Document filename:	**NPFIT-FNT-TO-TOCLNSA-1306.02 CRM Agile Development Implementation Guidance v1.0**		
Directorate / Programme	Solution Design Standards and Assurance	**Project**	Clinical Risk Management
Document Reference		**NPFIT-FNT-TO-TOCLNSA-1306.02**	
Project Manager	Rob Shaw	**Status**	Approved
Owner	Stuart Harrison	**Version**	1.0
Author	Ian Dugdale	**Version issue date**	16.04.2013

Clinical Risk Management: Agile Development Implementation Guidance

Document Management

Revision History

Version	Date	Summary of Changes
0.1	14.09.2012	First draft
0.2	08.10.2012	Revised following review by Safety engineers appraisal.
0.3	16.10.2013	Revised following review by Safety engineers appraisal.
0.4	18.10.2012	Revised following review by Safety engineers appraisal.
0.5	01.02.2013	Revised following review by Safety engineers appraisal.
0.6	01.03.2013	Revised following review by Clinical Safety Officers and external appraisal.
1.0	16.04.2013	First issue

Reviewers

This document must be reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
	HSCIC Safety Engineers	01.02.2013	0.6
	HSCIC Clinical Safety Officers	01.02.2013	0.6

Approved by

This document must be approved by the following people:

Name	Title	Date	Version
Stuart Harrison	Lead Safety Engineer	25.03.2013	0.6
Dr Maureen Baker	Clinical Director of Patient Safety	11.04.2013	1.0
Rob Shaw	National Integration Centre and Assurance Director	11.04.2013	1.0

Glossary of Terms

Term / Abbreviation	What it stands for
Backlog	A list of user stories, features or technical tasks which the team maintains and which, at a given moment, are known to be necessary and sufficient to complete a project or a release: http://guide.agilealliance.org/guide/backlog.html
Clinical Safety Officer (previously referred to as Responsible Person)	Person in a Health Organisation \ Manufacturer's organisation responsible for ensuring the safety of a Health IT System in target organisation through the application of risk management.

Term / Abbreviation	What it stands for
Clinical risk	Combination of the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk analysis	Systematic use of available information to identify and estimate a risk.
Clinical risk control	Process in which decisions are made and measures implemented by which clinical risks are reduced to, or maintained within, specified levels.
Clinical risk estimation	Process used to assign values to the severity of harm to a patient and the likelihood of occurrence of that harm.
Clinical risk evaluation	Process of comparing a clinical risk against given risk criteria to determine the acceptability of the clinical risk.
Clinical risk management	Systematic application of management policies, procedures and practices to the tasks of analysing, evaluating and controlling clinical risk.
Clinical Risk Management File	Repository of all records and other documents that are produced by the clinical risk management process.
Clinical Risk Management Plan	A plan which documents how the Health Organisation \ Manufacture's organisation will conduct clinical risk management of Health IT Systems.
Clinical safety	Freedom from unacceptable clinical risk to patients.
Clinical Safety Case	Accumulation and organisation of product and business process documentation and supporting evidence, through the life cycle of the Health IT System.
Clinical Safety Case Report	Report that presents the arguments and supporting evidence that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given environment at a defined point in a Health IT System's lifecycle.
Daily scrum	A meeting to bring all team members up to date on the information that is vital for coordination: each team members briefly describes any completed contributions and any obstacles that stand in their way http://guide.agilealliance.org/guide/daily.html
Harm	Death, physical injury, psychological trauma and/or damage to the health or well-being of a patient.
Hazard	Potential source of harm to a patient.
Hazard Log	Repository to record the results of the clinical risk analysis and clinical risk evaluation.
Health Organisation	Organisation within which health software is deployed or used for a health purpose.
Health IT System	Product used to provide electronic information for health or social care purposes. The product may be hardware, software or a combination.
Intended use	Use of a product, process or service in accordance with the specifications, instructions and information provided by the Manufacturer to customers.
Likelihood	Measure of the occurrence of harm.
Lifecycle	All phases in the life of a Health IT System, from the initial conception to final decommissioning and disposal.

