
Document filename: ITK 2 0 Trust Operating Model Clinical Safety Guidance v1.0.docx			
Directorate / Programme :	HSCIC - Architecture	Project	Interoperability
Document Reference :		HSCIC-ITK-ARCH-203	
Project Manager :	Rob Shaw	Status :	Final
Owner :	George Hope	Document Version :	1.0
Author :	George Hope	Version issue date :	23/06/2014

ITK Trust Operating Model Clinical Safety Guidance

Document Management

Revision History

Version	Date	Summary of Changes
1.0	31/05/2014	First version issued by HSCIC

Reviewers

This document was reviewed by the following people:

Reviewer name	Title / Responsibility	Date	Version
George Hope	ITK Architecture Lead	30/04/2014	1.0
Sanjay Paul	ITK Architect	30/04/2014	1.0
Richard Dobson	ITK Accreditation Manager	30/04/2014	1.0
David Barnet	ITK Communication and Messaging	30/04/2014	1.0
Nigel Saville	ITK Accreditation	30/04/2014	1.0

Approved by

This document was approved by the following people:

Name	Signature	Title	Date	Version
Shaun Fletcher		Head of Architecture	31/05/2014	1.0
Rob Shaw		Director Operational Services	31/05/2014	1.0

Reference Documents

Ref no	Doc Reference Number	Title	Version
1.			
2.			
3.			
4.			

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	4
1.1	Purpose of Document	4
1.2	TOM Documentation Set	5
1.3	Audience	5
1.4	Document Scope	5
1.5	Document Overview	6
2	Clinical Safety Best Practices	7
3	Signoff Levels and Criteria	8
4	Architectural and Other Safety Considerations	10
4.1	Patient Identification	10
4.2	Access Control	10
4.3	Architecture	11

1 Introduction

This document forms part of the overall document set for the Interoperability Toolkit (ITK).

1.1 Purpose of Document

This document is part of the Trust Operating Model component of the Interoperability Toolkit. See the document “Trust Operating Model – Overview” for a more complete description of the document set.

This specific document covers the clinical safety aspects relating to Local Application Integration. It outlines a recommended approach to clinical safety for local developments, with reference to existing documentation. It suggests “escalation points” at which local clinical authorities (e.g. Clinical Safety Officer) should consider or may at some point be required, to consult with the HSCIC safety team.

Specifically, this document introduces a Framework for self-evaluation¹ of Locally Assured Systems against a set of Clinical Safety criteria.



This document is intended to provide information to support the “Clinical Safety” tab of the Self-Evaluation Checklist. Having read this document, the Clinical Safety tab should be completed.

¹ The approach is primarily based on self-evaluation, although the process identifies specifically where HSCIC may also need to be involved.

1.2 TOM Documentation Set

The position of this document in relation to the document set is shown below.

