as a consideration of which type of network connectivity is required.
- Protocol – GSM or CDMA depending on priority of data over voice and vice versa. Can also be WI-FI (although this may not be popular in the context of an operator whose revenue strategy depends primarily on network usage).
- Coverage – particularly if the service is designed around helping places access healthcare in remote areas. If there are areas where there is no coverage, the service may well to have an offline as well as an online component (e.g. for content to be downloaded into the device and then synched up when network coverage is available).
- Availability – depending on the service quality that is being marketed (e.g. if it is an emergency hotline service), to what extent can constant availability be guaranteed. These are also critical considerations for provision of EMR/EHR systems over the Cloud.
- Bandwidth, which comes into consideration if the service is reliant on large volume data transfer, for example for high-res diagnostic quality images (a typical diagnostic quality radiological image or specimen image for pathology would be in the 10MB range) or video.

Managing network transmission of all the services mentioned above is taken as given. While no net new capabilities are needed, considerations for coverage and availability will be different for rolling out Mobile Health services (which carry significant liability) than for rolling out consumer services.

Identification

Once the information or request reaches the service provider, there is a need to securely identify the source of the information, establish whether or not the request can be put through based on the identity (and potentially the role) of the requestor. While there is already a certain level of security already inbuilt within mobile communications at present, the level of incremental security put around Mobile Health solutions is largely driven by regulatory requirements and local expectations of personal security and personal privacy.

- Server-side security – these are considerations that are paired with whatever encryption and authentication features are provided and required at the device end.
- Identity – while MNOs are currently able to use the device as a proxy for identifying the user, more robust methods of establishing identity (tied in with an appropriate security strategy) will have to be considered if medical information is being transmitted (e.g. using passwords, or in advanced cases voice recognition or some other biometric identification). For services that connect into an electronic medical record of some sort, there will also need to be identification not only of the individual, but the role the individual has in relation to the record being accessed (e.g. an attending doctor vs a new doctor) and the rights that role has to that individual. Role-based identification and access are typically built into the functionality of most mature electronic medical record systems.
- Consent – Consent considerations really only matter if the MNO is interested in rolling out a system that collects/shares medical record data. One needs to consider the different types of consent models and also different needs for parts of the record to be "hidden" (for example, if HIV status is recorded somewhere). Again, most mature electronic medical record systems should have this capability. However, what the MNO needs to consider is the extent to which it may impact one's device strategy, particularly if the device is the means by which consent is taken.

Managing security of the transaction as well as identifying the device and owner of the signal is already an existing capability of most service providers. Net new considerations only need to be considered if personal health information is being recorded and accessed. There will then be a need for a strategy around unique patient identification, role-based access and consent-taking.

Management

Upon the request being validated as being appropriate for the service in question, the MNO would need to consider the different applications which map to the product and service in question. There can be a great variety of different services provided, as many as there are different types of Mobile Health services. Here we illustrate a few key ones corresponding to what is currently in the market:

- Health Content Management – these involve the distribution of general health content based on generic profiling of the customers. MNOs should already be very familiar with these models, as they are no different from existing information VAS models for news, sports, entertainment and so on. The only difference is the sourcing of the content providers and how they interact with the existing VAS infrastructure owned by the MNO.

- Health Knowledge Applications – these are distinguished from Health Content Management in that they incorporate specific medical knowledge and rules. In addition, the usage of these systems is significantly more regulated than Health Content Management systems. They range from decision support tools with medical knowledge bases behind them (often with prescribing content), to tools that incorporate care pathways (typically for chronic disease management services).
- Health Service Directories – these are applications, packaged with other services in this category, which are integrated into and create referrals into other components of the health system (like clinics, hospitals, or emergency services), usually through appointment scheduling services.
- Medical Call Centres – these applications revolve around the provision of health advice over the phone connecting health professionals to consumers. Core technologies are no different from normal call centre and CRM (Customer Relationship Management) technologies, which some MNOs should already be familiar with. However, there are several key considerations around the health personnel that man these lines, and how calls are routed to them. In many developing countries, health professionals are a rare resource to begin with and manning a call centre will require drawing upon these scarce resources.
- Billing and Cost Management – these are typically competencies already possessed by MNOs, but additional capabilities may need to be considered if billing needs to be integrated with insurer systems
    - Service costs
    - Transaction costs
    - Customer billing
    - Corporate billing
- Service Management – also currently possessed by MNOs, but with additional capabilities also needed if these services need to apply to specific medical devices or health applications which are outside current domain of knowledge
    - Provisioning, deployment and upgrading
    - Fault management
    - Configuration management

Billing, cost management as well as service management should already be competencies possessed by MNOs. The main considerations are in the selection of health applications that suit the service being rolled out to the market, the degree to which they should be outsourced, and the level of integration needed to existing carrier systems.