Term / Abbreviation	What it stands for
Manufacturer	Person or organisation with responsibility for the design, manufacture, packaging or labelling of a Health IT System, assembling a system, or adapting a Health IT System before it is placed on the market and/or put into service, regardless of whether these operations are carried out by that person or on that person's behalf by a third party.
Patient	A person who is the recipient of healthcare.
Patient safety	Freedom from harm to the patient.
Post-deployment	That part of the life cycle of the Health IT System after it has been manufactured, released, deployed and is ready for use by the Health Organisation.
Procedure	Specified way to carry out an activity or a process.
Process	Set of interrelated or interacting activities which transform inputs into outputs.
Release	A specific configuration of a Health IT System delivered to a Health Organisation by the Manufacturer as a result of the introduction of new or modified functionality.
Residual clinical risk	Clinical risk remaining after the application of risk control measures.
Safety incident	Any unintended or unexpected incident which could have, or did, lead to harm for one or more patients receiving healthcare.
Safety Incident Management Log	Tool to record the reporting, management and resolution of safety related incidents associated with the Health IT System.
Severity	Measure of the possible consequences of a hazard.
Sprint or iteration	In the context of an Agile project, is a period of time during which development takes place, the duration of which may vary from project to project (usually between 1 and 4 weeks), is in most cases fixed for the duration of a given project. http://guide.agilealliance.org/guide/iteration.html
Top Management	Person or group of people who direct(s) and control(s) the Health Organisation and has overall accountability for a Health IT System.
Upgrade path matrix	Matrix which defines supported and unsupported upgrade paths. It provides useful information to Health Organisations when deciding to upgrade or perform a clean install/implementation.
User story	is one or more sentences in the everyday or business language of the end user or user of a system that captures, who the user is, what a user does or needs to function and why it is needed. http://guide.agilealliance.org/guide/stories.html

Related Documents

Ref	Doc. Reference No.	Title
1.	ISB 0129 Amd 39/2012	Clinical Risk Management: its Application in the Manufacture of Health Systems – Specification http://www.isb.nhs.uk/documents/isb-0129
2.	ISB 0160 Amd 38/2012	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems – Specification http://www.isb.nhs.uk/documents/isb-0160
3.	NPFIT-FNT-TO-TOCLNSA-1300.02	Clinical Risk Management: its Application in the Manufacture of Health Systems – Implementation Guidance
4.	NPFIT-FNT-TO-TOCLNSA-1293.03	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems - Implementation Guidance

Document Control

The controlled copy of this document is maintained in the HSCIC corporate network. Any copies of this document held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Contents

1 Introduction

1.1 Background

Development processes that align with the 'Agile Manifesto'[1] and 'Agile Principles'[2] are considered to be Agile development processes.

An Agile development continuously reviews the total functionality required (backlog), divides it and focuses on small prioritised, manageable pieces for development called iterations. It is not one long development cycle followed by a testing cycle found, for example, in the waterfall model. Instead, it is viewed as small sets of incremental deliverables that lead to complete delivery. An understanding of such processes is a prerequisite to this guidance. The guidance is not intended to be an 'all-inclusive' methodology to system development or software development lifecycle.

Agile is the current approach being taken within HSCIC however this guidance may also be applicable to other similar development processes and practices including Scrum, XP, Kanban and Lean.

A structured clinical risk management approach is essential to ensure that Health IT Systems deployed in Health Organisations are as safe as design and forethought will allow, and will support clinicians to practice safely.

1.2 Audience

The primary audience of this guidance are Manufacturers of Health IT Systems designing, developing, and maintaining Health IT systems and seeking to demonstrate compliance with ISB 0129 [Ref. 1] when following an 'Agile' or 'iterative' development approach.

It will also be of use to Health Organisations working in partnership with Manufacturers in following an 'Agile' or 'iterative' development approach.

1.3 Scope

This document is designed to provide an overview of the key clinical safety activities that are of particular importance when using an 'Agile' approach to developing Health IT Systems. It is intended as a supplement to the ISB 0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems – Implementation Guidance [Ref. 3]. The activities described will assist Manufacturers in managing, tracing and communicating safety related system requirements in compliance to ISB 0129 [Ref. 1].

[1] http://www.agilealliance.org/the-alliance/the-agile-manifesto/ (accessed January 2013)

[2] http://www.agilealliance.org/the-alliance/the-agile-manifesto/the-twelve-principles-of-agile-software/ (accessed January 2013)

1.4 Assumptions and Constraints

The following assumptions have been identified and apply to all projects using an 'Agile' approach to develop Health IT Systems. The absence of any of these assumptions should be subjected to a risk assessment and managed appropriately and will influence project feasibility:

- the high level concept or objective of the project will not change substantially to warrant a full reassessment during the project lifecycle
- sufficient resource from stakeholders involved in development activities, meetings, document reviews, demonstrations to users (often called 'Show and Tells') will be made available in agreed timeframes
- it is crucial that all stakeholders understand and accept their individual responsibilities to ensure the scrum or sprint planning and review meetings capture the clinical safety hazard assessments, goals are achieved and lesson learnt
- appropriate facilities and test environments will be available for development and any necessary 'Show and Tell' sessions. This may include access to external systems or virtual environments to simulate a live environment and remote access facilities.

