EU mHealth Green Paper: Members' Responses

Introduction

The sections below are organised according to the requests for comment in the EU Green Paper on mHealth. The responses given reflect the stated views of the current 185 members of the Digital Health And Care Alliance (DHACA) who are drawn from across the board of government, academic, large corporate, SME and charity sectors, and include both patient and mHealth developer representation.

Summary

DHACA supports the European Commission's drive to improve the beneficial use of mHealth technology. In our response, below, we have evidenced a range of initiatives in the UK that we believe could be beneficial if adopted across the EU, as well as evidencing some excellent exemplars elsewhere in the EU.

Of particular note are our proposals that:

- Health data should be treated as a separate classification of personal data in the Data Protection Directive;
- The CE mark concept be extended to cover data protection & information privacy;
- Attention should be paid to ensuring conformance of mHealth apps with existing legislation;
- The many different (and for many, confusing) regulations affecting mHealth should be simplified;
- A national or EU-wide organisation should take on the role of determining the cost-effectiveness of mHealth apps;

- Suppliers should be encouraged to promote more responsible and better quality app development and health system adoption, aided by a public awareness campaign;
- The guidance on information governance within EU health-providers should be updated to reflect the need for data sharing with mHealth solutions;
- There is a specific beneficial role that the EC should accept to enable those creating apps that they wish to offer for free to do so (i.e. without needing to charge users, in order to pay for costly liability insurance).

Finally, whilst the emphasis on m in mHealth is welcome DHACA believes that EU policy needs to embrace the Internet as well; mHealth should be seen as part of eHealth systems and solutions that help bridge the gaps between care and cure, wellness and illness, and condition and clinicians.

Data protection & security:

1. **Which specific security safeguards in mHealth solutions could help to prevent unnecessary and unauthorised processing of health data in an mHealth context?**

Response:

EU data protection legislation attempts to balance the rights of citizens against organisational ownership of the use of health data, although in our opinion enforcement is currently weak and ineffective across global borders. Global brands are however vulnerable to reputational and consequential financial damage and therefore more likely to invest in developing customer trust. The ecosystems they create should be held accountable to one or more international standards for privacy and confidentiality.

DHACA supports the 2010 resolution of the International Conference of Data Protection and Privacy Commissioners for the development of a binding international instrument on personal data protection and privacy. ISO27001 is a recognised information security standard, however there is no similar international standard for data protection and privacy. DHACA supports the principle of developing a consistent and predictable international data protection and privacy standard that is technology neutral. This should be underpinned by an internationally accepted set of data protection principles.

Health is increasingly treated as a separate classification of personal data. Whilst classified as Sensitive Personal Data in the Data Protection Directive, it is inconsistently differentiated within member countries and recognised differently in the global context.

DHACA asserts that personal health data should be differentiated in law. Within the UK, the Common Law 'Duty of Confidentiality' applies to clinical consultations and the personal data these interactions generate. Clinical mHealth applications that connect patients to their clinicians should be differentiated in a similar manner and this included in data protection law. This offers a clear legal distinction between clinical and lifestyle applications, allowing the market to respond and apply security features appropriately. Of course, this would need further research and consultation to determine what taxonomies are fit for purpose across EU member states and could expect reasonably to be implemented.

DHACA believes there is a need for quality assurance for clinical mHealth applications. This is likely to be self-regulation through one or more non-governmental subscription organisations with a remit for impartiality. Establishing appropriate industry-agreed accreditation principles and implementation bodies will be important. Emphasising (and demonstrating) the business value of investment in accreditation processes (e.g. increased sales potential, decreased risk) will be vital for extending compliance.

DHACA welcomes proposals for privacy by design and by default contained in the proposed General Data Protection Regulations, and in particular the proposed approach to consent. Evidence of informed consent must be explicit and recorded for clinical applications, and ownership of personal data must be legally attributed to the data subject, with a right to erasure (aka 'right-to-be-forgotten'). Research will be necessary to develop the principle of 'privacy by design' to the reality of interoperable, standards-compliant privacy by design and its implementation as a matter of course. We are concerned that the Regulations may outpace the implementation potential by some months (or even longer).

The complexities of provider organisations and ecosystems require informed consent to be made more manageable. DHACA supports simplifying privacy notices around the batching of consents into 'one-click' options with granular controls for those who prefer greater control. There should also be simple consent options for disclosing personal data for the research or common good, e.g. ranging from 'I consent to my anonymised data being made available for research purposes', or 'I do not consent to my data being used for any additional purpose'.

