Enabling mHealth While Assuring Compliance
Reliable and Secure Information Access in a Mobile World

Axel Wirth

mHealth is defined as the practice of medicine or the provision of health services supported by mobile wireless technology. This includes the utilization of consumer mobile devices such as tablets or smartphones but also purpose-built systems such as home monitoring equipment. These advanced features are provided through a wide range of mobile technologies such as Wi-Fi, 3G, 4G, GPS, Bluetooth, or Zigbee. Functionality relies on an infrastructure of private and public networks for voice, SMS, MMS, data, and other messaging services.

mHealth has the opportunity to fundamentally transform the way providers deliver healthcare and how patients consume health services. This will lead to, for example, new and more flexible care models, access to mobile diagnostic devices, secure sharing of clinical information, clinical collaboration, and continuing educational opportunities.

For patients, mHealth can provide improved access to their health information, more consistent and reliable health services, flexible communication with their physicians, and access to enhanced education. As patients become more adept at communicating with their caregivers and recording important health information, their ability to participate in decision making and the care process will also be enhanced.

Taking healthcare services mobile will fundamentally alter the way healthcare providers and patients interact, enabling a shift towards a more open healthcare system—away from the traditional hospital-centric model to a more patient-centric model.

mHealth has the potential to empower patients and make them more active participants in the care process, all made possible through the improved information exchange in the mobile ecosystem. The goal is to enhance quality of care, improve continuity of care, and provide access to many different kinds of health services, independent of patient or clinician location.

As part of Health Information Technology for Economic and Clinical Health (HITECH) of the American Recovery and Reinvestment Act (ARRA), the U.S. federal government has provided $19 billion in incentives to encourage medical providers to adopt and use electronic health records (EHR). At the same time, clinicians are embracing mobile technologies through the adoption of teleHealth and other mobile services at rapid speed.

We are seeing an unprecedented combination of push (government incentives) and pull...
mHealth Challenges

Data Deluge
Information generated by EHRs, picture archiving and communication system (PACS), billing, and customer care systems increases the need for secure, robust, and clean bandwidth that is growing as rapidly as the need for data availability, business continuity, and efficient storage management. Not least is the necessity of providing timely information access and audit trails for regulatory requirements.

Regulation and Compliance
Healthcare regulatory requirements such as HIPAA, government agencies such as the FDA or HHS, state agencies, etc., are implementing standards and regulations with stricter requirements and higher penalties for non-compliance. In addition to the clinical data alluded to previously, providers must also collect data to support regulatory reporting and be used to demonstrate compliance (e.g. audit logs). All this data must also be retained for secure retrieval and discovery in the event of legal challenges.

Privacy
Security and privacy concerns around personal information in the wireless ecosystem are justified. Data must be tracked and encrypted; access should be managed reliably through a public key infrastructure (PKI), enabling users of a non-secure public network such as the Internet to securely and privately exchange data.

Certification and Authentication
Multiple concerns need to be addressed under the umbrella of certification and authentication. Is a user authorized to access certain information? Is a device authenticated to operate on the network? Is an app certified and approved to be installed and used? These complex questions can only be addressed through a reliable automated system that can ensure the desired level of compliance without impacting user productivity.

Insider Risk
With greater power to access information remotely comes greater opportunity for knowledgeable and privileged insiders to take advantage or cause problems, sometimes unintentionally. Information monitoring solutions such as data loss prevention (DLP) can identify the location and prevent the release (accidentally or intentionally) of privileged information.

Cybersecurity
Cybersecurity for a mobile health infrastructure is a personal and national security concern. Networks and devices connected to the Internet have been demonstrated to be vulnerable to cyber-attack, for the purposes of monetary gain, identity theft, or in the case of medical records, possible blackmail.

(physician adoption of mobile workflow), both leading to a shift in how we access and deliver health information and services. In addition to provider incentives, HITECH and ARRA include funding for initiatives to improve healthcare access, including broadband improvements for rural and underserved areas. Manhattan Research estimates that over 81% of U.S. physicians and other healthcare workers use smartphones and tablets.2 App stores (Apple iTunes and the Android marketplace) list over 12,000 apps for mHealth of which many are used for remote monitoring and health management. App functionality ranges from personal fitness, weight management, patient reminders, and clinical communication, to remote monitoring.

But with all the rich opportunities in mHealth, there are also some challenges. In general, consumer acceptance of mHealth is growing, but there are concerns about maintaining privacy, record integrity and authenticity, as well as preventing improper access which could lead to breaches, medical, and billing errors.

In addition, federal and state regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA) Security Rule requirements for information confidentiality, integrity, and availability must be met. Understandably, consumers express concerns about cybersecurity, medical identity theft, reliability and accuracy of clinical information, and the availability of their Electronic Health Records (EHR).