2 Guidance

An increasing number of Manufacturers are opting for an ‘Agile’ approach to developing Health IT Systems. Figure 1 provides a pictorial representation of an Agile clinical risk management process.

The adaptability and early release of skeletal functionality that is offered by this approach may be beneficial but also raises challenges to clinical risk management that must be addressed. Early clinical safety hazard identification together with ongoing assessments enables the developing product design to avoid as many hazards as possible and build in mitigations rather than add on safety controls. Incorporating this guidance into Health IT system development lifecycles will help demonstration of good design.

The Clinical Safety Case Report is an iterative document that presents the arguments and supporting evidence that a system is safe for a given application in a given environment at a defined point in a Health IT System’s lifecycle.

During the Scoping phase, the first Clinical Safety Case Report should be produced when the user story(s) have been collated and prioritised and before the commencement of any development. It documents potential clinical risks, identified through an initial hazard assessment, which could arise from the system, its deployment and use. It is recommended that approval from the Manufacturer’s Clinical Safety Officer is granted before commencing to the Product elaboration and development phase. Where the development is being undertaken in consultation with a Health Organisation, then the Clinical Safety Officer from the Health Organisation should also accept the Clinical Safety Case Report.

During the Product elaboration and development phase the Clinical Safety Case Report is up-issued as part of each sprint or prior to release. It is recommended that approval from the Manufacturer Clinical Safety Officers is granted before commencing to delivery phase. Where the development is being undertaken in consultation with a Health Organisation, then the Clinical Safety Officer from the Health Organisation should also accept the Clinical Safety Case Report. The level of approval for deployment will be dependent upon the clinical risk, which is determined on a release by release basis.

Each new version of this document should include details of functional changes/related performance, a summary of all the clinical risks it contains, instructions to ensure safe operation post deployment, shortfalls/limitations and an overall statement of safety compliance for the Health IT System. This information is required to provide evidence that the overall Clinical Risk of the product is acceptable.

