mHealth – companies that meet the legal issues early will get a head start on the commercial benefits of this market.

The rise of mHealth opens up the possibility of empowering patients to choose where and when they engage with healthcare services. Imagine being able to go on holiday and still have your heart check up; just as BMW provides remote diagnostics for your car, your doctor will be able to do the same for your heart. These developments need close cross-sector collaboration from those in the healthcare and TMT sectors.

This paper discusses the main legal issues which those in the mHealth market need to anticipate and work with.

Technology providers must find ways to overcome the unique challenges that come with this new territory. These include data security concerns, a rapidly evolving legal and regulatory landscape, changing models for IP protection and the increasing importance of interoperability standards. Companies that can find innovative ways to tackle these issues will be the main commercial beneficiaries in the coming mHealth revolution.

ABI Research predicts that the worldwide revenues from mobile health will be $5 billion in 2014.
Source: Accenture: mHealth
What are the key issues?

The most important legal risk points for technology providers are:

1. **Addressing the concerns around data security**
   The main challenge is making sure that the underlying IT infrastructure for mHealth services is secure and that patient data privacy is properly protected. This will involve a combination of regulation as well as technology innovation. At the moment, there are no standards specific to mHealth and so auditing suppliers for data risk is a bespoke (but necessary) process. Security is often thought of as down to the technology, but it is as much a matter of behavioural or organisational issues – for example, how many organisations or healthcare professionals in the supply chain will have access to mHealth data, and to what datasets?

2. **Keeping up with evolving medicinal and medical devices regulation**
   The regulatory landscape for medicinal and medical devices is changing. It will be important for technology providers to keep abreast of these changes and actively work with industry and other stakeholders in developing standards and systems of interoperability. This will be critical in building trust in the innovations that are coming through. There are some big issues to think through – for example, to what extent will consumer devices or apps need a prescription? The challenge will be to work towards an array of mHealth services that can deliver safe and high quality care without burdening the system with red tape.

3. **Protecting innovation from copycats but encouraging this market and meeting the need for standards**
   This will mean thinking strategically about IP protection and how best to protect your investment in research and development. This may also require a rethink of some of the more typical models of IP commercialisation.

4. **Allowing this market to develop within the broader development of technology platforms which can partition markets**
   This will need to sit alongside broader government agendas of keeping health management and treatment open to all. The approach taken by some governments (such as in the UK) is to try to adopt royalty-free interoperability standards where possible, or to only select standards where the royalties are low as this reduces the risk of the uptake of technology being delayed due to patent protection.

"The European Commission will also be releasing a study on the interoperability of electronic health records later this year and a more comprehensive Green Paper by the end of 2014. The issue of mHealth is therefore firmly on the agenda for European governments and policymakers."
What is mHealth and how is it shaking up the healthcare industry?

Mobile health (or mHealth) is a part of the broader eHealth initiative that will provide medical resources and deliver healthcare services by electronic means. mHealth is specifically the provision of healthcare services and information through mobile devices such as mobile phones, wireless monitors, video and online conferences and personal healthcare devices. It can cover diagnoses, treatment, prevention and monitoring, as well as emergency responses and healthcare practitioner support.

The current interest in mHealth is driven by two relatively recent phenomena: the use of mobile technology and the increasing demands being placed on healthcare services. Across Europe, an ageing population, shrinking government budgets and dramatic rises in healthcare costs have translated into long waiting lists, high demand for long term health management and a “postcode lottery” for access to treatment for chronic diseases such as cancer. The ubiquity of wireless technology can help deliver practical solutions to these problems. For instance, the ability to use devices such as mobile phones to access information on healthcare, remotely book appointments and monitor patients can improve accessibility to healthcare services without driving up costs. Mobile devices can also (securely) hold customised data relating to a patient’s medical history which can help improve the quality of healthcare services. GP Bullhound, a leading US headquartered technology corporate finance adviser, predicts that the health app market will enjoy a breakthrough in 2013. We are starting to see this play out in practice with companies such as Microsoft, Dell and Samsung all announcing mHealth related features on their latest consumer devices.

mHealth is ultimately all about increasing efficiency, accessibility and the quality of healthcare through the use of technology. However, like any disruptive technology, mHealth brings with it a unique set of challenges.

In 2012, an Economist Intelligence Unit report, commissioned by PwC, found that 46% of patients said that they would begin to use mHealth, or increase their use of it, if it enables them to access healthcare providers more conveniently or effectively. Source: Emerging mHealth: Paths for growth, PwC, June 2012

Worldwide, over 700 million smartphones were shipped in 2012, an increase on 2011 of over 40%. Almost half of all handsets shipped were smartphones. Sources: Strategy Analytics (February 2013) and mobiThinking.
The most common concerns with mHealth relate to the collection, storage, processing and usage of patient data. A recent PwC study found that whilst over half of the patients believe mHealth initiatives will make healthcare more convenient and accessible, doctors and patients are both concerned that the existing IT infrastructure may not be sufficiently secure and that behavioural security issues have not been addressed properly. The usual trade off that is made in other sectors between user convenience and security does not adapt well for mHealth given the sensitive nature of the underlying data.

