

Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2015.

Published by BSI Standards Limited 2015.

ISBN 978 0 580 87164 1

ICS 03.120.01, 35.080 and 35.240.80

Publication history

First published April 2015

No copying without BSI permission as permitted by copyright law.

Contents

Foreword	ii
Innovate UK statement	iii
Introduction	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Fitness and purpose	4
5 Quality criteria	5
6 App project life cycle	6
7 Risk management	13
8 App project governance	15
9 Configuration management	16
10 Support	17
Bibliography	26
Annexes	
Annex A (informative) Relationship between PAS 277 and BS EN 62304:2006	18
Annex B (informative) Relationship between PAS 277 and ISB 0129	19
Annex C (informative) Relationship between PAS 277 and Health on the Net (HoN) quality criteria	20
Annex D (informative) Relationship between PAS 277 and eEurope 2002	21
Annex E (informative) Example health and wellness apps	22
Annex F (informative) Example risk repository analysis	24
List of tables	
Table 1 – Example risk score	14
Table A.1 – Table of clauses in BS EN 62304:2006 and PAS 277	18
Table B.1 – Table of contents for ISB 0129	19
Table C.1 – Relationship between PAS 277 and Health on the Net (HoN)	20
Table D.1 – Relationship between PAS 277 and eEurope 2002	21
Table F.1 – Example risks	25

Foreword

This PAS was sponsored by Innovate UK. Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 30 April 2015.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the steering group:

- Association of British Healthcare Industries (ABHI)
- BT
- BUPA
- Caton Bell Limited
- Digital Health & Care Alliance
- Health & Social Care Information Centre (HSCIC)
- Innovate UK
- INPUT Patient Advocacy
- INPS
- NHS England
- NIHR Mindtech Healthcare Technology Cooperative
- Omron Healthcare
- Royal College of Physicians
- South West Academic Health Science Network (SWAHSN)

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

The PAS process enables a code of practice to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a code of practice, this PAS takes the form of recommendations and guidance. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this PAS is expected to be able to justify any course of action that deviates from its recommendations.

Presentational conventions

The provisions of this standard are presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is “should”.

Commentary, explanation and general informative material is presented in italic type, and does not constitute a normative element.

The word “should” is used to express recommendations of this standard. The word “may” is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word “can” is used to express possibility, e.g. a consequence of an action or an event.

Notes are provided throughout the text of this standard. Notes give references and additional information that are important but do not form part of the recommendations.

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a PAS cannot confer immunity from legal obligations.

Particular attention is drawn to the following specific regulations:

- Medical Devices Directive (93/42/EEC) [1]
- Data Protection Act 1998 [2]
- Consumer Protection Act 1987 [3]

Innovate UK statement

Innovate UK – the new name for the Technology Strategy Board – is the UK’s innovation agency. We fund, support and connect innovative businesses to accelerate sustainable economic growth.

Timely, consensus-based use of standards plays a vital role in ensuring that the knowledge created in the UK’s research base is commercialized and brought to market as well as playing an important role in driving innovation.

Innovate UK is working with BSI, the Research Councils and Catapults to establish new standards earlier in the development of technologies. We are collaborating in four areas of innovation to define standards that aim to accelerate the development of those technologies and services to provide UK businesses with a competitive “first mover advantage”, including the subject of this document: independent living.

The demand for support of those with long term health conditions is set to grow rapidly over the next 15 years and beyond. If the NHS and other UK organizations are to continue to offer high standards of health and care services, they will need to embrace more technology-enabled products, services and systems to provide more home-based care and self-care.

Innovate UK’s Long Term Care Revolution work is aimed at changing conventional thinking about the institutional approach to long term care and stimulating disruptive innovation. If there is to be a significant move away from institutionalized care, this disruptive innovation needs to be supported by a range of standards that set out the principles for provision in the new environment, help to manage the risks involved, and provide clarity and consistency for consumers.

Through the Independent Living Innovation Platform, Innovate UK is delivering a wide-ranging programme to enable the ageing population and those with long term health conditions to live with greater independence.

In 2012 the Independent Living Innovation Platform launched dallas (delivering assisted living lifestyles at scale), a large scale demonstrator of independent living products and services, joint funded by the National Institute for Health Research and the Scottish Government. Read more here: <https://connect.innovateuk.org/web/dallas>

More widely, health and care is a key priority area in our work – with major innovation programmes to stimulate the development of new technologies, products and services, building on the UK’s world-class science and technology base and its global presence in the biopharmaceutical and health technology sectors.

Read more about Innovate UK and our plans in health, care and other areas here: www.innovateuk.gov.uk or contact support@innovateuk.gov.uk

Introduction

The purpose of this PAS is to develop a set of principles for health and wellness app developers to follow throughout an app project life cycle, so that health care professionals, patients and the public trust their products and services. It has been developed for use in the United Kingdom. This PAS aims to encourage innovation in health care and the development of safe and effective apps that are of a high quality, and that are fit for purpose. These apps have the potential to change the way that health care is delivered in the future.

This PAS does not cover the requirements for apps that are classified as medical devices, nor is it a rigorous document to aid in classifying a health and wellness app as a medical device. The Medicines and Healthcare Products Regulatory Agency (MHRA) provides regulatory guidance [4] to establish whether an app meets the criteria defined in the Medical Devices Directive [1], and what steps need to be taken in that instance.

This PAS is primarily for app developers to define the quality criteria for app registries and app repositories, but may also be used by:

- health care professionals selecting apps to recommend; and
- providers, charities, and community organizations commissioning bespoke apps.

This PAS draws on existing standards for software life cycle processes in medical devices (see BS EN 62304), addressing risk, and for developing quality software (see BS EN ISO 14971). The structure of the PAS is based on BS EN 62304, and the correlations are outlined in Annex A.

The emergence of app platforms, and the app registries and repositories that are associated with them, has created a new environment that enables apps to be developed with limited amounts of new code, and reuse of functionality delivered by the platform.

Health and wellness apps may link with other apps on the platform and with network services to provide a rich user experience, that may include accessing electronic health record systems.

Apps and app registries and repositories are not limited to mobile app platforms – the same paradigm applies to apps that run on other computing platforms, such as desktop computers and terminals.

The combination of the rapidly evolving platforms and integration with other products introduces a new set of product opportunities and risks. This PAS aims to bring together current good practices of app development and health care information management to address these opportunities and risks, but is not appropriate for the development of more complex software applications (e.g. Health IT systems or medical software). Annex B outlines the relationship between this PAS and ISB 0129 – Clinical risk management [5], while Annex C and Annex D show the relationship between this PAS and other industry standards and guidance available at the time this PAS was published.

This PAS is equally applicable to a range of software development methodologies, including agile and waterfall.

1 Scope

This PAS gives recommendations for developers of health and wellness apps, intending to meet the needs of health care professionals, patients, carers and the wider public. It includes a set of quality criteria and covers the app project life cycle, through the development, testing, releasing and updating of an app, including native, hybrid and web based apps, those apps associated with wearable, ambient and other health equipment and apps that are linked to other apps. It also addresses fitness for purpose and the monitoring of usage.

This PAS does not cover the processes or criteria that an app developer or publisher follow to establish whether a health and wellness app is subject to regulatory control (e.g. as a medical device, or related to information governance).

This PAS informs the development of health and wellness apps irrespective of whether they are placed in the market, and including free of charge.

NOTE 1 *The development and placing on the market, including free of charge, of a health and wellness app may be covered by certain legislation, for example the Medical Devices Directive [1].*

NOTE 2 *The focus of this PAS is on commodity apps available through app repositories, but may also be relevant to specialized applications running on other platforms.*

NOTE 3 *This PAS is not intended to replace documentation provided by platform curators on requirements for apps made available on the platform, unless referenced by platform curators.*

NOTE 4 *It is not intended to cover apps for enforcement or legal advice purposes. For example, apps used to monitor alcohol levels for drivers are out of scope.*

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS ISO/IEC 90003, *Software engineering – Guidelines for the application of ISO 9001:2000 to computer software*

3 Terms and definitions

For the purpose of this PAS the following terms and definitions apply.