Storage

- Records – these are systems which govern the storage and management of both non-clinical and clinical data. There will be incremental data management requirements even with non-clinical services, but with the storage of actual health data or health media there will be a completely different set of regulatory and architectural considerations. The key considerations behind the provision of electronic medical records are around the use case – whether or not it is just for personal use by the individual (Personal Health Record), or for clinical use that has much deeper needs which are structured around the clinical workflow for hospitals and healthcare providers.
    - Administrative Data – Customer ID, billing history
    - Health Data – EMR / PHR / MHR etc.
    - Media – PACS

- Messaging Standards – HL7 is the main standard for health data exchange. However, there are many versions of this standard and they are typically not backwards compatible. IHE profiles are a way in which subsets of HL7 components have been defined for use in specific use-cases.
- Coding Standards – applying also to health data, they are standard clinical codings of diagnoses and clinical content (e.g. SNOMED and ICD10). Most EMR systems are compliant to these standards. DICOM is the primary coding standard for health media (i.e. radiological images).
- Integration into non-Health Systems – theoretically, if clinical data can be paired with the customer and location data already possessed by MNOs, this could represent a significant competitive advantage. This may be the future direction of MNOs participating in the EMR space.

As with the Management section, MNOs should already have some capability to store customer data, billing and transaction data. Net new capabilities for storage would come at two levels: 1) storage of new customer data which is not health related (e.g. customer profiles which drive SMS reminders on when to take your next pill, or when to go for your next appointment), and 2) storage of actual personal health data. The latter represents a significant additional layer of considerations whether the service provider decides to partner with an existing health record provider or decides in invest in their own capability. These range from navigating complex local regulations on privacy, data storage, security, consent, as well as considering the legal liabilities and responsibilities needed to accurately host medical data in a world where information is used in life-or-death situations.

In Practice: Technical Considerations for a Health Hotline

The above considerations are applied for a health hotline service to illustrate the usage of this framework:

1) Communication

   As the exercise is to cater to as broad a handset audience as possible, there are no key device side considerations – anything that can carry voice will suffice.

2) Transmission

   Network considerations are basic, so a 2G transmission is sufficient. However, there may be availability or coverage considerations if the service is meant to carry emergency services or have 24/7 availability.

3) Identification

   This depends on whether the service is meant to provide advice based on a single encounter or whether the service also carries with it an on-going monitoring function to cater for repeat calls. The former carries with it no identification requirements, whereas the latter will have to be integrated into a simple health record system (but will have to adhere to local regulation on access of a health record and all the standards that will entail).

4) Management

   The key consideration is the CRM software and the knowledge base used to provide the service. For basic services where health advice is provided by health professionals, the system only needs to redirect and load balance calls (and depending on the staffing strategy, cater for redirection to remote staff). For services that offer more specific health advice, there may be incorporation into simple decision support systems which provide health advice through a health knowledge base.

5) Storage

   Health advice services will not require unique storage requirements. However, for those which cater for repeat calls, this will entail integration into a health record system of some description.

There are wide variety of different use-cases to which these considerations can be applied, ranging from remote monitoring using embedded devices for the chronically ill end-consumer, to hosted eHealth solutions for healthcare providers, to corporate solutions for insurers and pharmaceutical companies. We are working to develop a number of these use-cases for the future.

Next Steps and Future Research

The above aims to describe a practical process by which a potential Mobile Health player can consider major technical topics, prior to developing an architecture to support the roll-out of any particular Mobile Health service (or before considering which technical components to outsource and to who to outsource to). Further details of some of the component pieces, as well as the debate around data standards, can be found in the GSMA document: An Introduction to Mobile Health Architectures.

Further research from the GSMA will include:

- Detailed architectures for sample use-cases for other Mobile Health products and services, along with the practical technical issues and challenges involved in rolling out such use-cases.
- An analysis of the different technology players that are in the market supporting some or all of the technical capabilities listed above.