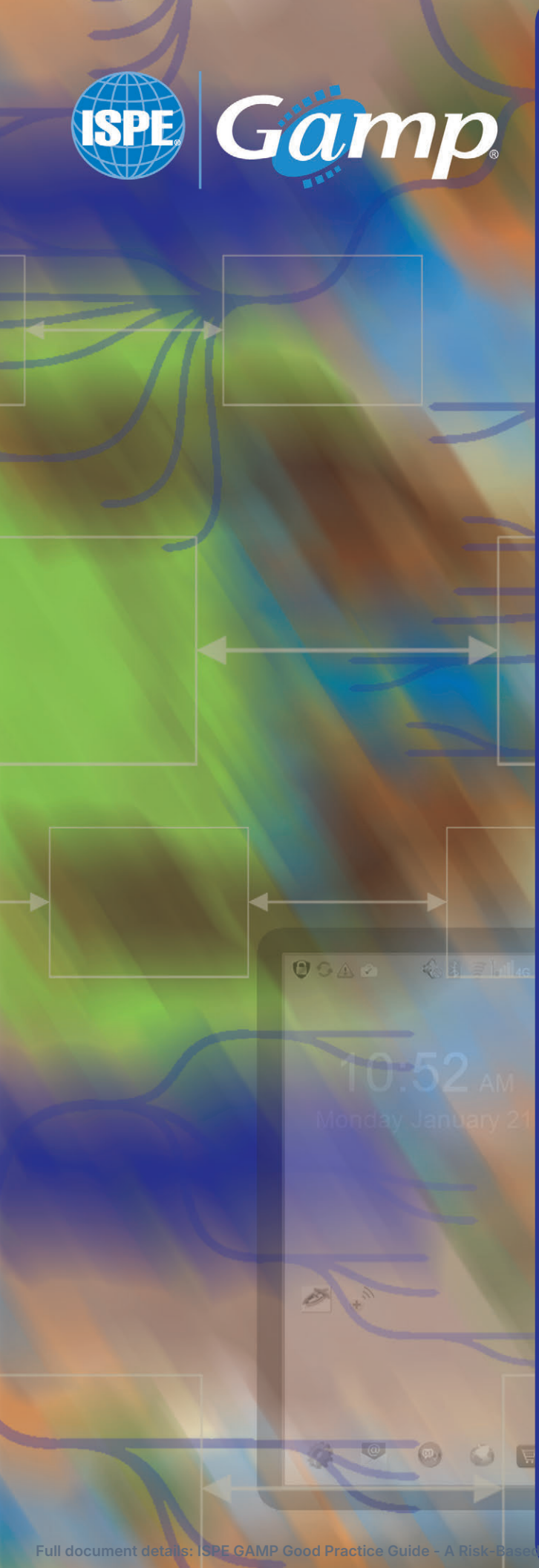
ISPE Gamp

GAMP Good Practice Guide

A Risk-Based Approach to Regulated Mobile Applications



AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

GAMP Good Practice Guide

A Risk-Based Approach to Regulated Mobile Applications

Disclaimer:
This Guide is intended to provide a risk-based approach to implementing and supporting regulated mobile apps. ISPE cannot ensure and does not warrant that a system managed in accordance with this Guide will be acceptable to regulatory authorities. Further, this Guide does not replace the need for hiring professional engineers or technicians.

Limitation of Liability
In no event shall ISPE or any of its affiliates, or the officers, directors, employees, members, or agents of each of them, or the authors, be liable for any damages of any kind, including without limitation any special, incidental, indirect, or consequential damages, whether or not advised of the possibility of such damages, and on any theory of liability whatsoever, arising out of or in connection with the use of this information.

© Copyright ISPE 2014. All rights reserved.

All rights reserved. No part of this document may be reproduced or copied in any form or by any means – graphic, electronic, or mechanical, including photocopying, taping, or information storage and retrieval systems – without written permission of ISPE.

All trademarks used are acknowledged.

ISBN 978-1-936379-75-0

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Preface

The use of mobile platforms – including smartphones, tablets, and wearable devices – by the general public has increased hugely. In 2013, sales of smartphones exceeded the sales of standard mobile phones, and this trend shows no sign of slowing. As reported on the FDA website, according to industry estimates, 500 million smartphone users worldwide will be using a health care application by 2015, and by 2018, 50 percent of the more than 3.4 billion smartphone and tablet users will have downloaded mobile health applications. These users include health care professionals, consumers, and patients. With this much computing power in everyone's pocket, it was inevitable that regulated companies would recognize an opportunity to use it for a variety of purposes. Some examples are:

- To improve patient compliance to a medical regimen
- As a marketing tool
- To make medical literature more available to physicians
- As a channel for patient reporting
- As an interface to a medical device
- To control a medical device

In addition to the above, mobile devices are an attractive option as interfaces to GxP systems in a manufacturing plant or laboratory, e.g.:

- Tool for warehouse management, including goods receipt or movement
- Dashboard interface to a large number of laboratory systems
- Interface to manufacturing equipment, possibly with the ability to adjust setpoints
- To access enterprise applications, such as Enterprise Resource Planning (ERP)

The universality of the mobile device market makes it increasingly attractive to develop mobile applications for varied uses. It may not be immediately obvious to all teams and departments that there are regulatory implications. Hence building awareness within all affected areas of regulated companies is critical.

By their very nature mobile devices present a significant challenge to control. The possibility of putting regulated applications, some of which may be classified as medical devices, into the pockets of the public is new ground for the industry. Never before has regulated software run on platforms where life science companies have little or no control over the platform.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Acknowledgements

The Guide was produced by a Task Team led by Arthur (Randy) Perez (Novartis Pharmaceuticals Corporation). The work was supported by the ISPE GAMP Community of Practice (COP).

Core Team / Chapter Leaders

The following individuals took lead roles in the preparation of this document and each managed one or more chapter teams made up of writers and contributors.