3.1 app

3.1.1 app

software application that can be executed (run) on a computing platform, and is typically a small application run or accessed on mobile devices

NOTE 1 Apps were initially established as a category of software developed to run on mobile platforms for a single or limited number of purposes. However, the distinction between apps and other software applications has become less clear as a wider range of computing platforms are marketed as supporting apps and app repositories, and as apps with a wider range of functions are developed.

NOTE 2 An example is, a handheld commercial off-the-shelf computing platform, with or without wireless connectivity, or a web-based software application that is tailored to a mobile platform but is executed on a server.

3.1.2 health and wellness app

app that contributes to any aspect of the physical, mental or social wellbeing of the user (3.20) or any other subject of care or wellbeing (3.19)

{Adapted from WHO definition of “health”[6]}

3.1.3 native app

app that has been developed and distributed to run on a specific platform, and as such may take advantage of application programming interfaces and functionality that is unique to that platform, and that can be distributed and updated via an app repository (3.8) associated with that platform

3.1.4 web based app

website that is created to look and feel like a native app but that is accessed by web browser software (e.g. Chrome or Safari) running on a mobile device

NOTE 1 The app developer makes the app available from a web server in a similar way to a regular website, as a link rather than an app repository.

NOTE 2 Some native device functions (e.g. GPS, device motion) may still be available to the web-app via the

web application programming interface (e.g. HTML5 or Javascript).

3.1.5 hybrid app

app that is installed in the same way as a native app (3.1.3), but includes functionality that is delivered using an embedded browser from a web server

NOTE Hybrid apps may be used to deliver richer functionality than web based apps by providing access to platform-specific functionality, and may be distributed and updated using the app repository associated with that platform.

3.2 app developer

individual or organization responsible for the development and maintenance of an app

NOTE The app developer may also be the app publisher (3.6).

3.3 app project

set of activities and tasks that comprise the app project life cycle (3.4)

NOTE In practice an app project may be managed as activities and tasks within a series of separate projects.

3.4 app project life cycle

follows the app from initial vision, through development and use, to final discontinuation of support

NOTE 1 The app project life cycle is a framework for the tasks and activities that are undertaken by an app publisher.

NOTE 2 Where the term is not qualified it may be assumed to apply to both the product life cycle and project life cycle.

3.5 app project outputs

set of items that are the result of the app project (3.3)

NOTE Some examples of outputs include product requirement, design and test specifications, the risk register, project documentation, marketing material,

and source code, as well as the software release that is made available in the app store.

3.6 app publisher

individual or organization who is responsible for making the app available to users

NOTE The app publisher may also be the app developer (3.2).

3.7 app registry

listing of apps and related information that has a governance process to determine how entries may be added and removed from the list

NOTE 1 The entries in the app registry include a pointer to where the app is made available for use, that may include the product description for app, or a reference to it.

NOTE 2 An app registry is often used in combination with an app repository.

3.8 app repository

portal that makes apps available for use

NOTE An app store is an example of an app repository.

3.9 computing platform

combination of hardware and software which provides a defined set of platform services that may be used by software applications that run on the platform

NOTE The software and hardware used to deliver the platform may vary as long as the definitions of the platform services are respected.

3.10 discontinuation of support

point in time when the app publisher ceases being responsible for the app being available to users, but after which the app may remain in use

3.11 intended use

what an app is supposed to be used for

NOTE This may be according to the app publisher's specifications, instructions, intentions or other information.

3.12 mobile platform

commercial or open computing platforms, with or without wireless connectivity, that are hand held in nature

NOTE Examples of these mobile platforms include mobile platforms such as smart phones, tablet computers or other portable computers, and wearable technology.

3.13 personal data

any information relating to an identified or identifiable natural person

NOTE 1 For further information see DD ISO TS 25237 and Directive 95/46/EC [7].

NOTE 2 A natural person is a real human being, as opposed to a legal person, and may also be a public or private organization.

3.14 platform curator

organization that maintains the definition of the platform

NOTE 1 The platform curator may provide the hardware and software needed to realize the platform, or this may be provided by a third party which asserts conformance to the platform.

NOTE 2 The platform curator may provide validation services for products that are intended to provide the platform, and/or for products that are intended to run on the platform. Such validation services may be provided independently from the platform curator.

NOTE 3 For example, at the time of publication the curator of iOS is Apple, the curator of Android is Google, and the curator of the POSIX platform is IEEE.

3.15 platform version identifier

identifier that refers to the relevant specifications and characteristics of the version of the hardware and software components of the computing platform in question

3.16 product description

narrative definition of the app, which may include multimedia, and is made available to prospective users and purchasers of the app

3.17 purpose

practical advantage or intended effect of the app

NOTE See also Clause 4.

[BS ISO/IEC 15414:2006, 6.2.1]

3.18 quality

degree to which the system satisfies the stated and implied needs of its various stakeholders

3.19 subject of care or wellbeing

person whose care or wellbeing is being supported by use of the app

NOTE There may be one or more people with whom the user has a formal or informal caring relationship.

3.20 user

person who is directly using the app interface

NOTE 1 This may be the subject of care or wellbeing directly, or an individual assisting (as proxy for) the subject of care or wellbeing. An app may have one or more subjects of care or wellbeing interacting with the same device, either under the same subject of care or wellbeing account or using individual subject of care or wellbeing accounts. Each user may have one or more proxy users, either under the same user account or individual user accounts.

NOTE 2 Defining the users of an app may include describing the different groups of people that are intended to use the app, their defining characteristics (e.g. demographics, motivations, attitudes, behaviours) and approximate number of people within each group.

3.21 validation

confirmation that the needs of the user (3.20) and other identified stakeholders are met, whether specified or not

3.22 verification

confirmation, through the provision of objective evidence, that specified requirements have been fulfilled

NOTE See also 6.2.4.

[BS EN ISO 14971:2012, 2.28]

4 Fitness for purpose

Fitness for purpose is a term that encompasses all technical requirements and quality criteria for a health and wellness app, as defined by the app developer at the start of a project. The health and wellness app should meet all of these in order to be accepted by its app publisher (3.6) and users (3.20) for its intended use (3.12).

The intended use of the app by the user should be defined in the product description (3.16) by the app publisher in relevant app registries (3.7) and repositories (3.8) in accordance with 6.2.1.

The product description should be elaborated and updated in accordance with 6.7 throughout the app project (3.3) alongside a requirements analysis document that defines the capabilities of the app in a way that can be tested in accordance with 6.3.

In accordance with Clause 7 a risk registry should identify ways that the user of the app may be unable to use the app to achieve the intended use, how these risks may be mitigated and what contingencies should be in place to minimize the impact.

5 Quality criteria

5.1 Quality criteria are aspects of quality (3.18) which should be described or measured throughout a health and wellness app project. The quality criteria (see 5.2) provides a structured way to check that the app and related products and services meet the relevant needs of the:

- subject of care or wellbeing;
- user, if different;
- any third parties, if necessary;
- health care professionals, if applicable;
- platform curator;
- app developer; and
- regulatory and legal authorities, if applicable.

5.2 The following types of quality criteria should be considered for a health and wellness app.

- a) Regulatory and legal compliance – it is important to be aware of specific regulations and laws that might apply, and to ensure that compliance can be described in terms used in the regulations.
 - b) Functionality – covers the functions that are required to support the intended use of the app for the user, and functions the app require to meet the relevant needs of any other stakeholders (see 5.1).
 - c) Usability and user experience – including considerations of accessibility for different types of users, and how using the app might fit in with related activities that the user performs.
 - d) Reliability, performance, and scalability – to cover both the performance of the app itself, and the supporting infrastructure, such as web services that the app may rely on.
 - e) Security and privacy – to include effective controls over the app and information that it collects, while ensuring that before choosing to use the app, the user is made aware of how personal information is collected, stored and used.
- NOTE 1** Attention is drawn to the Data Protection Act 1998 [2].
- f) Safety – including patient safety ¹⁾ where relevant, as well as safety considerations that would apply to any software product.

¹⁾ For further information on patient safety see NHS England's publication, *Patient Safety* [8].

