Evaluating mHealth Adoption Barriers: Privacy and Regulation

Insights Guide

power to you

PROTECTING YOUR PATIENTS PRIVACY IN A MOBILE WORLD
Welcome

Welcome to the third Vodafone mHealth Solutions Insights Guide, part of our Health Debate publication series.

The Vodafone Health Debate series is part of our continuing commitment to thought leadership in healthcare. It brings together senior pharma, public and private health stakeholders to learn, share and debate on issues and new thinking brought forward by renowned thought leaders and industry experts.

The first in the series examined barriers presented by human behaviour: issues of culture change for healthcare organisations; doctors; and patients. The second covered “politics and economics” – the need for governments to develop new policies and strategies for healthcare delivery to embrace the new world of flexible, mobile services centred around the patient that is rushing upon them; and the linked need to change funding systems so that doctors and healthcare providers can commission the new types of services – often involving less physical contact with a patient, for example – without losing revenue unfairly and with the right incentives to improve patient health and care.

This guide, the third and final chapter in the series, builds on the first two by expanding our examination of two major areas that connect the human barriers with the politics: privacy and security in mHealth systems; and regulation of mHealth systems and devices.

These are complex areas: as mobile systems become ever more powerful and interconnected, and the possibilities increase of linking up corporate IT systems with telecommunications networks, off-the-shelf consumer mobile devices and medical sensors, we enter a brave new interconnected world which no-one ever envisaged when they were designing the individual elements of these systems in years gone by.

There are technical challenges to face, with hardware, software and networks; and there are cultural challenges, within healthcare organisations and for patients. The debate around these challenges starts here.

Tony Kane
Head of mHealth Solutions
Vodafone Global Enterprise
Executive summary

Safety and security in a mobile world

When it comes to mHealth, there is one aspect on which everyone agrees: the technology is here now, and projects are developing rapidly on the ground locally, nationally and internationally as part of a wave of innovation that seems certain to change healthcare forever, focus it far more on the patient and increase patients’ freedom of movement and ability to be treated at home and in their communities. It is also clear however, that the mHealth revolution represents huge shifts in the tectonic plates of healthcare provision – and there is far less agreement about how to respond to these shifts, at all levels of the system.

Protecting patient privacy in a mobile world

With the rise of mHealth, patients are becoming ever more actively involved in their own care. But one area where this has significant implications is patient privacy – if contact with patients is more flexible and frequent, can it always be kept confidential?

Data gathered by mHealth applications may be accessible to the patient, but it may also be shared with others such as physicians; family members or carers; or scientific researchers. There are also considerations about the way data is stored and processed, creating a need for strong security and audit trails.

In the context of all these major changes, there is a growing body of evidence suggesting that many systems of individual consent to use of personal data are not particularly well-constructed. Until now it has been a one-off commitment made at the start of the relationship, but we may now need a rethink, moving towards an ongoing dialogue. Work is also needed to overcome legal and cultural differences over privacy between nations and global regions.

Security difficulties are also present. The key challenges include managing who has access to a health record – whether a patient or a healthcare professional – and ensuring that only secure, approved devices and applications can access data.

Assurances of anonymity are a top priority for gaining the trust of patients, but location data in particular is a challenge for anonymity in mHealth applications.

Ultimately, to make strong progress with mHealth, policymakers must draft the laws, regulations, and standards needed to protect patient privacy, and enforcement agencies must ensure these are implemented. Involvement by technology developers will also be essential.

Above all, the patient’s needs should always remain at the centre – remembering that the free flow of data is vital for improving care, as long as privacy is protected.

Key points:

• There is a growing body of evidence suggesting that current systems of individual consent to use of personal data are not well-constructed for mHealth

• Work is also needed to overcome legal and cultural differences over privacy between nations and global regions

• Assurances of anonymity are a top priority for gaining the trust of patients, but location data in particular is a challenge for anonymity in mHealth applications

• Above all, the patient’s needs should always remain at the centre: free flow of data is vital for improving care.
mHealth and regulation – medicine or telecommunications?

In the mHealth arena two types of device – medical and telecommunications – are converging, and regulators are struggling to keep up.

Regulators of mHealth systems are faced with a basic question: between sensors and apps handling lifestyle, fitness and clinical data – what constitutes a medical device?

One key is to identify the stakeholders involved from three broad areas: policy, suppliers, and users. Who are they, how are they defined, and what do they stand to gain – or lose – from regulation?

In the US, Congress has also asked the country’s Food and Drug Administration to draw up guidelines for regulating mobile medical apps. A separate advisory body has recommended that federal agencies regulating telecoms and medical devices should collaborate more closely.

Meanwhile a key European working group has examined the medical regulation of software. Software forms a particularly complex part of the mHealth ecosystem because applications are increasingly developed to run on standard devices, rather than specialist hardware. One obvious example of this is that of mobile phone apps, which can be used to connect with other devices and services that can be used to monitor a person’s health. Understanding which parts of such a system would be classified as a medical device – or whether the whole system would be classified together – is a key challenge for stakeholders.

For many purposes, regulators distinguish between systems and devices created for medical purposes and more general systems and devices put to medical uses. But there are many grey areas.

Overall, regulations can pose a bureaucratic hurdle, but they are also there to provide clarity for technology companies and healthcare organisations as they try to innovate and improve care quality. Manufacturers in particular must pay close attention when assessing their products to see if they fall under the mandate of medical device regulation.
# Table of contents

- **02** Welcome
- **03** Executive Summary
- **05** Table of contents
- **06** Safety and security in a mobile world
- **09** Protecting patient privacy in a mobile world
- **10** User consent: What is the best way to agree?
- **14** Case study: EU healthcare – towards borderless provision
- **15** mHealth security – high risk, low awareness?
- **18** Towards a framework for public trust
- **19** Case study: Standards are a foundation for trust
- **20** mHealth and regulation – when is a device medical?
- **21** Case study: Regulatory Convergence in the Real World
- **28** Case study: Regulation in Japan
- **30** Conclusion
- **34** Vodafone Global Enterprise
- **36** References
Every month brings a new report charting its expansion in both developed and developing markets; the guide you now hold in your hands is the next step in this process of examination and analysis.

Our focus this time, however, is on two less explored areas of the mHealth revolution. In the last Insights Guide we looked at market expansion, funding incentives, and the three pillars of mHealth policy as now being developed by governments worldwide: localisation, infrastructure building and patient empowerment.

Here, we look in-depth at two potential barriers to mHealth development that, with the right planning, can be transformed into enablers: privacy and security of patient records and mHealth systems; and regulation of mHealth systems and devices.

Overall, it is clear that mHealth is already benefiting quality of care for patients: and patients themselves are beginning to understand the potential benefits of the changes which are about to take place.

Cost savings for the patient will include reduced costs of travel needed to and from the doctor, and less need to take time off work to attend clinics, the PwC global survey says.*

Given the timescale of these predictions – just three years – these findings show mHealth awareness is now breaking into the mainstream.

It builds on an internet revolution that has already been changing healthcare now for over a decade: the more informed patient, accessing the internet.

The mHealth revolution takes this empowerment one step further, involving patients more deeply not only in researching and understanding their conditions but in monitoring them and managing them from day to day.

---

*Roughly one-half of patients interviewed by PwC in a (2012) global survey “Emerging mHealth: Paths for Growth” predict that mHealth will improve the convenience (52%), quality (48%) and cost (46%) of their healthcare in the next three years.
But with this deeper involvement comes a level of new risk. Specifically relating to exchanging data and receiving care using mHealth, 47% of respondents to the PwC survey say mHealth will change "how I measure and share my vital health information" in the same time period of the next three years; 48% say it will change how they manage their chronic conditions and medication; and the same percentage say it will change "how my healthcare providers and I communicate".

Patients are now coming to their doctor visits armed with copies of information from websites, and lots of questions. That's a good thing. They are taking control with the information that helps them better understand and manage their diseases. This dynamic changes the patient-clinician relationship in a positive way.

Benjamin Heywood, Co-founder and President of PatientsLikeMe, a US-based patient community
Focusing on the mention here of information exchange and communication between patient and healthcare provider, security of health records and patient privacy are emerging as a key concern for mHealth projects.

According to the PwC report both doctors and healthcare funders list privacy and security concerns as barriers to greater use of mHealth, and only around half of doctors believe that the mobile internet facilities at their workplace are reasonably secure.

