digital health and care alliance
dhaca

Medical apps - processes

Guide - D019

NORTH WEST COAST
ACADEMIC HEALTH
SCIENCE NETWORK

Innovate UK

Document Details

Subject	First published version
Category	Guide
Title	Medical apps - processes
Document number	D019
First Publication Date	**23 September 2015**
Last Revision Date	23 September 2015
Revision	First published version V1.0

Revision History

V1.0	23 September 2015	First published version
V1.1	5th November 2015	With amendments suggested by the MHRA

Medical Apps - introduction

The term 'medical apps' is used in this document to refer to apps that are expected to have a significant impact on improving a user's health & wellbeing, including assisting with managing a disability. It therefore includes regulated medical devices, as well as those serious apps that do not qualify, yet anyway, for the description of medical device. Out of scope are the more frivolous apps that are primarily for leisure or entertainment purposes. This still leaves a wide range of types of app and app user to cover, including the NHS and other organisations, doctors & other NHS staff, social care organisations & carers, lay consumers of wellness and health apps, patients or subjects of care (qualitatively different from the person in the street visiting an app store). Of necessity therefore some issues and considerations will be of particular relevance to some groups of readers of this document, more than others.

This document was originally intended as a medical apps developer's guide to EU/UK regulation, as research by Charles Lowe, DHACA Managing Director, revealed a widespread interest by that community in gaining a greater understanding of the complexity of the topic. However as work began it became clear that the desire to improve understanding was common among all three communities impacted by this new type of aid to improved health & wellbeing: commissioners, developers & users. DHACA has therefore produced three inter-related sets of guidance to help with the commissioning, developing & acquisition by patients of medical apps.

DHACA is especially appreciative of the kind sponsorship by Innovate UK and the North West Coast AHSN for the development of this document.

The document begins with a description of the app commissioning process, aiming to cover both the commissioning of a new app, and the selection from a range of existing apps. As part of the procurement process includes issues such as clinical risk assessment, this is covered at this point.

There is also a range of other considerations when procuring digital health software which is picked up in greater detail in the following section on the medical app development process. This falls into six interrelated parts:

- The initial business decision;
- The actual development of the app;
- Medical device regulation;
- Data privacy regulation;
- Consumer protection regulation;
- Sales monitoring.

This leads on to the final section, informed by extensive user research, which summarises the sort of concerns that users have when seeking to select an app.

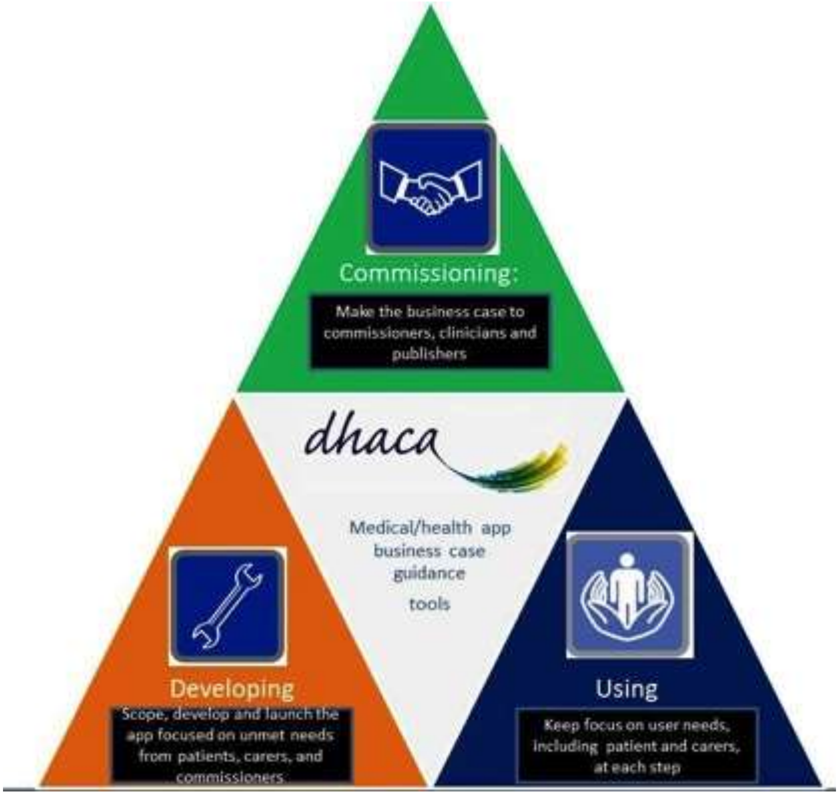
Only in putting all this information together has it become apparent quite how daunting the task of covering the topic is so, in producing this first version, DHACA is asking all readers please to feel free to draw our attention to further aspects of medical apps that need covering.

The diagram below seeks to summarise how this document helps the three communities to:

- Recognise decision-making processes at each stage of app development, from gaining interest from health commissioners and publishers, through the development process, to end-users' decisions to download and use
- Identify key actions developers need to take to help scope their business case, and ensure more sustainable benefits for their patients and carers, clinicians, commissioners, and their own business
- Identify and manage risk at each step of the process, from regulatory requirements through to technical risks and sustainability.

Each of the three guidelines contains step-by-step decision flowcharts, with supporting checklists and guidance for each step.

Note that all the active documents referred to in the text are current for NHS England; some may not necessarily be appropriate for other parts of the UK.



Commissioning:

Make the business case to commissioners, clinicians and publishers

dhaca

Medical/health app business case guidance tools

Developing

Scope, develop and launch the app focused on unmet needs from patients, carers, and commissioners

Using

Keep focus on user needs, including patient and carers, at each step

Caution

These guidelines have been developed by DHACA members, specifically to guide fellow members through what we realised, once we had started writing them down, was an extremely complex process.

During the development of this work, legal advice was taken, and freely given. However none of the authors of this work are lawyers, and the work has not been reviewed as a whole by lawyers familiar with this field.

In addition the regulation of medical devices is a fast-moving area. Two important EU regulations – on data protection and on medical devices – are expected within the period 2016-2017. Additionally, the interpretation of legislation is changing – most visibly in the US – as regulators get to grips with what is actually high risk.

Therefore, for both the above reasons, before any DHACA member relies on any legal statement in here, it is imperative that they check that statement for both correctness and continued applicability with appropriate legal counsel before relying on it; DHACA can take no responsibility for any actions taken without subsequent legal approval being sought and obtained.

The document brings together work by many individuals, with different styles, which will take some time completely to harmonise.

It is also a work in progress: no one who has looked at these process diagrams in draft had previously been aware of their full complexity. Just looking at them has revealed new insights which we have captured, whilst anticipating that as the document is read by more people, further suggestions for improvement will arise. As they do, do please email charles.lowe@dhaca.org.uk with your suggestions.

Medical apps SIG contributors:
Mike Clark
Janet Jadavji
Charles Lowe
Tony Newbold
Anthony Shimmin
Greg Smart
Richard Stubbs
Rob Turpin (SIG Champion)
Ritu Yaday

Valerie Field and David Grainger of the MHRA have been most helpful in ensuring accuracy. In addition, the following people kindly made really helpful positive contributions in review: Robert Coop, Nigel Dallard, Keith Hackett, Claudia Pagliari, Andrew Ruck, Hugo Vaughan, and Alex Wyke.

Table of Contents

High level medical app commissioning process diagrams 9

App Commissioning 11

Are the financial commitment and selection criteria understood? 11

How are intellectual property (IP) matters being addressed? 11

Are the business reasons for commissioning the app clear and understood?...............................11

What are the legal aspects that I need to be aware of?..11

Will there be any barriers to explaining how to access and use the app? 12

Does the app present an acceptable level of risk in terms of: 12

Will the app provide a beneficial outcome to the user, and how will this compare to other forms of treatment? 12

Can the app sustain itself as a high quality solution that will benefit users and professionals throughout the intended period of use? 13

Once the app is recommended and in use, how will it be reviewed? 13

Clinical risk assessment...14

Purpose 14

Generic process..14

Clinical risk guidance for digital health and other remote patient monitoring equipment 15

Risk assessment – practical considerations 16

Specific risks 16

Risk mitigation...16

High level medical app development, maintenance & closure process diagrams 17

Actions related to the process diagrams 20

Consulting potential users 20

Clarifying requirements 20

Identifying customers 20

Duty of care..20

Selling your app..21

Aiming to produce a medical device?...22

Funding & business model 22

Project management 22

Develop App.. 23

Classifying apps according to intended usage 23

Process: Developing the App 23

Outer Process – Managing the Development of a Medical App...24

User Stories 24

Architectural Planning..24

Regulatory, Liability and Ethical Requirements 25

The Information Governance Statement of Compliance (IG SoC) 25

Support and In Service Operation..26

Inner Process – Developing Medical Apps..26

Iteration Planning...26

User Interface Design...26

Development: Front and Backend 26

Testing and documentation 26

Deployment and Learning...27

Legislation and standards referred to on the flow chart...28

MEDDEV 2.1/6 & EU medical device legislation 28

EU data protection legislation 30

EU-level concepts..30

Privacy Impact Assessments (PIAs)...31

Data security..32

Quality anagement...33

ISO 14971 - Application of risk management to medical devices 33

IEC 62304 – Medical device: software cycle processes 33

ISO 13485 Medical devices -- Quality management systems -- Requirements for regulatory purposes..33

Other considerations...35

Significant changes...35

EU consumer protection legislation...35

ISB 0129 v2 Clinical Risk Management: its Application in the Manufacture of Health IT Systems...35

PAS 277 – Health and wellness apps – Quality criteria across the lifecycle..............................35

Also worth bearing in mind though not featured on the flowchart 35

Health on the Net Foundation (HoN)....35

EUROPEAN COMMISSION. Commission of the European Communities eEurope 2002: Quality criteria for health related websites 36

Directive 1999/5/EC of the European Parliament and of the Council 36

Wearables and other hardware 36

Getting listed by a search engine 36

Apple 36

Google 37

Developers' licences....37

Withdrawals/recalls....37

High level patient and carer decision-making process diagram 38

Found a trusted source? 40

Am I clear what the app will do and I believe it will do it? 40

Am I clear who is behind the app and that I trust them and their processes?.... 40

Am I clear what I will pay or the commitment I am making, and I accept this?.... 41

Am I clear how I can keep control of my privacy, data and details? 41

Am I clear that the app will work for me as long as I need it?.... 42

Weighing the risks up, am I clear about the risks I am taking in downloading and using the app? Do I find the level of risk acceptable?.... 42

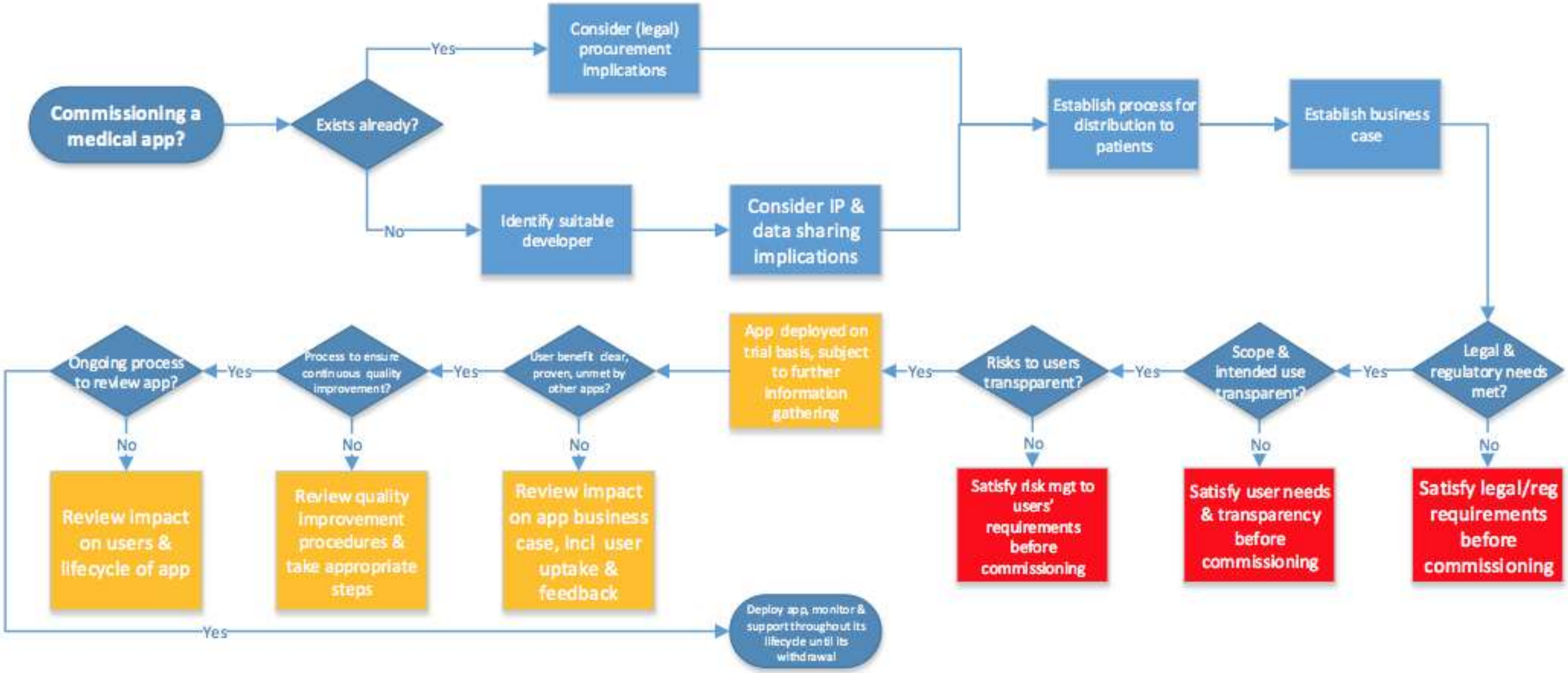
How to find relevant and trusted health-related apps.... 43

myhealthapps 2015-2016 directory....44

High level medical app commissioning process diagrams

The following pages comprise a process diagram followed by suggested questions that commissioners should be asking at each step of the process. In some cases it should hopefully be clear what a good answer to these questions is; in others we have pointed the enquirer via bookmarks to sections in the Developer process that describe the concepts in more detail. There is however one exception to this: clinical risk assessment, which is the sole responsibility of the commissioning organisation, so at the end we have given a brief description of the process and the key issues to be aware of.

High level medical app* - commissioning process



Commissioning a medical app?
Exists already?
Yes
Consider (legal) procurement implications
No
Identify suitable developer
Consider IP & data sharing implications
Establish process for distribution to patients
Establish business case
Legal & regulatory needs met?
No
Satisfy legal/reg requirements before commissioning
Yes
Scope & intended use transparent?
No
Satisfy user needs & transparency before commissioning
Yes
Risks to users transpparent?
No
Satisfy risk mgt to users' requirements before commissioning
Yes
App deployed on trial basis, subject to further information gathering
User benefit clear, proven, unmet by other apps?
No
Review impact on app business case, incl user uptake & feedback
Yes
Process to ensure continuous quality improvement?
No
Review quality improvement procedures & take appropriate steps
Yes
Ongoing process to review app?
No
Review impact on users & lifecycle of app
Yes
Deploy app, monitor & support throughout its lifecycle until its withdrawal

*Note that the term 'medical app', as previously defined, refers only to any serious health & care app. It could also be a medical device, although it does not have to be.

App Commissioning

Are the financial commitment and selection criteria understood?

(Note these will vary depending on the procuring organisation)

- What are the legal (or other) rules regarding procurement (e.g. OJEU contract size)?
- Are there unique supplier rules that could apply?
- Has the app been commissioned before?
- Are there any endorsements or recommendations?
- Is the app listed in any supply chain catalogues or government framework contracts?
- How many users are there?
- What feedback is available?

How are intellectual property (IP) matters being addressed?

- Has a suitable app developer been identified?
- What IP issues need to be addressed?
- What information governance/data sharing aspects need to be considered?

Are the business reasons for commissioning the app clear and understood?

- Is there a clear business case for commissioning the app (costs, perceived benefits /outcomes)?
- What are the supply chain procedures?
- Have other relevant parties been involved (clinicians, patients, information governance officers)?
- What level of finance is required?
- What other commitments are needed?
- Will the app offer value for money?
- What other approvals are needed?

What are the legal aspects that I need to be aware of?

- Is the app certified as a Medical Device (Under the EU Directives/Regulations) and does it carry a CE mark?
- If not, is the app being used for a therapeutic/diagnostic purpose that would define it as a medical device (under the EU legislation)?
- If the app collects or transfers personal data, does it meet the principles of the Data Protection Act/Privacy Regulations?
- Are there any other regulations or legislation that could be applicable (e.g. trading and advertising standards; R&TTE Directive)?
- Who would be liable if there was an issue with the app?
- Am I effectively covered against potential litigation?

Will there be any barriers to explaining how to access and use the app?

- Are there clear instructions for use?
- Has the user been defined?
- Are there clear guidelines for recommending the app?
- Are all the costs explained (including differences between free and premium services)?
- Is there transparency of other criteria (e.g. of the collection and sharing of personal data, the sponsor for developing the app)?
- Can the app be accessed through an appropriate app store, and via the technology of the user's choice?

Does the app present an acceptable level of risk in terms of:

- Relevance to the user?
- Usability, inclusivity and accessibility?
- Clinical risk?
- Financial cost and commitment?
- Privacy and data sharing?
- Technical (e.g. software upgrades) and integration with other systems?
- Reliability and sustainability of the app developer?
- Future-proofing?

Will the app provide a beneficial outcome to the user, and how will this compare to other forms of treatment?

- Have the expected outcomes of using the app been defined?
- Has an app trial taken place?
- Is there a cost benefit in using the app instead of other traditional treatments?
- Has any post-launch evidence been published to show the efficacy of the app?
- Are any reviews about patient experience available?
- Have users been involved in the process of assessing the suitability of the app?
- Is the evidence obtained in proportion with the risks of using the app?
- Has user testing taken place and been reported?

Can the app sustain itself as a high quality solution that will benefit users and professionals throughout the intended period of use?

- Are there procedures in place for future-proofing, updating or withdrawing the app?
- Is there a facility for providing feedback on the app?
- Has the app developer implemented a quality management system (such as ISO 9001 or ISO 13485)?
- Is there a clear understanding and consent surrounding any data that could be shared, and any privacy aspects?
- Where applicable, does the app comply with relevant NHS (or other professional) standards (e.g. ISB 0129 v2)?
- Can the app be integrated with other software/digital tools as required?
- Can the app be continually accessed by those who need to use it?

Once the app is recommended and in use, how will it be reviewed?

- How often will the impact of using the app be assessed with the patient?
- Will the user provide feedback on their experience?
- Will professional feedback be provided?
- How will future changes in clinical outcomes, technical revisions or changes in practices be communicated?
- Does the app developer have a systematic process for reviewing their app?
- Is there a clear process established for withdrawal of an app?

Clinical risk assessment

Purpose

The purpose of a clinical risk assessment is to minimise the risk of a piece of equipment, software, or an intervention causing harm to a patient, carer or clinician.

Generic process

What follows is drawn from Healthcare risk assessment made easy produced in March 2007 by the NHS National Patient Safety Agency – before conducting a risk assessment, a full reading of this easy-to-use document is highly recommended.

Step 1 Identify the hazards (what can go wrong?)

To prevent harm it is important to understand not only what is likely to go wrong but also how and why it may go wrong. Consider the activity within the context of the physical and emotional environment, and the culture of the organisation and the staff who perform the activity. Learn from the past, e.g. by consulting appropriate records to understand what has gone wrong in the past and near-miss incidents.