- g) Compatibility and portability – including compatibility of the app with different platform configurations and the ways that information collected or used by the app may be reused, under appropriate privacy controls.
- h) Maintainability – it is important that the app is maintained so that it can deliver the intended use, or at least until support is discontinued by the app publisher. It should cover all the considerations that are relevant to the reliable and cost effective provision of maintenance services (see 6.7) and configuration control (see Clause 9).

NOTE 2 These quality criteria are based on the quality models defined in the SQuaRE series of standards, for further information see BS ISO/IEC 25010 and BS ISO/IEC 25012.

NOTE 3 Appendix C provides mapping between PAS 277 and a set of quality criteria from Health on the Net Foundation [9] for medical and health websites.

5.3 The quality criteria should be referenced throughout the app project and in particular when:

- defining the requirements for a health and wellness app in accordance with 6.3;
- elaborating the design in accordance with 6.4;
- application testing in accordance with 6.5; and
- overseeing risk management in accordance with Clause 7.

6 App project life cycle

6.1 Life cycle selection

Any health and wellness app project life cycle should have phases that correspond to the following areas, with iterations at any or all phases as required:

- planning (see 6.2);
- requirements analysis and research (see 6.3);
- design (see 6.4);
- application testing (see 6.5);
- implementation (see 6.6);
- release (see 6.6);
- maintenance (see 6.7); and
- discontinuation of app project life cycle.

App developers should select or develop a life cycle that suits their app project. When selecting or developing an app project life cycle the following should be taken into account:

- life cycles used for other projects and products within the organization or wider community involved in the development and use of the app;
- reporting and regulatory requirements, where necessary and expected;
- the size of the app project; and
- information management tools and resources available to track activity against the app project life cycle.

NOTE This PAS focuses on the app developer's and publisher's perspective. Purchasers, app repository custodians, regulators, users and others might run projects to manage their relationship with an app and these might have different life cycle phases.

6.2 Planning

6.2.1 Setting the scope

The scope of a health and wellness app should be defined at the start of the app project to analyze and manage risks relating to the use of an app in accordance with 7.2.

In defining the scope an app developer or publisher should consider, as a minimum, the following topics:

- What mobile platforms and platform version identifiers is the app intended to work on?
- Who are the users of the app?
- Who are the subjects of care and wellbeing of the app?
- What is the app's intended use?
- What problem is the app trying to solve?
- What are the health and wellness outcomes that may be achieved?
- What kinds of information is the app handling?
- Scenarios describing typical use of the app.
- Explicit limitations relating to the requirements or use of the app.
- Support and sustainability for the anticipated life of the app.
- The impact on users of discontinuing support for the app and planning for this. The impact of withdrawing the app from app repositories or other distribution channels.

NOTE For example, removing apps that support mental health conditions may have psychological/mental health effects for a user.

The scope should be reviewed, refined and elaborated throughout the app project. Any changes to the scope and other requirements should be managed and implemented in a controlled manner in accordance with Clause 9.

6.2.2 Project planning

All the tasks and activities in the selected health and wellness app project life cycle should be planned, in particular:

- the software, methods and tools to be used;
- the project documentation (see 6.2.3) to be produced to support and verify each task in the development process; and
- the availability of resources needed.

NOTE Examples of resources that might be required for the project are facilities, equipment, finances, intellectual property rights, and human resources.

6.2.3 Project documentation

The following project documentation should be created and maintained, if applicable, throughout the app project to provide a basis for governance during the project and supporting evidence upon completion.

- a) Unmet need evidence – collection of evidence of an unmet need should start as early as possible, as this may be used to inform the planning and requirements analysis (see 6.3) including, clinical evidence. Where the intended use and design of a health and wellness app is based on existing clinical evidence, the evidence that supports claims or propositions of any medical or health benefits by using the app, should be kept and made available in the product description, where appropriate by the app publisher.

NOTE 1 For example, for mental health apps, an explicit reference to any underlying psychological approach employed might be useful to the intended user.

- b) Credentials – name and credentials of all human and/or institutional providers of information, including dates at which credentials were received.
- c) Testing – a test plan should be created and maintained. The app publisher or developer should retain all protocols, results and evidence of testing in accordance with 6.5, including, clinical benefits. During testing evidence should be collected to validate any clinical benefits that the app's intended use delivers.

NOTE 2 Documents relating to testing might be made available for contractual, regulatory or legal reasons.

NOTE 3 Such evidence might also be of use when tracking down faults that might have been introduced into the app during development or maintenance.

- d) Risk register – evidence should be gathered during the identification and management of specific risks, and also to maintain evidence that a risk management process is being followed.
- e) Product description – the intended use of the health and wellness app from the perspective of the subject of care or wellbeing, the user, other subjects, and the app repository should be described in the product description provided in the app repository, or in material referenced in that description. The source and date of the evidence should be provided, along with a link to the source, where possible.

- f) Privacy statement – a statement on personal information should be made available to any potential or actual user of the app, so that they are aware of how it is collected and handled as a result of using the app.

NOTE 4 Annex E provides example health and wellness apps currently available and their intended use.

6.2.4 Test planning

Testing includes both validation that the health and wellness app meets the needs of its users and other stakeholders and verification that the app and project documentation are consistent.

Reasons for validating a health and wellness app should be identified at the start of the project so that the relevant project documentation is available when needed. Reasons include:

- conformance with relevant regulations, if applicable;
- *NOTE 1 Relevant regulations might include those relating to medical devices or data protection.*
- to be included in the listings of an app repository;
- as part of the app developer's quality management system; and
- to establish acceptance of an app by the user.

Verification of a health and wellness app should be completed to:

- check that the app fulfils the documented requirements;
- check that the design has been implemented correctly; and
- check that critical functions (e.g. safety related) operate correctly and be able to demonstrate what tests were carried out and the results.

The app project should define as a minimum one final quality gate, that includes testing (validation and verification) to establish that the app is fit for purpose in accordance with Clause 4 prior to the release of a health and wellness app through any medium or for any purpose.

NOTE 2 It is good software development practice and more efficient to establish quality gates with criteria at earlier points in the app project life cycle.

NOTE 3 Where available and relevant toolkits, such as the MindTech checklist [14], for appraising mental health apps may be used.

6.3 Requirements analysis

6.3.1 This subclause gives a list of topics that should be reviewed during the requirements analysis of a health and wellness app to fulfil the quality criteria in accordance with Clause 5. All requirements should be traceable throughout the app project life cycle in accordance with BS ISO/IEC 90003.

NOTE 1 *It is important to note this is not an exhaustive list.*

a) Regulatory and legal compliance

The app developer should research current compliance regulations governing, for example medical devices, data protection and other relevant standards, and include these processes in the requirements. Requirements stated by the applicable regulations should also be included in the analysis.

b) Functionality

- 1) Functional requirements of the app should be determined using case studies and user stories, and should include information about the app's relevance to the following types of care, specifically how the app enhances or inhibits such care:
 - i. self-directed care;
 - ii. informal care; or
 - iii. professional care.
- 2) Age-appropriate functionality should be considered. If the app is intended for use by children then the content should be appropriate, if not then the app publisher should take steps to make it available only to the intended users. Apps may be used by children in a variety of ways including: alone, under supervision, or indirectly with an adult mediating between the child and the app. The requirements analysis should take this into account where relevant.

NOTE 2 *Many platforms may provide facilities to support managing distribution of age-restricted apps in a consistent way.*

NOTE 3 *There may be a requirement to refresh content or functionality if updates are not performed in a timely fashion. The app publisher may consider reminding or requiring the user to perform updates after a period of time.*

c) Usability and user experience

- 1) Accessibility requirements should be addressed to check that the app can be used by the intended users, and that any restrictions on usability are identified.
- 2) Usability is a critical property.

NOTE 4 *Although this PAS is not intended to cover apps that are medical devices, there is useful and relevant guidance in the medical device standards. For example, BS EN 62366-1 or the FDA's usability guidance [10].*

- 3) Rules for validating data when it is collected from the user and protecting against other anticipated user errors should be addressed.
- 4) Specific documentation for app repositories or other channels (e.g. product description) should be addressed.
- 5) User documentation should be addressed.

d) Reliability, performance and scalability

- 1) For apps that may be used on a device that has intermittent network connectivity, the requirements should address how this is likely to impact the use of the app.

NOTE 5 *This may highlight associated risks to track (see Clause 7).*
- 2) Whether options need to be described for the user if the app is temporarily or permanently not available, such as using paper notes should be addressed.
- 3) App load and response times, and other time related behaviours should be addressed.
- 4) Memory and processor power requirements should be addressed.
- 5) Data storage requirements, whether directly accessible in the app platform, or available as networked resources should be addressed.
- 6) Battery life and impact of temporary loss of power.

e) Security and privacy

- 1) Requirements for confidentiality, data integrity, non-repudiation, accountability and authenticity should be addressed.
- 2) Personal data that is used or collected by the app should be described in the privacy statement document. This may be information about the user, the subjects of care or wellbeing, or other subjects and should include:
 - i. the information to be captured or used by the app;
 - ii. whether the information is likely to be stored (on or off a mobile device);

- iii. where any stored information is held – takes into account backups, information synchronized between devices, security, where relevant, and information for incomplete transactions that is persisted on the mobile device to maintain application state;
 - iv. how the user should be informed about and be able to manage the sharing of any personal data with other apps or medical app repositories (e.g. Apple’s Health Kit or Google Fit);
 - v. what triggers the removal of personal data that is no longer relevant to the intended use of the app; and
 - vi. what happens to personal data when the user chooses to delete the app. If the data is not all deleted then this should be made clear in the product description.
- NOTE 6** For further information see the *Data Protection Act [2] or other relevant regulations.*
- 3) Anonymized data requirements state how anonymity should be maintained were the data to be combined with other data and contextual information that may be available. The assumption should be that information subjects are indirectly identifiable unless the app publisher can show otherwise. Where the information subject is indirectly identifiable, the data should be treated as personal data.
- f) Safety
- 1) Safety considerations should be designed into the app.
 - 2) Specific requirements relating to safety may be identified during the risk analysis in accordance with Clause 7.
- g) Compatibility and portability
- 1) Standards and industry guidance should be used for health care information where the app shares information or is used alongside other information systems. SNOMED CT [11] should be considered for clinical concepts as requested by NHS England.
- NOTE 7** Information structures for representing demographic information such as names and addresses may follow the standards used by the NHS.
- NOTE 8** SNOMED CT is available for use in the UK at no charge and is available from the UK Terminology Centre [12].
- NOTE 9** The HSCIC interoperability toolkit framework [13] may be used if there is a requirement to interact with NHS England systems, or with systems that have adopted this framework.
- 2) A health and wellness app might only function as intended if other apps or services upon which it is dependant are available. If this is the case then this should be explicitly included in the requirements, with appropriate behaviours defined for when the apps or services are not available. It should be stated if there are other apps or services which can add functionality to the app if available. If there are any such apps or services then the following information should be included in the requirements:
- i. version information;
 - ii. functionality from the app or service that is likely to be supported; and
 - iii. which parts of the app or service API are likely to be used.
- NOTE 10** For example, a health monitoring app could support posting information to some GP information systems if there is a connector for the GP system available to the app. The product description might state which GP systems are supported so that the user can make an informed decision.
- 3) Platforms and platform version identifiers that the app should support – the app developer should consider costs of supporting the app on multiple platforms and the intended user’s platform preferences when deciding which platforms to support.
- NOTE 11** Hardware and software platform requirements may be considered.
- 4) The app design should take into account the range of platforms that need to be supported.
 - 5) An effective mechanism should be provided for uninstalling the app and if appropriate, making data collected by the app available to the user so that the app can be replaced.
 - 6) If appropriate, how the user can transfer the app and associated data onto another device or platform should be described, or the app should be made usable on multiple devices with the same data.

h) Maintainability

- 1) Requirements for upgrading the app should be considered, including what mechanisms are needed to inform the user that upgrades are available.
- 2) In some cases the app might require the user to regularly check for and install upgrades in order to continue using the app. The benefits of ensuring that current content and functionality is available should be weighed against the risks that this sometimes causes the app to be unavailable for its intended use.
- 3) Maintenance is not limited to the app itself, but also includes information that the app provides access to, and the products and services that are made available alongside the app. Requirements for a maintenance processes to ensure that these are kept aligned should be considered.

6.3.2 All proposed requirements should be tested as early as possible in the app project, and include the following methods:

- a review of existing publications, including academic research on user needs and practices published in specialist magazines, conference proceedings and journals;
- user interviews, to understand how intended users currently achieve the purpose intended for the app;
- the review of wireframes and prototypes of the app;
- the provision of signup opportunities, to see how many potential users are willing to pre-register for an app that is described as meeting the requirement; or evaluating similar apps that are available in the target app repository or other app repositories; and/or
- field testing of the app.

NOTE 12 *Where an iterative methodology is used, field testing of early releases may be used to inform the requirements for subsequent releases of the app.*

NOTE 13 *The number of users able to use early versions of the app may be controlled by issuing activation codes if the app repository does not provide other means for the app publisher to restrict access to a limited group of test users.*

6.4 Design

The design of a health and wellness app should take into account the requirements as defined by the requirements analysis (see 6.3) including:

- a) Regulatory and legal compliance;

NOTE 1 *Regulations may have impacts on how design decisions are documented.*
- b) Functionality – should be described in the product description and the requirements analysis. Any functional requirements discovered during the design phase should be added to these documents;
- c) Usability and user experience:
 - 1) a health and wellness app should take advantage of the features of the selected platform, where possible, to provide a consistent user experience and to minimize the need for reinvention of functionality. The design should take into account the user needs; and
 - 2) the advantages and disadvantages of such reuse should be considered by the app developer in the context of the intended use for the app;
- d) Reliability, performance and scalability:
 - 1) the design should take account of reasonable demands for reliability, performance and scalability; and
 - 2) the design should include mechanisms for detecting when performance is outside of the acceptable range, so that the user and/or app publisher can take appropriate action;
- e) Security and privacy:
 - 1) the user interface for the app should include a way to access the app's privacy statement; and
 - 2) the app should ensure that personal information collected by the app is kept secure, and that it is processed according to the privacy statement;
- f) Safety:
 - 1) if advertising is delivered through or alongside the app, there is a risk that the advertising could pop-up, obscure, interfere with or be mistaken for information provided by the app. Health and wellness apps should be designed in a way that such issues do not arise when health information is being displayed on the user's device;
 - 2) where the user is prompted to enter data, implausible values should be tested for and handled appropriately, for example by prompting the user to confirm; and
 - 3) where there are calculations made in the app, implausible results should be tested for and handled appropriately, for example by informing the user;

g) Compatibility and portability:

- 1) functionality that is dependent upon the underlying platform, and so might need to be changed when the app is supported on a different platform, should be designed as a separate component and that can be replaced without affecting the rest of the app code; and

NOTE 2 For example if location information is needed, a “location” component may be defined that provides a consistent interface for the rest of the app code, to whatever underlying platform services are used to obtain the location information.

- 2) the design should include tests for the configuration of the platform that the app is running on, so that the user can be informed if the platform is not supported;

h) Maintainability:

- 1) a modular design should be used;
- 2) frameworks, components and toolkits including those that have been designed specifically for health and wellness app development should be considered. The quality of any such framework should be considered, bearing in mind that third party or open source components have the potential to introduce risks that may not be within the developer’s ability to control;

NOTE 3 An example framework and toolkit is the HSCIC interoperability toolkit framework [13].

- 3) the design should take into account the need for application testing; and
- 4) the purpose of each component of the app should be documented in the source code together with the information on the meaning of any parameters. Code or algorithms should be explained to help app developers use the function correctly. Components and function within them should be named so as to facilitate understanding of their purpose.

6.5 Application testing

The app developer should test each iteration of the health and wellness app with all relevant user groups in accordance with 6.2.4. Data collected from all user tests should be collated, analyzed and the results used to inform the final quality gate decision as to whether the app is fit for purpose and may be released in accordance with 6.6.

For each of the requirements defined in 6.3 test results and feedback should be documented together. These tests should be used to verify that the app meets the requirement.

Application testing should apply to both the app and project documentation.

The app should be tested on all the platforms that it is planned to be released on.

The test plan should describe what testing is to be done when there is a change to the product description, app or to a platform that it runs on.

NOTE For many app platforms the operating system is updated regularly, and this is a change to the platform that the app runs on.

Any issues encountered during testing should be logged and inform subsequent iterations of the app in accordance with 6.7.

6.6 Release and installation

A version of the app should only be released after it has passed the set of tests defined in the final quality gate and is deemed fit for purpose by the app publisher in accordance with 6.5.

An incremental release policy should be considered, where possible, so that the app is trialed by a limited number of users in pilot implementations before being made generally available.

The installation process of the health and wellness app should verify that:

- the installation is taking place on a supported platform and the platform version identifier; and
- that any required apps or services are available.

If there are required items missing then:

- the installation process should install the missing components if possible;
- if this cannot be done immediately as part of the installation process then an informative message should be displayed to the user, with any installed components removed; and
- the user’s device returned to the state that it was in before the installation was attempted.

6.7 Maintenance

A maintenance process should be put in place for receiving, tracking and resolving reported issues and product improvement suggestions. This process should include:

- a statement to those submitting an issue report whether they are likely to receive feedback with a response timeframe (e.g. one day, one week or one month);
- tracking feedback submitted on app repositories alongside other issue reports;
- evaluating issue reports to establish whether changes to the product description, app, or other app project outputs are required. All issue reports should be tracked and where there is evidence of harm or potential harm to the user, the appropriate regulatory authorities should be notified;
- periodic review of health information and knowledge incorporated in the app and product description, and the frequency of such reviews should be stated in the product description. The date when the last review was undertaken should be made available for the user in the app and/or in the product description; and

***NOTE 1** A review period of two years may be appropriate in many cases, but the frequency may be set based on the rate at which evidence and knowledge about the intended use of the app is changing.*

- the app publisher identifying unintended uses and assessing whether they pose any safety risks that should be addressed, or indicating opportunities to extend the intended purpose.

***NOTE 2** Examples of unintended uses might be that an end user intentionally sends data collected by the app to unintended recipients (e.g. GP or healthcare professional) rather than the intended friend or family member with the expectation that they might monitor, act on or respond to the data. Or end users may share an app that is intended for individual use, such as a couple both using a dietary monitoring app.*

***NOTE 3** Opportunities can be highlighted by encouraging user feedback or through the use of surveys. The app publisher's ability to monitor usage may be limited by the need to respect the privacy of users, especially if the app collects personal information, or if personal data can be inferred from use of the app. However, where ethical, legal, well justified and done with the knowledge of the user, such research can deliver important benefits.*

***NOTE 4** Where the app meets the definition of a medical device serious incidents are reported to the relevant authority (e.g. MHRA in the UK) under vigilance requirements.*

7 Risk management

7.1 Risk management strategy

A documented risk management strategy should be initiated and maintained throughout the app project, including the maintenance of one or more risk registers in accordance with 7.2.

The app publisher should ensure that risks associated with use of the app are managed.

The risk management strategy should be capable of:

- describing the situations where things could go wrong when using the app (potential failure scenarios);
- listing the specific events or conditions that could lead to an undesirable outcome (hazards);
- assessing the likelihood of each event happening, and the severity of the outcome (risk); and
- describing how the risk should be avoided, or detected and their impact reduced.

NOTE 1 The strategy to be used for a particular app may build upon existing risk management practices in the organization or regulatory requirements.

NOTE 2 Annex B describes the relationship between this PAS and ISB 0129 [5] that provides a framework for a risk management strategy. Further relevant guidance may also be found in BS EN ISO 14971.

NOTE 3 Different organizations and individuals involved in the production of the app might have different risk management strategies, and different risks to address. In particular the app publisher and app developer might operate separate risk management processes.

A health and wellness app project should include risk management activities intended to identify and manage safety hazards, security threats or other types of risk. It can be advantageous to separate these activities as this can better reveal conflicts between them.

Risks arising from a number of root causes should be considered, including:

- the app being used in ways other than those intended by the app publisher;
- incomplete or ambiguous requirements; and
- mistakes/oversights during implementation.

The requirements analysis should take account of product-related risks that have been identified and identify requirements that already address these risks or create additional requirements to prevent this risk from being realized, or mitigate the consequences.

The app developer may use the quality criteria listed in Clause 5 to classify types of risk during the course of the app project (see 7.2).

NOTE 4 In addition to these quality criteria there may be project risks associated with the availability of appropriate resources and people to deliver the app in the time available, and risks associated with establishing intellectual property and the possibility of patent infringement.

NOTE 5 Each of the risk types is a specialist area in itself. It is therefore common for risks associated with different quality criteria to be managed separately, although there is some overlap between regulatory risks and both safety and security. Annex F sets out an example health and wellness app risk reporting analysis.

NOTE 6 Separation of the management of different types of risk allows risks and issues to be managed by people with the right expertise. Even for a sole app developer, managing risks separately is likely to be beneficial as the requirements and methods for managing the different types of risk differ.

NOTE 7 Annex F provides some examples of safety hazards identified within an example health and wellness app. App developers may consider taking a similar approach with other types of risk.

Application testing activities should be undertaken in accordance with 6.5 to validate that this risk reduction activity is effective.

Where the app or project documentation is modified to reduce risks, tests should be conducted to verify that the change has been correctly implemented. Where risks are managed by proposing changes in behaviour of people or organizations, the anticipated reduction in risk should be verified using techniques such as reviews, walkthroughs or by inspection.

Any changes to an app require the risks and risk reduction plans to be reviewed. A review should also be completed when there is a change in the environment in which the app is used.

The appropriate level of rigour for such testing should be chosen taking into account the intended use, the nature of any risks identified and the changes that have been made. For example, if the app receives or sends data to other systems or stores data for later retrieval, then it might be necessary to undertake additional testing to ensure that all those functions still operate correctly following the update.

7.2 Risk register

A risk register should include, as a minimum, the following details for each risk:

- name;
- description (this may include potential causes);
- probability (the probability of the risk materializing);
- severity (a measure of how serious the consequences of the risk materializing would be);
- risk score (this is derived from the probability and severity);

NOTE 1 Probability, severity, and risk score may be categories (such as high, medium, low) or continuous values such as percentages.

- impact (a description of the consequence of the risk materializing);

NOTE 2 These may include an estimated schedule delay, financial cost or patient safety.

- indication (how to tell that the risk has materialized and moves from being a risk to a reality);
- mitigation (actions planned and done to avoid the risk materializing); and
- contingency (actions to be done if, and when, the risk materializes and becomes a reality).

The severity and probability should take account of mitigation and contingency plans that are in place, and mitigation actions that have been undertaken.

NOTE 3 The impact of a risk could be experienced by the user of the app, the app publisher, a subject of care or wellbeing, or others involved in the app project life cycle.

Where the probability and severity are both categories, Table 1 gives an example approach to determine the risk score.

The precision of the probability and severity metrics, and the number of risks tracked in the register, should be appropriate to the app project, such that the process of risk management adds value.

Table 1 – Example risk score

Severity	Probability: High	Probability: Medium	Probability: Low
High	Risk: High	Risk: High	Risk: Medium
Medium	Risk: High	Risk: Medium	Risk: Medium
Low	Risk: Medium	Risk: Low	Risk: Low

8 App project governance

Throughout the app project life cycle the viability of the app project should be reviewed. In particular, the following questions should be asked and assessments made by the app publisher and app developer.

- Is the app project sustainable?
- Has a project and product risk assessment been done?

NOTE 1 An example project and product risk assessment is given in Annex F.

- Is there evidence to support assumptions about the value of the intended use of the app for (and from) the intended users of the app?
- Are plans in place to ensure that the app conforms with all relevant legal, licensing and regulatory requirements, if applicable?

NOTE 2 The Medical Devices Directive [1], the Data Protection Act [2], the Consumer Protection Act [3], and the Active Implantable Medical Devices Directive [15] are examples of regulations an app publisher might consider.

An app publisher should be prepared to cancel or revise an app project if circumstances change or critical assumptions are found to be incorrect.

9 Configuration management

9.1 Configuration management plan

Configuration management should be undertaken so that components of the app are consistently referenced in all project and user documentation, and to enable the management of issues encountered during use.

A configuration management plan should exist for the entirety of the app project life cycle.

NOTE 1 *This may be a document created specifically for the project, a section within another project document such as a quality plan, or it may be a policy document that applies to many projects and products.*

The configuration management plan should include, as a minimum, the following:

- a definition of the types of configuration items that are managed for the app;

NOTE 2 *Examples of possible component types include; app screens, software modules, resource files, documents, document fragments, externally maintained apps, web services, risk register entries and app requirements.*

NOTE 3 *A component, for example, may be a document that includes a reference to a collection of document fragments.*

- for each component type there should be a way to name or identify configuration items that are instances of that type; and

NOTE 4 *For example, documents may be identified using a document naming convention.*

NOTE 5 *Many components may change without requiring a new identifier to be issued. In this case a version identifier may be issued. For example, the welcome screen for an app might be changed as a result of feedback from users. If the welcome screen is reused across multiple apps then a new version identifier may be issued. If it is only used on one app then it might be sufficient to track the version identifier for the app as a whole.*

- for each component type the configuration management plan should describe the criteria for issuing new component identifiers, and component version identifiers, and for describing how and where they should be used.

9.2 Change control

Changes to the app or app project should be associated with new requirements or one or more issue reports identified in accordance with 6.7.

Proposed changes should be carefully assessed to identify the potential impact on:

- functional requirements such as safety and security related functions, compliance with technical standards and Interoperability;
- non-functional requirements such as performance/scalability and usability;
- the intended purpose, user processes and training; and
- project timescales.

Changes that impact safety related functions should be risk assessed to check that the residual risk for any new or changed hazards can be justified.

The approach taken for testing changes should be designed to provide renewed assurance that any important safety, security or functional properties of the app are not adversely affected by the changes.

9.3 Configuration status accounting

The user of an app should be able to determine which version of the app they are using, and obtain information so that all component versions that make up the app can be determined.

10 Support

Service level expectations should be stated in the product description. Feedback and comments posted in any app repository listing should be monitored. Any comments that raise product quality issues should be replied to, where possible, and the issue should be tracked through to closure following the maintenance procedure in accordance with 6.7.

The current name, physical and electronic address of the app publisher should be made available to the app user. An email address or web page should be provided for users to submit issue reports.

NOTE *This may be achieved in a variety of ways including:*

- *by providing an “about” screen in the app;*
- *by providing a link to an app registry or repository; or*
- *by providing a link to the app publishers website.*

If premium support services are offered as an additional paid option, then this should be made explicit in the product description along with a clear explanation of what is provided at each level.

Annex A (informative)

Relationship between PAS 277 and BS EN 62304:2006

PAS 277 follows the same document structure as BS EN 62304:2006 and is intended to be compatible with it.

The relationship between sections in this PAS and BS EN 62304:2006 are listed in Table A.1.

Table A.1 – Table of clauses in BS EN 62304:2006 and PAS 277

BS EN 62304 clause	PAS 277 clause
4 General requirements	4 Fitness for purpose
	5 Quality criteria
	6.2.3 Project documentation
5 Software development process	6 App project life cycle
6 Software maintenance process	6.7 Maintenance
7 Risk management process	7 Risk management
8 Software configuration management process	9 Configuration management
9 Software problem resolution process	10 Support

Annex B (informative)

Relationship between PAS 277 and ISB 0129

ISB 0129 Clinical risk management: Its application in the manufacture of Health IT systems [5], is focused on clinical risk management and is more specific than PAS 277 in the area of risk management (see Clause 7). Table B.1 provides a summary of the contents of ISB 0129.

There are benefits to having a consistent approach to risk management across an organization and within a group of stakeholders. For health and wellness apps

this may often be determined by regulation, and at the time of writing ISB 0129 forms part of the regulations maintained by NHS England.

PAS 277 does not specifically itemize risk management responsibilities, activities and outputs through the app project life cycle.

NOTE It is beyond the scope of this PAS to determine the detail of the terms to be used and processes to be followed in managing risk.

Table B.1 – Table of contents for ISB 0129

Section title	Section number
General requirements	2.2 Top management responsibilities
	2.3 Clinical safety officer
	2.4 Competencies of personnel
	2.5 Non-health products and COTS products
	2.6 Regular clinical risk management process review
Project safety documentation	3.1 Clinical risk management file
	3.2 Clinical risk management plan
	3.3 Hazard log
	3.4 Clinical safety case
	3.5 Clinical safety case report
	3.6 Safety incident management log
Clinical risk analysis	4.1 Clinical risk analysis process
	4.2 Health IT system scope definition
	4.3 Identification of hazards to patients
	4.4 Estimation of the clinical risks
Clinical risk evaluation	5.1 Initial clinical risk evaluation
Clinical risk control	6.1 Clinical risk control option analysis
	6.2 Clinical risk benefit analysis
	6.3 Implementation of clinical risk control measures
	6.4 Completeness of clinical risk control
Delivery, monitoring and modification	7.1 Delivery
	7.2 Post deployment monitoring
	7.3 Modification

Annex C (informative)

Relationship between PAS 277 and Health on the Net (HoN) quality criteria

The Health on the Net Foundation [9] provides a set of quality criteria for medical and health websites, and a certification programme to assert conformance. Table C.1 outlines the relationship between HoN and PAS 277.

Table C.1 – Relationship between PAS 277 and Health on the Net (HoN)

Topic (HoN principle)	HoN guidance summary	PAS 277 clause
Authoritative	All medical information shall be attributed to an author, and the author's training in the field mentioned.	See 6.2.3
Complementary	It shall be clear that the information and services provided by the site support do not replace the patient's relationship with a doctor.	See 6.3 a)
Privacy	The privacy of patients and users is respected, and the website owners undertake to respect local laws wherever the app is distributed and used.	See 6.3 a)
Attribution	Where appropriate information shall be attributed with the source and date accessed for information. Links to the source shall be provided where possible.	See 6.2.3
Justifiability	All claims relating to benefits for the app shall be supported by balanced appropriate evidence.	See 6.2.3
Transparency	The publisher shall provide contact details including an email address for support and further information.	See Clause 10
Financial disclosure	Support for the app shall be clearly identified, including the identities of commercial and non-commercial organizations that contributed to the funding and production of the app.	This is not included in the PAS. <i>NOTE Such financial transparency is not required for apps outside the health and wellness sector, or for other products in the health and wellness sector.</i>
Advertising policy	If advertising is a source of funding this shall be clearly stated, and advertising material shall be clearly distinguished from material that is part of the app itself.	See 6.4

Annex D (informative)

Relationship between PAS 277 and eEurope 2002

The European Commission provides a document on the quality criteria for health related websites [16]. Table D.1 outlines the relationship between this quality criteria and PAS 277.

Table D.1 – Relationship between PAS 277 and eEurope 2002

eEurope quality criteria	eEurope 2002 guidance (paraphrased)	PAS 277 clause
Transparency	Transparency of provider of site – including name, physical address and electronic address of the person or organization responsible for the site.	See 6.7
	Transparency of purpose and objective of the site.	See Clause 4
	Target audience clearly defined (further detail on purpose, multiple audience could be defined at different levels).	See Clause 5 and 6.2.1
	Transparency of all sources of funding for site (grants, sponsors, advertisers, non-profit, voluntary assistance).	This has not been included as it is not a requirement for other health and wellness software products, nor is it a requirement for other app products.
Authority	Clear statement of sources for all information provided and date of publication of source.	See 6.2.3
	Name and credentials of all human/institutional providers of information put up on the site, including dates at which credentials were received.	See 6.2.3
Privacy and data protection	Privacy and data protection policy and system for the processing of personal data, including processing invisible to users, to be clearly defined in accordance with community Data Protection legislation (Directives 95/46/EC and 2002/58/EC).	See 6.3.1 a)
Updating of health related information	Clear and regular updating of the site, with date of update clearly displayed for each page and/or item as relevant. Regular checking of relevance of information.	See 6.7
Accountability	Accountability – user feedback, and appropriate oversight responsibility (such as a named quality compliance officer for each site).	See 6.7
	Responsible partnering – all efforts should be made to ensure that partnering or linking to other websites is undertaken only with trustworthy individuals and organizations who themselves comply with relevant codes of good practice.	Not included
	Editorial policy – clear statement describing which procedure was used for selection of content.	See 6.7 and Clause 10
Accessibility	Accessibility – attention to guidelines on physical accessibility as well as general findability, searchability, readability, usability, etc.	See 6.3

Annex E (informative)

Example health and wellness apps

E.1 General

The following examples of health and wellness apps are intended to illustrate the range of apps within scope of this PAS.

NOTE The full product descriptions are not provided, but they do illustrate what might be included in a product description.

E.2 Exercise monitoring application

An app that tracks daily activity by using sensors on the device to detect walking and other forms of exercise, and also allows the user to enter details of activity undertaken.

It might be used for the following purposes:

- tracking calories burned when doing exercise;
- planning an exercise schedule, and comparing actual activity with planned activity;
- providing suggestions as to new activities based on planned and recorded activity;
- sharing activity information with friends;
- sharing activity information with other apps such as diet tracking apps;
- linking to knowledge bases to get exercise related information and training material;
- sharing information with a personal trainer and/or health care professionals;
- sharing information with sports-club membership; and
- providing evidence for team selection.

E.3 Managing end-of-life care

An app that helps clinicians to provide best possible care for patients as they approach the end of life.

It might be used to:

- see a list of patients currently on an end-of-life register;
- see lists of patients who might be considered for inclusion on an end-of-life register;
- see preferences for end-of-life care that have been recorded;
- see a patient's relevant care plan;
- check that end-of-life care plan documentation is consistent across care organizations (e.g. in hospital, GP, hospice, care home) by looking at timestamps for when they have been updated, and where possible doing document or data level comparisons; and
- manage the sharing of information with carers and other health care providers.

NOTE This includes careful management and documentation of consent for information sharing.

E.4 Managing mood

An app that allows a user to track their mood, gives distraction tasks and contains wellbeing tips and links to further advice and assistance where needed.

It might be used to:

- rate a user's mood on a particular day;
- share their mood with friends, family, or carer;
- record and display their mood selection over time;
- give wellbeing tips and web-links to sources of further information;
- access phone functions for distraction including, music, images, videos; and
- access phone functions for communications including contacts for help or advice.

NOTE The app is intended for the general public and is not restricted to NHS service users, but may be prescribed by a GP.

E.5 Sleep activity app

The app allows an intended user to record and analyze their sleep patterns, access advice about improving sleep, and includes an audio facility intended to help a person fall asleep.

It uses the users' phone or tablet's accelerometer (and where available, gyroscope) to record motion activity during sleep.

The app may be used to:

- automatically classify periods of REM and deep sleep and to record overall sleep time, to record time taken to fall asleep and the number of times a user wakes up in the night;
- give general advice, in the form of text and videos, about improving quality of sleep; and
- set an audio tone to be played for a set period after going to bed, intended to help the user fall sleep.

The app is a web based app and only works on devices with HTML5 Javascript Device Motion API support.

As an option, the app also captures location from GPS using the HTML5 Javascript geolocation API.

No information is sent remotely and is stored locally on the device (phone memory or SD card).

Annex F (informative)

Example risk repository analysis

F.1 General

The following example is provided to illustrate how risk analysis as described in Clause 7 may be applied to a health and wellness app project. It does not include qualitative categories or matrices required for a full risk management analysis, nor does it include a full set of requirements or product description for the app under consideration.

NOTE A detailed definition of risk management strategy is beyond the scope of this PAS, and the reader is encouraged to look at risk management specifications such as ISB 0129 [5] for a more detailed description of a relevant risk management process.

F.2 Example medication reminder app

The purpose of the example medication reminder app is to help with the management of medications that need to be taken or administered for one or more subjects of care or wellbeing. The user might be the subject of care or wellbeing or a carer.

The app might be used to:

- enable the user to select the subject of care or wellbeing;
- capture, view and edit details of all medications that have been prescribed for the subject of care or wellbeing;
- look up and display information published by the medication manufacturers about each medication that has been prescribed;
- display a log of what medications have been recorded as having been taken;
- alert and remind the user at certain times of day and inform them of whatever dose of medications needs to be taken at that time;
- continue to alert the user or escalate to a first responder by SMS message if no action is taken to acknowledge the alert; and
- record that each dose has been given.

NOTE Even with the above level of detail it is clear that there may be safety hazards relating to medications management. This clearly increases the likely impact of any postulated hazards above that which would apply if this app were recording daily exercise for example.

F.3 Risk analysis

It is not usually possible to install an app twice on a mobile platform so, for a couple or a family, it might be necessary to be able to select one or more subjects of care or wellbeing. For this app, there is likely to be a hazard associated with confusion between one subject of care or wellbeing and another when displaying medication data.

Whilst in this example it might be clear that this situation would be unacceptable, a more formal risk assessment might proceed as follows, using a qualitative scale of severities, and taking account of the context of medications and multiple users in a household, the likely severity might be assessed as "moderate".

Then, using a qualitative scale of likelihoods, the likelihood of an occurrence of a "moderate" event might be assessed as "frequent". Since risk is defined as being a combination of severity and likelihood, these two values can be combined using a risk matrix. This might lead the developer to conclude that the scenario they have just assessed be rated as "high". This is a clear indication that unless controls already exist to prevent this hazard, the app might need to be re-designed.

In this case the app developer might decide to control this hazard by adding a requirement to ensure that the app clearly displays the relevant subject of care on each page in their app. They would then be able to reference this design feature as evidence of risk reduction in their risk register. A reassessment of the scenario with the controls in place could be expected to conclude that in this case the severity of the scenario remains the same at "moderate" but that the likelihood of an occurrence may be reduced from "frequent" to "probable". Re-applying the risk matrix may show that the level of risk had been reduced from "high" to "medium" which is now a level that is justified.

F.4 Example risks

NOTE The below table is not intended to be a complete set of risks to be considered, but provide some examples of the risk types defined in Clause 7.

Table F.1 sets out example risks that may be relevant for the medication reminder app (see F.2).

Table F.1 – Example risks

Type of risk (see 7.2)	Risk	Consequence
Safety	App no longer supported	User without medication reminders from the app
	Flat battery	User without medication reminders from the app
	Device left at home	User without medication reminders from the app
	Device lost/stolen	User without medication reminders from the app
Security and Privacy	Data shared with other apps without the user realizing, or in error	Legal liabilities for app publisher, and loss of privacy for app user
	Data posted to social media without the user realizing, or in error	
	User pulls more information than expected from a clinical system (e.g. downloading a full clinical summary rather than just a medication list that becomes available to other users of the device)	
	Device is lost/stolen	A combination of these hazards might result in the inappropriate release of personal information about medications being taken
	Friend finds unlocked phone	
	Friend given phone to look at photos and opens app	
	File system access to the device provides access to clinical information Backups of the app data to the cloud or local media gives inappropriate access	
Project risks	Sickness; or recruitment issues	Insufficient resource to deliver on time might delay release of the app
	Insufficient experience within the development team	Lack of domain knowledge to identify gaps or errors in requirements; or Team might not have experience of compliance with regulatory requirements

Bibliography

Standards publications

For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

BS EN 62304:2006, *Medical device software – Software life-cycle processes*

BS EN 62366:2008, *Medical devices – Application of usability engineering to medical devices*

BS EN ISO 13485, *Medical devices – Quality management systems – Requirements for regulatory purposes*

BS EN ISO 14971, *Medical devices – Application of risk management to medical devices*

BS ISO/IEC 15414:2006, *Information technology – Open distributed processing – Reference model – Enterprise language*

BS ISO/IEC 25010, *Systems and software engineering – Systems and software quality requirements and evaluation (SQuaRE) – Systems and software quality models*

BS ISO/IEC 25012, *Software engineering – Software product quality requirements and evaluation (SQuaRE) – Data quality model*

DD ISO TS 25237, *Health informatics – Pseudonymization*

Other publications and websites

[1] EUROPEAN COMMISSION. Directive 93/42/EEC. European Parliament and Council Directive 93/42/EEC of 14 June 1993 concerning medical devices OJ L 169 of 12 July 1993. Luxembourg: The Publications Office of the European Union, 1993.

[2] GREAT BRITAIN. The Data Protection Act 1998. London: The Stationery Office.

[3] GREAT BRITAIN. The Consumer Protection Act 1987. London: The Stationery Office.

[4] MEDICINES AND HEALTHCARE PRODUCTS REGULATORY AGENCY. *How we regulate devices*. Open Government Licence. Available from: <http://www.mhra.gov.uk/Howweregulate/Devices/index.htm> [viewed April 2015].

[5] THE INFORMATION STANDARDS BOARD FOR HEALTH AND SOCIAL CARE. *ISB 0129 Clinical risk management: Its application in the manufacture of health IT systems v2 – Specification*. Open Government Licence, 2013. Available from: <http://systems.hscic.gov.uk/clinsafety/dscn> [viewed April 2015].

[6] WORLD HEALTH ORGANIZATION. *Constitution of the World Health Organization*. International Health Conference, 1948. Available from: <http://www.who.int/about/definition/en/print.html> [viewed April 2015].

[7] EUROPEAN COMMISSION. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Publications Office of the European Union, 1995.

[8] NHS England. *Patient Safety*. Available from: <http://www.england.nhs.uk/ourwork/patientsafety/> [viewed April 2015].

[9] HEALTH ON THE NET FOUNDATION. Available from: <http://www.hon.ch> [viewed April 2015].

[10] U.S. Food and Drug Administration. *Draft guidance for industry and food and drug administration staff – Applying human factor and usability engineering to optimize medical device design*. FDA, June 2011.

[11] SNOMED *Clinical terms*. Available from: <http://ihtsdo.org/snomed-ct/> [viewed April 2015].

[12] HEALTH & SOCIAL CARE INFORMATION CENTRE. UK Terminology Centre (UKTC). Available from: <http://systems.hscic.gov.uk/data/uktc> [viewed April 2015].

[13] HEALTH & SOCIAL CARE INFORMATION CENTRE. *HSCIC interoperability toolkit (ITK)*. Available from: <http://systems.hscic.gov.uk/interop/background/itk/faqs> [viewed April 2015].

[14] MINDTECH HEALTHCARE TECHNOLOGY CO-OPERATIVE. *Toolkit for appraising digital mental health products*. Available from: <http://mindtech.org.uk/projects/71-digital-mental-health-tools-evaluation-criteria-technology-theme.html> [viewed April 2015].

[15] EUROPEAN COMMISSION. Directive 90/385/EEC 20 June 1990 on the approximation of the laws of the Member States relating to active implantable medical devices. The Publications Office of the European Union, 1990.

[16] EUROPEAN COMMISSION. *Commission of the European Communities eEurope 2002: Quality criteria for health related websites*. Available from: http://www.hon.ch/HONcode/Webmasters/HON_CCE_en.htm [viewed April 2015].

NATIONAL INFORMATION BOARD and DEPARTMENT OF HEALTH. *Personalised Health and Care 2020: a framework for action*. Available from: <https://www.gov.uk/government/publications/personalised-health-and-care-2020> [viewed April 2015].

PATIENT VIEW. *My health apps*. Available from: www.myhealthapps.net [viewed April 2015].

SUBSTITUTABLE MEDICAL APPLICATIONS AND REUSABLE TECHNOLOGY (SMART). *Healthcare platforms for apps development*. Available from: <http://smartplatforms.org/smart-on-fhir/> [viewed April 2015].

Further reading

APPLE. *App review guidelines*. Available from: <https://developer.apple.com/app-store/review/> [viewed April 2015].

APPLE. *Designing for iOS*. Available from: <https://developer.apple.com/library/ios/documentation/UserExperience/Conceptual/MobileHIG/> [viewed April 2015].

GOOGLE. *Google fit*. Available from: <https://developers.google.com/fit/> [viewed April 2015].

HEALTHCARE SERVICES PLATFORM CONSORTIUM. *Intermountain healthcare led consortium*. 2013. Available from: http://healthcaresoa.org/uploads/Consortium_Discussion_06122013L_v7__3_.pdf [viewed April 2015].

HEALTH & SOCIAL CARE INFORMATION CENTRE. *Good practice guidelines*. Available from: http://systems.hscic.gov.uk/infogov/security/infrasec/gpg/index_html [viewed April 2015].

HEALTH & SOCIAL CARE INFORMATION CENTRE. *The information governance assurance programme*. Available from: <http://systems.hscic.gov.uk/infogov/igap> [viewed April 2015].

ISO/TC 210, *Quality management and corresponding general aspects for medical devices*

British Standards Institution (BSI)

BSI is the independent national body responsible for preparing British Standards and other standards-related publications, information and services. It presents the UK view on standards in Europe and at the international level.

BSI is incorporated by Royal Charter. British Standards and other standardization products are published by BSI Standards Limited.

Revisions

British Standards and PASs are periodically updated by amendment or revision. Users of British Standards and PASs should make sure that they possess the latest amendments or editions.

It is the constant aim of BSI to improve the quality of our products and services. We would be grateful if anyone finding an inaccuracy or ambiguity while using British Standards would inform the Secretary of the technical committee responsible, the identity of which can be found on the inside front cover. Similarly for PASs, please notify BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001

BSI offers BSI Subscribing Members an individual updating service called PLUS which ensures that subscribers automatically receive the latest editions of British Standards and PASs.

Tel: +44 (0)20 8996 7669 Fax: +44 (0)20 8996 7001
Email: plus@bsigroup.com

Buying standards

You may buy PDF and hard copy versions of standards directly using a credit card from the BSI Shop on the website www.bsigroup.com/shop. In addition all orders for BSI, international and foreign standards publications can be addressed to BSI Customer Services.

Tel: +44 (0)20 8996 9001 Fax: +44 (0)20 8996 7001
Email: orders@bsigroup.com

In response to orders for international standards, BSI will supply the British Standard implementation of the relevant international standard, unless otherwise requested.

Information on standards

BSI provides a wide range of information on national, European and international standards through its Knowledge Centre.

Tel: +44 (0)20 8996 7004 Fax: +44 (0)20 8996 7005
Email: knowledgecentre@bsigroup.com

BSI Subscribing Members are kept up to date with standards developments and receive substantial discounts on the purchase price of standards. For details of these and other benefits contact Membership Administration.

Tel: +44 (0)20 8996 7002 Fax: +44 (0)20 8996 7001
Email: membership@bsigroup.com

Information regarding online access to British Standards and PASs via British Standards Online can be found at <http://shop.bsigroup.com/bsol>

Further information about British Standards is available on the BSI website at www.bsigroup.com/standards

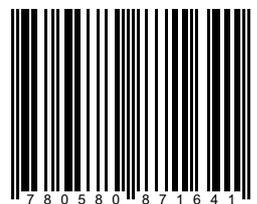
Copyright

All the data, software and documentation set out in all British Standards and other BSI publications are the property of and copyrighted by BSI, or some person or entity that owns copyright in the information used (such as the international standardization bodies) has formally licensed such information to BSI for commercial publication and use. Except as permitted under the Copyright, Designs and Patents Act 1988 no extract may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, photocopying, recording or otherwise – without prior written permission from BSI. This does not preclude the free use, in the course of implementing the standard, of necessary details such as symbols, and size, type or grade designations. If these details are to be used for any other purpose than implementation then the prior written permission of BSI must be obtained. Details and advice can be obtained from the Copyright & Licensing Department.

Tel: +44 (0)20 8996 7070
Email: copyright@bsigroup.com



BSI, 389 Chiswick High Road
London W4 4AL
United Kingdom
www.bsigroup.com



9 780580 871641