Of course, the field of data security and computer security is well-developed, and there are many ways of approaching security of communications, such as encryption. The problem is, mHealth is about a great deal more than communication through devices such as smartphones and apps: it is a diverse, hybrid discipline embracing all sorts of devices and situations.

Consider the Persona project, a European Commission-funded initiative led by a consortium of academic, medical, and private technology organisations in Italy, Spain, Greece, Germany, Denmark and Norway tasked with developing a range of Ambient Assisted Living (AAL) technologies that help disabled and older people to live in their homes for longer.

The project aims to deliver four major benefits: alleviation of loneliness and isolation; support in performing daily tasks and activities inside and outside the home; creation of a living environment where individuals feel safe; and increasing people’s mobility.

To achieve these goals, the mobile technologies used span a range of communications and medical devices including sensors, actuators, smart and intelligent textiles, user devices, user interfaces, user interaction, and external information systems.

Applications include health management, with doctors using a remote web application to prompt users to take medications; automatic event reminders for appointments or other treatment events; risk and emergency management; help when outside the home; and chat and video communications with relatives, caregivers and other users.

The scope of this project both in terms of technologies used and operating locations and environments show there are many new areas where potentially sensitive patient information is generated, and hence where security and privacy could be a risk.

Many of these risks can be minimised by automating transmission of information over the internet directly to secure servers. This can be done through machine to machine (M2M) systems with security such as encryption built in.

But issues remain, not least of a potential crossover of regulation between medical devices and telecommunications devices. Because if patients are increasingly playing a part in the management of their care, this means that mHealth devices are more than communication devices – they are medical devices in their own right.

One issue here – apart from working out when a device is a medical device and when a device is a communications device – is regulation. Communications devices are regulated, and medical devices are regulated – but generally up to now they have been regulated separately, and by separate regulatory bodies.

If they are starting to overlap, what do our regulatory systems need to do to keep up, and how far are they already being adapted?

These adaptations and those needed to tackle the privacy and security concerns surrounding mHealth will not be easy, but they are essential and also achievable as long as all stakeholders work together to tackle the issues outlined in this report.

What do our regulatory systems need to do to keep up, and how far are they already being adapted?
With the rise of mHealth, the relationships between patients, medical professionals, healthcare providers and policymakers are changing radically, with contact potentially becoming more frequent and less formal.

Patients are becoming even keener to be more actively involved in their healthcare. A clear sign of this comes from the growth in patient groups, a trend that is seen globally. "The patient movement...is proving to be an exception to the rule that change is slow in healthcare systems", says UK-based consultant PatientView. "Patient groups and other health non-governmental organisations (NGO) are expanding rapidly. Their growth is fuelled by the damage inflicted upon mainstream national healthcare systems by tough new doses of fiscal austerity, and by ever-increasing patient demand for services."

With mHealth solutions, patients can often be granted this wish for greater involvement and control. But one area where this has significant implications is patient privacy – if contact with patients is more flexible and less controlled, can it always be kept confidential?

In mHealth applications, an internet-enabled device such as a smartphone will often connect wirelessly to wearable, portable, or possibly even embeddable sensors which might track or measure a patient’s health, or even just their movements. This tracking might take place in real-time, with or without the patient’s intervention or approval at each moment.

The data gathered may be accessible to, and acted on, by the patient directly but it may also be simultaneously shared with others such as physicians; family members, friends or carers; sports trainers; insurance companies; or scientific researchers. Information can also be gathered directly in the field. This represents a major break with the past relationship between patients and healthcare providers, whereby health information was gathered only at certain locations face to face such as hospital, clinic or home visits.

The sheer potential quantity of potentially sensitive data collected about an individual further sets mHealth apart from previous care models. Then there is its nature: it may carry not only finely-detailed information about a person’s health, but also about their habits, location and movements.

Finally, there are wider changes in the way data is stored and processed, given the possibility of data moving across national borders and jurisdictions, for example where international companies or NGOs are involved. Even within countries, data can be moved from place to place in an instant, creating a need for strong security and audit trails.

In the context of all these major changes, privacy is a complex issue, requiring the user to negotiate a new range of relationships.

If contact with patients is more flexible and less controlled, can it always be kept confidential?
User consent: What is the best way to agree?

There is a growing body of evidence suggesting that systems of individual consent to use of their personal data are not particularly well-constructed in any area of our modern digital society.

A humorous example illustrates this: on 1 April 2010 the retailer Gamestation temporarily altered its terms and conditions for customers as an April Fools’ Day prank. They stated: “By placing an order via this website on the first day of the fourth month of the year 2010 Anno Domini, you agree to grant us a non transferable option to claim, for now and for evermore, your immortal soul”. It was reported that of the 7,500 customers who made purchases that day, none clicked on a link to nullify this Faustian pact.

Clearly, in other words, no-one reads the small print. So what is the best way of obtaining someone’s genuine consent for a particular use of their personal data?

The UK’s Information Commissioner’s Office (ICO) stress there is a fundamental difference between telling a person how you intend to use their personal information, and obtaining their consent for this. “In many cases it is enough to be transparent. In other cases a person’s positive agreement will be needed”.

Across the Atlantic, the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants recently released a voluntary code of practice entitled Generally Accepted Privacy Principles. This requires an organisation to describe “the choices available to the individual related to the use and disclosure of their information, and to obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information” – a comprehensive and thorough approach.

Researchers are also taking a closer interest in this field. In 2008, a cross-sector group of UK researchers launched EnCoRe: Ensuring Consent and Revocation, a four-year research project that examined possible new ways for individuals to grant and, “more importantly, revoke their consent to the use, storage and sharing of their personal data by others”.

EnCoRe set up a focus group of privacy experts, data protection professionals, the public sector and small businesses to extract insights from the everyday practice of data protection, and elicit views on how individual consent might be obtained and handled more effectively in the digital age.
The degree to which individual consent is genuinely informed was among the issues discussed. Currently, the way citizens are informed of privacy policies tends to be one of two polar opposites: they are either presented with a short and vague catch-all statement, or a long and very complex document, against which a simple “I agree” button can seem like a tempting escape route.

“The evidence gathered from our expert focus groups strongly indicates that informed consent rarely functions well in online interactions in the sense that it is unlikely to be truly informed and freely given,” EnCoRe researchers Edgar Whitley and Nadja Kanellopoulou concluded in a project report.

We operate within a model of consent that no longer serves the needs of the online relationships we are forging, the researchers suggested. Until now it has been a one-off commitment made at the start of the relationship, dispensed with as quickly and cheaply as can be squared with legal and regulatory compliance. We may now need a rethink, shifting the emphasis towards the individual and making them more of a participant in an ongoing dialogue.

As Whitley and Kanellopoulou say, in relation to health: “In medical treatment and research, consent is to be secured as the individual’s free and informed choice, through communication and apprehension of the risks and benefits of a particular medical intervention.”

Clearly, in other words, no-one reads the small print. So what is the best way of obtaining someone’s genuine consent for a particular use of their personal data?
How do governments address the challenge of personal privacy in the digital age?

Many governments and international bodies have realised there is a problem to solve here, and have moved to address the challenges of personal privacy in the digital age.

EU
EU legislation has sought to address privacy by articulating the rights of individuals, favouring high level statements of principles which allow a degree of freedom in how they are implemented.

US
The US, on the other hand, has taken a more piecemeal approach focused on preventing privacy breaches by setting out fine-grained requirements and prohibitions for bodies carrying out specific data processing acts. Attempts to bridge these different approaches and allow data exchange between Europe and the US have been made with so-called Safe Harbor agreements that include specific requirements for personal health data.

New Zealand
The 1993 Privacy Act of New Zealand is one of the most comprehensive pieces of privacy legislation in the world. It includes principles based on early OECD guidelines ‘Guidelines: On the Protection of Privacy and Transborder of Personal Data’ (OECD, 1980) but goes beyond these, requiring data collectors to specify how data is collected, check it for correctness, and keep it no longer than necessary. The 1994 Health Information Privacy Code sets out guidelines for health information.

Asia Pacific
In the broader Asia Pacific region Australia, Japan, Hong Kong, South Korea and Taiwan have adopted some form of data privacy legislation; while Thailand, China, Malaysia and the Philippines are in the process of drafting laws. Singapore, Vietnam and Indonesia have privacy laws covering only certain sectors and do not specifically address health data. For a comprehensive survey see: ‘Asia Pacific Legislative Analysis: Current and Pending Online Safety and Cybercrime Laws. A Study by Microsoft’.