Many mHealth applications are likely to make use of cloud data storage. Just as the financial services sector has discovered that the existing legal framework is not well adapted to enable the use of financial data in the cloud, mHealth will have to work through similar issues. The legal framework assumes national (or at least European) ring-fencing of patient data – whereas the cloud allows storage in any geography. In financial services, providers of cloud services like Microsoft have adapted some products as a specific regulatory play – allowing the purchaser of cloud services to see (i) where their data is and (ii) which parties in the supply chain have access to their data.

Cloud storage is however a possible solution to big data security although the regulation which will specifically accredit cloud storage for data security does not exist yet. Public clouds certainly are not suitable for medical data. A way through this will have to be found because cloud is the obvious data storage solution for mobile services, given that it is so large-scale. Companies developing the necessary IT infrastructure need to be conscious of the obligations imposed under data protection legislation for the storage of such data and alive to the concerns relating to patient privacy. At the moment, this means auditing your data storage solution for comfort on security – no accreditation scheme is going to do that for you. The emphasis in the proposed EU Data Protection Regulation on "privacy by design" will also require providers of technology to "design in" privacy into the architecture of their products and services; this means privacy featuring at a much earlier stage in product/service design than is typically the case in many other sectors.

The platforms that are developing for the exchange of mHealth services for classes of patients (for example, in the areas of disease prevention, monitoring or management) need to be assessed for data security on a platform by platform basis. For instance, there are already software applications and devices on the market that allow clinicians to collect data remotely and monitor medical data about patients. If this exchange takes place over standard telecommunications networks (e.g. 3G or wireless networks), both the healthcare operator and IT companies will need to ensure that there are appropriate protections in place to prevent leakage of the data. Ensuring that patient privacy is properly protected will be critical in securing public confidence in mHealth. This is likely to happen through a mix of regulation and secure technology.

Concerns have also been raised over how patient data may be used in the context of health insurance. For instance, some patients are concerned that if they share their health data using mHealth services, health insurance companies could get access to the data and potentially use it to raise premiums. In addition, the data streams released as a result of patients using monitoring devices could be exploited; those companies wishing to use a commercial model to exploit this will need to tackle questions about IP ownership in such data resources as well as the potential negative public reactions to the use of such data. Whilst some of these concerns may be overblown, there is a real need for public debate to help focus the policy options. This is particularly relevant given that in most developed countries, mHealth initiatives are likely to be largely funded by the Government and the private health insurance industry, who will have potentially competing agendas on data access.
It is no secret that the healthcare industry is conservative. Even small technological developments can take a long time to get the regulatory stamp of approval. mHealth will be no different. In fact, the regulatory issues facing mHealth are likely to be even more challenging for at least two reasons. The first is that mHealth fundamentally redefines the long-standing social contract between doctors and patients. Patients using mHealth services will have more ability to actively take part in their own health management and treatment. The second is that the technology is still in its nascent stages and many of the regulatory issues have not yet crystallised. With any technology that empowers people, there is an institutional reaction which is to not trust the individual to use it wisely.

There are already steps underway to help cut through some of the issues. For instance, the US Food and Drug Administration (FDA) recently issued a description of low-risk mHealth areas, such as patient self-management, that will not be regulated. This is good news. In Europe, there are forthcoming regulations on medical devices, which will have an impact on how quickly mHealth can be implemented. The proposed EU wide medical devices regulation that is currently being debated by policymakers will also have to be coordinated with the regulatory framework on radio equipment and telecommunications.

The new regulatory framework will need to find answers to various conceptual as well as practical challenges. This will include:

**Ensuring that regulation is sufficiently clear whilst retaining a degree of flexibility**

There is a danger in defining regulatory obligations too narrowly. For instance, it is unclear how “medical device” definitions and classifications will work for mHealth products and services. This could be particularly significant where products have both medical and consumer related functionality – an example is a mobile phone which can be adapted to work as a heart monitor. The rapidly changing nature of the technology and unpredictable patient behaviour will further compound these issues. In addition, developer, device manufacturer and everyone else in the supply chain need to be properly adapted to mHealth systems.

**Striking the right balance between pre-market scrutiny and post-market surveillance**

The products and services potentially covered by mHealth technologies could range from simple services such as to make booking appointments easier, to complex remote diagnostic and treatment tools. This means that regulation necessarily needs to build in a level of flexibility. Recognising this, the recent proposal by the EU Commission to overhaul Europe’s medical devices regulatory scheme is built on a “lifecycle” approach to regulation which places greater emphasis on post-market regulation and surveillance for products in lower-risk categories. However, it remains to be seen how this will play out in practice for products that are purely software-based, or services that rely on input from a number of different people.

**Protecting patient safety**

Most mHealth initiatives involve reducing the level of direct interaction between doctors and patients. Understandably, doctors are concerned about the prospect of patients self-medicating without having proper regard to professional medical advice. To some extent, the genie is already out of the bottle because of the exponential growth of patients ordering over-the-counter and prescription medicines over the internet. There is no simple solution to doctors’ concerns. However, the proposed EU regulations suggest that the authorities will increasingly take a more “risk based” approach to regulation rather than impose prescriptive rules. For instance, the recently issued guidance from the FDA suggests that medical “apps” are likely to be assessed on the basis of how much harm they could cause if there were problems with the app itself or the information it contains.