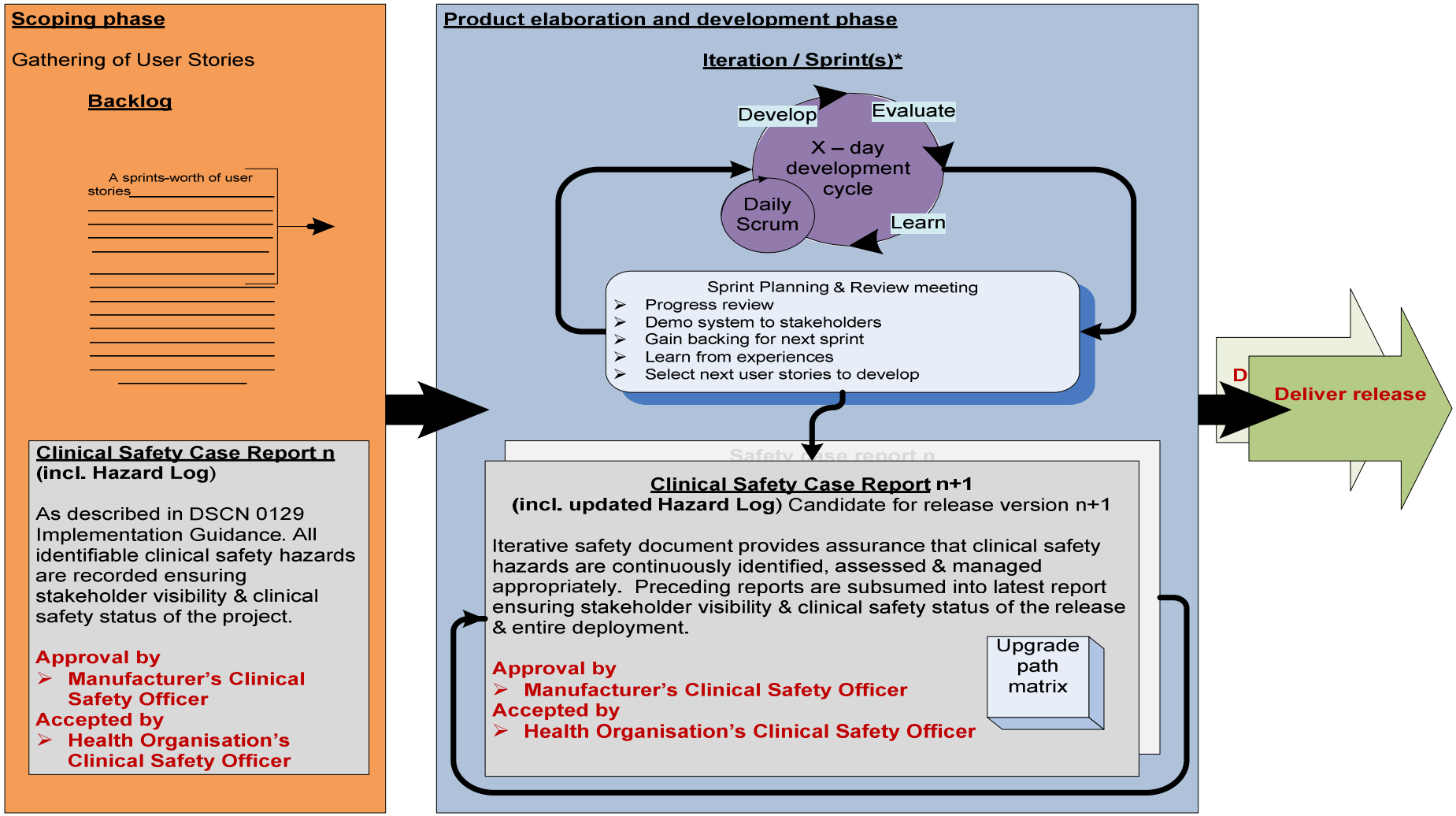

Figure 1. Pictorial overview of a typical Agile clinical risk management process

At and post the Deployment Phase the Clinical Safety Case Report should be up issued to support any modification to the Health IT System that changes its clinical risk. Further requirements and guidance for deployment and use of Health IT Systems is covered by ISB 0160 [Refs. 2 and 4].

Within the documentation, it is essential to differentiate between different versions of the same product, dependencies, and supported upgrade paths should also be recorded (See Figure 1 upgrade path matrix).

Each Iteration / Sprint must include all necessary test activities including Positive, Negative and Regression testing.

The key activities listed below need special consideration in 'Agile' approaches and will be explained in detail, in subsequent sections of this report:

- Clinical Risk Management Plan — ISB 0129 section 3
- Initial hazard identification and assessment — ISB 0129 section 4
- Prioritisation and selection of user stories — ISB 0129 sections 6.4 and 7
- Constraints and limitations of releases — ISB 0129 section 3
- Delivery, Monitoring and Modification — ISB 0129 section 7

2.1 Clinical Risk Management Plan

3.2.1	The Manufacturer MUST produce at the start of a project a Clinical Risk Management Plan, which will include risk acceptability criteria, for the new Health IT System.

For an 'Agile' development project it is recognised that the deployment plan may not provide fixed timescales or an absolute specification of features to be delivered in each release. However, the Clinical Risk Management Plan will provide the following important safety benefits to a project:

- an agreed version of the system
- estimates to the frequency and content of releases and Clinical Safety Case Reports. These estimates will also provide an indication of resource required from stakeholders.

2.2 Initial hazard identification and assessment

4.3.1	The Manufacturer MUST identify and document known and foreseeable hazards to patients with respect to the intended use of the Health IT System in both normal and fault conditions.
4.4.1	For each identified hazard the Manufacturer MUST estimate, using the criteria specified in the Clinical Risk Management Plan: • the severity of the hazard • the likelihood of the hazard • the resulting clinical risk.

The preferred approach to clinical hazard control is to reduce the exposure to hazards through the application of good design. Typically, the root causes of hazards that lead to risks to patient safety arise either as a result of the specified functionality itself giving rise to a hazardous condition or through a fault, defect or systematic design flaw in the manufactured software. It is also possible that elaboration of specified functionality by Manufacturers could generate outcomes with patient safety implications.