India
India has no specific legislation setting out a right to privacy, although some parts of the country’s common law, criminal law and constitution are relevant to privacy issues. The Information Technology Act of 2000 also covers some aspects of data privacy, but without setting out the precise scope of personal data. The Personal Data Protection bill, which is based on the EU’s Data Privacy Directive, was introduced in 2006 but has yet to be approved by the country’s parliament.

Latin America
There are important cultural differences between regions, too. For example in Latin America, constitutional guarantees of privacy may bear little relation to everyday practice. “As with so many Latin American countries, Mexico’s constitution guarantees a broad-sounding right to privacy: each Mexican’s personal possessions and home are free from being “molested except by virtue of a written order by a proper authority” and all Mexicans enjoy an explicit constitutional right safeguarding privacy in their private communications, their mail – even their run-ins with the law,” says White & Case.

Mexico
“However, as of 2006, Mexico had never implemented this right by statute. Mexican lawyers regularly tell anyone who asks that their law imposes no significant limits on businesses processing personal data,” the firm says.

One example is the Asia Pacific Economic Conference (APEC) Privacy Framework, which suggests to APEC member countries – as diverse as Chile and Singapore – that they adopt data privacy laws, but without specifically spelling out what those laws should be.

"Unlike the EU Directive, which requires the EU member states to enact ("transpose") comprehensive data protection laws, the APEC Privacy Framework is best described as aspirational: It sets out nine data privacy principles, but it does not mandate that countries adopt them", the law firm says.
Research into how we use technology shows that there is often a mismatch between user expectations and the way data access consent works in practice. For example, studies\(^\text{12}\) of smartphones show a lack of awareness among users about when a downloaded application can access their data. Generally, users seem to assume that granting permission is more noticeable than is actually the case. Mobile device applications that are downloaded typically seek permission from the user to use data at the time of installation or at the time of use, but there are potential problems with both these approaches.

At installation the user may have little idea of what the application is like to use or what they want it to do, and may have difficulty making an informed decision when confronted with a sometimes long and complicated list of choices for data access. There is therefore a danger of granting too much access, a decision that could have a serious impact on privacy further down the line.

By contrast, prompting for permission in use is more tuned to actual user behaviour, but it can seem intrusive and boring to use, with a risk again that users will not consider their responses carefully.

One example of a potentially less intrusive way of asking for and granting permission inside new downloaded applications is set out in "User-driven access control: rethinking permission granting in modern operating systems"\(^\text{13}\). In this paper, researchers from Washington University and Microsoft explore an approach by which the user would be guided through some general decisions about what data applications can access at the time they are installed, but the bulk of the work of permission granting would happen on the fly.

The way this would be made less intrusive would be to only ask for the minimum permissions needed to function (least permission), rather than general permissions; and by using commands and keystrokes that are standardised and minimised, becoming less intrusive than traditional pop-up windows.

These easier, more flexible methods may be part of the way forward for downloaded applications, but difficulties linger due to the growing complexity of applications and their interactions with each other. Applications may be embedded inside other applications, and for some tasks data may need to be pulled together from several different applications, for example. This could be a concern for mHealth applications, which are expected to collect data from a wide range of sources, including physiological data as well as information about a patient's lifestyle and activities, including their food habits, diet details, location, and physical exercise.

If, as is increasingly thought, patient consent must be more of an ongoing dialogue than a one-off commitment, questions arise about how consent should be managed in practice.

Some of the most significant efforts have come from the US, specifically the Markle Foundation’s Connecting for Health initiative\(^\text{14}\). It distinguishes between General Consent, which is a broad framework of policies covering privacy and terms of use, and Independent Consent, which identifies actions needing separate and specific consent by the patient.

Efforts are underway to implement this kind of consent framework in healthcare ICT, notably by the Healthcare IT Standards Panel (HITSP)\(^\text{15}\), a public-private partnership between US government and health sector organisations. HITSP has released an interoperability standard setting out how to produce machine-readable consent decisions on access, collection, use and disclosure of patient data. This kind of detail and sophistication is likely to form a key part of future solutions.
Case study: EU healthcare – towards borderless provision

The ability for people to move freely across national borders has always been a guiding principle for the EU, but only recently were the practical consequences of this made clear for health services.

Research by Oxford University’s Migration Observatory shows that by 2010, EU migrants accounted for 35% of all migrants in EU member states and in Luxembourg, the Czech Republic, Slovakia and Ireland, EU migrants account for more than 70% of all migrants. These flows of people can put severe pressure on national health services, as the aim is to make provision of healthcare within the EU as borderless as the movement of its citizens.

A new EU Directive on the rights of patients is set to be implemented by member states by October 2013. Article 14 of the Directive deals with healthcare ICT specifically, supporting the setting up of a “voluntary network” of national authorities tasked with promoting exchanges of healthcare information.

This network will have as its goal delivering healthcare ICT systems, services and applications “with a view to achieving a high level of trust and security, enhancing continuity of care and ensuring access to safe and high-quality healthcare.”

But the flow of health data across borders and jurisdictions threatens to conflict with another right that EU citizens are increasingly concerned to protect: the right to privacy. To gauge public feeling, and to pave the way for a re-examination of the EU Data Protection Directive, in 2009 the European Commission launched a public consultation on personal data. It sought contributions from all industry sectors and also from individuals. Although quite general in its scope, healthcare emerged as a central concern for citizens.

While organisations were generally looking for greater clarity about the detail and scope of their responsibilities, citizens sought reassurance about the privacy of their own personal data (*See below). Citizens are particularly apprehensive about the application of new technologies to healthcare, especially implants or sensors that collect and transmit health data on a continuous basis, the consultation found. “The increase in biometric data is a common worry and respondents want it to be addressed in the new legal framework.”

*Concerns about personal health data were found to fall into the following broad categories:

- How and when data is collected;
- What steps are taken to ensure data is accurate;
- How data is protected against unauthorised use; and
- How data is protected against access by unauthorised persons.

At a more detailed level, the European Commission notes the growing concern of citizens about an issue closely linked to privacy: consent, which they worry will be swept aside in the rush to implement new healthcare technologies. “Some want the legal framework to include a mechanism for cancelling consent,” the Commission says.
mHealth security – high risk, low awareness?

The privacy and security risks associated with mHealth must always be weighed against their huge potential benefits.

“Smartphones offer new opportunities in every sector of society – from mobile productivity to e-health, augmented reality and electronic payments,” says a 2010 study from the European Network and Information Security Agency (ENISA), the body responsible for advising EU institutions on IT security issues. “We stress that the risks should be balanced against the potential benefits of smartphones. To give just one example however, smartphones are being used as smart-health sensors, allowing heart patients to stay at home safely, while having their heart issues controlled and monitored by medical staff. In this way smartphones increase a patient’s quality of life and, at the same time, save healthcare costs,” ENISA said.

Later that year, having put smartphone security risks in context, the agency published an in-depth study of these risks and how they might be mitigated. As part of this study, ENISA examined three types of usage scenario, including consumer use of smartphones for health purposes.

Among the most significant of the risks is data leakage, as when a stolen or lost phone with unprotected memory allows an attacker to access any sensitive data that happens to be stored on it. In the UK, for example, some 2% of all users reported the theft of a mobile in the previous year, the BBC reported in 2010. Young users appear to be especially vulnerable, with three times this figure reporting thefts.

Even when ownership changes in a legitimate way there may be security risks where data has been stored locally. “Due to a growing awareness of identity theft many people and organisations now destroy or wipe computer hard drives before decommissioning. However, the same thing is not yet happening with smartphones. At the same time, more and more devices are being recycled,” ENISA says.

User awareness of risk was a key part of the study. “Most apps have privacy settings for controlling how and when location data is transmitted, but many users are unaware – or do not recall – that the data is being transmitted, let alone know of the existence of the privacy setting to prevent this,” says ENISA. Mitigating such risks will be a challenge: “...it should be mentioned that years of raising awareness have done little to prevent large-scale virus outbreaks on PCs,” it warns.

On the other hand, many of these problems can be side-stepped by the use of the more secure embedded applications and systems that come pre-loaded onto mobile devices such as text messaging or web browsers. If mHealth applications are held in remote servers in the cloud, and accessed securely over the internet by mobile browsers, for example, the issues of permission granting and data security can be handled separately, and flexibly.

Alongside the challenges of securing data on a smartphone, mHealth systems will often also face the challenges of securing health records. The key challenges are managing who has access to a health record – whether a patient or a healthcare professional – and ensuring that only secure, approved devices and applications can gain access to and process the data it contains.

...it should be mentioned that years of raising awareness have done little to prevent large-scale virus outbreaks on PCs
Until recently, the standard approach to controlling the access people have to electronic patient records has been by username and password. However, although widely implemented, password protection is increasingly seen as insecure, with a growing body of evidence indicating its vulnerability to attack.

At one time, the cracking of passwords took so much time and knowledge that they were considered safe, but the landscape has changed greatly in recent years. Launching such attacks no longer requires great expertise, with the ready availability of password cracking kits online. As a result, most healthcare providers are moving to some form of two-factor authentication, with access requiring provision of at least two of the three factors “something the user knows”, “something the user has”, and “something the user is”.

An example of this is Verizon Universal Identity Services (UIS) for healthcare, a cloud-based service from enterprise telecoms solutions provider Verizon aimed at clinical applications. Verizon UIS provides flexible two-factor authentication, giving users a choice of second factor such as hard token (such as a swipe card or tag), soft token (embedded in software), text or voice messages, and more.

Although an improvement on password protection, even these more powerful forms of authentication are not always cast iron.

An example of the difficulties in maintaining security even with the use of hard tokens is provided by the National Health Service (NHS) in the UK, with its implementation of a Care Records Service linking patient information from different agencies within the NHS. A registration authority within each of these agencies is responsible for verifying the identities of healthcare professionals and support staff, and maintaining a register of those allowed access to the service.

Members of staff are issued with a smart card printed with the user’s name, photo and a unique identity number, and the system maintains an audit trail which is available to the patient on request. However, there have been reports of sharing of passwords and PINs by staff, with some doctors allowing their staff to use their login credentials to save time, for example.

As in the UK, standards bodies in the US have typically used a role-based access control (RBAC) model for deciding who has access to healthcare ICT systems. On this approach it is what you do rather than who you are that decides whether you have the right to access patient information. This model is a natural fit for organisations where people and agencies have clearly defined roles that remain fairly static over time, but it is increasingly debated whether this is the best model for the new, flexible, innovative projects springing up under mHealth.

A general concern is that RBAC serves the hierarchical structure of organisations rather than the privacy needs of the patient. Critics point out that RBAC is not tuned to privacy as such: access is simply granted or denied. In response it can be argued that RBAC can be fine-tuned for different types of patient data, though practical experience of implementing such sophistication is lacking.
Insights Guide

At the technical level, encryption is another important aspect of managing access control, but important questions remain to be settled here too, such as who or what encrypts and decrypts the data and manage the keys.

An added complication for authentication in mHealth is the need to ensure that sensor data is being collected from the correct patient. Devices too must be capable of authenticating themselves: the healthcare IT system and a smartphone to each other, and the smartphone and its sensors too.

These problems are not insurmountable, however. The latest versions of the Bluetooth short-range wireless communication system have supported encryption for some time, and have been accepted as secure enough for use in banking – so medical sensors should not be an issue. Mobile networks are also encrypted as standard.

Of course, whatever security technology is chosen must be easy to use by the patient. In particular, it must be easy for the patient to add a new sensor to their mHealth network. Here, research in pervasive computing may have much to offer. One promising area of research could see the user holding two devices together and physically shaking them in a certain way. Internal accelerometers would create an electronic “signature” for the shaking action, and use this to generate cryptographic keys which would then be exchanged between the devices over a short-range secure radio connection\(^\text{20}\).

Keys may also be created using simultaneous readings of their immediate radio environment, or perhaps some other physical features of it.

Overall, ensuring that mobile devices are fit for purpose for healthcare ICT will require a significant contribution from industry: the developers of devices, their operating systems and applications.

One thing that is clear is that, given the challenges of securing data stored on smartphones and likely difficulties with user awareness of security, downloaded apps are not the most promising route for many forms of mHealth development.

There are plenty of safer options, however. Systems can also make use of a mobile phone or mobile device’s more secure native applications, such as SMS text messaging, for many purposes. Devices can also communicate with mHealth systems in the cloud using mobile web browsers – enhancing access control and avoiding the need for sensitive data to be downloaded locally.

In many cases, there is not even the need for any human involvement at all: so-called machine-to-machine (M2M) communication describes systems whereby health data from sensors is transmitted over the internet to remote servers with minimal involvement by the patient.

Heart rate monitors, for example, could be directly connected to the internet, which is easier for the user, and means the data transmitted can be inherently encrypted.

ENISA is just one of many stakeholders arguing for a greater focus on “security by design” principles. Conventional wisdom in IT security has it that no application can be more secure than the operating system it runs on, and some security researchers are looking afresh at how security is implemented in the applications and operating systems of smartphones, and alternative mHealth technologies.

---

Ensuring that mobile devices are fit for purpose for healthcare ICT will require a significant contribution from industry.
A huge growth in the collection of healthcare and treatment data in recent times has important implications for medical research, and for monitoring the quality and effectiveness of services. It is vital however that patients remain properly informed about the choices available to them, and retain trust in any process devised to gain their consent to share their data for these purposes.

Assurances of anonymity are a top priority for gaining the trust of patients, and here, efforts are focused on addressing the practical difficulties associated with anonymising data thoroughly and completely.

In the US, efforts have been made in this direction through the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA Privacy Rule states that health data can be disclosed or shared without restriction provided specific conditions are met. Bodies intending to release such data must check that anonymity is preserved using approved statistical methods, or by removing 18 elements that could be used to identify the patient or their relatives, employers, or household members. These 18 elements include the patient’s name, ZIP (postal) code, phone number, all dates except the year, and any biometric data.

Location data in particular is a challenge for anonymity in mHealth applications. Privacy campaigners often express concern that location data in general can compromise the privacy of mobile device users, but for some mHealth uses location data is an essential part of the application, as when a patient wants to be more physically active, for example.

In such a case the mHealth application may collect data about the places, times and distances spent walking, running, or cycling. The patient may desire the benefits from having a detailed record of these facts, but feel less happy sharing the fine detail with medical professionals, or they may be comfortable sharing it with their personal physician, but not with other health services.

The difficulty in practice is that anonymity comes in degrees rather than absolutes. In numerous experiments security researchers have shown that sources of “anonymised” data can be cross-checked or combined with physical observation to identify an individual. Even when data cannot directly pick out a person, it still contains enough general information to identify them indirectly.

Researchers have tested ways of preserving data such as distance travelled over a given time, while obfuscating data that shows a specific location, but ingenious as many are, they can often be defeated by a resourceful attacker. For example, it has been shown that it’s possible to recover user identity from WiFi network traffic even if the MAC and IP addresses – data that identify devices to the network – are regularly changed. It seems likely that strong anonymity of network data will remain a difficult challenge.

Among the other provisions of HIPAA is a requirement on providers to take appropriate steps to ensure the integrity of health records, to protect them from improper alteration or destruction. In addition to HIPAA, the Health Information Technology for Economic and Clinical Health (HITECH) Act, signed into law in 2009, will have an important role in shaping mHealth in the US. It specifically addresses key issues for mHealth providers such as a requirement to provide an audit trail of changes to health records.

HITECH requires healthcare providers to account for disclosures by their partner organisations, or to identify their partners organisations, who then account for disclosures to individual patients. An important question for mHealth will be how to ensure adequate audit mechanisms are to be implemented in sensor networks with limited computational resources. HIPAA and HITECH also set out mandatory requirements on the transmission of health data. HIPAA Security Rules require “technical security measures to guard against unauthorised access to electronic protected health information...transmitted over an electronic communications network”, a requirement that HITECH extends to business associates. The security net is widening.
Case study: Standards are a foundation for trust

Ensuring there is international cohesion on security and privacy in mHealth requires input from a wide range of standards bodies and professional organisations. This includes the professional bodies representing clinicians and healthcare providers, but also those focused on IT and telecoms.

Due to the complexity and fast pace of development in mHealth, bodies such as Health Level Seven International (HL7) have been formed. A not-for-profit organisation with working groups focused on mHealth and security, HL7 develops standards for the exchange, integration, sharing, and retrieval of electronic health information and has around 500 corporate members representing more than 90% of the information systems vendors serving healthcare.

A key question is how to extend the work of bodies such as HL7 beyond Europe into regions such as Africa, for example. "There is increasing recognition of the need for the global information technology community to subscribe to one form of computer language coding, such as for instance, HL7, to provide for interoperability of information systems on an international level," say researchers from the Medical Research Council and University Of The Western Cape. In a survey of the barriers to mHealth in their own country of South Africa, the researchers note that it has no agreed interoperability standards for at present, and also does not have a local chapter of the HL7.

While this is so it will be difficult to make progress with standards for mHealth security and privacy in South Africa, the researchers say. And agreeing security and privacy standards is only part of the challenge: it is also essential to engage with the wider public if their trust is to be won. "Whilst technical solutions exist to restrict access to information and to secure the privacy of data, this may not be enough reassurance for many stakeholders involved in healthcare," they warn.

Ultimately, to make strong progress with mHealth, policymakers must draft the laws, regulations, and standards needed to protect patient privacy, and enforcement agencies must ensure these are implemented. Certification bodies responsible for checking compliance with security standards will have a key role in upholding public trust in mHealth products and services.

Involvement by technology developers will be essential if we are to have the hardware and software, including healthcare ICT, mobile applications and sensor devices we need. Such complex networks of devices will require robust distribution and management if security and privacy is to be maintained. Devices must be physically distributed to users in a secure way, and user authentication must be flexible and robust.

All this must be achieved while engaging the public. Without people’s trust and support these efforts will be wasted. In many respects this echoes the challenges faced by other e-services, but mHealth faces both tougher challenges and greater potential rewards.

In this new dispersed environment, it must always be remembered that the patient’s needs and outcomes should always remain at the centre — and that the free flow and use of data is vital for improving care, as long as privacy is protected.

“We fundamentally believe that the Internet can democratise patient data and accelerate research like never before”, says Benjamin Heywood, Co-founder of the US-based patient community PatientsLikeMe. “We also believe data belongs to the patient to share with other patients, caregivers, physicians, researchers, pharmaceutical and medical device companies, and anyone else that can help make patients’ lives better.”
mHealth and regulation – when is a device medical?

In 1948, when the UK unveiled the National Health Service, the closest thing to mobile healthcare was a visiting doctor. Telemedicine involved calling the GP and relaying symptoms over the phone, and telephone switchboards were still manually operated. We have come a long way since then, and the pace of development is only increasing.

The creation of new forms of healthcare assisted by communications technologies, such as mHealth, has created fresh challenges, particularly with regards to regulation.

Regulatory bodies for both medical devices and telecommunications devices are tasked with protecting the public from devices that are unfit for purpose and potentially damaging to health. These regulations are difficult to create, because they must cover multiple types of device and many different eventualities. Yet, while the policymakers labour over rule sets, the market continues to innovate at a breakneck pace. Add to that the fact that in the mHealth arena the two types of device – medical and telecommunications – are converging, and it is not surprising that lawmakers struggle to keep up.

Currently, while mHealth already offers huge potential to improve quality and flexibility of patient care, the regulatory guidelines governing it are still unclear. How can it be effectively regulated? Regulators must answer key questions, including the most basic one: what constitutes a medical device?

There are significant dangers in not regulating devices – whether software or hardware-based – that are used for medical purposes. Much comes down to what those purposes are, and it is important to differentiate between clinical or treatment use on the one hand, and healthy lifestyle or wellbeing on the other.

For example, there are many fitness gadgets that provide basic health information but which may not be used for critical decision making. Devices such as the Fitbit are designed to be worn all the time, and track information such as the number of steps people take, the number of stairs they climb and the number of hours they sleep. They work alongside other everyday communications technologies such as their own smartphone apps.

Nike’s FuelBand – a bracelet with embedded accelerometer – does something similar, tracking walking and running and awarding the user motivational points based on their activities. Both of these are designed to be connected to the Internet using various communications mechanisms to relay information to a central repository, but neither of them would be used for critical medical decisions such as ascertaining medicinal dosages.

However that is not to say that devices very similar to these could not be used for medical treatment purposes. For example, a device that monitors a person’s blood glucose may be little more than a sensor that plugs into a smartphone, with an accompanying piece of software. While this may seem similar to the fitness technologies mentioned above, the results returned by that glucometer device could be used as the basis for decisions that will directly impact the user’s health. If the number is inaccurate, then the user could unwittingly harm themselves.
In June 2012, the US Federal Communications Commission (FCC) formed a mHealth task force to explore its regulatory capacity for mHealth technologies. The task force made several recommendations designed to help the commission take a leadership role in advancing mHealth adoption. It advised the commission to appoint a healthcare director, who would support the regulatory needs of the healthcare technology sector. This would also help it to improve educational outreach activities to healthcare organisations, the task force said. This activity could be assisted by a website, operated by the FCC, which would continue to seek public input on regulatory issues spanning the telecommunications and healthcare sectors, it said.

The task force also recommended that federal agencies collaborate more intimately to promote innovation and protect patient safety as mHealth technologies develop. In particular, the FCC and the US Food and Drug Administration (FDA) should accelerate their collaboration and provide clarity on overlapping issues to avoid duplication of regulatory efforts, it said. Other parties with which it should collaborate are the Centre for Medicare and Medicaid Services (CMS), and the Office of the National Coordinator for Health Information Technology (ONC). The three agencies should share data on healthcare providers that qualify for exemptions from certain telecommunications regulations.

The third broad goal for the FCC is to build on existing programs, linking them where possible to expand broadband access for healthcare, the task force said. This includes updating the Rural Healthcare Programme, an initiative that provides discounts on the purchase of telecommunications services by eligible rural healthcare providers, and adding healthcare delivery as a goal for the Lifeline Program for Broadband, exploring ways to get broadband services to America’s low-income population.

The FCC should continue efforts to increase the capacity, reliability and interoperability of mHealth technologies, the task force said. Steps involved in this include making more licensed spectrum available for mobile broadband, and working with international counterparts to standardise the spectrum used for mobile health services.

The US government approach to mHealth regulation points to one practical approach that other administrations could follow.
Stakeholders in regulation

To better understand the risks, challenges, and rewards associated with the clinical regulation of mHealth devices, it is important to identify the stakeholders involved. Who are they, how are they defined, and what do they stand to gain – or lose – from regulation? The stakeholders involved come from three broad areas: policy, suppliers, and users.

Policy stakeholders

Regulators
The regulatory bodies are usually governmental agencies tasked with preventing risk to the public through the use of devices that have no clinical value, or worse, a negative effect on health. These bodies must find a balance between the needs of the clinicians and users, who must be protected and who want to be able to trust the manufacturers and distributors of their products, and the manufacturers and distributors, who are keen to innovate and add value to products and services.

Consultants
These groups, often specialist legal firms, are interested in guiding clients (often manufacturers and service providers) through the regulatory framework. James Sherwin, executive director of non-profit think-tank d4, argues that those professionally equipped to advise can find incentives in representing regulation as complex and work-intensive. “If you’re a notified body that provides consulting services to help manufacturers of medical devices go through the necessary steps, I believe there’s a conflict of interest to say that they may err on the side of caution,” he says.

Interest groups
Third-party interest groups include industry associations and patients’ groups with specific goals in the context of healthcare and telecommunications. Bodies like these often try to shape policy development on behalf of their members, as well as having other roles such as developing practical guidance, which can see them becoming supplier and user stakeholders as well.

Supplier stakeholders

Manufacturers
Manufacturers design, create, and label mHealth systems. They may manufacture dedicated hardware, but could also be software development companies working on mobile applications, or on web-based services pertaining to the mHealth market. The EU Medical Device Directive defines them as “the natural or legal person with responsibility for the design, manufacture, packaging and labeling of a device before it is placed on the market under his own name, regardless of whether these operations are carried out by that person himself or on his behalf by a third party.”

Distributors
Distributors are those organisations that provide mHealth devices or applications to the clinicians and/or users that operate them. As such, they constitute the manufacturer’s supply chain.

Ecosystem providers
These players provide the ecosystem that enables the mHealth devices to be used. Carriers provide the communications networks, while electronic health record (EHR) providers enable patient data to be stored in secure digital records. Some ecosystem providers may be co-opted into manufacturer status, depending on regulatory parameters. For example, a phone handset manufacturer could be deemed a medical device provider or simply part of the ecosystem, depending on how the regulatory frameworks are interpreted (this issue is discussed in more detail elsewhere in this chapter).

User stakeholders

Clinicians
Clinicians are the clinical users that deploy mHealth solutions for the benefit of their patients.

Users
A user employers the mHealth device in practice, and may use it to gather and/or conduct analyses on data at home. The word ‘user’ is preferred to ‘patient’ because of concerns voiced by industry over the potential for mHealth definitions to fall into more general health and wellness categories, as discussed earlier in this report. The word is also preferred because it expands the definition to include friends, family, and carers who may be responsible for the healthcare of a patient even while not working directly in a clinical professional capacity.
Approaches to definition

The ambiguity of the law in regulating mHealth devices is a particular problem for European policy makers because state laws in Europe generally filter down from European directives, and must therefore be interpreted into national legislations and regulations.

There are some commonalities between the two approaches however – in the EU and the US – since at a broad level, both regimes concentrate on the intended use of the device to decide whether it should be regulated.

Europe

The European definition is driven by the European Medical Devices Directive (93/42/EEC), which regulates a broad range of devices from first aid bandages and tongue depressors, through to highly technical specialist equipment such as X-ray machines.

In Europe, there are three classes of active medical device, all of which have different risk classes. Devices are classified under Rules 9-11 of the Directive. If a device is designed to administer energy in some way for therapeutic purposes, to monitor radioactive pharmaceutical products (used for medical imaging purposes) or monitor vital physiological processes, then it can be seen as a class Ila device, as it can be if it is administering or removing medicines to the body. If it is supposed to go further, to administer or exchanging potentially dangerous levels of energy, to emit ionizing radiation, or to monitor vital signs where variations in monitored levels could be immediately dangerous, then it would be a class Iib device. All other active devices are seen as class I devices, which are considered lower risk.

There has been some further work on definition among “competent authorities” – the member state organisations tasked with interpreting the European directive into national regulations – and one key area of this work has been to look at the position of software when it comes to medical regulation. The authorities have been meeting as part of a working group chaired by Sweden, called the Medical Products Agency’s Working Group on Medical Information Systems.

In 2009, a Swedish regulatory document on the classification of software as a medical device was produced which served as a blueprint for wider European adoption, although work is ongoing.

This document, called “A proposal for guidelines regarding classification of software based information systems used in healthcare”, constituted some of the first extensively articulated thoughts on the interpretation of the Medical Device Directive in the area of software regulation.

Software forms a particularly complex part of the mHealth ecosystem because software applications are increasingly developed to run on or work with standard devices, rather than just on custom or specialist hardware. One sub-set of this is mobile applications.

Mobile applications – whether running locally or through a mobile browser – can also be combined with various innate features and abilities of smartphones, which are increasingly imbued with sensors including accelerometers and light sensors, and geolocation capabilities.

These devices can also connect – via a range of communication technologies including WiFi, cellular networks and Bluetooth – with other devices and services that can be used to monitor a person’s health. It is possible to connect a generic smartphone wirelessly to a blood glucose meter, for example, and to have the software process that data, to or have it relayed to a third party service that processes it for the user and/or a clinician.

Understanding which parts of such a system would be classified as a medical device – or whether the whole system would be classified together – is a key challenge for stakeholders. And given that much of the intellectual property resides in software, understanding the regulatory landscape as it applies to software applications is crucial to businesses’ commercial interests as well.

On 21 March 2010, new European legislation came into effect that enabled standalone software to be classified as a medical device, so long as it is being used for medical purposes.

According to clause 6: “It is necessary to clarify that software in its own right, when specifically intended by the manufacturer to be used for one or more of the medical purposes set out in the definition of a medical device, is a medical device. Software for general purposes when used in a healthcare setting is not a medical device”.

The European Working Group argues that classification rules for medical devices were not written with software in mind, however. Therefore, a large number of software devices fall into class I, where compliance is based on self-declaration, not on any third party assessment.

The Swedish proposal for guidelines regarding classification of software based information systems used in healthcare arrived at some interesting conclusions. It interpreted the law to mean that the Medical Device definition should not apply to devices intended for diagnosis or treatment of a broad population, such as broad statistical tools.
The European Medical Devices Directive (93/42/EC) identifies a medical device as:

- Any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purposes of:
  - Diagnosis, prevention, monitoring, treatment or alleviation of disease;
  - Diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap;
  - Investigation, replacement or modification of the anatomy or of a physiological process;
  - Control of conception.

However in 1976 the PC and the mobile phone were science fiction, and the technology landscape has shifted seismically since then. In the meantime a lack of clear regulatory guidance has led to complaints of a delay in market development by some mHealth manufacturers.

The US

In the US, the Food and Drug Administration (FDA) is responsible for regulating medical devices. Like Competent Authorities in Europe, it has been relatively slow to regulate mHealth devices and mobile applications, but is now catching up.

The current legal framework on medical devices in the US dates back to 1976, under the Medical Device Amendments to the Federal Food, Drug, and Cosmetic Act. This enacted several key changes to medical device regulation, namely classifying devices into classes (a process which wasn’t completed by the FDA until 11 years later), and multi-tier controls based on those classes. Manufacturers also had to notify the Administration 90 days in advance of introducing a new product to market.

On July 9, 2012, President Obama signed legislation that allowed the FDA to continue with its work regulating mobile medical applications, and the agency is expected to release its final guidelines by the end of 2012. However, legal analyses of the current guidelines highlight several themes. In particular, the mHealth Regulatory Coalition (MRC) requested several broad changes to the FDA’s guidance.

Among other things, the coalition urged the FDA to:

- Focus on regulation of mobile medical applications that involve high-risk;
- Define important terms, including electronic health records, personal health records, general health, and wellness;
- Describe the premarket notification or approval process for mobile medical applications and the information the agency expects to see in a submission;
- Clarify the position for accessories plugged into mobile devices;
- Detail the agency’s expectations for distributors and platform manufacturers.

Brad Thompson, the author of the MRC recommendations, argues that ever since the 1976 Amendments were enacted, lobbyists have had ongoing problems with the scope of regulation.
“The FDA regulates [treatments for] disease, but it doesn’t regulate overall health and wellness,” he says. “For the first couple of decades, that wasn’t too bad because disease was something that you went to the doctor for. Not too much that you used at home was considered a medical device.”

However, mHealth applications have the potential to change that, Thompson warns.

Even daily health management such as getting enough sleep or exercise can be interpreted as reducing the risk of a disease, he says. And when applications are used in wellness areas that are linked to recognised diseases, such as depression, the regulatory guidelines become fuzzy.

“Healthcare and wellness have converged.”

Thompson points to real-world events where companies have inadvertently stepped over regulatory boundaries in the US. In 2009, the FDA sent a warning to General Mills after the manufacturer advertised that Cheerios can be used to help reduce cholesterol.

“This happens all the time with dietary supplements where marketers cross the line and draw a connection to a disease.”

Clarification of the accessory issue is also important, says Thompson, who points to a “long standing rule” at the FDA that something plugged into a medical device becomes regulated in the same manner as the device. “When you have a mobile phone and these mobile apps, there are a lot of things that people want to plug into,” he says. “Which of those articles are regulated? The FDA doesn’t address that in the draft.”

In February 2011, prior to the publication of its most recent guidelines, the FDA introduced a regulation defining a Medical Device Data System (MDDS). This class of mobile device is used to store and transmit data collected from a medical device to a physician or a health record or another ultimate endpoint. Devices of this kind can be ‘downgraded’ from higher-class devices to class I units. “So if the software on a mobile phone collects data from any of those sources and does nothing but collect, transmit, display in original form or convert from one set of parameters to another, then it’s a class I medical device regulated by the FDA,” Thompson says.

A class I medical device in the US is still subject to some fairly stringent controls. These include establishment registration, medical device listing, quality system regulation, labelling requirements, medical device reporting, premarket notification, and reporting corrections and removals.

However, it would be relatively easy for a mHealth app to remain regulated as a higher-class medical device, Thompson says. “If the original medical device produced ordered pairs, all the mobile phone app could do is display those ordered pairs in the same format as they’re gathered by the medical device,” he says. “If instead the app graphs them, it’s not the original display, and it’s not a class I medical device.”

The FDA regulates [treatments for] disease, but it doesn’t regulate overall health and wellness

Brad Thompson, the author of the MRC recommendations
Is your software medical?

How can manufacturers ascertain whether their software is subject to regulation as a medical device? One key can be found in current EU thinking on the subject, as outlined in January 2012. The European Commission published further guidelines then, designed to clarify the classification of software as a medical device. These guidelines, while not legally binding, were "drafted through a process of consultation of the various interested parties (competent authorities, commission services, industry and notified bodies in the medical device sector)" and are expected to make their way into law.

The guidelines include a flowchart, which describes the process thus:

1) If a computer program is embedded in a medical device, then it is regulatable

2) If it is stand-alone software but does more than storage, archiving, lossless compression, or simple search, and it is for the benefit of individual patients, and its action is in the scope of purposes for medical devices outlined by the Medical Devices Directive, then it is regulatable

3) If it does all of the things above, but it is outside the scope of the MDD, but is still considered an accessory to a medical device, then it is regulatable.

When it comes to that sub-class of software which is mobile applications used for medical purposes, some examples are cited in the US FDA Draft Guidance for Industry and Food and Drug Administration Staff on mobile medical applications. These include the following, which could be useful towards a wider description of mHealth software:

- Applications that allow the user to view medical images on a mobile platform and perform an analysis or process for diagnosis;
- Applications that connect to medical image servers and provide processing functions such as pan, zoom, measurement, auto contrasting, automatic detection of features, and other similar functionality;
- Applications that analyse, assess, or interpret electrocardiogram or electroencephalogram data;
- Applications that connect the mobile platform to vital signs monitors, bedside monitors, cardiac monitors, or other similar devices;
- Applications that connect to a home use diagnostic medical device such as a blood pressure meter, body composition analyser, or blood glucose meter;
- Applications that control a blood-pressure cuff connected to a mobile platform to inflate the cuff and measure a person’s blood pressure;
- Applications that act as wireless remote controls or synchronisation devices for MRI or X-ray machines.

These guidelines also cover mobile medical applications that transform or make the mobile platform into a regulated medical device by using attachments or sensors or similar medical device functions.

Both the FDA and the EU position regarding medical software applications, including mobile medical applications (see panel), open up some vendors to potential problems. Thompson says that his company took 100 downloadable apps from iTunes and categorised them as either regulatable, non-regulatable, or falling into a grey area. Roughly eight fell into the regulatable category; most were non-regulatable; but a full third of the apps surveyed fell into the grey area.

Given the number of downloadable mobile apps being published to smartphone app stores, this scale of uncertainty could present a real problem for this particular kind of mobile application. The iTunes store alone holds more than 13,600 iPhone health and wellness apps. This doesn’t take into account the broader app stores for other platforms such as Google’s Android, and Microsoft’s Nascent Windows 8 store. Extrapolating Thompson’s figures, roughly 4,500 apps in the iTunes App Store would already be worthy of review.

The review process itself will be time-consuming, and the steps involved in certifying an application will take still more time. This is a problem, because it contrasts directly with the fast-paced nature of the mobile apps business. Regulatory uncertainty and increased bureaucracy is anathema to innovation.
The steps to regulating an app

If a mobile application requires regulation as a class I device under EU law, then it is the manufacturer’s responsibility to go through the relevant steps. These are as follows, as laid out in the MHRA documentation:

1. **Preparation of relevant technical documentation**
   - Including raw materials and component documentation; final product documentation and packaging and labelling documentation.

2. **Development of corrective action and vigilance procedures**
   - This shows the measures that will be taken should the medical device be involved in a problem, such as a death or serious injury (what would a software developer do if its blood glucose monitoring application delivered inaccurate results that harmed a user, for example?)

3. **Notify the Authority of any proposals to carry out a clinical investigation**
   - All manufacturers should review the intended use of the product. They should be prepared to prove any medical claims that they are making, using test results or proof of experience. The MHRA says that this needn’t require a custom process. “Many class I devices will not require a special clinical investigation to establish data on performance and safety or side effects,” it says.

4. **Draw up the “EC Declaration of Conformity”**
   - This involves stating that the products meet the requirements in the Medical Devices Directive.

The ins and outs of regulation

The distributor (such as the owner of an App Store) cannot be expected to help with any of the above steps. Apple’s developer guide, for example, doesn’t verify that the content of a downloadable mobile app is correct, or that it functions properly according to industry-specific parameters. “If I made an app that passes Apple guidelines but contained absolute nonsense in terms of medical advice, it would still be part of the App Store,” says James Sherwin of d4, whose report outlines some key issues in the area of medical device regulation and its application to mobile software applications.

Another problem to tackle is that a medical device is rarely viewed as an entity on its own. Most often software and hardware exist within a broader ecosystem that often includes a communication network, a back-end processing function, and data archiving and storage. For example, if a software application is construed as a medical device under the definitions laid out by the Medical Device Directive or the FDA guidelines, is the hardware that it runs on part of that device? Does the network that it runs on, or the server that it communicates with, also part of that medical device? If it communicates with an electronic health record, is that also a medical device?

One of the issues facing mHealth device manufacturers is whether a mobile device itself such as a smartphone can be regulated as a medical device, when running a medical application. In this regard, at least, there is some clarity. The MHRA believes that if a manufacturer is packaging and marketing smartphone hardware and medical software to clinicians as a combined unit, then in theory the hardware would have to be certified as well. Conversely, if the phone is sold simply as a phone, then only the application would be potentially regulated as a medical device.

When it comes to infrastructure, the Medical Products Agency’s Working Group on Medical Information Systems distinguishes between systems created for a specialist purpose and general supply systems used for a variety of tasks. It classifies internal, external and telecommunications networks as general supply systems. “General networks are often not regarded as medical devices but instead as general supply systems,” it says. Back-end systems comprised of electronic patient records and patient portals could be another matter. The EU Working Group argues that electronic patient records can be classified as medical devices, and that portals containing interactive access to patient health information can also be classified as medical devices under the European Commission Medical Devices Directive (EC MDD).

“Other functions that are becoming available are to gather patient information by using different functions in the portal, like for instance making the patient enter information directly into the electronic patient record himself. If this information is intended for diagnosis, treatment or monitoring of a patient, then those parts should be handled as medical devices,” it says. The FDA has not yet taken a strong position here.
The regulation of mobile devices for healthcare in Japan has not been a top priority in a regime where existing regulatory frameworks are outdated and in need of reform.

The telecommunications regime has shifted dramatically over the past 15 years to encourage new entrants and the development of new service markets. However, the US has worked with the Japanese to try and kick start a medical regulatory system that appears to lack momentum. The US Trade Representative has encouraged the country to “take measures to ensure Japan’s policies appropriately support the availability of innovative pharmaceuticals and medical devices for Japanese patients.”

In Japan, medical devices are regulated by the Pharmaceuticals and Medical Devices Agency (PMDA), which operates within the Japanese Ministry of Health, Labour and Welfare. There is little if anything published about the role of mobile devices and software apps for mHealth by the PDMA, although other agencies have been eager to promote telemedicine, especially in rural areas. In 2008, the Ministry of Internal Affairs and Communications (MIC) joined forces with the Ministry of Health, Labor and Welfare to create a Panel on Telemedicine Promotion Measures. The panel explores the use of telemedicine in rural areas.

The country classifies medical devices into three broad areas:

- general medical devices (class I)
- controlled medical devices (class II)
- and specially controlled medical devices (classes III and IV).
The approval of medical devices in Japan is governed by the Japanese Pharmaceutical Affairs Law (PAL). Class I general medical devices affectively jump straight to premarket submission to the PMDA. They do not require a certificate. Class II devices must be measured against ISO 13485, a quality management system standard before gaining premarket certification. The class II device is then subject to a quality management system audit before being granted a premarket certificate. The two classes above are subject to a premarket approval application, and manufacturers must also prepare a registration dossier before submitting the application to the PMDA, which then conducts the quality audit. After that, the device may be given a premarket approval certificate. Key to this process is the Marketing Authorisation Holder (MAH), an authority often held by a device distributor, who handles the regulatory responsibilities.

Overall, the Japanese medical device regulation process is relatively complex. It is not helped by the relative age of the laws involved. The PAL was last updated significantly in 2005, and is only now up for review again, following lobbying in July 2011 by the Japan Federation of Medical Device Associations. One of the biggest complaints is that the law as it stands subjects pharmaceuticals and medical devices to the same regulatory processes. One of the biggest changes that has been requested is a separation of these categories, and revised laws that focus specifically on medical devices.

In this regard, Japan seems to lag other regions such as the US and the European Union. However, the properties by which medical devices are classified are fairly straightforward. A class I device has “extremely low risk to the human body”. An example would be an X-ray film. A class II device has a low risk. MRI machines and digestive catheters are given as examples. Class III and class IV devices have medium and high risk to the body. Artificial bones, pacemakers, and artificial heart valves are good examples.

One other potential problem facing mHealth developers is the misuse of the device, either intentional or otherwise. “It gets tricky where applications behave in a way that wasn’t intended by the developers,” says Deven McGraw, director of the Health Privacy Project at the Center for Democracy & Technology. “That happens after-market, but there isn’t anyone that will go back and look at that and regulate it.

Hackers are known for their propensity to dismantle and repurpose hardware and software. “The developer might not control that,” McGraw says. The European Working Group on the topic acknowledges says that while manufacturers are responsible for extending their usability analysis to predict foreseeable misuse through user error, the user is entirely responsible for deliberate, abnormal use.

“The liability then rests fully on the user but does not automatically free the manufacturer from updating the risk analysis, monitoring and minimising the consequences for possible misuse if it is reasonable,” it says.

Overall, regulations can pose a bureaucratic hurdle, but they are also there to provide clarity for technology companies and healthcare organisations as they try to innovate and improve care quality. Manufacturers in particular must pay close attention when assessing their products to see if they fall under the mandate of medical device regulation. Many products will be clearly outside the regulatory mandate, but there will be some that fall into a grey area. Given the relatively low barrier to entry for class I medical device certification, those manufacturers with any doubts might be well-advised to take the plunge and submit their device for medical regulation to cover their bases.
Conclusion

As they grow in scale, mHealth initiatives will allow ever larger numbers of patients including older people to have greater involvement in their care; help manage their own long-term conditions; and enjoy more independent, active lives.

But as this report has shown, there are also several potential concerns over patient privacy, and security of health data, that need to be addressed to ensure new systems will achieve success.

With mHealth systems often tracking and monitoring patients in real-time, with or without their intervention, and with that data potentially accessible by various groups of people, security and regulation are vital to protect people’s privacy. Further complexity is added where there is the possibility of data moving across national borders and jurisdictions, for example where international companies or NGOs are involved.

One area that needs to be looked at closely is user consent. We need to move from a box-ticking approach to compliance that simply asks people to click once at the outset on “I agree” buttons – which people invariably do without bothering to read the small print – towards a much more sophisticated and flexible ongoing dialogue with the patient about data usage and consent.

There is also clearly a need to develop and monitor robust but usable data security technologies for both specialist mHealth devices and general devices such as smartphones that may be used for healthcare purposes.

Role-based access to health records may not be the best model for the new, flexible, innovative projects springing up under mHealth: increasingly, security will need to be designed in to systems in more complex ways.

This report has also shown that there are other major challenges for mHealth systems relating to regulation.

This stems partly from the fact that mHealth falls between two regulated areas: medical devices, and telecommunication systems. Governments and regulators need to work hard to clarify issues including what constitutes a medical device; how medical software should be regulated; and the regulation of networks of different types of device. And again, where there is an international element, matters will become even more complicated.

Ultimately, to make strong progress with mHealth, policymakers must draft the laws, regulations, and standards needed to protect patient privacy, and enforcement agencies must ensure these are implemented.

Involvement by technology developers will also be essential. Above all, as we found in our previous insights guide on the politics and economics of mHealth, it is crucial for all stakeholders to collaborate to allow for innovative mHealth technologies to transform our health systems in a safe and sustainable way (also see pages 32 and 33).
Overall, mHealth systems are leading the way towards a new wave of patient-focused care in the home and in the community.

They also have the potential to expand and accelerate healthcare research, adding elements of large scale live monitoring and feedback.

But patients’ needs must also be placed centre stage when looking at issues of personal privacy, data security and device regulation.

We are still at an early stage in our understanding of many of these issues, which are at the intersection of many connected fields, and cross between the use of general consumer technologies and specialist professional clinical technologies.

With these two fields converging, and innovation in both proceeding at a breakneck pace, regulation is a particular challenge. Regulatory uncertainty is anathema to innovation: but so is unnecessarily cumbersome bureaucracy. All stakeholders must move fast, but tread lightly.
National governments

- National governments must move to review and update data protection and privacy laws, regulations, and standards needed to protect patient privacy in the context of mHealth development.
- High level statements of principles must be complemented by more detailed requirements for bodies carrying out specific data processing acts.
- Efforts must be made by governments to explain data protection and privacy issues to patients, and win public trust for mHealth development.
- Governments must work to ensure that data protection and privacy cultures within businesses and healthcare organisations are strengthened in line with legal requirements, and that organisations support awareness campaigns to boost citizen and patient awareness as above.
- Governments need to review and harmonise systems of medical device and telecoms regulation to co-ordinate activity and open up technology and healthcare markets.

International bodies

- International associations and intergovernmental bodies must review policies and agreements relating to secure storing and processing of data between national borders and jurisdictions in a healthcare context.
- International agreements in this field are urgently needed beyond the US and Europe into Asia and Africa.
- Countries and global regions must develop programmes to share ideas and best practice in these fields, for example in ways of securing patient consent for data use.

Healthcare funders and providers

- Healthcare funders and providers should try to ensure any systems used in clinical trials of mHealth have been properly assessed by medical device regulators where appropriate.
- Healthcare providers should review their research policies to ensure there is effective anonymisation of data gathered by mHealth networks, given the challenges of anonymising location-based information.
- Funders and providers should assess the options of balancing patient-controlled mHealth systems and automated “M2M” systems in constructing mHealth networks, systems and trials.

Technology and telecoms companies

- Manufacturers must pay close attention when assessing their products to see if they may fall under the mandate of medical device regulation.
- Technology and telecoms suppliers need to build in systems of patient consent to devices and software with potential mHealth uses.
- Smartphone security for apps and data needs to be usable, strong and take into account the potential diversity of mHealth uses and networks.
- Suppliers need to collaborate with other stakeholders to develop user education programmes to promote awareness of health data security measures and good practice.

Considerations for key stakeholder groups

to help them collectively tackle the barriers we all face
Medical device regulators
- Medical device regulators must draw up clear guidelines to help differentiate between devices for clinical use and lifestyle or wellbeing use; general use devices, and specialist devices; accessories plugged into other devices; and devices that collect, transmit, control and monitor data.
- For each class of device, regulators must clearly specify what controls are needed such as registration, documentation and plans for vigilance and corrective action.
- Medical device regulators must collaborate (and avoid duplication of effort) with telecoms regulators in the field of mHealth regulation, particularly in areas such as transmission of data to and from devices; data integrity and audit trail.

Pharmaceutical and medical device industries
- The medical device industry must ensure data security is paramount in their development programmes, including for sensors with low computational power.
- The industry must strive to ensure systems for patients to grant and revoke consent for all uses of their data are appropriate and flexible.
- The industry must also place standards and interoperability at the heart of their work, so it is as easy as possible for patients to securely add new devices such as sensors to their networks.

Technology and telecoms regulators
- Technology and telecoms regulators must collaborate with medical device regulators for the same reasons set out above, and to promote innovation in their own industries.
- Telecoms regulators must promote capacity, reliability and interoperability of telecoms networks serving mHealth projects.
- Telecoms regulators should ensure their mHealth work connects with broadband access projects, to ensure good inclusion in rural areas for mHealth projects.

stakeholder groups
Vodafone Global Enterprise

This Insights Guide has been commissioned by Vodafone Global Enterprise

Vodafone has been active in healthcare for over a decade and set up Vodafone mHealth Solutions in 2009 within our Vodafone Global Enterprise unit. Vodafone Global Enterprise provides services to Vodafone’s multinational customers, including most of the world’s leading pharmaceutical, medical technology and health insurance providers.

The range of opportunities for mobile technology within the health sector is almost limitless. Ageing demographics and the global increase of chronic disease across the healthcare landscape require healthcare to become more accessible and affordable. Healthcare professionals need to make efficient use of their time and companies in the sector need to maximise their budgets and market position. Emerging network and mobile technologies will help to transform the health industry.

For more information, please visit: enterprise.vodafone.com/healthcare
• How to protect patient privacy in a mobile world?
• User consent: what is the best way to agree?
• mHealth security – high risk, low awareness?
• mHealth and regulation – when is a device medical?

What is your view?
Join the online debate now:

#mhealthbarriers @Vodafone_VGE
mhealth.vodafone.com/linkedin
References