From a provider perspective, many mobile health use cases lead to direct cost and time savings, as the rapid adoption of tablets and smartphones by physicians and nurses suggests. But other use cases, for example home care or remote monitoring, may require changes to reimbursement models to remove financial adoption barriers.

In addition, technical barriers exist, such as accessing data on traditional, hospital-based information systems, like the EHR, on mobile devices with very different user interface constraints. However, we are starting to see new and exciting mHealth technologies on the horizon, such as wireless pillboxes, secure dispensing, remote monitoring, real time location tracking system (RTLS), and mobile computerized physician order entry (CPOE) systems.
Communications service providers are being asked to ensure that there are no disruptions in mobile access, provide the quality of service (QoS) necessary to maintain reliable care and real time feedback, and eliminate gaps in coverage and inconsistent bandwidth. In fact, standards work is underway to define high-reliability, medical grade networks, and assign a dedicated spectrum for critical health data.¹

The problem we need to solve is an obvious one: how do we derive cost and clinical benefits from mHealth opportunities, maintain privacy of information and securing the infrastructure, and not impact clinical workflows or patient care? Only well thought-through, automated IT management and compliance solutions will enable us to solve this conundrum.

A New Information Management Paradigm
The advance of mobile use cases and user-based trends like BYOD/BYOA (bring your own device/bring your own app), combined with new storage and delivery platforms such as the cloud and increasingly virtualized platforms, make the task of securing our infrastructure even more complex.

Only a few years ago, a common security paradigm asked for complete protection from “edge to endpoint.” But this is no longer sufficient. Where is the edge when your users utilize cloud-based services? How do you control your endpoint when the device in question is mobile and possibly owned by the users themselves?

These trends require shifting to a totally new information management and protection paradigm: from a device-centric to an information-centric approach. It’s not about the device, it’s all about the data.¹

mHealth Scope and IT Impact
The great opportunities afforded by the deployment of mHealth technologies for automation, management, cost, and consumer/provider empowerments also come with some challenges. mHealth relies on the availability of secure and sufficient bandwidth for networked enabled devices, clean and secure information transfer to EHR, greater collaboration, and connectivity among healthcare professionals.

All of these unfortunately increase risks, vulnerabilities, and the incidence of security attacks. A few challenges associated with mHealth are listed in the sidebar—these are not new and have existed long before in the traditional “wired” world; but introducing mobility into the picture compounds the problem.

A Comprehensive, Layered Approach, Applying the Right Technology In the Right Place
Deploying mHealth solutions in an institution or across a larger public infrastructure requires a strategic end-to-end approach which maps the appropriate security and protection technology to each component of the ecosystem.

It is essential to employ a comprehensive, layered security approach, sometimes called “defense in depth”. “Defense in depth” refers to more than just technical security tools; it includes compliance automation, and ensures that users do not inadvertently risk confidential information exposure.

A comprehensive approach therefore also implies policy and operations planning, user training, compliance controls, information life-cycle and IT/risk management, and defense against attempts to gain unauthorized access to restricted information resources. It is also essential to recognize the need for high availability and system redundancy.

mHealth Example Use Cases
According to the World Health Organization (WHO), “the use of mobile and wireless technologies to support the achievement of health objectives (mHealth) will transform the face of health service delivery across the globe.”²

We are only at the beginning of a market-changing trend, and the range of use cases is wide. Four representative scenarios of evolving mHealth use cases and a discussion of their IT implications are:

1. Access to Resources
Doctors and nurses are constantly on the move, providing healthcare at the patient’s location, inside the hospital, as well as outside. Accessing relevant clinical information resources, such as patient charts or PACS images, becomes a must-have capability. Nurses use tablets to...
review patient charts at the bedside, and doctors use their smartphones to review patient’s lab results or authorize orders.

But this has to happen while maintaining privacy and security, and guaranteeing the confidentiality, integrity, and availability of sensitive electronic protected health information (ePHI). To support mHealth on an infrastructure level requires a highly reliable, medical grade network and sufficient bandwidth, both on the hospital’s private network as well as on public communications networks.

Protecting and securing all communication channels, such as SMS, MMS, e-mail, and web access, is critical to providing reliable services. Note that at the time of this writing, a common definition or a standard for what constitutes a ‘medical grade network’ does not exist. However, efforts are underway to establish such guidance.

In addition to infrastructure, confidentiality and integrity of information that is transmitted and stored must be protected. Encryption technologies can be implemented on the network level for data in motion (e.g. by using the appropriate wireless encryption protocols, like WPA2 for a private network), as well as on the device level (e.g., encryption tools) to protect data at rest.