1. Walk around the workplace or clinical area and talk to patients and staff.
2. Map or describe the activity to be assessed.
3. The risk assessment may require a multi-disciplinary team.

Step 2 Decide who might be harmed and how (what can go wrong? who is exposed to the hazard?)

People will make mistakes. It is necessary to anticipate some degree of human error and try to prevent the error from resulting in harm.

1. Consider the number of patients that might be affected over a stated period of time. When quoting the number of patients affected you should always state the length of the assessment period.
2. Remember that the most vulnerable patients are more likely to suffer harm.
3. Think about the complexity of the task.

Step 3 Evaluate the risks (how bad? how often?) and decide on the precautions (is there a need for further action?) Consider both consequence (how bad?) and likelihood (how often?). Is there a need for additional action?

The law requires everyone providing a service to do everything reasonably practicable to protect patients from harm.

1. Use your organisation's risk matrix – an example can be found in appendix 2
2. Decide on the precautions (controls) that will most effectively reduce consequence and/or likelihood.
3. Re-evaluate the risks assuming the precautions (controls) have been taken.

Step 4 Record your findings, proposed action and identify who will lead on what action.

Record the date of implementation Risk assessments and action planning should be reviewed and changed when necessary. This is easy only if the assessment is well recorded and the logic behind the decisions transparent. An efficient and succinct system of documentation is essential.

You need to show that:

1. A thorough check was made to identify all the hazards and treat all the significant risks;
2. The precautions are reasonable and the remaining risk is acceptable;
3. The solutions are realistic, sustainable and effective. It may be reasonable to accept some degree of preventable risk, if the benefits to be gained outweigh the risk.

Step 5 Review your assessment and update if necessary

Good documentation is important because things are always changing. Research and new developments increase the pace of change, and those changes can alter existing and/or introduce new hazards.

Review your risk assessment:

1. When you are planning a change;
2. Routinely at least on an annual basis;
3. When there has been a significant change.

Clinical risk guidance for digital health and other remote patient monitoring equipment

Two standards apply here, specifically relating to clinical risk assessment.

1. The first is ISB 0129 v2 specifically places an onus on the manufacturer/supplier of the equipment (which can include software only).
2. The second is ISB 0160 which specifically places an onus on the organisation using the equipment (which can include software only).

Both of the above are extremely explicit and detailed in their requirements. They require following in detail, and therefore need to be read in detail by the appropriate individuals in each organisation, so little merit would seem to be gained by quoting from either.

Risk assessment – practical considerations

Specific risks

Clearly any purchase of an app that will form part of a treatment plan will require assurances from the supplier/manufacturer that the data protection considerations and ISB 0129 v2 have been fully complied with.

Using information provided by the supplier and from their own organisations, the deploying organisation should then complete both a PIA and an ISB 0160 clinical risk assessment.

Very little discussion has taken place of actual patient-related incidents specific to digital health – a report due to be produced by the Good Governance Institute on digital health safety has been delayed for so long now that it is hard to believe it will ever see the light of day.

Where an app is used for some form of patient monitoring, for example in telehealth, the principal risk area identified in discussions is a lack of coordination between a patient's GP/consultant and the monitoring service. This has, on occasions, resulted in the GP/consultant taking decisions/intervening whilst the patient is being treated by the monitoring organisation, and vice versa.

Another is being unaware that the patient is suffering from dementia as this, for example in the case of telecare, can alter the appropriate responses, because people with dementia often do not report what is actually happening (e.g. failing to be aware of a fire).

Risk mitigation

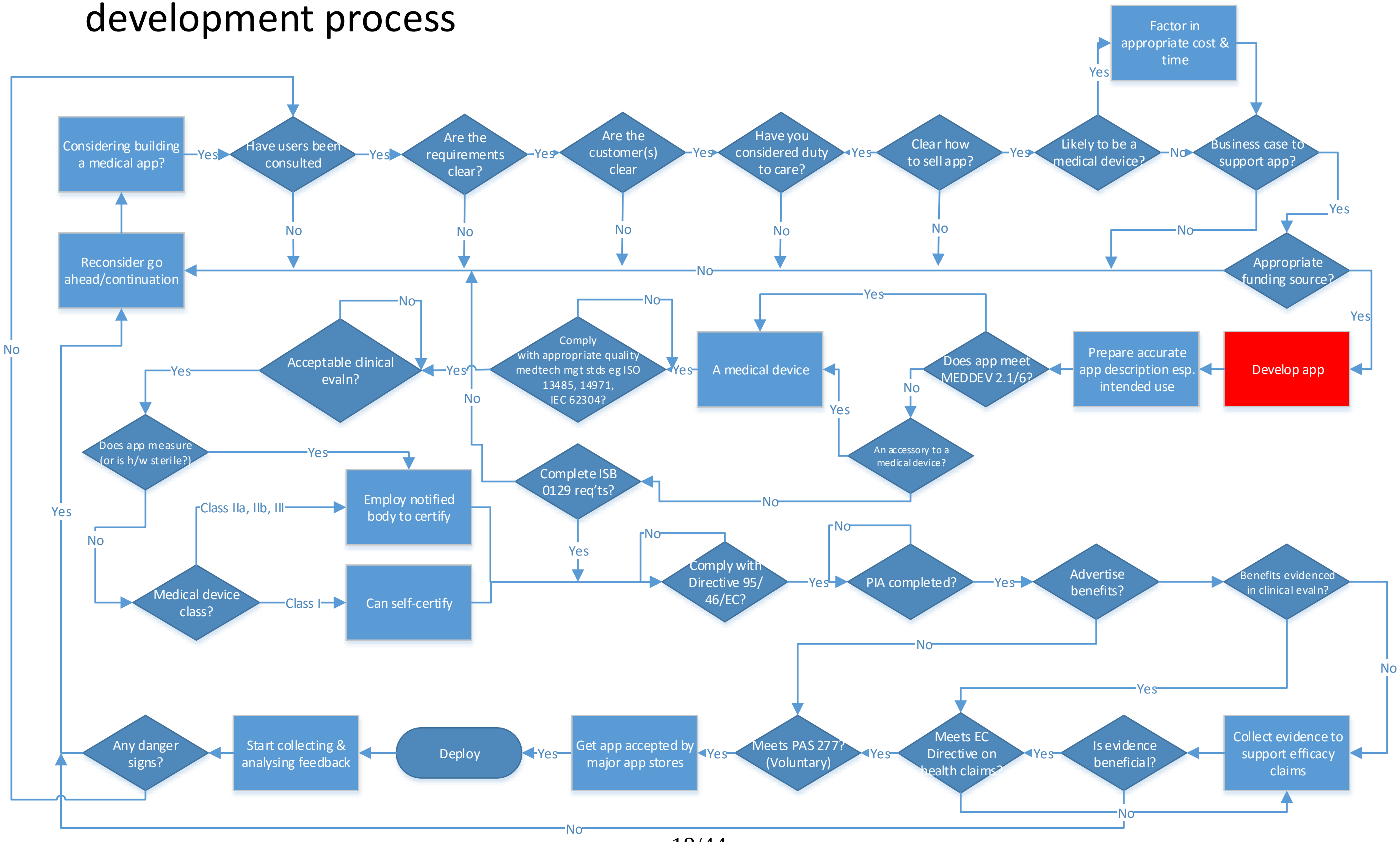
The following steps are typically employed when remote monitoring is introduced to a patient, so may be useful pointers when deploying apps that involve some reporting back to the health service:

1) Take reasonable care to ensure that any monitoring organisation is aware of whether the patient has dementia, and configure services accordingly;

2) Ensure that the patient (or responsible carer) signs a form confirming they understand that the service is not an emergency service (unless it is!); in the event of the patient feeling unwell they will call 999/112 and not rely on the remote monitoring system to alert emergency services.

High level medical app development, maintenance & closure process diagrams

High Level medical app development process



Considering building a medical app?

Have users been consulted

Are the requirements clear?

Are the customer(s) clear

Have you considered duty to care?

Clear how to sell app?

Likely to be a medical device?

Factor in appropriate cost & time

Business case to support app?

Appropriate funding source?

Reconsider go ahead/continuation

Develop app

Prepare accurate app description esp. intended use

Does app meet MEDDEV 2.1/6?

A medical device

An accessory to a medical device?

Comply with appropriate quality medtech mgt stds eg ISO 13485, 14971, IEC 62304?

Acceptable clinical evaln?

Does app measure (or is h/w sterile?)

Employ notified body to certify

Medical device class?

Can self-certify

Complete ISB 0129 req'ts?

Comply with Directive 95/ 46/EC?

PIA completed?

Advertise benefits?

Benefits evidenced in clinical evaln?

Collect evidence to support efficacy claims

Is evidence beneficial?

Meets EC Directive on health claims?

Meets PAS 277? (Voluntary)

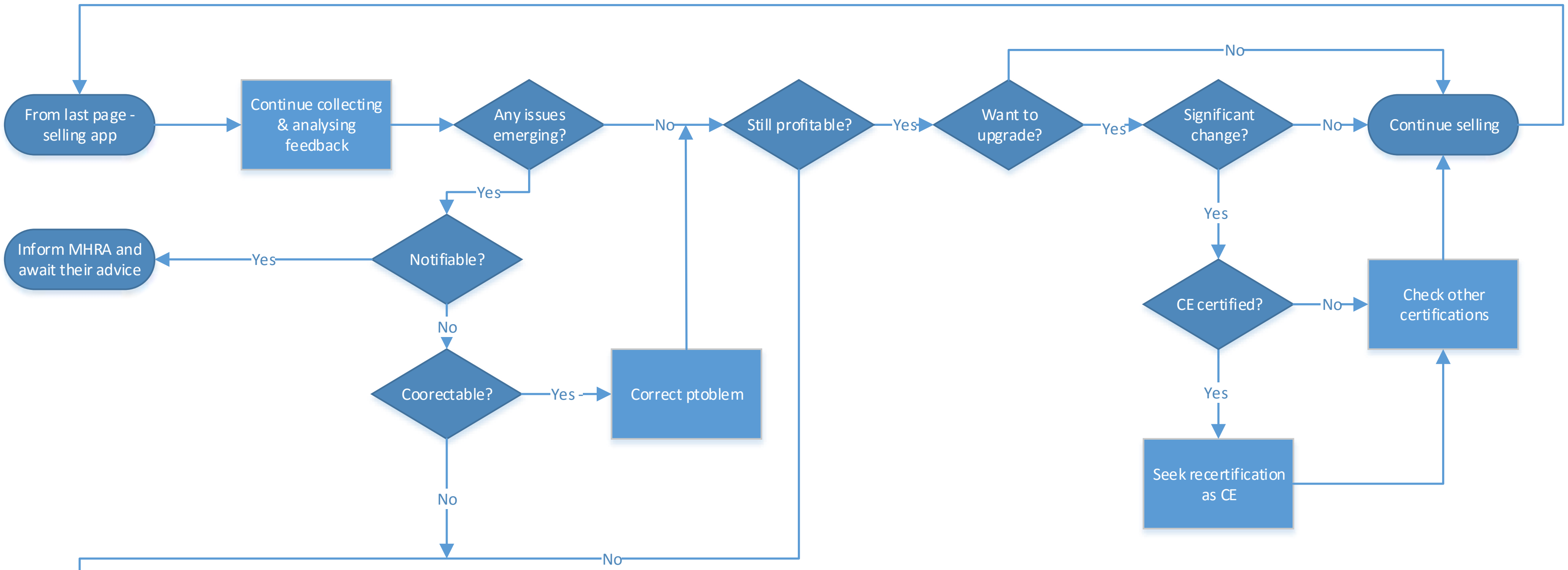
Get app accepted by major app stores

Deploy

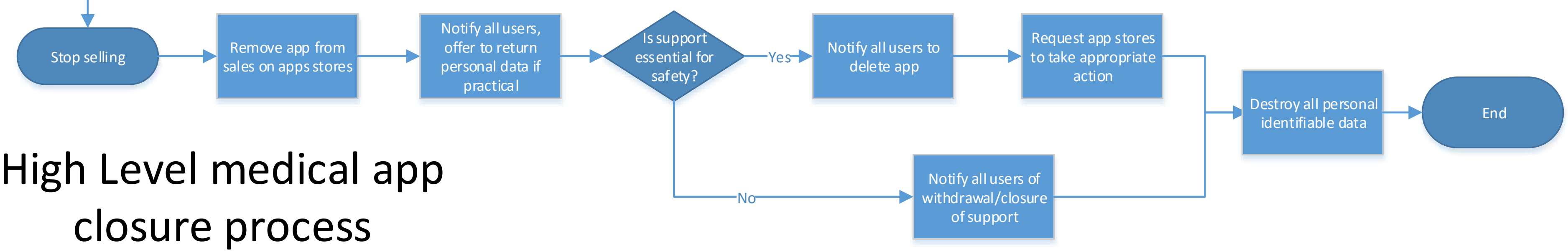
Start collecting & analysing feedback

Any danger signs?

High Level medical app maintenance process



High Level medical app closure process


Stop selling
Remove app from sales on apps stores
Notify all users, offer to return personal data if practical
Is support essential for safety?
Yes
Notify all users to delete app
Request app stores to take appropriate action
No
Notify all users of withdrawal/closure of support
Destroy all personal identifiable data
End

Actions related to the process diagrams

Consulting potential users

Surprisingly, in discussions with many app developers, checking user requirements before embarking on the development of a medical app is often ignored. This almost inevitably results in an app that works well for highly technical users, though is less appropriate for less technically competent users. Extensive consultation – ideally involving rechecking of the design as it develops – is highly recommended.

Clarifying requirements

Having consulted potential users, the next step is to ensure that the requirements as given by them are clear and unambiguous.

Identifying customers

It is important to establish who the customer(s) of the apps will be, both to ensure that their requirements are met, and to establish who will pay for the app in the end.

Equally it is important to identify the price that those customers might reasonably be expected to pay for the app, perhaps by checking against competing products or surveying potential purchasers.

Note that for medical apps, there are often two sets of users – the final user who is typically the patient or their carer, and the professional user, who could be a clinician or social care worker. Either of those groups could the customer who pays for the medical app, or it could be a third party – for example a public health department, a pharma company, or a health or social care administration function. Developers need to be very clear on all these categories for their app, because only then can they work out how to sell it.

Duty of care

The duty of care is a concept that overrides any specific consideration of individual regulatory instrument, so should be in developers' minds throughout the process of designing and building a medical app. According to the Social Care Institute for Excellence, Duty of Care is defined simply as a legal obligation to:

- Always act in the best interest of individuals and others
- Not act or fail to act in a way that results in harm
- Act within your competence and not take on anything you do not believe you can safely do.

In tort law, a duty of care is a legal obligation which is imposed on an individual requiring adherence to a standard of reasonable care while performing any acts that could foreseeably harm others. It is the first element that must be established to proceed with a legal action in negligence. All developers designing applications to assist people in managing their health and well-being must pay due attention to their duty of care. Where possible companies should provide a resilient service and be sustainable from a performance and commercial viability perspective.

Particular aspects worth stressing not brought out elsewhere in the process diagram are:

- In the event that a supplier is unable to provide a service due to affordability, the supplier should be able to offer a continuity of service methodology;
- Advisory content (for example what to do if a patient has increasingly high blood pressure having recently had a surgical procedure) should be provided directly, validated and acted upon by a trusted source, on the basis that most application developers are not clinical experts.
- Any bespoke advice should be traceable to a named practitioner registered on the application(s). In the event that the patient is unsure, the application provider should have a means of requesting further information from the source, or be advised to seek further clarification or validation.
- Disclosure of patient content within applications should only be achieved with patient consent (or by means of a professionally provided power of attorney). Disclosure of patient or patient group content for reasons of research or commercial gain should be clearly defined within the application provider's terms and conditions, and ideally further advisory notifications are given when an action within the system could result in this.

Selling your app

As long as the previous steps have been undertaken fully, the developer should be clear what is required, by whom, and who is prepared to pay the price proposed. Therefore actually selling the app should be straightforward. However all too often it is at this point that developers begin to complain at the challenges of selling, particularly to the NHS. However perseverance inevitably finds a way if there is a genuine demand for the app at the price requested.

Important points to remember include:

1) All UK public bodies are covered by the EU law on procurement which requires competitive tenders for services or products over a Euro limit (in 2015 of €207 for councils & €134k for the NHS); breaking this law is a serious matter;
2) Many public bodies have a substantially lower limit for competitive tenders, albeit with less stringent tender requirements;
3) The exemptions to both the above include situations where no-one else can provide the goods or service (an exemption much used by drugs manufacturers); however this decision has to be auditable;
4) Another means of selling a novel service is as a trial, which is subsequently scaled up as time goes by, always being aware of competitive tender limits & exemptions.

Aiming to produce a medical device?

As will be apparent from the diagram, if an app is classified as a medical device, there are a significantly greater number of hurdles to overcome.

Producing an honest, accurate and full description of the app as early as possible in the development process is the best means of checking the likely classification.

However because an app that is genuinely a medical device is likely to have a more valuable role to fulfil, a correct medical device classification is not necessarily financially disadvantageous. In addition, the process under way to evaluate medical apps in the UK which is expected to include a measure of clinical effectiveness is currently expected to prioritise apps that are medical devices. This will enable developers unequivocally to advertise the clinical benefits of their app.

Funding & business model

If all the previous points have been attended to, building a business model that is attractive to potential funders should be no problem. Note that potential funders will ask about all the above aspects of the proposal as well as others, including the details of the developer's organisation, their personal commitment etc.

A particular concern of funders is how the app will be sold. Many for example will stop the conversation if the NHS is mentioned as a customer as there is a view that it is impossible to sell to the NHS, in spite of the fact that the NHS's expenditure on items other than salaries, contractors and medicines is over £20bn pa. It is therefore especially important to recognise this concern and set minds at rest before covering any other part of the pitch.

Project management

Clearly the implementation of the app project needs to be well managed (PRINCE2 is typically the methodology of choice in the UK public sector although as mentioned in more detail later on, there are specific quality/risk management standards that should be carefully considered too). Most importantly, whoever is responsible for commercialising the app should take care to define success measures, from the various perspectives of active stakeholders, as well as how that success is to be managed. This is all basic project management, however agreeing this information at the outset ensures the levers are in place to manage the implementation pro

Develop App

(High Level Medical App Development Process)

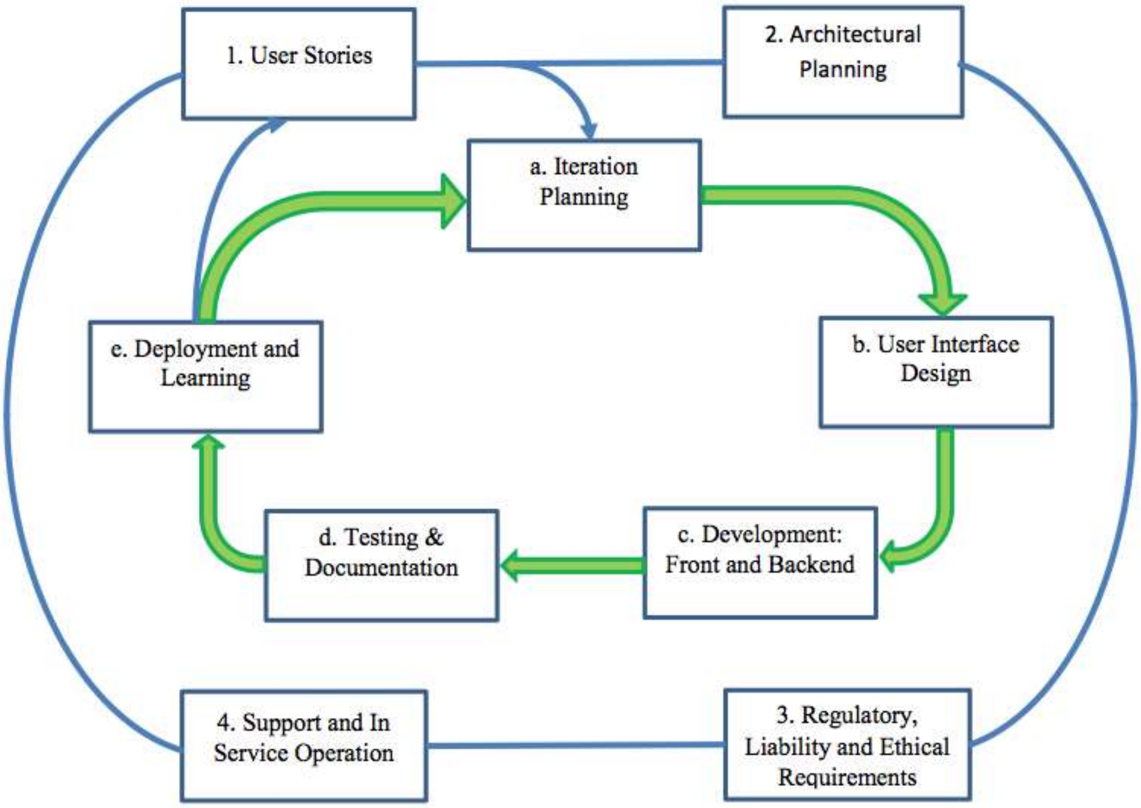
Classifying apps according to intended usage

The key determinant here is whether the medical app is planned to connect to personal health & care data held in another database/other databases. For the purposes of this review we have assumed that these databases are managed within the NHS environment, although they could be held by a local authority, or a private provider, in which case appropriate variations to what follows will be appropriate.

A Medical App specification document can vary tremendously depending on whether the app is targeted for NHS use or for an individual use without having to interact with any NHS IT Systems. Developers need to understand completely & comply with the NHS Codes of practice & legal obligations to develop a successful medical app intended for NHS.

Additionally, an app being used by or recommended by NHS carries a lot of weight, credibility & reliability; however if the app is sold through any other platforms then the developer needs to be a reliable source for an individual. One way to ensure this is by providing transparent & clear answers to the high level patient & carer decision making process. Additionally, these apps need to have a well-defined exit plan especially for free apps.

Process: Developing the App


1. User Stories
2. Architectural Planning
a. Iteration Planning
b. User Interface Design
c. Development: Front and Backend
d. Testing & Documentation
e. Deployment and Learning
3. Regulatory, Liability and Ethical Requirements
4. Support and In Service Operation

Outer Process – Managing the Development of a Medical App

This process addresses some of the governance issues which are particular to apps which have a medical, health or fitness purpose.

User Stories

Medical apps often have to work with multiple stakeholders who may have different objectives. In the wider developers' process the clarity of the various user requirements will have been checked. A good way to do this is through creation of User Stories, or some similar approach to describing the required functionality of the system from the various users' perspectives. User Stories can then be used as a key input into the development process, indicating to the development team what functionality they need to deliver.

Good practice also extends to considering how users may 'misuse' the system as well as how it may be used in intended ways. Developers should also consider where their users are likely to be from and whether they have taken adequate account of the user's language, culture and working practices.

Architectural Planning

The majority of medical apps are not standalone pieces of software, but rather fit into a wider ecosystem. For example it is commonplace for apps to communicate with a backend server, which will most likely be a web server and database. This backend in turn may communicate with third party systems, used both by the apps end-users and by others associated with their care.

If the app is intended to interact with one or more IT systems existing in various departments or sectors of healthcare, an integration module should be well thought out from the beginning as the existing systems may vary in the standards & ways they exchange information with third party apps. It will for instance be important to consider read/write functions and permissions between the app, or information stored via the app, and for example the national 'Spine' systems on the one hand, & installed EHRs or other organisation wide record systems, on the other. The arrangements for integration with any other system within the healthcare environment should be in place too as this might affect the functionality of the app & hence the future of the application being adopted.

A suitable architecture may well consider the physical architecture in which the system is deployed, a logical architecture to show how the functionality is apportioned between system components, and a data architecture which considers the critical data entities which enable the system to function.

The architecture should also consider the type of app being created. For example it could be a native app written for one specific platform (for example iOS), it could be developed using a cross platform tool which generates native apps for multiple platforms, it could be a 'container' app which behaves like a native app but is primarily a container for a system delivered from a web server, or it could be a 'web app' which is accessed via a browser on the phone. Even if the app is a native app, a web interface may also be desired to maximise opportunities to access the functionality or to provide an administrative interface.

Developers should also consider different platform options. Sometimes a 'cloud' based deployment is appropriate, other times software will be deployed on specific servers. It is important to understand the issues of security and privacy that impact on the system. In particular the physical location of data is controlled by data protection and privacy legislation in many jurisdictions.

Regulatory, Liability and Ethical Requirements

The wider development process considers the regulatory framework in which a medical app must operate, and the liability that an app developer may face. It is highly likely that these constraints will impose requirements on the development process. Hence Information Governance requirements should be well understood from the beginning.

The Information Governance Statement of Compliance (IG SoC)

IG SoC isthe process by which organisations enter into an agreement with HSCIC for access to the NHS National Network (N3). The process includes elements that set out terms and conditions for use of HSCIC systems and services including the N3, in order to preserve the integrity of those systems and services.

Confidentiality: The 'Confidentiality: NHS Code of Practice' sets out the required standards of practice concerning confidentiality and patients' consent to use their health records. This has been incorporated in a 2014 Confidentiality Policy

Information Security Management: The 'Information Security Management: NHS Code of Practice' is a guide to the methods and required standards of practice in the management of information security, for those who work within or under contract to, or in business partnership with NHS organisations in England.

NHS Records Management: This policy sets out the required standards of practice in the management of records for those who work within or under contract to NHS organisations in England, based on current legal requirements and professional best practice.

Legal obligations: There are a range of complex legal and professional obligations that limit, prohibit or set conditions in respect of the management, use and disclosure of information and, similarly, a range of statutes that permit or require information to be used or disclosed.

The IG Toolkit provides good practical guidance on acceptable information governance issues

Note: In Wales NWIS is the prime IG protocol provider.

Support and In Service Operation

Providing effective support to users is often vital to ensure that a medical app is used effectively and safely. Regardless of safety considerations, responding to user concerns, fixing bugs and resolving problems will enhance the overall user experience, increasing the chances that the app will be successful.

Inner Process – Developing Medical Apps

Development may be managed in many different ways but for the purposes of this guide they have been arranged in an interactive process.

Iteration Planning

The development team should take the user stories & plan which they intend to address in the next iteration.

User Interface Design

The user stories should be considered by a user experience or user interface designer. The designer should produce designs for the specific app screens to be developed and create the graphical elements which app developers incorporate into the app user interface. With medical apps it is often the case that potential users are not familiar consumer electronic technology. They may also face issues with their sight and fine motor control. Issues of usability and accessibility for the target audience should therefore be considered in the design.

Development: Front and Backend

Developers should take the user stories and interface design and write the software code to create the app, web interface and backend.

Adherence to NHS Data Standards is of course essential (even to humble items like date, always written in the NHS as DD-MMM-YYYY where the MMM is in approved alpha abbreviation).

Where an interface with the NHS Spine is contemplated, it is essential for developers to be aware of the NHS Warranted Environment Specification which will shortly be extended to mobile working.

Testing and documentation

The software developed will also need to be tested as part of the development process itself. This may be done through an approach like Test Driven Development, through the development of automated tests, or through more manual testing processes.

Testing is usually divided into verification and validation. Verification refers to testing by the development team to ensure that they have correctly implemented the requirements. Validation refers to testing with users which demonstrates that the system is used in the way intended.

It is common to create multiple platforms to facilitate testing and release in a controlled way. For example, a development platform may be used only by the development team, a test platform can be used for formal testing and a live platform used for final deployment to end users.

Deployment and Learning

Once developed and tested, the software will then need to be deployed. For apps this will often mean deployment to third party sites like the Google Play Store or Apple's iTunes. Server software will also need to be deployed in a controlled way, ensuring that it is able to handle any versions of the app which may be live.

No app developer can afford to release their app and hope for the best. They will need to study how the app is used, how many people download it and use it, in what way and for how long. It is common to instrument apps to generate data on its use and this data needs to be observed and studied. The insights gained from doing so, alongside all the other feedback received from users should be used to plan further development iterations. These can be expressed through the creation of new user stories, or changes to existing ones. This feedback is also a powerful means of identifying any bugs and correcting them fast.

NB – in the consultation process, DHACA member Hugo Vaughan of Glue Reply has pointed out that where an app is connected, there are additional important considerations, notably:

- *Accessibility – finding the device*
- *Interoperability – adverse events and other, potentially new, regulated messages*
- *Authorisation and Identity – who can do what, and how are they identified*
- *Security – DDoS, hacking, vulnerabilities. PCI does this well.*
- *Privacy – protection of information from inappropriate access*

Of these privacy is well handled in this document, and the issue of IoT security is about to be explored by a DHACA SIG. Suggestions are welcomed regarding how best to expand coverage of the top three.

Legislation & standards referred to in the flow chart

MEDDEV 2.1/6 & EU medical device legislation

EU legislation in this area is incorporated into UK legislation as the Medical Devices Regulations 2002 (“MDR”). This includes the Medical Devices Directive 93/42EEC (“MDD”) and the In Vitro Devices Directive 98/79EC (“IVDD” – applies where a sample of bodily tissue or fluid is taken) cover the definition of what is a medical device; if it is, then these regulations further classify the class of device which in turn affects how it is assessed before it can be given a CE marking. Currently the interpretation of MDD/IVDD legislation varies across the EU, however it is expected that by 2018 an EU-wide regulation will be approved by the EU Parliament/Council of Ministers to harmonise the interpretation of the law across all EU member states.

Whilst the precise definition of a medical device could cover many pages and is very much the province of an expert legal advisor, it is perhaps just worth rehearsing that Article 1 (2) of the MDD defines 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 purpose 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,

…and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means;”

The key concept here is intended use, an issue that has been brilliantly explained, albeit in a US context by Bradley Merrill Thompson (be sure to read the second page).

Medical devices can be software-only (e.g. as apps) if they meet the definition; the precise definition of whether an app is a medical device is given by the EU’s Medical Devices Expert Group in MEDDEV 2.1/6 on Standalone Software.

There is also much more detail available, including in additional DHACA material, and particularly on issues like whether the app is an accessory. In the MDD, all apps are classed as active medical devices. Risk class (I being the lowest, progressing through IIa & IIb to III, the highest) specifically for active medical devices is quite tightly defined in Annex IX (note that apps are unlikely to fall into Class IIb and III but may if implementing rule 2.3 applies: “Software, which drives a device or influences the use of a device, falls automatically in the same class.”). Risk class in turn affects the degree of scrutiny before a CE mark can be applied, Class I devices being self-certifiable, except (see Annex VII (5)) where the medical device has a measurement function (often referred to as Class Im) or (for hardware) is sterile

(Class Is). For Classes Im, Is, IIa, IIb & III it is necessary to employ a notified body – many suppliers also use such organisations also for Class I because of their expertise. There are five notified bodies in the UK[1] able to handle medical devices.

One requirement of CE certification is the use of a recognised medical technology quality management system to develop the device. This is essential because it is not possible with many apps to test all potential pathways that patient data can use, so the development has to be managed in such a way to ensure that, when in use, a previously untested pathway still gives a valid & safe result. Here it is suggested that at minimum ISO 13485 be used, which is usually deployed in conjunction with ISO 14971 & IEC 62304.

Another requirement is to do a clinical evaluation to evidence the safety and intended operation of the app (MDD Annex X). Note in particular the requirement to demonstrate that the "…devices must achieve the performances intended by the manufacturer…". This may be combined with a benefits evaluation as required by EU legislation if there is an intention to advertise the benefits of the app. Alternatively this benefit evaluation may be done separately, especially if it is likely to be lengthy.

All manufacturers of medical devices in the UK need to register with the MHRA's Device Online Registration Service (DORS) system, including where a supplier is self-certifying a Class I device. This costs (2015) £70/registration, and the same sum for amendments.

(Note that type approvals are not listed today across an EU wide database or in a single directory, so the penetration of CE certification can only be judged by hearsay – out of an estimated 500 medical apps[2] expected to require certification, the editors of this document are aware of certifications only for Airstrip, Medopad, Mersey Burns, Mersey Micro, & Oncoassist, plus of course the accessory apps to devices like the AliveCor ECG peripheral and Sanofi's iBGStar.)

[1] To see the five you need to specify '93/42/EEC Medical devices' in the Legislation box.

[2] Note this is only a rough guess based on an undocumented sample that suggested that one out of 100 medical apps was a medical device.

EU data protection legislation

EU-level concepts

The European Commission advocates three approaches to minimising privacy-related risks:

1. Data minimisation – the principle of "data minimisation" means that a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose. They should also retain the data only for as long as is necessary to fulfil that purpose. In other words, data controllers should collect only the personal data they really need, and should keep it only for as long as they need it. The data minimisation principle derives from Article 6.1(b) and (c) of Directive 95/46/EC and Article 4.1(b) and (c) of Regulation EC (No) 45/2001, which provide that personal data must be "collected for specified, explicit and legitimate purposes" and must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed".

2. Data protection by design is an approach to projects that promotes privacy and data protection compliance from the start. It requires that controllers of data – whether companies or public bodies – take a positive approach to protecting privacy, by embedding it into the technology (for example hardware like computer chips or services like social networking platforms) and into their organisational policies (through, for example, the completion of privacy impact assessments). This requires thinking of privacy and data protection from the beginning of the development of a product or service: "Do we really need to collect these data? Is there a way to have the same functionality without collecting them?" This concept is currently not a requirement of the Data Protection Act, although it will help organisations comply with their obligations under the legislation as it is being introduced in Article 23 of the Proposed REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. The ICO in the UK greatly encourages organisations to ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout its lifecycle. For example especially when:

- building new IT systems for storing or accessing personal data;
- developing policy or strategies that have privacy implications;
- embarking on a data sharing initiative; or
- using data for new purposes.

[2] Note this is only a rough guess based on an undocumented sample that suggested that one out of 100 medical apps was a medical device.

3. Data protection by default, like the previous item (with which it is sometimes combined), is being introduced in Article 23 of the new regulation. It which means that when a user receives a product or service, privacy settings should be set by default as strict as possible, without the user having to change them. This way, everyone is guaranteed a high level of protection, allowing everyone the opportunity to consciously choose the privacy setting that they feel most comfortable with – rather than the service provider making a guess about what they might prefer. Service providers should support their users in this and also supply understandable privacy policies. Data protection by default is implemented on some social networks already, so it is neither a new nor a revolutionary idea.

Privacy Impact Assessments (PIAs)

PIAs are an integral part of taking a privacy-by-design and by-default approach. The UK was the first country in Europe to develop and promulgate a privacy impact assessment methodology. The Information Commissioner's Office (ICO) first published a PIA Handbook in December 2007. After a number of revisions, the current code of practice was published in 2014. Article 33 of the draft EU data protection regulation referred to above would make PIAs mandatory for both public and private sector organisations throughout Europe where processing operations are likely to present specific risks to the rights and freedoms of data subjects.

A PIA should incorporate the following steps:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

PIAs are, briefly, a tool to use to identify and reduce the privacy risks of a project. A PIA can reduce the risks of harm to individuals through the misuse of their personal information. It can also help the design of more efficient and effective processes for handling personal data. The core principles of the PIA process should be integrated into an organisation's existing project and risk management policies. This will reduce the resources necessary to conduct the assessment and spreads awareness of privacy throughout the organisation. As with the project management approach itself, the time and resources dedicated to a PIA should be scaled to fit the nature of the project. A PIA should begin early in the life of a project, but can run alongside the project development process.

A PIA should incorporate the following steps:

- Identify the need for a PIA
- Describe the information flows
- Identify the privacy and related risks
- Identify and evaluate the privacy solutions
- Sign off and record the PIA outcomes
- Integrate the outcomes into the project plan
- Consult with internal and external stakeholders as needed throughout the process

The ICO handbook on PIAs covers 50 pages and gives excellent advice on the finer points of how best to do the above.

There is however one further interesting classification, largely missing from the subsequent EU draft legislation - the four different types of privacy invasion that a person can suffer:

- Intrusion of Solitude
- Appropriation of Name or Likeness
- Public Disclosure of Private Facts
- Putting a person in a ‘False Light’

Data security

Whilst the arcana of data security are outside the remit of this document, it is perhaps worth drawing readers’ attention to HSCIC’s Good Practice Guides covering technology-specific areas of information security and information governance. Other links that may be helpful include UK government advice & guidance on cybersecurity & information assurance, and on cloud security.

Quality management

ISO 14971 - Application of risk management to medical devices

ISO 14971 is an ISO standard for the application of risk management to medical devices. The latest version with worldwide applicability is ISO 14971:2007[3]. It establishes the requirements for risk management to determine the safety of a medical device by the manufacturer during the product life cycle. Such activity is required by higher level regulation and other quality management system standards such as ISO 13485 (below). In 2012, a European (only) version of this standard was adopted by CEN as EN ISO 14971:2012. The layout of this version is harmonized with the EU MDD (above) – the content is identical to the 2007 version.

IEC 62304 – Medical device: software cycle processes

This international standard specifies life cycle requirements for the development of medical software and software within medical devices. It is harmonized by the EU and the United States.

One of the key elements is that, based on the potential to create a hazard that could result in an injury, the manufacturer has to assign a safety class to the software system as a whole:

- Safety Class A: No injury or damage to health is possible.
- Safety Class B: Non serious injury is possible.
- Safety Class C: Death or serious injury is possible.

The effort for the development of medical devices depends on these security classes. It is obvious that effort and cost is much higher for the development assigned to class C then for class B or class A.

It can be purchased here (for £226 for non-members).

ISO 13485 Medical devices -- Quality management systems -- Requirements for regulatory purposes

This is a standard that manufacturers of medical devices should meet. It is self-certificating. The primary objective of ISO 13485 is to facilitate harmonised medical device regulatory requirements for quality management systems. As a result, it includes some particular requirements for medical devices and excludes some of the requirements of ISO 9001 that are not appropriate as regulatory

[3] There is a guidance document too ISO/TR 24971:2013

requirements. (Because of these exclusions, organizations whose quality management systems conform to this International Standard cannot de facto claim conformity to ISO 9001 unless their quality management systems also conform to all the requirements of ISO 9001.)

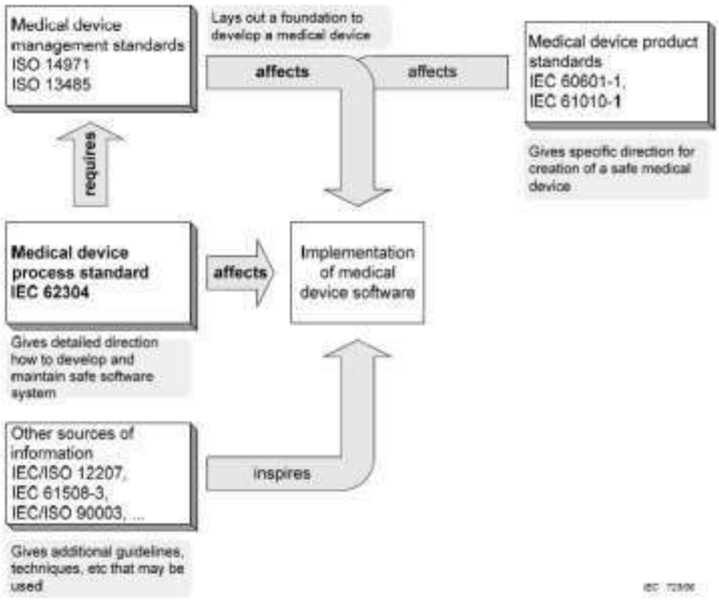
This standard was published as a draft on 6/02/15, and intended to replace the original published in 2003, and the 2009 corrigendum. It may therefore change – until finalised, technically the 2003 standard plus corrigendum remains in force.

CEN have also published an equivalent of 13485:2003 – EN ISO 13485:2012. As with ISO 14971 this also is harmonised with the MDD and IVDD.

This standard and ISO 14971 mentioned previously do get confused so just to explain that they are complementary: they address different criteria in the medical device regulations:

- 13485 addresses the requirement to have a quality management system, and it is possible to issue a certification certificate against it (in the same way as ISO 9001). It identifies the need to manage risks.
- 14971 is the recognised standard detailing how a medical device manufacturer should manage risks. It isn't a certification standard, unlike 13485, but it is cited by the EU, FDA etc. as a harmonized/consensus standard that demonstrates 'presumption of conformity' with the regulations.

At the risk of introducing further complexity, the attached diagram seeks to tie all this together. If required, ISO 13485 can be purchased here (for CHF118 for the pdf file).


Medical device management standards ISO 14971 ISO 13485
Lays out a foundation to develop a medical device
affects
affects
Medical device product standards IEC 60601-1, IEC 61010-1
Gives specific direction for creation of a safe medical device
requires
Medical device process standard IEC 62304
affects
Implementation of medical device software
Gives detailed direction how to develop and maintain safe software system
Other sources of information IEC/ISO 12207, IEC 61508-3, IEC/ISO 90003, ...
inspires
Gives additional guidelines, techniques, etc that may be used
IEC 723/06

Other considerations

Significant changes

Following initial compliance with the initial set of appropriate regulations and standards, developers should hopefully be aware of which changes are most likely to require a recheck of compliance.

For CE certified devices, significant changes require recertification at the appropriate (or perhaps new) class.

There is an inherent conflict here with the need to keep apps high in the app store rankings, so developers may wish, in advance, to identify a range of aspects of their app, such as background colour and font that could be changed without impacting on regulatory status.

EU consumer protection legislation

Likewise, EU consumer protection legislation applies to all remote monitoring hardware & software irrespective of whether it is a medical device. This requires, for example, that any product or service making a health or wellbeing claim must be able to support that claim with good evidence.

The onus here is on the supplier only to make claims supported by evidence; there should be no requirement for the purchaser to take an interest as long as appropriate evidence is forthcoming.

ISB 0129 v2 Clinical Risk Management: its Application in the Manufacture of Health IT Systems

ISB 0129 v2 specifically places an onus on the manufacturer/supplier of the equipment (which can include software only) to minimise clinical risk. Its partner on the purchasing side is ISB 160. As it is extremely detailed, little merit would be had from quoting it here.

PAS 277 – Health and wellness apps – Quality criteria across the life cycle

The BSI has very recently published this voluntary standard which relates specifically to mHealth apps. In spite of this tight focus, as mHealth apps are increasingly being used as a means of delivering telehealth, telecare and teleconsultation, this standard should be of interest to those purchasing remote consultation services or products. It is currently free of charge if downloaded in electronic form.

The standard is aimed mainly at developers, as a reminder of the various aspects to consider when building an app. However as it covers the app lifecycle and projects involving apps, it does have some interest to purchasers.

Also worth bearing in mind though not featured on the flowchart

Health on the Net Foundation (HoN)

This Foundation “promotes and guides the deployment of useful and reliable online health information, and its appropriate and efficient use.” Created in 1995, HoN is a non-profit, non-governmental organization, accredited to the Economic and Social Council of the United Nations. It is aimed at both professional users (clinicians) and end users (patients & carers).

For 15 years, HoN has focused on the essential question of the provision of health information to citizens, information that respects ethical standards. To cope with the unprecedented volume of healthcare information available on the Net, the HONcode of conduct offers a multi-stakeholder consensus on standards to protect citizens from misleading health information.

Appendix C of PAS277 links that standard with the HoN quality criteria.

EUROPEAN COMMISSION. Commission of the European Communities eEurope 2002: Quality criteria for health related websites

This publication, covering EC recommendations on quality criteria for health-related websites, has not been updated since publication in 2002.

Directive 1999/5/EC of the European Parliament and of the Council

It is perhaps worth mentioning the EU R+TTE Directive which originally covered various aspects of hardware that use radio waves. However as smartphones, peripherals using Bluetooth, wireless sensors and such like have increasingly complex embedded software there is obvious potential for overlap with the above. The principal concern of the directive is to minimise interference for legitimate users. It is in the process of being revised to reflect the vast increase in radio device usage since it was established in 1999.

Wearables and other hardware

If there is hardware involved, this is also required to meet the following directives:

- Electromagnetic compatibility directive (2004/108/EC).
- Radio equipment and telecommunications terminal equipment (RTTE) directive (1995/5/EC).
- Restriction of the use of certain hazardous substances in electrical and electronic equipment directive (2011/65/EU)

Getting listed by a search engine

Both Apple and Google have a few foibles that those seeking listing need to be aware of.

Apple

Apple's submission guidelines are here.

This Venturebeat item describes nine points to note:

1) Use of the word “beta” or otherwise indicating that your app is unfinished;
2) Long load time;
3) Linking to payment schemes outside the Apple infrastructure;
4) Mentioning other supported platforms (e.g. Android);
5) Localisation issues (e.g. with different currencies, negative latitude/longitude numbers);
6) Improper use of storage and file systems;
7) Crashes from users denying permissions;
8) Improper use of icons & buttons;
9) Misuse of trademarks and logos.

Read the item for more details on each one. Note that in an emergency, Apple provides an expedited review process which can be used for critical bug fixes or to address security issues. However developers who overuse this will be barred from future use.

Google

Google Play’s submission guidelines are here.

Advice from Dr Claudia Pagliari, Senior Lecturer in Primary Care, University of Edinburgh College of Medicine and Veterinary Medicine, is that Google Play has traditionally been very lax: apps have been pushed out almost immediately after only a basic algorithmic review process. However in March 2015 they announced the introduction of human screening (more here), which is designed to spot 'policy infringers' early on and to detect code for malware. This is in addition to a machine review of the developer's self-completed checklist. It's still far more lightweight than Apple's screening and will take only a matter of hours from submission to decision. It is currently unclear what, if anything, this does to the products in health.

Developers’ licences

It takes a month to get a developer’s licence from Apple and a similar time for others platforms, so remember to apply in plenty of time before your app is ready to roll!

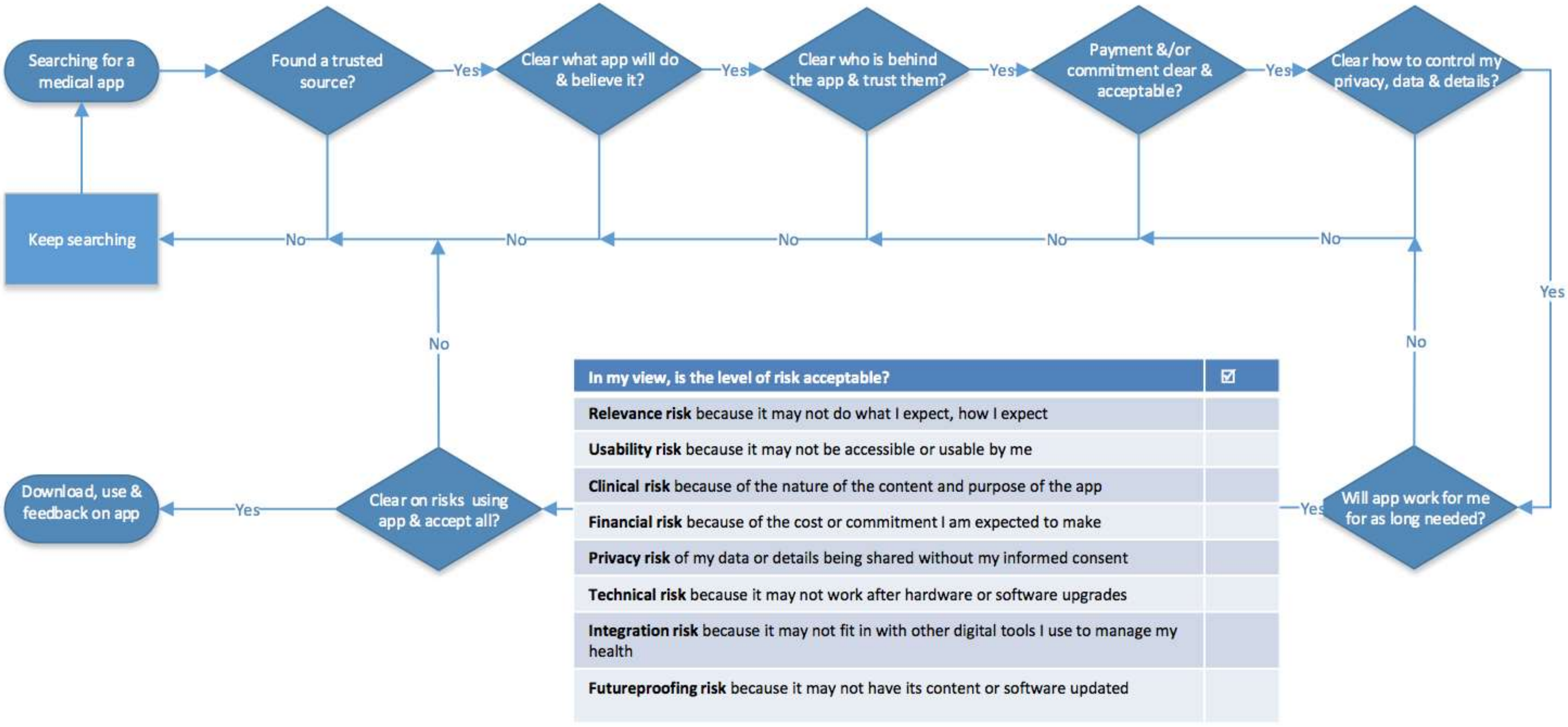
Withdrawal/recalls

Note that the MDD (Annex X) encourages the establishment of a post-market surveillance plan. The process diagram for maintenance/withdrawal shows the normal process for continuously reviewing feedback and events. Clearly if these indicate a serious issue, the MHRA needs to be notified, and appropriate action taken.

It perhaps also worth mentioning that at the request of DHACA, the MHRA succeeded in getting Google Play to remove an app that had already been declared to be unsafe by the US FTC (Apple had already removed it), so this can be done.

High level patient and carer decision - making process diagram

High level patient & carer - decision-making process


Searching for a medical app
Found a trusted source?
Yes
Clear what app will do & believe it?
Yes
Clear who is behind the app & trust them?
Yes
Payment &/or commitment clear & acceptable?
Yes
Clear how to control my privacy, data & details?
Yes
Keep searching
No
No
No
No
No
No
No
Yes
Will app work for me for as long needed?
Yes
Clear on risks using app & accept all?
Yes
Download, use & feedback on app

In my view, is the level of risk acceptable?	☑
Relevance risk because it may not do what I expect, how I expect	
Usability risk because it may not be accessible or usable by me	
Clinical risk because of the nature of the content and purpose of the app	
Financial risk because of the cost or commitment I am expected to make	
Privacy risk of my data or details being shared without my informed consent	
Technical risk because it may not work after hardware or software upgrades	
Integration risk because it may not fit in with other digital tools I use to manage my health	
Futureproofing risk because it may not have its content or software updated	

High level patient & carer decision-making process

Found a trusted source?

- Where can I look for the app I need amongst the thousands available?
- Where can I find trusted and independent reviews of apps to help me compare them?
- Where can I find relevant reviews because they are written by people like me?

If I have found suitable apps to compare from a source I trust...

- If no apps are found, I keep searching
- How can my most relevant patient or carer group help?
- If I believe no such app exists yet, how can I make developers aware of my need?

Am I clear what the app will do and I believe it will do it?

- Do I trust the description?
- Is the description comprehensive and clear, including who the app is aimed at, which countries it is intended to be used in, and what it does?
- Are the screen shots relevant to my needs?
- Do the reviews tell me what I need to know about what the app does, or does not, do?
- Are the reviews from patients or carers like me?
- Has the developer shown how they have involved patients or carers like me in the development of the app?
- Given any health condition or disability I or the person I care for has, will we be able to access and use the app effectively?
- If I believe it is a medical app, does it carry a CE mark, or other marks that I trust to show that it has been thoroughly tested and assessed?

If I think the app will do what I need it to...if I do not believe the app will help me, I keep searching.

Am I clear who is behind the app and that I trust them and their processes?

- Can I see who commissioned, created and financed the app? Do I trust them?
- Who clinically approved the app?
- How do I know any medical information or guidance is accurate and up to date?
- Has any recognised clinical body approved the app?
- If any clinical evidence is shown, for example proven outcomes for the app or results of trials with patients, how credible is this? Has it been independently assessed?
- Has the app been recommended or prescribed by any doctor or nurse I trust?

Am I clear what I will pay or the commitment I am making, and I accept this?

- Am I clear about all the terms and conditions? If I believe the app to be trustworthy...if I do not trust the app, I keep searching.
- Is the app ***really*** free?
- If they are offering a free trial, is it clear how long this lasts for?
- If it is free, how is the developer making money from this?
- Is the developer making their money from advertising?
- Is the developer selling my data or details on to finance the app?
- If I am paying, is it clear how much, what I will get for the money, and for how long?
- Will I have to pay to extra content and premium services? Is it clear how much and what I will get?

If I believe the app to be worth downloading, paying for or making other commitments...if I do not want to pay for the app, or make other commitments expected by the developer, I keep searching.

Am I clear how I can keep control of my privacy, data and details?

- How clear are the terms and conditions around protecting my privacy, details and data?
- Does the app give me control of my data, allowing me to share or withhold it from specific groups?
- Do I trust this app and developer to be clear about if and how they want to use my data?
- Is it clear who `owns' and makes decisions about my data (for example, the publisher, the app commissioner, or the developer)?
- Is it clear how long the owner of my data will hold it for?
- Is it clear how long I will have access to any data I put into the app?
- How can I be sure that my data will be stored safely and accurately?

If I believe the app protects my data, or allows me to control my data in the way I want...if I do not want to risk losing control of my data because of the terms and conditions, I keep searching.

Am I clear that the app will work for me as long as I need it?

If I believe the app will be supported for as long as I need it....if I do not believe the app will be supported for as long as I need it, I keep searching.

- How do I know that the developer will keep the information and guidance up to date?
- What commitment does the developer make to review any information in the app regularly, for example annually?
- Are there clear and easy ways to feed back on the app, and make contact with the developer about improvements?
- Is there a fast track way to alert the developer of any safety issues, such as medical guidance becoming out of date?
- How do I know the developer will ensure that it will work across all the devices I want it to use it on?
- How do I know that the app will still work after upgrades to software and devices?
- How do I know that the developer will continue to support the app?
- How do I contact the developer in case of a technical problem, or in case a piece of guidance has become out of date or inaccurate?
- How do I know the developer will inform me if they are withdrawing support from the app?
- How do I know the developer will remove the app if it is shown to have safety issues?

Weighing the risks up, am I clear about the risks I am taking in downloading and using the app? Do I find the level of risk acceptable?

How do I estimate the risks of the app to me, (high, medium, low)?

- **Relevance risk** because it may not do what I expect, how I expect
- **Usability risk** because it may not be accessible or usable by me
- **Clinical risk** because of the nature of the content and purpose of the app
- **Financial risk** because of the cost or commitment I am expected to make
- **Privacy risk** if my data or details being shared without my informed consent
- **Technical risk** because it may not work after hardware or software upgrades
- **Integration risk** because it may not fit in with other digital tools I use to manage my health
- **Futureproofing risk** because it may not have its content or software updated in line with future developments.

If I believe the app will benefit me with a level of risk I accept, I will download it…if I feel the risks of the app outweighs the potential benefits, I keep searching.

How to find relevant and trusted health-related apps

The National Information Board (NIB) Workstream 1.2 is developing a process for approval of medical apps which is expected to be put to a UK Treasury endorsement process in November 2015. If approved, this will in 2016 begin a four stage process:

1) Self-assessment by providers using an online form as a prelude to
2) Crowdsourcing views – if accepted gets some form of low level NHS approval leading to
3) Impact assessment using an as yet undecided to-be-approved-by-NICE[4]-when-it-is technique before finally submitting to Independent evaluation

Trials of this process are just beginning (September 2015).

Another means of seeking advice is **myhealthapps.net,** a site helping patients and carers to find:

- Relevant and useful healthcare recommended by people with similar needs.
- Trusted apps to make a difference to their health, and support those they care for.

The National Institute for Health & Care Excellence (NICE) currently has very little involvement with medical apps. However were they to perform a similar role to that that they perform for pharmaceuticals, their future engagement would be substantial. In particular many GPs currently quote absence of NICE endorsement as their principal reason for not endorsing any apps as without it they are potentially individually liable. The Scottish equivalent of NICE is the Scottish Intergovernmental Governance Network (SIGN).

Each app is recommended by healthcare communities from all over the world, including:

- Empowered consumers
- patients
- Carers
- Patient groups
- charities and other not-for-profit organisations

myhealthapps.net works together with this network to:

- Highlight best practice in health app development
- highlight the unmet needs of public, patients and carers to app developers
- Bridge the gap between public, patients and carers with app developers to improve the relevance, quality and health impact of apps

The result is the best healthcare apps, recommended by empowered consumers, patients and carers.

In addition to the website, there is a range of downloadable publications available from **myhealthapps.net** and its sister organisation, PatientView, including:

- A toolkit to help patients and carers find the right apps for their needs, and get the most from those apps
- Research and white papers into what patients and carers need most from apps, and how commissioners and developers can address these needs

myhealthapps 2015-2016 directory

myhealthapps.net also produced in September 2015 a print directory to accompany and support the website. The directory is available to download here.

The directory classifies apps to make it easier for users to find the app that suits their personal needs and raise awareness among users that different apps carry with them different risks. There are many ways to do this; from the perspective of how people use health apps, and their perception of risk, myhealthapps uses these three classes (note that some apps may fall into more than one class and that this directory defines medical apps slightly differently to the rest of this medical apps process document):

- **Disability**—health apps that enable people to cope with daily living and provide support to people with any type of disability, including physical, mental and sensory impairment. For example, text-to-speech apps that help people who have speaking difficulties or limited verbal abilities, to augment their communication skills.
- **Health, wellness and care in the community** are health apps that allow us to manage our health and healthcare without the necessity for medical assistance, and which do not result in clinical decision-making by the user, or require input from a health professional. Apps not included in this class are ones that provide information to help people decide whether they should go and visit their doctor, which are classified as medical apps—in that the person is making a medical decision based on the information received. Also not included are most of the health apps that support glucose monitoring in diabetes (unless they provide diet or nutritional advice), since the results generated by these apps do result in a clinical decision being made by the patient as to whether they should take their diabetes medication.
- **Medical apps.** These are health apps that lead to any sort of clinical decision-making, diagnosis or treatment. Health apps that work alongside medical devices are included in this class as well. Generally speaking, medical apps will pose more safety risks to the public and patients because they involve clinical decision-making processes (though for some patients, say with renal disease, the food they eat can mean the difference between life and death). A further directory of medical apps will follow in 2016.

www.myhealthapps.net

www.patient-view.com