Differential-consent software innovations are another option to consider, for example those which allow the citizen to specify n advance whether their data may be shared for certain purposes or by certain users, and any time restrictions they wish to make.

Lifestyle applications should be able to use standard web authentication and security protocols such as SSL, TLS etc.

Within the UK, the Public Service Network and Public Service Network (Health) impose stringent constraints that effectively prohibit external access to personal data held on connected public

service systems. Within such an intolerant regime it is unlikely that personal data will be released to external apps other than in aggregated and anonymised form or through a read-only portal using a recognised ID provider. The value of personal health information (e.g. lifestyle or bodily functions) in clinical consultations must be recognised, and some standardised means of making these available from mHealth providers to clinicians must be considered, (e.g. quarantine and validation). An alternative might be the provision of intermediate spaces where data from patients' own devices, and consented data from health systems, can be brought together in a non-firewalled but secure shared area in the cloud.

Within the EU there is a strong case for the use of government approved ID providers where they are in place to validate user accounts to assure clinical interactions via the web. The UK government's ID Assurance Programme is a good example of an effective mix of the private and public sector in assuring online identities.

Clinical applications should in all cases be subject to a formal technical risk assessment to international standards, and service providers should not be approved unless a properly scoped ISO27001 certification is in place.

All communications between consumers and mHealth applications should as a minimum encrypt against an Extended Validation (EV) Certificate.

2. **How could app developers best implement the principles of "data minimisation" and of "data protection by design, and "data protection by default"[1] in mHealth apps?**

Response:

App developers should be required to be open and transparent about the data used by each mHealth solution. In particular, the app developer should provide a public statement on the purpose of a solution, a description of what data is used, and why this data is needed to achieve the solution's purpose. App developers should incorporate the principles of data protection-by-design/default/minimisation into their development lifecycle and train their development, test and marketing teams to apply the principles as part of the organisation's processes and procedures for creating mHealth solutions.

Our preference would be to require certification of adherence to the above principles in a data protection version of the "CE" mark – ideally we would like to see the CE mark covering

[1] As per Article 23 of the Proposed REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

compliance with both medical and data protection/information privacy regulations though we recognise that might prove challenging.

If none of the proposals in the last paragraph is acceptable, all mHealth apps that do not comply with these principles should require users to accept a risk warning, like investment risk warnings which are required by law. Ultimately, once fully elaborated, developers of health-related apps sold in the EU should be required by law to comply with the principles.

As noted in previously, major investment is needed in order to establish and maintain appropriate accreditation authorities and enforce compliance where necessary. In the interim, the completion of standardised templates for developers to complete (e.g. structured terms and conditions forms with strict word limits to aid user reading) could be a minimum requirement and could be easily enforced by app stores and such like.

Big data

1. **What measures are needed to fully realise the potential of mHealth generated "Big Data" in the EU whilst complying with legal and ethical requirements?**

Response:

The insights from analysis of large data sets (aka Big Data) in the form of improved medical diagnosis and treatment, particularly when allied with genomic data, will be immense. mHealth as well as other modes of patient care will all benefit greatly. A prerequisite for successful deployment of Big Data is the ability to access and analyse large datasets from real patients. This, in turn, requires a high level of trust to be established, not just for those within the health and allied professions, but among patients and carers – and is especially necessary as the technologies utilised have the capability to gather, store, share or analyse increasing amounts of both health and *lifestyle* data. The broadening scope from a health condition to a lifestyle focus means that the impact of breaches of privacy can, therefore, be heightened and must be countered by ensuring that there are accessible audit trails and the putting in place of arrangements for data sharing, etc. within the context of creative commons licenses or similar.

For useful analytical work, data must be patient centred and holistic, including information from multiple sources (incl. social services, pharmacy, optician, volunteers, charities, family etc.). Otherwise the improved understanding of outcomes from complex situations cannot be made. This makes it difficult to anonymise the information and instead suggests a greater onus be placed on data aggregators and processors to retain privacy.

There is significant concern expressed by legal experts that many of the provisions of the proposed General Data Protection Regulation expected to be implemented in 2015 will severely limit the ability to access such data in an analysable form. We would therefore request that this regulation be carefully scrutinised so as not to increase further the constraints on big data analytics.

We would also flag the challenges involved in moving between organisation-centred and person-centred data environments, which remains an area of great complexity and uncertainty.

Applicable EU legal framework:

1. **Are safety and performance requirements of lifestyle and wellbeing apps adequately covered by the current EU legal framework?**

Response:

Yes we believe they are – however the issue, certainly in the UK, is that there is little if any policing to ensure compliance, and to prevent those not meeting the framework from continuing to offer their product.

Our principal concern here is where a lifestyle/wellbeing app actually performs an important medical function although is so worded as to escape classification under the EU medical device framework. An example of this is apps that purport to identify changes in mole size, as these risk giving users a false sense of security, putting off a visit to the doctor until after the cancer has metastasised.

Whilst the number of health & wellbeing apps, depending on how they are classified, is already in the 40,000+ range and so hard for a central body to review systematically, we feel that at least there should be an organisation – either centrally within the EU or in each EU country that consumer and medical organisations should be able to refer apps to that has the power ultimately to ban their use if requested changes are not made. Existing legislation should be sufficient to enable this to happen. This should be supported by a public awareness campaign to help people understand the clinical and data protection risks associated with medical apps that have not been safety checked or CE certified within the EU. There is of course also the issue that, using the Internet, people can download apps from websites in other countries that would bypass any such EU controls, analogously to the purchase of drugs in other countries. This merely endorses the need to improve public awareness of the dangers of uncertified apps.

2. **Is there a need to strengthen the enforcement of EU legislation applicable to mHealth by competent authorities and courts; if yes, why and how?**

Response:

With specific reference to compliance with the Medical Devices Directive the Active Implantable Medical Devices Directive and the In Vitro Devices Directive, currently in the UK the MHRA by their own admission has insufficient staff to enforce legislation although they say they will investigate any concerns raised with them about specific apps that should be CE certified.

Currently some health authorities in the UK still appear to be relaxed about clinicians in their employ using mHealth apps that have not been checked for safety/CE compliance although with the recent appearance of the first CE-certified hospital app platform, there is now less excuse. The concern is that resultant death or serious injury blamed on a rogue app will result in a widespread ban on their use which would have serious knock-on effects in reducing efficiency of care delivery especially in hospitals as these apps – especially those that perform complex calculations – save considerable time for clinicians as well as enabling faster treatment for patients.

One way of making the policing problem more manageable might be to refine the categories into which apps fall and then policing each appropriately.

With specific reference to compliance with data protection regulations, we await the detailed content of the new regulation. Enforcing compliance will be difficult in the current environment. Strong EU engagement with the major app stores and app clearing houses (e.g. NHS apps library) will be vital for ensuring appropriate expectations for developers are disseminated and filtering proposed products.

Note that, as mentioned elsewhere in this response, there are also a number of other EU directives that mHealth needs to comply with that are handled by different organisations in the UK. Rather than strengthening legislation further, perhaps drawing together and simplifying the legislation affecting mHealth would be better.

A major issue is the ownership of personal data rights within this ecosystem. It can be hard to determine who owns what, where the data are going and whether it is being resold in ways that compromise individual privacy. Changes to the European regulations, for example right-to-be-forgotten, will be helpful but greater transparency on the part of vendors is vital.

Patient safety and transparency of information

1. **What good practices exist to better inform end-users about the quality and safety of mHealth solutions (e.g. certification schemes)?**

Response:

In the UK, the NHS runs an Apps Library which currently lists over 200 health & wellbeing patient-facing apps. Where there is a potential safety issue these are reviewed against the UK NHS safety standard ISB0129; only those passing are listed. This library only checks for safety issues and relies on providers informing them of upgrades to apps; no regular checks are carried out. Where an app is likely to require CE certification, the library staff initially refer the submitter to the MHRA; although no patient-facing app is known to DHACA yet to have received CE certification in the UK, the library staff say they would accept an app with CE certification.

Although the matter is under active discussion, currently there are no plans to extend the NHS Apps Library to clinician-facing apps, or prescription-only apps. The view has been expressed that the Royal Colleges in the UK, which oversee each medical specialty, would be the most appropriate bodies to administer clinician-facing apps, and indeed some, most notably the Royal College of Physicians and the Royal College of Paediatrics are taking a strong interest. Apps that span more than one medical specialty do pose a problem for this approach though.

For patient-facing apps, there are curation sites that are not part of the NHS that primarily use patient/user feedback to recommend apps. An example is myhealthapps.

For clinician facing apps and apps that provide an interaction between patients and clinicians companies like OurMobileHealth provide a process and managed service, so that hospitals and healthcare providers can confidently provide and offer their clinicians and patients with trusted tested apps.

2. **Which policy action should be taken, if any, to ensure/verify the efficacy of mHealth solutions?**

Response:

In the UK, the National Institute for Health & Care Excellence (NICE) verifies the efficacy of drugs and medical hardware. It would seem natural therefore to extend the remit of NICE to include medical apps. Just as drugs include both over-the-counter and prescription drugs, apps range from health & wellbeing-type to those with a serious medical purpose; this proposal only affects the latter, just as NICE currently typically only reviews the efficacy of prescription drugs.

In order further to reduce the workload on NICE, NICE personnel have pointed out that currently they often review the drug development process at a supplier and then are happy to list drugs that have completed that process without reviewing eac one individually. They are proposing to take a similar approach to medical apps.

Note that whilst the verification by NICE is under discussion at various levels, it has not yet been confirmed by NICE's sponsors: the UK Dept. of Health and NHS England.

NICE has recently begun providing authoritative Medtech Briefings too, to give advice to local managers on new technologies. Finally it is perhaps worth noting that NICE has an international arm that is able to provide services almost anywhere in the world, should they be required.

3. How to ensure the safe use of mHealth solutions for citizens assessing their health and wellbeing?

Response:

There is currently widespread misunderstanding and confusion among both citizens and clinicians in the UK over safety matters.

Although the question specifically mentions 'citizens', research funded by the UK's Technology Strategy Board indicates that one of the key reasons why citizens adopt new medical practices is when recommended by their GP or specialist. One way of ensuring safe use therefore is to educate clinicians so that they can educate their patients.

Alongside this, the NHS Apps Library's safety check would seem to be the minimum necessary to ensure safe usage, with improved CE certification (as mentioned earlier) for 'serious' apps.

Yet another area of significant risk not specifically mentioned is ongoing monitoring of app performance, both to ensure that apps continue to function satisfactorily as the operating system changes, and also to check on safety performance following upgrades. Thankfully, the connectivity can provide the means of automatically recording such checks.

Note that currently the NHS Apps Library mentioned above does not recheck that an app continues to function well after first approving it.

One course of action we recommend – that DHACA can assist with in the UK – is to work with industry to ensure that responsible organisations to encourage and promote more responsible and better quality app development and health system adoption.

We also believe that, as mentioned earlier, it is now an appropriate time for a public awareness campaign to ensure people understand the benefits of mHealth and to make them aware, without scaremongering, of the risks they are taking using apps that have not been properly checked. In order to ensure do not frighten the public, perhaps configuring the message as education in what to look for in a good app and how to spot a bad one would work best.

mHealth role in healthcare systems and equal access:

1. **Do you have evidence on the uptake of mHealth solutions within EU's healthcare systems?**

Response:

The largest mHealth project as such in the UK is Florence, which to date has had some 17,000 users and collected in excess of 500,000 vital signs readings. This project uses simple text messaging to collect information on patient health and to disseminate responses from clinicians. It has proved so successful that the Connected Health team in the Dept. of Veteran Affairs in the US is now in discussion to licence the technology and develop version with more open APIs. There are two other big EU projects that we are aware of. One is the mHealth project in Catalonia in Spain and the other (rediforhealth) is in Oulu in Finland.

If the EU is to continue to attract investment into the mHealth sector, in addition to the simplification of regulation already mentioned, it will need to introduce and maintain stability and certainty in the business climate.

2. **What good practices exist in the organisation of healthcare to maximise the use of mHealth for higher quality care (e.g. clinical guidelines for use of mHealth)?**

Response:

As yet there is very little in the way of clinical guidelines in the UK regarding mHealth. The best example we are aware of is the Mersey Burns app, which has replaced the previous manual methodology, worldwide, for determining the appropriate fluid infusion for victims of severe burns as best practice.

3. **Do you have evidence of the contribution that mHealth could make to constrain or curb healthcare costs in the EU?**

Response:

There have been many such attempts to calculate a figure, all by organisations with a point to make – possibly one of the figures with the greatest credibility is that provided by the PWC report sponsored by the GSMA last autumn, of €99bn savings by 2017.

We believe that the single most important contribution that mHealth can make is in supporting greater self-care, both in terms of providing the tools for people to treat themselves for minor illnesses, and, because mobile phones are carried with people most of the time, 'nudging' them to change to healthier lifestyles.

One of our contributors, a healthcare academic, observes that mHealth can of course initially increase costs in the early stages, for example, by drawing attention to symptoms that are not being well managed and may require intervention. In the long run by so doing, costs are reduced though by earlier treatment initiation.

In this section it is perhaps worth adding that mobility and internet-based solutions can overcome geographic divides, provide better access to clinicians or specialists, and could be seen as a most effective route towards a more unified single European health market.

4. **What policy action could be appropriate at EU, as well as at national, level to support equal access and accessibility to healthcare via mHealth?**

Response:

There are four principal, related, reasons why as yet mHealth has not enabled greater equality of healthcare access:

- People at lower socioeconomic levels by definition do not have the disposable income to procure state-of-the-art equipment and so are less likely to be able to use the latest equipment;
- Such people also often do not accept responsibility for their own health, believing it to be for their doctor to manage; as a result they tend to live less healthy lifestyles.
- There is a generally low level of health literacy as a consequence of which the potential health gains are in some part negated, regardless of the opportunity that mHealth might afford;

- Social and environmental factors predispose many people to poorer health regardless of their access to services.

However, particularly via community routes, mHealth solutions can also help provide access to health care services as well as health education to citizens and groups of citizens who wouldn't typically engage with the traditional health service. Examples include ethnic minority groups, men under the age of 40, teenagers, or citizens suffering with mental health issues. This can also apply even those who don't have easy access to healthcare, due to the location of where they live or the nature of their work. MHealth solutions can complement traditional services and in particular can help overcome some of the barriers of accessing healthcare. In addition mHealth services can improve the quality of life for those physically or mentally impaired. For example apps, which are able to track eye movement to help people communicate.

In response to the question therefore, the need to promote greater self-care (see response to previous question) in the EU is clearly a top priority, so improving accessibility to healthcare is a vital part of that. One appropriate policy action therefore would be to ensure that mHealth apps will run on the vast majority of smartphones in use in the EU will help, as will ensuring greater penetration of faster mobile networks that the EC is already pushing hard.

A harder policy action to determine is to overcome the perception by many that government accepts responsibility for peoples' health. Work is clearly needed to understand what will motivate engagement and to design systems that deliver perceivable benefits to the user; creative partnerships with network providers to broadcast health messages and free apps at the point of care will undoubtedly help. There is no doubt though that mHealth, by offering short, 'nudging' messages that respond to activity and vital signs information, could be a critical part of providing that solution. However solving this is beyond the remit of this response.

Interoperability:

1. **What, if anything, do you think should be done, in addition to the proposed actions of the eHealth Action Plan 2012-2020, in order to increase interoperability of mHealth solutions?**

Response:

Two key issues must be addressed for effective interoperability:

1. Commercial platforms are the only de-facto delivery mechanisms for interoperable online services. Regulation or legislation can (and should) influence the design of applications and hardware but interoperability will be reliant on the dominant mass consumer device

market. The two main platforms are Apple iOS and Google Android. They are already developing or have launched mHealth toolkits/ecosystems (e.g. Apple HealthKit).

2. The other issue is assured online identities for clinical applications. The UK government ID Assurance Programme and its underpinning service design process are more likely to produce sustainable uptake within an environment of trust. The adoption of an approach to ID Assurance that allows citizens to consent to services and control privacy on a granular basis through an ID provider that is independent of government is a significant advance.

The guidance on information governance within EU health-providers (such as the NHS and local government in the UK) needs to be updated to reflect the need for data sharing with mHealth solutions, and in particular with Personal Health Records that are used by some mHealth solutions in order to give patients a more comprehensive record and greater control over their data. This new guidance is needed to help enable greater use of mHealth solutions by a patient's circle of care, such as support workers, carers and professionals. This is so that data is shared in a way that reflects the need for information across care settings, whether in the home, in the community or within traditional providers.

The current guidance on information governance has established a culture where the focus is on data protection by individual providers; this has become a barrier to interoperability and the availability of data to members of a patient's circle of care at the point of care delivery. The evidence from *dallas* is that IG leads in NHS bodies are reluctant to share data even where a clear need for interoperability is established by a professional body and where such data sharing is based on explicit consent from an individual.

2. Do you think there is a need to work on ensuring interoperability of mHealth applications with Electronic Health Records? And if yes by whom and how?

Response:

Yes, there is a need to ensure interoperability of mHealth applications with Electronic Health Records. There is a need at the EU level for an organisation like the UK's Independent Information Governance Oversight Panel (IIGOP) chaired by Dame Fiona Caldicott to publish new guidance on the need for interoperability and data sharing between mHealth solutions and Electronic Health Records. Part of the remit of EU-level version of IIGOP should be to challenge the status quo of resistance to data sharing by working with professional bodies to redesign services and pathways so they become technology enabled and digital by default.

There is also a need to take into account existing interoperability requirements, such as those detailed in the Smart Cities Framework (SCF) - BSI PAS 181. The SCF considers technical,

semantic, organisational, legal and political barriers to interoperability. By promoting principles such as the use of open standards, open data and reuse of public data; procurers can support integration. The use of open standards is an alternative to reliance on multiple independent proprietary formats, which can be difficult and costly to maintain as time goes on. There may also be unanticipated exit costs. As well as making these mechanisms open, there is a need to agree inherent terms, definitions and structures. For example references such as SNOMED CT have been developed, however it is unclear how they are being applied in the context of mHealth. Without agreed and commonly understood terminology, there is a concern that misunderstanding, ambiguity and a lack of consistency compromises the quality of the deployed solution. There is also a need to consider how applications can be updated as these structures evolve over time.

Reimbursement:

1. **Which mHealth services are reimbursed in the EU Member States you operate in and to what extent?**

Response:

Reimbursement for mHealth services is currently sporadic in the UK. Where a particular GP, Clinical Commissioning Group or Hospital has an interest in a mHealth solution, it will be offered to patients on the basis that most treatments are offered to patients by hr NHS: free at the point of delivery. However if an mHealth service is offered by a social care service in the UK, a means test typically applies, as well as a test of the person's ability to look after themselves. The end result is that a social care service using mHealth may be free, may be subsidised or, for those whose do not meet the criteria of frailty and whose income/capital is above the level set, they may pay the full price.

In a very few cases, apps with a particular public health benefit, notably smoking cessation, have been distributed free in the UK – indications are that public health authorities in the UK are contemplating increasing such activity in the future as the cost of purchasing/commissioning such apps (typically games) is typically very small, given the wide distribution an attractive app can have. Even where the health benefits are modest, the cost/improved lifestyle can still be very attractive.

2. **What good practice do you know of that supports refund of mHealth services (e.g. payer-reimbursement model, fee-for-a service model, other)? Please give evidence.**

Response:

In the UK, suppliers of telehealth services (which may use mHealth devices/apps) have offered some customers a payment-by-results contract, whereby payment is dependent on the success of the service, typically in reducing unplanned hospitalisations. Unfortunately, metrics in the UK to justify a before-and-after calculation of reduction in hospitalisations are not very accurate as historically hospital systems have not captured information using the single patient identifier (NHS number in England & Wales, CHI number in Scotland), and GPs have not always been made aware of patient hospitalisations due to paper-driven discharge notes that do go astray. Customers have therefore, in the main, been unwilling to agree to such a reimbursement model until the metrics improve. With the big drive to improve information flow, metrics are now improving greatly so this model is likely to become increasingly popular as a way of sharing risk for new ways of providing care.

Liability:

1. **What recommendations should be made to mHealth manufacturers and healthcare professionals to help them mitigate the risks posed by the use and prescription of mHealth solutions?**

Response:

A particular case study in the UK is Mersey Burns which is a clinician facing app that calculates fluid infusion requirements for patients with serious burns. It offers significant benefits in the form of much improved accuracy of fluid calculation as well as saving some ten minutes in the 'golden hour' that emergency clinicians have to stabilise patients to maximise survival chances and minimise long-term damage.

As a result, the creators of the app were keen to offer it for free to any professional wanting to use it (and it is now in use in almost every country in the world as a result and has already saved many lives). However they were conscious that in spite of it receiving a CE mark (it was the first app so to do in the UK) there was a finite risk that at some point someone would sue the developers and so they needed liability coverage. As a result, the developers gave the intellectual property to their local NHS Foundation Trust in exchange for the trust accepting legal liability for any future claims.

This case study suggests that the EU might consider a system for mHealth apps that were offered free for the benefit of patients across the EU whereby in exchange for the intellectual property rights, an EU body accepted legal liability for future claims. Clearly to offer this service, there would need to be assurances of risk minimisation, such as CE certification. However if it proves impossible, an opportunity will be lost as any app producer who cannot rely on a philanthropic organisation to cover potential liability will need to make a charge to cover the liability insurance – which in the case of a subject like major burns is likely to be high.

As the barriers to creating and publishing an app are so low, many app developers and app publishers do not do sufficient enquiry to make themselves aware of their responsibilities when publishing an mHealth app. At conferences in the UK it's clear that awareness at a basic level of the legal issues surrounding copyright, and of the more complex issues around standards and regulations in the mHealth app area is poor. This, coupled with the lack of evidence underpinning mHealth app and the lack of technical rigour, means that many mHealth apps for sale in the major UK app stores aren't currently fit for purpose.

Under the heading of liability, it is perhaps just worth mentioning that one of the reasons mHealth is apparently advancing so much faster in the US is that clinicians can be sued for not using the latest healthcare in treating patients, whereas there is no such liability in the EU.

Research and innovation in mHealth:

1. **Could you provide specific topics for EU level research & innovation and deployment priorities for mHealth?**

Response:

DHACA believes that, at the EU level, the Horizon 2020 programme has already chosen a sufficiently wide range of mHealth topics for innovation & deployment priorities. Therefore we feel that the EU should focus spending on existing topics, notably those referred to above, and in particular the promotion of interoperability.

The topic of mHealth should, however, also be addressed within the complementary EU Health Programme – most notably with regard to the way that services can be re-structured and cultures changed in order to ensure that the mHealth opportunities can be harnessed by the widest range of people. Specific areas of concern include the way in which (for people of all ages) greater health and digital literacy can be promoted (putting in place, therefore, key preconditions for the adoption and maintenance of appropriate lifestyles and greater self-management); and the implications for the workforce and workforce skills at the interface of health and social care.

There is also a need for further evaluative studies (eg controlled trials) to demonstrate the cost-effectiveness and soft consequences of mHealth interventions. New methodological research is needed to find innovative ways of capturing evaluative insights in live projects not configured as research trials.

DHACA is particularly concerned that the EC's reaction to comments to this Green Paper might result in a stifling of innovation; we would urge that the EC works hard to ensure that innovation is encouraged in this young and very vibrant sector, as this will benefit all.

2. **How do you think satellite applications based on EU navigation systems (EGNOS and Galileo) can help the deployment of innovative mHealth solutions?**

Response:

Location is often a key element of eHealth services, especially those involving emergencies. So for example an app that detects a fall, especially when the faller subsequently is unable to respond to a call from the control centre, relies entirely on location to enable emergency services to reach the faller quickly; likewise the confused person who needs help to find their way home, or to their car.

The EC should consider learning from the mobile operators, who found that by opening up location based services to the development community, there was a surge in innovation in this area and entrepreneurs took the opportunity to develop applications and services which hadn't previously been available. A navigation system such as Galileo might open up services for those in rural areas, or district nurses which haven't previously been available.

International cooperation:

1. **Which issues should be tackled (as a priority) in the context of international cooperation to increase mHealth deployment and how?**

Response:

The most important protection is the robust application of a set of internationally agreed regulations on data protection and information security, such as ISO 27001

Given the huge number of medical apps in existence and the bursting need to safety check/certify them, any international cooperation – even simply to the point of notifying other international bodies of a concern about a particular app – would be most welcomed.

It is almost certainly too much to ask for an international harmonising of regulation that would make it easier for app developers by enabling them only to focus on meeting a single set of requirements!

2. **Which good practice in other major markets (e.g. US and Asia) could be implemented in the EU to boost mHealth deployment?**

Response:

We are unaware of any best practice elsewhere that merits consideration for implementation in the EU. In the US, for example, the FDA is said to have cleared 110 apps in the past eleven years, which is hardly inspiring. However Happtique in the USA claims to have vetted 15000 apps to date before suddenly stopping its vetting activities recently.

There are some very interesting examples of mHealth innovation in low and medium income countries such as China which should be investigated for their potential to support European patients and health systems.

In addition there may be some learning from Africa where the deployment of mHealth services are increasing access to healthcare for rural communities, aiding the adoption of digital electronic patient records as for example village nurses are using mHealth applications to keep track of patients and this information can for the first time be shared with the hospitals. In addition there are many examples of great health education and peer support projects in cities, such as improving education about living with Aids, managing adherence to treatments and public health initiatives. Another example has been a project to provide information to pregnant women (& separately their husbands) to help them look themselves during pregnancy and help dispel some of the cultural beliefs classified as medically unsafe.

Access of web entrepreneurs to the mHealth market:

1. **Is it a problem for web entrepreneurs to access the mHealth market? If yes, what challenges do they face? How can these be tackled and by whom?**

Response:

The biggest challenge that web entrepreneurs face is the uncertainty and doubt about the whole regulatory environment for medical apps. For example:

- In addition to the Medical Devices Directive 93/42EC ("MDD") and In Vitro Devices Directive 98/79EC/AIMDA device regulations, the Data Protection Directive 95/46EC,

expected now in 2015 to become an EU-wide regulation and EU consumer protection legislation, notably the Misleading & Comparative Advertising Directive 2006/114EC all apply, which are administered by two separate Directorates General (Sanco & Justice).

- Further, the EU R+TTE Directive which originally covered various aspects of hardware that use radio waves is in the process of being revised to reflect the vast increase in radio device usage since it was established in 1999.. The principal concern of the directive is to minimise interference for legitimate users. As smartphones, peripherals using Bluetooth, wireless sensors and such like have increasingly complex embedded software there is obvious potential for overlap with the directives in the previous paragraph. DG Enterprise and Industry leads on this.
- Different arms of UK government then administer the different regulations, which makes a single assessment of the position impossible.

Web entrepreneurs are typically small companies with limited resources: they are overwhelmed by the complexity of this regulatory environment, especially as it is changing so fast, too. In addition it is perhaps worth mentioning that these entrepreneurs then have to navigate the NHS's regulations and reimbursement environment before actually getting paid. It is for this reason that the organisation submitting this response, the Digital Health and Care alliance (DHACA) was formed, to guide members through this minefield.

2. **If needed, how could the Commission stimulate industry and entrepreneurs involvement in mHealth, e.g. through initiatives such as "Startup Europe" or the European Innovation Partnership on Active and Healthy Ageing?**

Response:

Our understanding is that the development of medical apps is already the subject of a Horizon2020 call. Given the rapid half-life of medical apps just now, it is worth pondering whether the structure of such calls, involving as they do many partners working together over a number of years, is the most appropriate vehicle for a product requiring such a rapid development.

Other related topics not covered specifically in the green paper

Clinician-facing apps

Though these are not explicitly mentioned in the green paper, conversations with hospital doctors – and others involved in the medical apps business – suggest that use of dosage calculation apps that have not been safety checked may already have killed patients. These

represent an extremely high risk, both directly to patients, and indirectly to the reputation of app usage, and so are particularly appropriate for early enforcement action.

Clinical training apps

Another area not mentioned specifically is the use of apps for training purposes. Clearly these are of a lower risk than the previous app type; however significant harm could still be done if say a visualisation for a surgical procedure training session put an artery in the wrong place leading to a surgeon making an incorrect cut.

Clinical evidence gathering

There is a slow but growing evidence base supporting the benefits of health apps; however the process for gathering clinical evidence is still under discussion with a number of academics now starting to focus and get involved in this area.

The EC could usefully support this research activity in academic centres of excellence through some short-term funding, as it will be essential for the successful establishment of cost-effectiveness rankings of medical apps referred to earlier.

Skills

No mention is made in the Green Paper of what professional ICT skills and certification are needed for mHealth. Without the certification this could be a bigger drag than budgets or other incentives.

Accessibility

Although such considerations are increasingly understood, there is no mention made in the Green Paper of the specific accessibility requirements of disabled people, eg those with hearing or visual disabilities.

Patient groups

The role of Patient groups and other online self-help groups does not appear to have been acknowledged in the Green Paper; their Online support to trials, apps testing and potential changes to care seems to be missing.

Boundaries

DHACA suggests that all mHealth related regulation should also include mHealth games, such as those to encourage smoking cessation. Care will be needed to define the point at which these become educational and no longer health-related.

In general it is important to recognise that the distinguishing point between wellness/lifestyle and medical/health is hard to define.