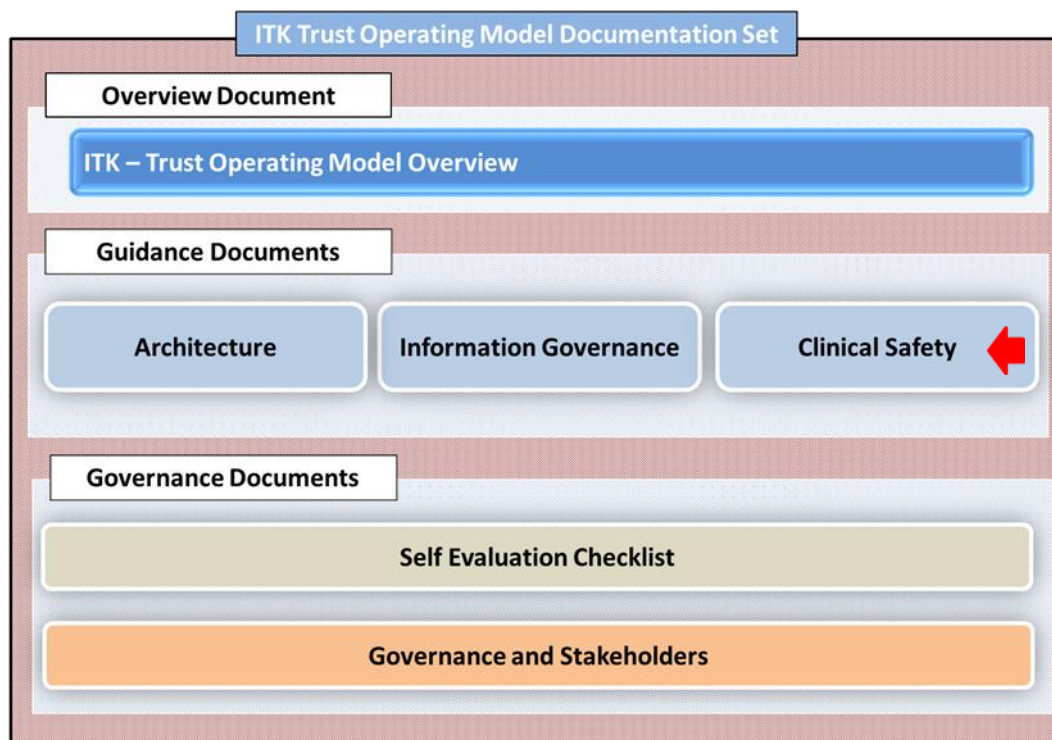


Figure 1 - The ITK Trust Operating Model Document Set

1.3 Audience

The primary audience for the Trust Operating Model is project teams within a Trust who are responsible for implementing a local integration project.

This document will be of particular relevance to those within a Trust with responsibility for Clinical Safety.

Secondary audiences may include 3rd parties such as suppliers and HSCIC architects

1.4 Document Scope

The Trust Operating Model focuses on integration between Local Trust Systems and Spine Compliant systems, and also on integration between Local Trust Systems and / or Non-NHS Systems within a Local Health Community environment. Please see the Overview document for further explanation of these concepts.

It does not cover integration at a National level through the Spine – existing Compliance documentation is already available on this topic.

Also note that the focus is on the integration-specific aspects of a project. General topics necessary for any successful project (e.g. training, communications, service management etc) are not covered.

1.5 Document Overview

The rest of this document covers the following topics:

- **Clinical Safety Best Practices**
A brief introduction to the topic of Clinical Safety and established best practices
- **Signoff Levels and Criteria**
A framework of signoff levels, based on a self-assessment of clinical risk

2 Clinical Safety Best Practices

NCRS Spine Compliant systems must meet a documented set of criteria including infrastructure, user identity, information governance and clinical safety.

However in some cases organisations need to construct local systems for processes which are un-supported by LSP or National services. These local systems are not covered by the NHS HSCIC Spine Compliance assurance procedures.

Despite this, in general, best practice is to follow the guidelines in the NHS HSCIC Clinical Safety Management System² and the Health Informatics risk management documentation³ and guidance⁴. (These documents may be downloaded from

<http://www.connectingforhealth.nhs.uk/dscn/dscn2009/data-set-change/>)

In summary, the requirement is:

- That a hazard assessment be conducted, and that where patient safety risk is identified, a safety case be prepared
- That each organisation⁵ appoints a Clinical Safety Officer (CSO)

Trusts and other organisations should ensure that their implementation of the NHS HSCIC Clinical Safety Incident Management Process (CSIMP)⁶ covers their local systems, and any safety incidents arising from those systems are managed through the CSIMP.

² See NPFIT-SHR-QMS-PRP-0167.02

³ NPFIT-FNT-TO-TOCLNSA-0830.01 Health Informatics — Application of clinical risk management to the manufacture of health software (formerly ISO/TS 29321:2008(E) DSCN14/2009

⁴ NPFIT-FNT-TO-TOCLNSA-0831.01 Health informatics - Guidance on the management of clinical risk relating to the deployment and use of health software (formerly ISO/TR 29322:2008(E) DSCN18/2009

⁵ This “organisation” may be a Trust, a CCG, or other organisational grouping meaningful to the NHS. The aim of this document is to describe the generic process.