Erik Anderson	Johnson & Johnson Family of Companies	USA
Niklas Bergvall	Oxford Instruments	United Kingdom
Winnie Cappucci	Bayer AG (retired)	USA
Christophe DuPont	Baxter	Belgium
Arthur (Randy) Perez	Novartis Pharmaceuticals Corporation	USA
Sion Wyn	Conformity Limited	United Kingdom

GAMP Editorial Board

The Core Team wish to thank the following individuals for their valuable contribution during the preparation of this document.

Chris Clark	Bard Pharmaceuticals Limited	United Kingdom
Colin Jones	Conformity Limited	United Kingdom

Regulatory Input and Review

Krishna Ghosh	U.S. Food and Drug Administration	USA
Stephen Grayson	Medicines and Healthcare products Regulatory Agency (MHRA)	United Kingdom
John Murray	U.S. Food and Drug Administration	USA
Phillip Pontikos	U.S. Food and Drug Administration	USA
Robert Tollefsen	U.S. Food and Drug Administration	USA

Subject Matter Expert Input and Review

Particular thanks for substantial and valuable contributions to the review process go to:

Chris Price	Aberystwyth University	United Kingdom
David Stokes	Venostic Solutions Group Limited	United Kingdom

The Team Leads would like to express their grateful thanks to the many individuals and companies from around the world who reviewed and provided comments during the preparation of this Guide; although they are too numerous to list here, their input is greatly appreciated.

Company affiliations are as of the final draft of the Guide.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Connecting a World of
Pharmaceutical Knowledge

ISPE Headquarters
600 N. Westshore Blvd., Suite 900, Tampa, Florida 33609 USA
Tel: +1-813-960-2105, Fax: +1-813-264-2816

www.ISPE.org

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Table of Contents

1 Introduction 7
1.1 Background 7
1.2 Purpose 8
1.3 Scope 9
1.4 How to Use this Guide 10

2 Specific Aspects of Mobile Apps 11

3 Application of GAMP® 5 to Mobile Apps 17

4 Quality Risk Management for Mobile Apps 19

5 Mobile App Life Cycle 21
5.1 Overview 21
5.2 Mobile App Product Life Cycle 21
5.3 Mobile App Data Life Cycle 28

6 Appendix 1 – Mobile Apps Risk Landscape 31
6.1 Overview 31
6.2 Concept Phase Risks 32
6.3 Production Phase Risks 33
6.4 Operational Phase Risks 35
6.5 Retirement Phase Risks 42

7 Appendix 2 – Quality Risk Management Approach 45
7.1 Step 1 – Perform Initial Risk Assessment and Determine Impact 46
7.2 Step 2 – Identify Functions with Impact on Patient Safety, Product Quality, and Regulated Data Integrity 46
7.3 Step 3 – Perform Functional Risk Assessments and Identify Controls 46
7.4 Step 4 – Implement And Verify Appropriate Controls 48
7.5 Step 5 – Review Risks and Monitor Controls 48

8 Appendix 3 – Requirements Definition for Mobile Apps 49
8.1 Overview 49
8.2 Prototyping 50
8.3 User Interface Requirements 51
8.4 Connectivity Requirements 52
8.5 Data Management Requirements 52
8.6 Target Platform Requirements 52
8.7 Requirements for Application with Associated Device (Non Stand-Alone) 52
8.8 Mobile Apps Retirement and Withdrawal 53
8.9 Mobile Apps Corrective or Removal Actions 53
8.10 Labelling Requirements 53

9 Appendix 4 – Mobile App Architecture 55
9.1 Device Connectivity 55
9.2 Device Components 55
9.3 Client Approach 56

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

10 Appendix 5 – Production Phase for Mobile Apps 59
10.1 Overview 59
10.2 Specifications 60
10.3 Design Reviews 60
10.4 Traceability 61
10.5 Software Production 61
10.6 Testing 61
10.7 Commercial Release and Distribution 64

11 Appendix 6 – Supplier Management and Good Practice 67
11.1 Introduction 67
11.2 Overview 67
11.3 Supplier Good Practice 68

12 Appendix 7 – Sample Mobile App Case Studies 73

13 Appendix 8 – References 87

14 Appendix 9 – Glossary 89
14.1 Acronyms and Abbreviations 89
14.2 Definitions 90

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

1 Introduction

1.1 Background

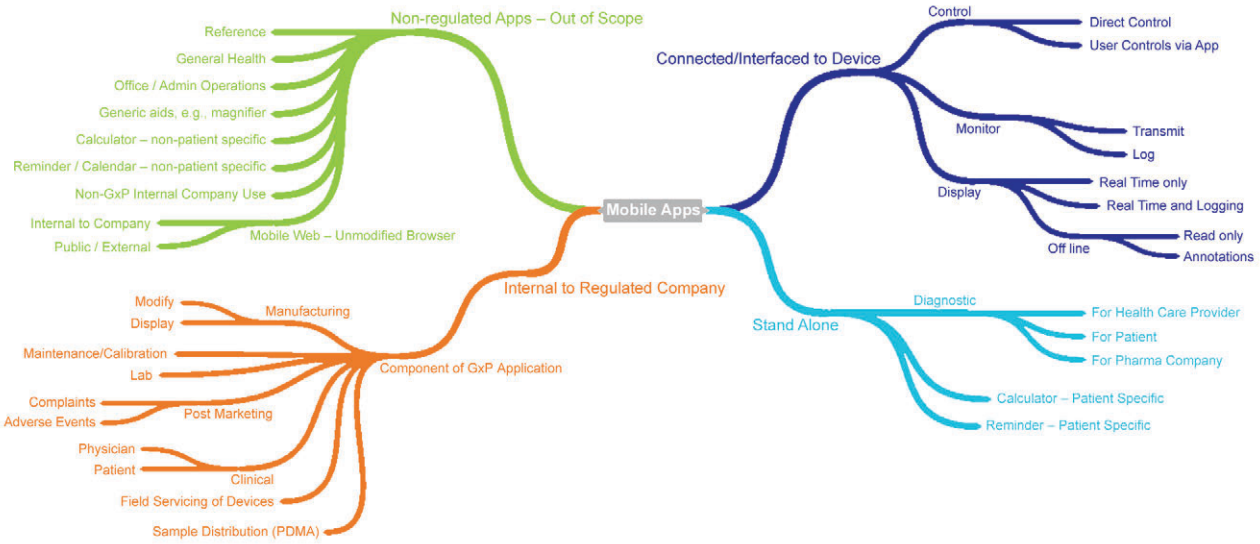
The development of mobile computing, particularly the increasing use of smartphones and tablets, has led to a significant change in how computers are used. A large proportion of the population can now carry considerable computing power in portable personal devices, and it was inevitable that these would be increasingly used within the life sciences industry.

In some cases, this will lead to regulatory implications as mobile applications may be subject to GxP regulations[1] (mobile apps).

For example, it is clear that the iPhone-based electrocardiograph approved by the U.S. Food and Drug Administration (FDA) in 2012 is a medical device, and that it requires a wide variety of controls just like other sophisticated electronic medical devices. However, many mobile applications are created for other purposes, such as support for marketing. Regulators have recognized an increased use of mobile medical apps, as illustrated by FDA's publication of guidance on the topic in 2013 [3]and the MHRA's guidance issued in 2014 [4].

Figure 1.1 provides an indication of the wide variety of different types of mobile apps that may be used within the life sciences industry.

Figure 1.1: Example Types of Mobile Apps



In general, unless a mobile app is used only for viewing static information, e.g., medical literature, it is likely that the mobile app would be regarded as regulated. Regulators have recognized this, and have begun inspecting and approving a variety of mobile apps as medical devices. Mobile apps also may be used as interfaces to GxP regulated instruments and equipment, and as components of GxP regulated computerized systems.

[1] GxP regulations are the underlying international pharmaceutical, medical device, or other life science requirements, such as those set forth in the US FD&C Act [1], US PHS Act [2], FDA regulations, EU Directives, Japanese regulations, or other applicable national legislation or regulations under which a regulated company operate. See Glossary for full definition.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

The largely uncontrolled nature of the mobile platforms, upon which such regulated mobile apps may run, present a challenge to companies wishing to use them. For traditional validated applications, one element of maintaining a state of control is controlling the platforms upon which they run (e.g., through formal qualification). When the platforms are mobile phones used informally by members of the public, the control of the platform becomes a significant challenge and qualification is not possible.

Regulatory input for this document was taken from five main sources:

1. Guidelines on the Qualification and Classification of Stand Alone Software Used in Healthcare within the Regulatory Framework of Medical Devices, European Commission DG Health and Consumer, January 2012 [5]

2. Regulation of Medical Software and Mobile Medical "Apps," Australian Therapeutic Goods Administration, 13 September 2013 [6]

3. Guidance on Medical Device Stand-Alone Software (including Apps), UK Medicines and Healthcare Products Regulatory Agency, 19 March 2014 [4]

4. Medical Information Systems – Guidance for Qualification and Classification of Standalone Software With a Medical Purpose; Swedish Medical Products Agency, 31 January 2013 [7]

5. Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff, US Food and Drug Administration, 25 September 2013 [3]

1.2 Purpose

This Guide is intended to provide a risk-based approach to implementing and supporting regulated mobile apps. It addresses the following issues:

1. Deciding whether or not the mobile app is regulated

2. Understanding when a regulated mobile app may be a medical device

3. The unique risks related to software that is partly managed by users

4. The implications of constant connectivity (or the loss thereof)

5. The complicated issues of managing software on a variety of operating systems at different version levels on many different devices

6. Ensuring compliance with applicable regulations, including implications for data integrity and data privacy/ protection

7. Recommendations for retiring mobile apps

This Guide applies the principles and practices described in GAMP® 5 [8] to the novel and unique challenges of the mobile environment, to provide the users with safe and effective solutions.

Note: for the purpose of this Guide, the term **users** include health care professionals, patients, and individual members of the public.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

1.3 Scope

This Guide covers two types of mobile apps:

1. Mobile medical apps, i.e., mobile apps that meet the definition of a medical device and are intended to be used in one of two ways:

    i. As an accessory to a regulated medical device (e.g., for remote display of data from bedside monitors)

    ii. To transform a mobile platform into a regulated medical device

(These correspond to mobile apps either connected or interfaced to a medical device, and stand-alone apps, as shown in Figure 1.1. These mobile apps require a complete life cycle approach as described in this guide).

2. Mobile apps that are used as part of GxP operations at a regulated company, as a component of a GxP regulated computerized system, such as an interface to an instrument or control system

(These mobile apps will typically be addressed as part of wider system validation or qualification activities as defined in the regulated company Quality Management System (QMS), taking into account the novel and particular aspects of mobile apps as described in this Guide).

This Guide covers a variety of application types that run on mobile platforms, including native apps and web apps for mobile devices.

The term *mobile platform* typically refers to smartphones and tablet computers. The majority of such systems will run on one of three operating systems:

1. Apple iOS®

2. Google Android®

3. Microsoft Windows®

Mobile platforms using other operating systems are also in scope. While all smartphones are capable of communication via cellular radio, tablet devices may or may not have that capability. However, most mobile devices do have Wi-Fi™ connectivity.

This Guide does not focus on the mobile platforms themselves although it does acknowledge and address their importance. Unlike traditional infrastructure, it may be difficult for a regulated company to exert control over the hardware or operating system. Mobile platforms are commodity items and are typically the property of individuals, rather than being corporate assets. This Guide focuses on the mobile app software development life cycle and software or procedural controls.

Some of the challenges presented by the inability to control the configuration of a user's mobile device need to be met with innovative controls, e.g., a "handshake" approach where specific software checks are executed prior to opening the mobile app. The need for such compensating controls should always be risk-based.

This Guide does not cover medical devices to which the mobile app may be interfaced, nor the software (e.g., firmware) included in such medical devices.

The Guide is intended to show how current industry good practice as described in GAMP® 5 [8] may be applied to mobile apps. The Guide is not intended to cover detailed requirements for medical device classification, registration, development, or support.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Detailed requirements for medical devices will vary from region to region, and it is the responsibility of organizations and individuals involved to identify, interpret, and apply such requirements as applicable. Companies should be familiar with local regulations in any region where they intend to deploy a regulated mobile app. Relevant international standards, such as ISO/IEC 62304 [9] and ISO 13485 [10], also should be consulted.

1.4 How to Use this Guide

This Guide contains this introduction, a main body, and a set of appendices. It has been structured to meet the needs of various readers, and contains, in increasing level of detail:

1. An overview of aspects and risks specific to mobile apps, along with a high level overview of how to address them

2. Further information on how to apply the GAMP® 5 [8] life cycle and Quality Risk Management (QRM) approach to mobile apps

3. More detailed “how to” guidance for specific topics

4. Example case studies

Readers requiring an overview of the topic should read this Introduction, plus Section 2, Specific Aspects of Mobile Apps, and Section 3, Application of GAMP® 5 [8] to Mobile Apps.

Readers seeking further information on the overall mobile apps life cycle, also should read the remaining sections of the main body.

Readers requiring detailed information on developing and supporting mobile apps also should consider the applicable appendices, based on their areas of interest and responsibility.

Suppliers of mobile apps should find Section 2 Specific Aspects of Mobile Apps, Section 3 Application of GAMP® 5 [8] to Mobile Apps, and Appendix 6 Supplier Management and Good Practice, particularly relevant.

All readers may find the example case studies in Appendix 7 useful when applying the guidance provided to specific situations. The case studies reflect a wide variety of types of mobile apps.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

2 Specific Aspects of Mobile Apps

Mobile platforms and mobile apps provide a rich and easily accessible toolset of functionality to users, which raise a number of questions in a regulated environment, such as those noted in Figure 2.1.

Figure 2.1: Example User Interface of a Mobile Device

This section addresses the novel and specific aspects of mobile apps that require specific consideration and action. This section also refers to other sections within the Guide that provide further guidance on these topics.

Tables 2.1 and 2.2 summarize those novel and particular aspects. Table 2.1 highlights topics related to management of mobile app development and operation, and Table 2.2 covers technical topics related to functionality and design.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Table 2.1: Topics Related to Management of Mobile App Development and Operation

Area	Aspect	Risk Factor	For More Information
Project Governance	Mobile App Classification	**The need to identify whether the proposed mobile app is regulated.** The project team may not have the knowledge, experience, or understanding of whether the mobile app is GxP regulated, and whether it is classified as a medical device.	Section 5.2
	Supplier Related	**Some mobile apps will be developed by very small development companies, e.g., "garage developers."** While this in itself is not a risk, the chance is greater that very small development companies will not understand the expectations of regulators and client companies.	Sections 6.2, 6.3 (Appendix 1) Appendix 6
	Supplier Related	**Software developers from small companies may be less financially stable.** If a mobile app is intended to be used for several years, special measures may be necessary to preserve software support services should the developer company fail.	Section 6.3 (Appendix 1) Appendix 6
	Project Goals	**Not all regulated mobile app projects start out with the intent or expectation of building a regulated app.** Mobile apps may be generated from a marketing idea for a patient or physician aid. During the project, it is recognized that the product will be a mobile medical app. If the initial phase of the project has been managed at a low level of formality, documentation that will meet medical device standards may be a particular challenge.	Section 5.2
	Project Team	**The mobile app project team may not have appropriate Subject Matter Experts (SMEs).** Where a mobile medical app was not the original intent, the project team may not have the appropriate expertise to produce a device that meets appropriate quality standards and regulatory requirements. In this case, SMEs should be added as soon as the regulatory relevance is recognized, and the team may have to remediate some of their initial output.	Section 5.2 Section 6.2 (Appendix 1)
	Project Size	**Mobile app projects may be very small.** Depending on the nature of the mobile app, development time may be as little as two to three weeks. As a result, mobile app project teams tend to be small, but with very aggressive timelines for completion. This can be a challenge for creating and approving documentation. Where the project is not recognized as GxP relevant from the point of conception, the short timeline can magnify the issue.	Section 6.3 (Appendix 1)
Operational Governance	Change Control	**In general, users have limited ability to address a problematic change.** If an upgrade fails, users may have no mechanism to back out a failed change.	Section 6.4 (Appendix 1)
	Calibration	**Some mobile apps may perform calculations based on data from attached input devices.** This functionality may require initial and periodic calibration to verify accuracy.	Section 5.2 Appendix 3
	Retirement	**It may be difficult to withdraw a mobile app from the market.** The mobile device may not belong to the mobile app provider. Users may continue to use retired versions of mobile apps until they replace their current device. In addition, there may be data residing on the device that should be retained, but does not result from user actions.	Section 5.2 Section 6.5 (Appendix 1)

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Table 2.2: Technical Topics Related to Functionality and Design

Area	Aspect	Risk Factor	For More Information
Design	Configuration	**Configuration requirements may vary between platforms.** For example, the ability to enable/disable audible alarms may be required, but may not be available on all platforms. In addition, the possibility of multiple configurations across platforms may introduce risk.	Appendix 3
	Browser	**There may be specific browser requirements to consider.** This could affect the use of the mobile app.	Appendix 3
	Messaging	**The mobile app may be required to send and receive e-mails and text messages.** This may impact the performance, security, and availability of the mobile app.	Appendix 3
	Clock / Calendar	**The mobile app may depend on accurate date and time functionality.** Critical records may need to be time and date stamped. Consideration should be given to the source and control of this functionality.	Appendix 3
Data	Data Management	**Data may reside on a device outside the regulated company's direct management.** Such devices probably will not be subject to the same level of control.	Section 5.3 Section 6.4 (Appendix 1)
	Data Storage	**Data on mobile devices is at risk.** Mobile apps may store records on the mobile device (long or short term). While on, the device records are more vulnerable to accidental or malicious loss or alteration. If timely transmission or synchronization of medical information is important and under control of a user, this also introduces risk.	Section 5.3 Section 6.4 (Appendix 1)
	Data Integrity	**Data integrity may be compromised by user action or inaction.** If a device is lost, damaged, or otherwise compromised, it is possible that important records residing on the device will be irretrievably lost. Access control may be problematic. For example, users trying to improve performance of their devices may destroy records by either deleting a mobile app or clearing memory. There are no restrictions on administrative rights.	Section 5.3 Section 6.4 (Appendix 1)
	Data Privacy	**The mobile app may originate, maintain, and/or process private data.** All applicable legislation may not have been considered in order to ensure the appropriate management of private and sensitive data.	Section 5.3 Section 6.4 (Appendix 1)
Usability	Human Interface Design	**The mobile app may be providing complex information to, and/or requesting data input from, the user.** Limited screen size and the wide variety of platforms available may lead to confusing or misleading information being displayed, or the incorrect information being collected.	Appendix 3
	User Sophistication	**Users will not have been formally trained.** Users may misunderstand the information being displayed or requested and take inappropriate action. Consideration also should be given to whether the mobile app is opened by the user or whether it is running in the background.	Section 4 Section 6.4 (Appendix 1) Section 10.7 (Appendix 5)

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Table 2.2: Technical Topics Related to Functionality and Design (continued)

Area	Aspect	Risk Factor	For More Information
Platforms	Platform Hardware	**Mobile app platforms are highly variable.** Many new mobile devices are introduced to the market annually. While there are some small differences in server or PC hardware, they are generally transparent to the operating system and applications. Mobile apps may run on several different hardware designs that can lead to problems with, e.g., operating system compatibility, screen image rendering, and limitations on communication protocols.	Appendix 1
	Platform Software	**A mobile app may have to run on a large number of software platforms.** While the number of operating system options available to mobile users is generally limited (three main options at time of publication), major operating system updates may occur more often than on PCs. Mobile apps are at risk of becoming non-functional as a result of an operating system upgrade. Conversely, some mobile device and/or service providers are reluctant to push operating system upgrades to mobile devices, so a user may be unable to obtain a critical update.	Appendix 1
	Platform Ownership	**Users select their own mobile devices and change them frequently.** Users may replace their mobile device about every two years. Mobile app suppliers have no way of ensuring that the hardware, operating system, and app version all meet expected standards. Users may jailbreak their devices, both increasing vulnerability to hacking and potentially voiding supplier support agreements.	Appendix 1
Platform Limitations	Inadequate Memory	**Mobile medical apps have to compete for devices resources.** Computing resources or storage space may run out because users employ their devices for several purposes, such as music or video.	Section 6.4 (Appendix 1)
	Battery Life	**Users can drain the batteries in their devices.** Where a mobile medical app needs to be running or needs to transmit data, this can present a risk.	Section 6.4 (Appendix 1)
	Emergency Conditions	**The ability of the mobile app provider to address an emergency could be highly dependent on user cooperation.** Where a mobile medical app becomes dangerous to the patient (e.g., due to communications issues, discovery of a software fault needing immediate remediation, the need for an important upgrade or patch), a mechanism (e.g., a notification) is needed to gain user attention and drive the user to accept the appropriate corrective action.	Appendix 1
	Malware Vulnerability	**Effective malware protection is at least partially at the discretion of users.** Mobile devices may not have the same level of protection against hacking or malicious code that is generally available to computers behind a firewall.	Appendix 1

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Table 2.2: Technical Topics Related to Functionality and Design (continued)

Area	Aspect	Risk Factor	For More Information
Communications	Interrupted Communications	**Incomplete communications are a much greater risk for mobile apps.** Communication between mobile apps and centralized data handling are at greater risk. This is due to the potential for events as varied as entering an area without a signal, turning off the device, exiting the mobile app, interference from another device, or accepting an incoming phone call.	Section 6.4 (Appendix 1) Appendix 4
	Prevented Communications	**Users can configure their own devices**. Mobile devices are not typically owned and managed by a healthcare provider who understands the risk related to a mobile app. Users can try to reduce cost or increase performance by turning off automatic updates. This could delay or prevent a critical software patch or upgrade, or compromise timely transmission of medical results.	Section 6.4 (Appendix 1)
	Communications Standards	**There are many communication protocols.** These may differ due to national standards, due to the quality of existing cellular infrastructure, or due to the nature of the device selected by the user. Protocols such as Bluetooth or Near Field Communications (NFCs) also need safeguards to reduce risk. The nature and speed of networks can introduce risk related to ensuring data transmissions are complete.	Appendix 4

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

3 Application of GAMP® 5 to Mobile Apps

The approach described in this Guide is based on the ISPE GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems [8], which covers compliance and validation of GxP regulated computerized systems. Key concepts which should be considered include:

Product and Process Understanding

A full understanding of the intended use and intended user-base is fundamental to accurately determining mobile app requirements. Such understanding is the basis for quality risk management. See Section 4.

Life Cycle Approach within a Quality Management System

The product life cycle should define the necessary activities to manage the development and support of mobile apps in a systematic way from conception to retirement. See Section 5.

Scalable Life Cycle Activities

Life cycle activities should be scaled according to:

- Impact on patient safety and data integrity
- Complexity and novelty of the app
- Assessment of any suppliers

Science Based Quality Risk Management (QRM)

QRM is a systematic process for the assessment, control, communication, and review of risks. Application of QRM enables effort to be focused on critical aspects of a mobile app. See Section 4.

Leveraging Supplier Involvement

Regulated companies should seek to leverage supplier knowledge, experience, and documentation throughout the life cycle. See Appendix 6.

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

4 Quality Risk Management for Mobile Apps

This section gives an overview of a suggested QRM approach, based on that described in GAMP® 5 [8] and aligned with the ISO 14971 Standard [11] for medical device risk management. A more detailed description of the approach is provided in Appendix 2.

While mobile applications share many of the same risks that are common to any software, there are many additional risks due to differences in intended use and the operating environment. These include:

- Mobile apps may be required to run on multiple operating systems and hardware platforms in order to reach the desired population. Mobile apps also may be required to run on different operating system version levels.
- The mobile platforms may not be under the control of an of a regulated company's Information Technology (IT) department.
- Connectivity with mobile platforms cannot be guaranteed.
- Users cannot be formally trained.
- User actions cannot be controlled – users can refuse updates, upgrade the operating system, or download other software without the controls normally applied though formal change management.
- Users could cause harm to themselves or others by misusing a mobile app.
- The risk of damage, loss, or misuse of hardware is much higher.
- Limited battery life may lead to data loss.

These and other risks specifically associated with mobile apps are discussed in detail in Appendix 1.

The approach is intended to be applicable to any mobile application with a potential impact on user safety, regardless of whether it is classified as a medical device.

A key aspect in the risk management framework is the intended use, which is defined as the use of a product, process, or service in accordance with the specifications, instructions, and information provided by the manufacturer. This should be considered when assessing mobile applications for public use.

The manufacturer should establish and maintain a process for:

- Identifying hazards associated with the use of a product
- Estimating and evaluating the associated risks
- Controlling these risks
- Monitoring the effectiveness of the control

AVA Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

This process should be documented in:

- Quality management system procedures
- Product design/development process document
- Appropriate plans, e.g., product quality plans, compliance plans

For medical devices, the process may be documented in separate formal risk management plans.

During analysis, the manufacturer should clearly define and describe the intended use, and any reasonably foreseeable misuse, as well as identifying the characteristics (such as functionality, accuracy, reliability, or other aspects) that could affect the safety of users.

Aspects of intended use that may be particularly relevant for mobile applications include:

- Medical/clinical purpose of the system
- User population (e.g., age, visual capability, or other health conditions)
- Platform characteristics
- Application: environment, frequency of use, location, connectivity requirements

The manufacturer should document known or foreseeable hazards associated with the use or misuse of the mobile application in both normal and fault conditions.

When risk analysis and evaluation indicates that risk reduction is required, the manufacturer should apply risk control measures, e.g.:

1. Inherent safety by design
2. Protective measures in the application itself or in the development process
3. Information for safety

These control measures are listed in order of priority and should be documented in specification and design information for the mobile app.

Note: for mobile apps, training and procedural adjustments are not usually an option, because of the limited level of influence over user actions.

The effectiveness of the risk control measures should be verified and the results of the verification should be documented. This can be achieved through development testing and product acceptance testing activities.

An appropriate report or other documented outcome should provide (or refer to) traceability for each hazard requiring control, through to verification of the risk control measures, and an assessment that the residual risk is acceptable.

Information about the performance, reliability, and effectiveness of the mobile app in the market should be gathered by the business process owner and evaluated for relevance to safety.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

5 Mobile App Life Cycle

5.1 Overview

Compliance with regulatory requirements and fitness for intended use may be supported by adopting a life cycle approach following good practice as defined in GAMP® 5 [8].

The product life cycle should define the activities necessary for the management of the development and support of mobile apps in a systematic way from conception to retirement. The life cycle of data captured or generated and maintained also should be considered.

The product life cycle described for a regulated company in this Guide should not be confused with the need for a defined approach or method for software development, which is typically the responsibility of the supplier. Appendix 6 describes good practices for suppliers, and these activities perform an important role in supporting regulated company activities.

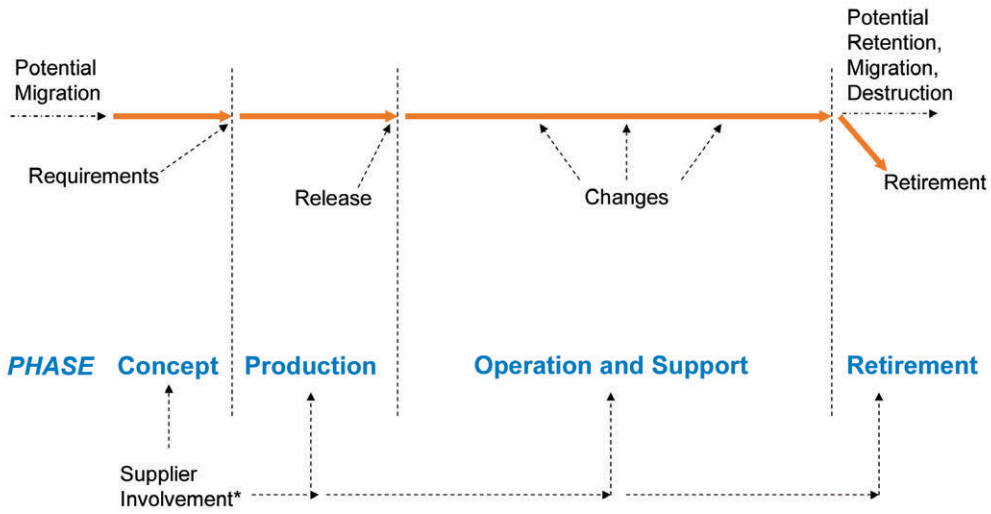
This Guide uses diagrams to represent the life cycle. These diagrams may present relationships in a linear representation. This is not intended to constrain the choice of development methods and models. Suppliers should use the most appropriate methods and models, which may include prototyping techniques.

5.2 Mobile App Product Life Cycle

The mobile app product life cycle is regarded as consisting of four main phases, consistent with those described in GAMP® 5 [8], but renamed to reflect the product life cycle, as shown in Figure 5.1.

- Concept
- Production
- Operation and support
- Retirement

Figure 5.1: Life Cycle Phases



*Supplier may provide knowledge, experience, documentation, and services throughout lifecycle.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

The approach described is intended to be aligned with ISO/IEC 62304 [9] and ISO 13485 [10].

During the **concept** phase, an initial risk assessment should be performed (including identifying whether the app is part of a GxP regulated system or a mobile medical app). Initial quality planning also should be performed and initial requirements should be defined.

The **production** phase involves further planning, supplier assessment and selection (where the product is not being developed internally by the regulated company), various levels of functional and design specification, coding, and verification leading to acceptance and release for operation.

Product operation and support is typically the longest phase and can present a significant risk. Data security and integrity, maintaining fitness for intended use and compliance of the mobile app are key aspects. Changes of different impact, scope, and complexity should be managed during this phase. Fault complaints and adverse events should be appropriately managed.

The final phase is **retirement**. This phase involves decisions about data retention, migration, or destruction, and the management and enforcement of these processes.

5.2.1 Concept

For each mobile app, a documented initial risk assessment should be performed. The initial risk assessment should be based on a defined main purpose, intended users, and intended features.

The risk assessment should be performed by appropriate Subject Matter Experts (SMEs), in conjunction with regulated company quality assurance and/or regulatory affairs representatives.

The risk assessment should determine and document whether the proposed mobile app is part of a GxP regulated system or is a mobile medical app. If it is a mobile medical app, the applicable medical device classification should be determined.

Applicable guidance and regulations should be consulted for all jurisdictions where the mobile app is to be deployed, e.g., FDA Mobile Medical Applications [3], and MHRA Guidance on Medical Device Stand-Alone Software [4].

Some applications may consist of both medical device and non-medical device modules or components. GxP regulated medical device modules must comply with the requirements of the applicable regulations. Additional requirements may apply, e.g., in the EU these GxP regulated medical device modules must carry the CE marking. Non-medical device modules are not subject to these requirements.

The manufacturer should clearly identify the boundaries and interfaces between the medical device and non-medical device components, based on their intended use. The manufacturer should ensure that the entire product, including the mobile device or other equipment, is safe and does not adversely affect the performance of the GxP regulated components.

The regulated company for whom a medical device (including a mobile medical app) is licensed bears responsibility for patient safety, but cannot assume liability on behalf of the manufacturer. For example, according to 21 CFR Part 807 [12], a software developer who produces a mobile medical app on behalf of a regulated company (i.e., *"makes a device for or on behalf of a specifications developer or any other person"*) is required to comply with the registration and listing requirements regardless of whether or not they also place the mobile medical app into commercial distribution.

However, a supplier for a regulated mobile app that is not a medical device may not be in a position to evaluate other types of regulatory risk, as this is heavily dependent on a number of factors that may be the responsibility of the regulated company buying the application or possibly a joint responsibility. The regulated company should clarify any supplier expectations, and these should be documented in a contract, a Service Level Agreement (SLA), or a plan.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

agreement. A product quality plan (or equivalent) should be produced for mobile medical apps and should document the product development process. Responsibilities of regulated companies and any suppliers should be clearly documented.

A product quality plan (or equivalent) can typically include:

- A brief description of the product, including a summary of goals and objectives
- An overview of planning activities, including selection of development method, identification of major tasks, activities, milestones, and related target timings or dependencies
- An outline of roles and responsibilities
- A description of interfaces between groups involved, including interfaces with third parties, e.g., mobile platform suppliers (hardware and software), customers, data providers, app stores
- The quality requirements to be met and procedures to be followed
- A listing of the deliverables associated with the product, e.g.:
    - Product requirements
    - Quality plan
    - Specification and design documentation
    - Traceability matrix
    - Design review documentation
    - Test documentation
    - Risk management documentation
    - User documentation

Note: much of the above will be considered part of the Design History File (DHF)[2] for mobile medical devices, and as such should be managed under formal change control.

The product quality plan should ensure that adequate resources, including appropriate SMEs, are allocated in order to achieve the desired level of documented quality and compliance.

Product requirements should be developed by gathering and defining user needs, intended use, and regulatory requirements including, where applicable, electronic record and signature requirements. Product requirement statements should be complete, consistent, unambiguous, and testable. See Appendix 3 for details of requirements definition for mobile apps.

High-level architecture factors which should be considered when planning for the different environments in which a mobile app may be used include:

- Device connectivity

[2] The DHF is a general regulatory requirement for medical devices. For example, from 21 CFR Part 820.3(e) [13] "Design History File (DHF) means a compilation of records which describes the design history of a finished device."

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

- Device components
- Mobile client approach

These architecture factors are described in Appendix 4.

Risks specific to mobile apps may be addressed effectively during planning and requirements definition. Examples of such risks are discussed in Appendix 1, Section 6.2.

Table 5.1 shows how medical device design control requirements, as defined 21 CFR Part 820 [13], may be met by the product life cycle activities described in this Guide. The approach described is also aligned with ISO/IEC 62304 [9] and ISO 13485[3] [10].

Table 5.1: Meeting Medical Device Requirements

Medical Device Requirement	How Met in this Guide
Design and Development Planning	Established product quality plans[4] should describe or reference the design and development activities and define responsibility for implementation.
Design Input	Established product requirements should define the intended use of the product including the needs of the user and patient.
Design Output	Product specifications and design documentation should define and document design output in terms that allow an adequate evaluation of conformance to design input requirements.
Design Review	Documented design reviews should be planned and conducted at appropriate stages of product development.
Design Verification	Product testing should confirm that the design output meets the design input requirements.
Design Validation	Product testing should ensure that products conform to defined user needs and intended uses
Design Transfer	Product testing should ensure that product design is correctly translated into production.
Design Changes	Product change management should ensure identification, documentation, review, approval, and testing of changes
Design History File	Product documentation should be adequate to demonstrate that the design was developed in accordance with the approved product quality plan, and under appropriate design control.

Regulated company Quality Assurance (QA) should perform an independent role in the approval or audit of specification and design activities that may impact public health, patient safety, or product quality.

5.2.2 Production

The development of mobile apps consists of the following activities:

- Finalizing and documenting product requirements, ensuring that they are clear, complete, testable, and unambiguous, including any prototyping and evaluation activities

[3] ISO 13485. This standard outlines QMS expectations that are compliant with EU regulations.
[4] A quality plan is a medical device requirement, e.g., as described in the US regulation 21 CFR Part 820.20(d) [13] or the Australian Therapeutic Goods (Medical Devices) Regulations 2002, section 4.4 [14]. Other regulators have similar requirements.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

- Assessment and management of suppliers
- Translating product requirements into:
  - Functional specifications
  - Design specifications
- QRM activities
- Performing design reviews
- Creating and maintaining traceability information
- For mobile medical apps, the creation and maintenance of a DHF
- Producing and managing the code for the mobile app
- Documented software testing – ensuring the developed mobile app is adequately verified
- Developing user documentation, instructions, and training
- Releasing the mobile app for use

These activities are described in further detail in Appendix 5 Production Phase for Mobile Apps and Appendix 6 Supplier Management.

These activities address the design input and design output elements of design control (required for mobile medical apps) by establishing requirements that define the intended use of the product, including the needs of the user, and establishing specification and design documentation that allows an adequate evaluation of conformance to requirements. Based on the medical device classification of a mobile medical app and the specific market regulations that could apply, obtaining premarket approval from one or more regulators may be required at the end of this phase.

Risk management techniques should be applied to identify quality risks and to remove or reduce them to an acceptable level. For mobile medical apps, risks to be evaluated should include potential patient risk, and regulated data integrity. For a mobile app that is classified as a mobile medical device, the supplier is a manufacturer as defined within applicable medical device regulations. This includes, but is not limited to, documentation standards relating to development and support of the mobile app.

Examples of risks associated with the production phase are discussed in Appendix 1, Section 6.3.

5.2.3 Operation and Support

Mobile apps should be supported and maintained in accordance with established procedures. These should cover:

- Change and configuration management
- Incident and problem management
- Product maintenance, updates, and release management
- Data integrity, security, and privacy
- Data backup and recovery

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

- Data retention, migration, or destruction
- Malware protection (if necessary based on risk)
- Management of distribution channels
- Planning for product retirement and withdrawal
- Medical device registration and listing (for mobile medical apps)
- Medical device post marketing surveillance and medical device reporting (for mobile medical apps)
- Medical device recall, field action and correction (for mobile medical apps)
- Periodic calibration, if required
- Periodic review

The infrastructure supporting mobile apps, such as associated websites and hardware, should be maintained in a state of control and compliance, following established procedures.

Mobile apps should be supported and maintained by appropriately trained, qualified, and experienced staff. For a mobile app, documented evidence of this will normally expected by regulators. Verification of successful installation of mobile medical apps may be required in some regions, e.g., *Medical Information Systems – Guidance for Qualification and Classification of Standalone Software With a Medical Purpose*, Swedish Medical Products Agency [7].

Patient and public data associated with mobile apps and subject to specific regulation should be identified, and should be protected by suitable controls to ensure their security, privacy, and compliance. This should include data managed or hosted by third parties on behalf of a regulated company.

A change and configuration management process should be established to ensure identification, documentation, review, approval, and testing of changes.

When changes are made to a mobile app, sufficient regression analysis and testing should be performed and documented to demonstrate that portions of the software not involved in the change were not adversely impacted. This is in addition to testing that evaluates the correctness of the implemented change(s).

Regression testing also should be performed for upgrades of the operating system of a mobile platform running a mobile app. The testing should verify that the app is compatible with the new operating systems (app stores may remove an app from the store if this is not verified), and that critical functionality is not adversely affected.

Note: the window for such regression testing may be very short for apps not on devices owned by the regulated company, as it is not possible to control when users install the operating system upgrade.

For mobile medical apps, new functions should be reviewed to identify any possible change in use that may lead to a change in device classification or in registration data, or may require re-registration with the health authority.

The range of hardware devices and operating systems upon which the mobile app will be available should be actively monitored and defined and documented during maintenance. Maintenance releases should be tested to ensure that the software continues to work correctly on the supported devices and allowed operating system versions.

An incident management process should be established to receive and address problems, incidents, comments, or complaints related to a mobile app, received either from users or other sources. This should coordinate with a problem identification and resolution process to ensure identification, documentation, and resolution of problems attributable to correctable faults with the mobile app or mobile service provider.

AVA Documents
Document Sharing Hub

Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014

User feedback mechanisms should be provided from within a mobile app, where possible. This may be via a form that is submitted to a web service, or mail-based feedback. Processes should be established to deal with feedback. Failure to provide an easy method of feedback or failure to respond to the feedback in a timely fashion may result in negative public evaluation of the mobile app (e.g., via social media). Users may resort to unintended channels, e.g., a regulated company's customer complaint line. This may introduce a high administrative burden that may be unhelpful or not cost effective.

Customer feedback may include a variety of topics including:

- Questions
- Compliments
- Incident reports
- Complaints
- Adverse events

Mechanisms should be established to deal appropriately with each. Local legal requirements may demand that feedback mechanisms are available in the local language.

Complaints regarding mobile medical apps should be managed according to established processes, which include medical device reporting requirements.

Provisions should be made to interface **any** customer feedback channels that allow free text with adverse event reporting systems; and ensure adequate review and analysis, e.g., part of the post-marketing surveillance and reporting process.

The content of a mobile app can become out-of-date. Planning for maintenance should include consideration of the need for regular assessments and possible updates of mobile app content to ensure that this content is still current and valid.

Prior to release of new product versions or upgrades containing new functionality, the initial risk assessment should be reviewed to ensure that the conclusions remain valid for the specific release in question. Software patches or updates should be evaluated to determine what should be pushed to user devices and what can wait for users to pull.

Examples of risks associated with the operation and support phase are discussed in Appendix 1.

For further information on operation and support of systems, see GAMP® 5 [8].

5.2.4 Retirement of Mobile Apps

The retirement, replacement, or withdrawal of mobile apps should be performed in accordance with an established process or plan. This plan should take into account potential risk to users should they lose access to the mobile app. Any technical measures required for retirement (e.g., disabling the app following a failed handshake protocol) should be addressed at the design state.

The retention, migration, or destruction of data associated with a mobile app product should be performed in accordance with an established process or plan, taking into account applicable regulatory and other legal record retention requirements.

Documents
Document Sharing Hub
Full document details: ISPE GAMP Good Practice Guide - A Risk-Based Approach to Regulated Mobile Applications 2014