Encryption always goes hand in hand with an appropriate key management system, be it provided through exiting standards (like WPA2 Enterprise) or commercial tools integrated with directory management services. Encryption addresses confidentiality requirements on a technical (data) level.

In addition privacy and information integrity must be ensured through identity and access management solutions (such as VeriSign PKI). Strong authentication services should assure reliable authentication, and DLP can be used to monitor users and protect data from misuse.

Many modern products allow for efficient and reliable management of institution as well as user-owned devices to assure reliable operation and compliance with corporate policies, without impacting end user productivity or reliability of services provided.

2. Point of Care Documentation

Today’s healthcare environment is burdened by administrative requirements and the need to document not only from a clinical but also regulatory and administrative perspective. The objective of these documentation requirements is to improve patient care, monitor progress but also compliance, and provide input to administrative processes like billing or resource management.

However, clinicians may feel that this takes time and attention away from their patients. Modern technology can minimize the impact of these administrative tasks, maximize staff efficiency, and improve documentation quality by, for example, enabling bedside charting on tablet devices or providing computerized physician order entry (CPOE) functionality on smartphones.

Point of care documentation usually occurs inside the hospital and on the private network. Some use cases require public network access, for example for home-visiting nurses. Protecting confidentiality and integrity of data stored on devices as well as data in transit can be accomplished by utilizing the right encryption technologies.

Both encryption and authentication systems require an automated key management system, ideally integrated with the enterprise identity management system of choice (such as Lightweight Directory Access Protocol or LDAP).

3. Professional Communication

Utilizing mobile technology to enhance healthcare delivery and improve quality of care enables efficient and secure knowledge exchange and communication among clinicians. This type of communication will, in most cases, span healthcare organizations and be a mix of proprietary (e.g., PHI) and general (public) information. DLP and data separation enables compliant coexistence of proprietary and public data, allowing open communication where needed, and preventing potential patient privacy violations.

This can be complemented with encryption and authentication technologies, as discussed previously, as well as automated mobile management solutions, providing for standardized ways of managing device configuration, deploying applications, and monitoring device compliance and user behavior.

Ideally, regulatory and technical content should be automatically mapped to policies.
and updated as regulations or corporate policies change. Utilization of cloud-based messaging services (including cloud-based security, encryption, and data loss prevention) allow for an efficient cross-enterprise message exchange platform.

4. Mobile Monitoring
All nations are facing future healthcare delivery challenges based on aging populations, driving the need to manage more patients with their chronic disease for a longer time. One solution is to enable home-based care and monitoring, enabling patients to remain in familiar surroundings, independent, and active.

A key requirement of these novel care models is a reliable and secure public network infrastructure. In addition to the device-based solutions discussed, communications service providers are implementing network-based technologies, to assure confidentiality of critical data transmitted across their networks, independent of the communication channel of choice: private or public network; email, SMS, or web based communication.

In addition, advanced high availability and backup solutions allow the underlying endpoint and server infrastructure to function with minimal risk of downtime, enabling quick restoration of device data and settings in case of loss or replacement.

Policy Driven Security and Compliance Approach to Prevent, Detect, and Respond
Numerous automation tools exist to help hospital IT staff deploy, manage, and secure mobile devices and information. Industry groups and government agencies are developing guidelines and are adapting standards to fit this new paradigm, and to address the following requirements and goals (summary):

Securing Healthcare Systems and Operations
The healthcare industry is at high risk of data breaches. Hospitals’ and physicians’ medical records are aggregators of birth and death records, and patient demographics (including bank information)—data that allows identity theft to go undetected for long periods of time, making it a prime target for cyber threats.

Healthcare IT is critical for accurate record keeping and clinical cooperation, and is the heart of managing and controlling good healthcare, even though for healthcare professionals and consumers it is not central to their every day mission.

The end user, clinician, or patient, should be able to use IT solutions and access mHealth solutions, without the need to worry about security and privacy. These are physically secured environments with protected perimeters, where the hard-earned security knowledge and techniques learned from years securing networks and complex datacenters can be applied.

Rigorous security can be implemented but should not impede operational effectiveness or clinical care. This environment can profit greatly from the deployment of advanced security solutions which will harden the environment, detect anomalies, and respond to threats, while continuously monitoring the interaction of this environment with remote medical devices and the Internet.

Managing the Data Explosion
Given the increased amount of control, status, and other information generated from mobile health environments; and with the potential deployment of hundreds of thousands if not millions of mHealth devices and diagnostic tools, it is no wonder that storing, reporting, analyzing, managing, protecting data while protecting customer privacy, and controlling critical information is high on the list of concerns for medical providers and their chief information security officers (CISOs), operational, and IT staff.

It has been estimated that millions of new mobile diagnostic apps would result in hundreds of additional petabytes (PB) of data to be managed. Storage challenges exist, from categorizing the information sufficiently to demonstrating regulatory compliance, proof of accurate customer billing, and responding to potential legal action. In addition, tracking and analyzing information to efficiently operate and respond quickly to emergencies, natural disasters, and possibly pan-epidemics also pose a significant challenge.

Utilization of cloud-based messaging services (including cloud-based security, encryption, and data loss prevention) allow for an efficient cross-enterprise message exchange platform.
**Embedding Security With the Data**

With different generations and types of technologies, and standards that are complex but not yet homogenized, it is critical yet difficult to assure that information is secured. One approach is to embed privacy with the data itself: Encrypt the data and authenticate every device the data touches.

In short, confidentiality, integrity, and authentication are essential to expand and gain acceptance of mHealth enabled devices. However, truly encrypting and authenticating the mHealth environment means managing certificates and keys at a significant scale.

As increasing number of mHealth devices have certificates/keys installed at the time of manufacture, embedded device manufacturers and hospitals need to have a means to issue, enroll, expire, revoke, validate, and generally manage certificates. Automated solutions can help solve these problems, for example through hosted PKI solutions which can operate on premises to manage certificates or even provide a managed service to perform this essential set of tasks.

**Manage the Mobile Endpoint**

With the number of devices and access routes increasing, the number of points for a potential data breach have also increased. It is necessary to manage endpoints to ensure they are in compliance with corporate policy, have the latest security patches, and are correctly and securely provisioned without costly and labor-intensive manual updates.

Maintaining a large number of mobile devices of different types and across different use cases can be mastered with a comprehensive and automated management system ideally including device provisioning and configuration; auditing, policy enforcement, and logging; app and patch deployment (for example via a corporate app store); user self-service for basic tasks like key management and password retrieval; and information destruction for lost or end-of-life devices.

**Summary**

An increasingly mobile clinical workforce rapidly adopting consumer devices to access mobile, cloud-based applications, complemented by the wide range of mobile storage devices and other portable electronics, such as digital cameras, MP3 players, can make it difficult to efficiently assure compliance without impacting user productivity. This article reviewed a number of healthcare use cases and introduced comprehensive concepts and possible automated solutions to meet the requirements of a highly complex infrastructure of devices accessing confidential information.

**References**


Meaningful Use is driving the convergence of clinical engineering and information technology. As a biomed, you need a deeper understanding of IT and its impact on healthcare delivery.

GE is a premier company rooted in healthcare, and offers a full curriculum of courses dedicated to healthcare IT networking. From switching and routing to HL7 and DICOM, our classes give you the knowledge and confidence to support this ever-changing environment.

Couple your unique understanding of equipment with our IT courses to tie it all together.

Learn more at www.gehealthcare.com/hcit or call 888-799-9921. And learn from the leader in Healthcare IT.
What Are You Missing?

Find out why...

Nearly 7,000 medical technology professionals are members of AAMI—a community dedicated to advancing the safety of medical technology.

Join AAMI to receive:

- Complimentary subscriptions to AAMI’s journal, newsletter, and other publications featuring important news
- Access to up-to-date activities about AAMI’s Sterilization committee
- Deep discounts on standards, guidance documents, webinars, and other educational programs
- Direct access to manufacturing experts, clinicians, and users of technology; as well as FDA and Joint Commission officials
- New information about patient safety initiatives, leading practices, cost-saving tips, and troubleshooting techniques
- Networking opportunities, career tools, other online resources, and much more

Join AAMI today—visit www.aami.org/membership or call +1-800-332-2264, ext. 214.
GO FURTHER WITH UL

As healthcare evolves, so does UL. We understand the regulatory environment is a challenge and global regulatory approvals are the number one concern for your business. UL’s dedicated Health Sciences industry team provides the support you need to gain regulatory approvals in global markets. And we have added technical expertise and services to support inactive, implantable and ophthalmic devices.

For more than 118 years, the UL business and brand has been built on trust. Find out more about just how much farther you can go with UL.

LEARN WHERE YOU CAN GO WITH UL, VISIT US AT WWW.UL.COM/GLOBAL-MEDICAL

LOCAL SERVICES TO SUPPORT GLOBAL REGULATORY APPROVALS:
- ISO 13485
- CMDCAS
- CE Marking
- CRO-ISO 14155
- Biocompatibility
- Usability
- Software
- Japan PAL
- Brazil INMETRO
- ISO 14971
- IEC 60601
- CB Scheme
- IEC 61010
- Packaging & Shelf Life
- Application Assistance

UL and the UL logo are trademarks of UL LLC © 2012. EDI 01/12 111210