⁶ Currently under review – no FileCM document reference

3 Signoff Levels and Criteria

In addition to the above best practices, for Local Trust integration the following levels of signoff are proposed⁷ based on a self-assessment of risk:

1. **None required.** In this case, the hazard assessment would indicate that the integration has no clinical or patient “touch points” and performs no functions that can result in clinical risk. Examples here might be integration of financial systems or others that deal with no clinical or patient-related information.
2. **Local-only (non-clinical).** Here the local integration implementation will have contact with patient information and may perform functions that have a potential impact on care. These are not necessarily directly clinical functions – for example systems that interface with administrative features of a PAS may touch no clinical data but may risk interrupting care. These should be signed-off by the local CSO.
3. **Local-only (clinical).** In this case the local integration implementation does handle clinical information, but it does so through “known” interfaces (for example via use of CSA, or coordinating views of referral information via the Choose and Book portal with data retrieved from a PAS) and does not attempt to process clinical records in any way. Local-only (clinical) includes a basic level of safe behaviour in terms of reliable facilities and processes for correct patient identification, use of legitimate relationships and other access control. These projects should be signed-off by the local CSO.
4. **HSCIC Assistance Recommended.** In this case the local integration implementation has implications for some processing that displays or uses the clinical record in a way different from that originally envisaged in the design of the systems with which the local application is interfacing. An example here might be the extraction of some clinical information from a subset, where there is a risk that the extraction “leaves behind” information essential to the accurate use of the extract. Another is the display of a clinical record via some custom interface or other transform which modifies layout without affecting the semantics of the information. Clinical authority sign-off is still local, but the assistance of the CSG is recommended. It is always open to the local CSO to request such assistance at their own discretion, for lower levels of hazard on this list.
5. **HSCIC Clinical Authority to Release required.** This is the highest level and a HSCIC signoff is mandated as for a Spine Compliant system. An example of risk here might be where a local application fuses clinical data from two sources in a single display; or performs transformations on data that changes their semantics (e.g. reporting substance concentrations in ug/l rather than an underlying umol/l). In this case whilst the local CSO is required to sign off their acceptance, HSCIC must provide sign-off also.

⁷ Level 5 pending review by HSCIC Clinical Safety Group

NB: In the case of assessing the project at Level 4 or 5 then it is strongly recommended to contact the HSCIC Clinical Safety Group at the earliest opportunity via the team mailbox at clinical.safety@nhs.net. They will then be able to provide further case-by-case guidance and input to planning.

4 Architectural and Other Safety Considerations

The purpose of this chapter is to highlight a number of specific topics which are important to consider as part of assessing the Clinical Safety implications of any proposed new application or integration work.

4.1 Patient Identification

A major starting point for safety is the correct identification of the patient, and the retention of that identification throughout care processes. Once the identity of the patient has been initially established (e.g. based on a combination of facts), best practice for maintaining and propagating this identity is to follow Department of Health policy and use the NHS number. In some cases use of the NHS number is not possible and local systems should document their alternative solutions. It is expected that this documentation covers existing practice rather than it being a requirement to be written from scratch. Topics to be considered include:

- How patient identification is performed, and tracked through the various integrated systems. In the case where due to patient incapacity or potential confusion, positive patient identity cannot be established, how does the system (and its methods of use) support patient identification for safe care. Examples here might be requests to the PAS to perform PDS trace, or business processes to call PDS “Number Allocation” requests in the case where patient identity cannot be established and a new NHS number is the safest way to proceed.
- How patient identity is maintained throughout integrated systems. Where the various systems use different identifiers (e.g. PACS or lab identifiers, hospital admission identifiers and so on) how are these coordinated, and what mechanisms exist to ensure that they all refer to the same patient.
- In the case of mistaken identity, or where a new identity must be created, what processes are in place to resolve the identity and merge or otherwise handle the resultant data issues.

4.2 Access Control

Spine-connected systems implement a variety of access control features, governing access to patient records – legitimate relationships, patient consent and sealing, for example. Whilst Locally Assured systems’ consideration of these is more correctly covered under Information Governance, Locally Assured systems should consider the impact of these on clinical safety and any process required (e.g. Caldicott Guardian) for managing access control issues. For example that “sensitivity flags” on patient records are honoured, or that clinicians are alerted to the presence of sealed parts of a patient’s care record.

4.3 Architecture

Locally Assured systems should consider the dependencies the provision of care, and clinical information, have on their reliability. Specifically:

- What is the impact on care or provision of clinical of any integration layer becoming unavailable, between local systems and LSP?
- What is the impact of a transactional failure, or a failure of a single request in a sequence of interactions?
- Are there any implications for “chains of systems” – such that changes to one system have clinical safety implications for other systems with which it is integrated?
- How are users informed of a failure so that they can react accordingly?
- How are applications informed of a failure to that they can support their users, and leave their systems in a safe, stable state?
- How are failures logged so that operations staff can understand what went wrong, and react accordingly?

*** End of Document ***