The Hazard log should record the identified hazards in both normal and fault conditions and document ways in which these hazards are to be reduced to acceptable levels of residual clinical risk. User stories should, where possible, be sufficiently detailed to allow an informed hazard identification and assessment to take place. However this may not always be possible given the high level nature of user stories, which may hinder hazards identification, therefore:

- initial hazard identification should be carried out in parallel with the original user story capture, elaboration and initial software scoping phase of the overall Health IT System development programme (see the Scoping phase of Figure 1). It is strongly recommended that a hazard workshop is run during the scoping phase to support complete hazard identification, as described in section 4.3 of Ref 3

- it is of primary importance that recognition is given to both the clinical and technical aspects of the Health IT System, Clinical Safety Officers and relevant subject matter experts with appropriate experience conduct the assessments

- on-going hazard assessment processes should be included in sprint activities throughout the development life cycle, and are essential in providing further means of hazard identification and risk reduction [Product elaboration and development phase of Figure 1].

- accurate cross referencing using unique identifier(s) should be used to maintain traceability between User Stories and related identified hazards. This will also ensure traceability throughout the systems life cycle.

Early clinical hazard identification enables the developing product design to avoid as many hazards as possible and build in mitigation. This is a clear demonstration of good design but in recognition of practicability and commercial constraints it is unlikely to be possible to eliminate all potential hazards.

2.3 Prioritisation and selection of user stories

6.4.1	The Manufacturer MUST ensure that the clinical risks from all identified hazards have been considered and accepted.
7.1.1	The Manufacturer MUST undertake a formal review of the Health IT System prior to its delivery to ensure that all of the requirements of this standard have been addressed.
7.1.2	The results of this review MUST be recorded in the Clinical Safety Case Report.
7.1.3	The Health IT System configuration for the release MUST be recorded in the Clinical Safety Case Report.

In Agile development the prioritisation and selection of user stories aims to identify the highest value or priority items going into each release (the lowest items may remain in a backlog). Prioritisation must be mindful of all identified clinical hazards associated to individual or groups of user stories and their dependencies to ensure completeness of clinical risk controls.

It is important to be able to confirm that all the identified hazards have been addressed. This can be achieved by ensuring that the overall hazard assessment and risk reduction process incorporates suitable means to be able to trace the history of each residual clinical risk or hazard, back to its initiating user story or root cause. The Clinical Safety Case Report should include details of all testing and other assurance activity (or references to the activity) that justifies how an acceptable level of residual clinical risk assurance has been achieved i.e. to provide evidence of the effectiveness of clinical risk control measures.

Selection of user stories for development of a particular release must consider related clinical safety concerns e.g. user stories with identified hazards must not be released without suitable clinical risk controls, as recorded in the Hazard Log. Furthermore, if during development one or more items cannot be fully developed with the sprint period , a suitable and sufficient clinical risk analysis, commensurate with the scale, complexity and extent of the release shall be undertaken to establish if omitting the item would compromise the clinical safety of the release.

2.4 Constraints and limitations of releases

3.5.1	The Manufacturer MUST produce a Clinical Safety Case Report at each lifecycle phase defined in the Clinical Risk Management Plan.

A Clinical Safety Case Report supporting a Health IT System release should contain information relating to its intended use in the defined clinical application and health IT environment. In particular it should contain details of any constraints or limitations in operation which, if exceeded, could lead to an increase in defined clinical risk.

2.5 Delivery, Monitoring and Modification

7.3.1	The Manufacturer MUST apply their clinical risk management process to any modifications or updates of the deployed Health IT System.
7.3.2	The application of this process MUST be commensurate with the scale and extent of the change and the introduction of any new clinical risks.
7.3.3	The Manufacturer MUST issue a Clinical Safety Case Report to support any modification to the Health IT System that changes its clinical risk.
7.3.4	The Manufacturer MUST maintain an audit trail of all versions and patches released for deployment.

If user stories are modified, deleted or new user stories are introduced adherence to change management processes are essential to accurately define the scope, limitations or mitigations that support the clinical safety of each release.

Whenever a Health IT System is modified, a suitable and sufficient clinical risk analysis, commensurate with the scale, complexity and extent of the modification (itself established by risk analysis), should be undertaken. This will establish what, if any, new clinical risks have been introduced. Where it is not possible to gather all stakeholders to attend a formal hazard workshop they must be fully consulted. This will ensure that no unacceptable clinical hazards are introduced as a result of a modification or by altering the basis of assessment of other parts of the Health IT System.

NOTE: The extent of the repeated clinical risk analysis will depend on the extent and the nature of the product modification. However, even apparently minor modifications can result in substantial clinical risks and thus, whatever the extent of the clinical risk analysis undertaken, it will need to be executed formally, rigorously and with due process.

An audit trail of all releases should be maintained as part of the Clinical Risk Management File and the Safety Case Report amended as appropriate to provide traceability in the event of a hazard alert.