**Standardisation and interoperability**

As mHealth technology matures over the next few years, it is likely that various aspects of the technology will become standardised. Standardisation is already prevalent in the telecommunications industry but is less common in the medical devices field. It will be important for technology providers to play a leading role in standards-setting as this will allow them to drive the technology agenda and give them an edge over their competitors. Where Government funding is involved, the use of open standards is likely to be encouraged. Many eHealth initiatives will also be platform technologies (for example telehealth services) and will need to be integrated with existing IT healthcare infrastructure. It is therefore essential that companies take a long term and a strategic view when entering into this space and that regulators focus on ensuring flexibility of infrastructure to allow patients long term choices of providers. To add to the complexity, competition authorities are also likely to keep a close eye on technology providers with significant IP holdings who can exert influence over different parts of the market.
Intellectual property protection will be critical in protecting the significant investments that companies are making to develop and implement mHealth solutions. However, given that the value proposition for mHealth centres on bringing together the expertise of healthcare professionals for the disparate needs of patients, it may be necessary to re-think some of the traditional business models.

Many mHealth initiatives are about developing suitable platforms or the necessary IT infrastructure to deliver healthcare services remotely. The success of these initiatives will depend on the level and the rate of adoption of these technologies. It may therefore make more sense for companies to adopt an open source or an open platform model to their IP in certain circumstances. This is because allowing others to innovate and develop solutions using these platforms and infrastructure will help drive up their value and enable technology providers to extract higher revenues through the provision of these basic services. It also means that technology providers will not have to always “second guess” what patients want or the best way healthcare services should be delivered.

The protection of the intellectual property itself will also bring new challenges. Recent developments in European law have narrowed the scope of copyright protection for software. Given that many innovations in mHealth will involve at least some elements of software, technology providers will need to think carefully about their IP strategy. It is possible that patents will be increasingly important in this area. Traditionally, it has been very difficult to get patents for software innovations which do not have a direct technical effect in the “real world”. Software innovations in mHealth may be able to overcome this hurdle more readily, given that software will often be used either directly by patients or integrated into hardware devices.

Conclusion
mHealth is transforming the healthcare landscape by revolutionising the way people interact with doctors and making healthcare services more efficient and accessible to more people. These changes require a rethink of some of the traditional approaches to regulation, data protection and IP protection. To succeed, technology providers need to find solutions to these unique challenges as well as to actively engage with the industry and regulators to shape policy.

For further information and advice in relation to mHealth issues, please contact:

**Matthew Godfrey-Faussett**
Partner, Big Data  
T: +44 (0)131 777 7101  
M: +44 (0)7776 198976  
E: matthew.godfrey-faussett@pinsentmasons.com

**Allistair Booth**
Partner, Intellectual Property  
T: +44 (0)20 7418 8272  
M: +44 (0)7500 883856  
E: allistair.booth@pinsentmasons.com

**Deborah Bould**
Partner, Intellectual Property  
T: +44 (0)20 7490 9306  
M: +44 (0)7717 488457  
E: deborah.bould@pinsentmasons.com

**Charles Waddell**
Partner, Business Models  
T: +44 (0)20 7418 8271  
M: +44 (0)7831 603449  
E: charles.waddell@pinsentmasons.com

**Barry Francis**
Partner, Pricing  
T: +44 (0)20 7418 7340  
M: +44 (0)7973 312150  
E: barry.francis@pinsentmasons.com

**Florian Von Baum**
Partner, Cross Border / Off Shoring  
T: +49 89 203043 537  
M: +49 172 368 01 88  
E: florian.vonbaum@pinsentmasons.com

**Indradeep Bhattacharya**
Author and Senior Associate, Intellectual Property  
T: +44 (0)20 7490 6385  
M: +44 (0)7836 616662  
E: indradeep.bhattacharya@pinsentmasons.com
This briefing does not constitute legal advice. Specific legal advice should be taken before acting on any of the topics covered.

Pinsent Masons LLP is a limited liability partnership registered in England & Wales (registered number: OC333653) authorised and regulated by the Solicitors Regulation Authority and the appropriate regulatory body in the other jurisdictions in which it operates. The word ‘partner’, used in relation to the LLP, refers to a member of the LLP or an employee or consultant of the LLP or any affiliated firm of equivalent standing. A list of the members of the LLP, and of those non-members who are designated as partners, is displayed at the LLP’s registered office: 30 Crown Place, London EC2A 4ES, United Kingdom. We use ‘Pinsent Masons’ to refer to Pinsent Masons LLP, its subsidiaries and any affiliates which it or its partners operate as separate businesses for regulatory or other reasons. Reference to ‘Pinsent Masons’ is to Pinsent Masons LLP and/or one or more of those subsidiaries or affiliates as the context requires. © Pinsent Masons LLP 2013.

For a full list of our locations around the globe please visit our websites: