

---

<b>Document filename:</b> ITK 2 0 Trust Operating Model Overview v1.0.docx			
<b>Directorate / Programme :</b>	HSCIC - Architecture	<b>Project</b>	Interoperability
<b>Document Reference :</b>		HSCIC-ITK-ARCH-200	
<b>Project Manager :</b>	Rob Shaw	<b>Status :</b>	Final
<b>Owner :</b>	George Hope	<b>Document Version :</b>	1.0
<b>Author :</b>	George Hope	<b>Version issue date :</b>	23/06/2014

## ITK Trust Operating Model Overview

# 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

---

<b>1</b>	<b>Introduction</b>	<b>4</b>
1.1	Purpose of Document	4
1.2	TOM Documentation Set	4
1.3	Audience	5
1.4	Document Scope	5
1.5	Document Overview	5
<b>2</b>	<b>Overview of the Trust Operating Model</b>	<b>6</b>
2.1	Background	6
2.2	Principles	7
2.3	Trust Operating Model Components	9
<b>3</b>	<b>Overview of Guidance Documents</b>	<b>10</b>
3.1	Architecture	10
3.2	Information Governance	10
3.3	Clinical Safety	12
<b>4</b>	<b>Overview of Governance Documents</b>	<b>13</b>
4.1	Self-Evaluation Checklist	13
4.2	Governance and Stakeholders	13

---

# 1 Introduction

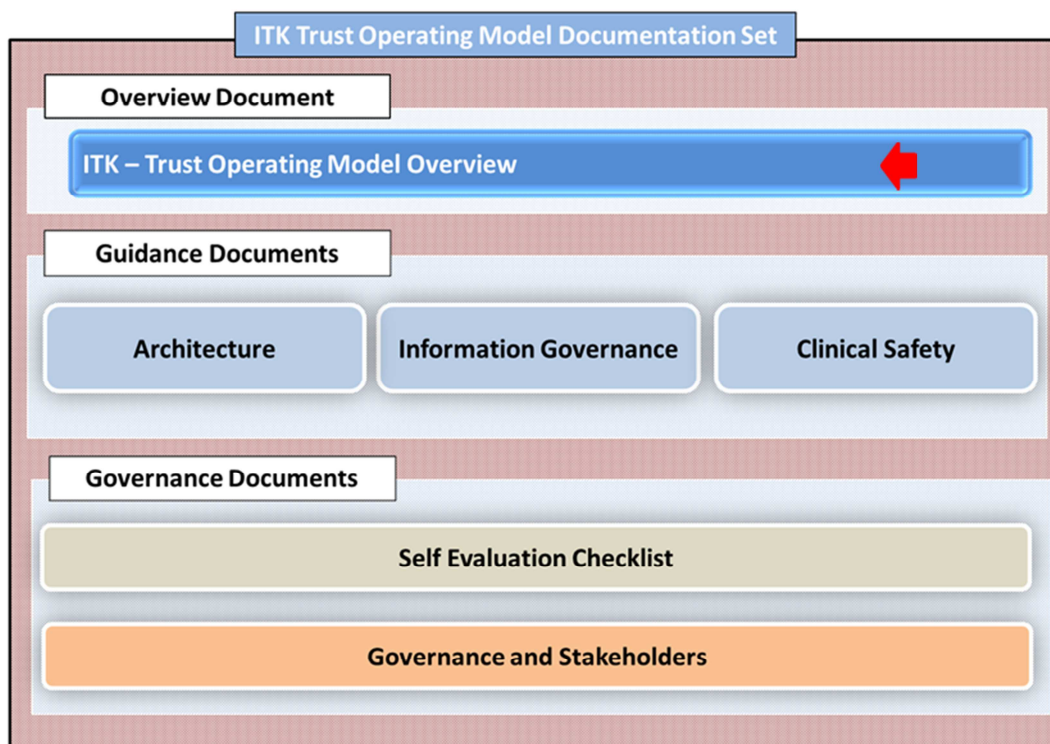
This document forms part of the overall document set for the ITK Trust Operating Model..

## 1.1 Purpose of Document

The purpose of this document is to provide a brief overview of the Trust Operating Model component of the Interoperability Toolkit. It explains the move that this Operating Model makes towards greater Trust responsibility for the decision to connect Locally Assured Systems to Spine Compliant Systems and / or each other. It outlines the principles underlying the Trust Operating Model, and summarises the purpose and key points of each of the more detailed Trust Operating Model documents.

## 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 Interoperability. Suppliers are envisaged as a secondary audience for the Trust Operating Model documentation.

Within a Trust, the Project Manager and technical team will find the entire document set relevant. Other experts may wish to consult specific topics based on their specialty (e.g. Architecture, Information Governance, and Clinical Safety).

Senior Management will find this overview document the most relevant, but may also wish to familiarise themselves with the additional information on Governance and Stakeholders.

## 1.4 Document Scope

The Trust Operating Model focuses on integration at 3 levels:

- **Local Intra Trust Context** - In this case the interoperability requirements may not require sophisticated levels of security, since the services are located, within a Trust's fire wall.
- **Local Health Community Context** - Here functionality and data are shared between local health economies for example, acute and primary care providers. This requires, among other things, greater levels of security and more sophisticated routing mechanisms.
- **National Context** - Finally, in cases requiring integration with national systems, or the establishment of national services, the requirements against the Toolkit are at their most comprehensive.

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:

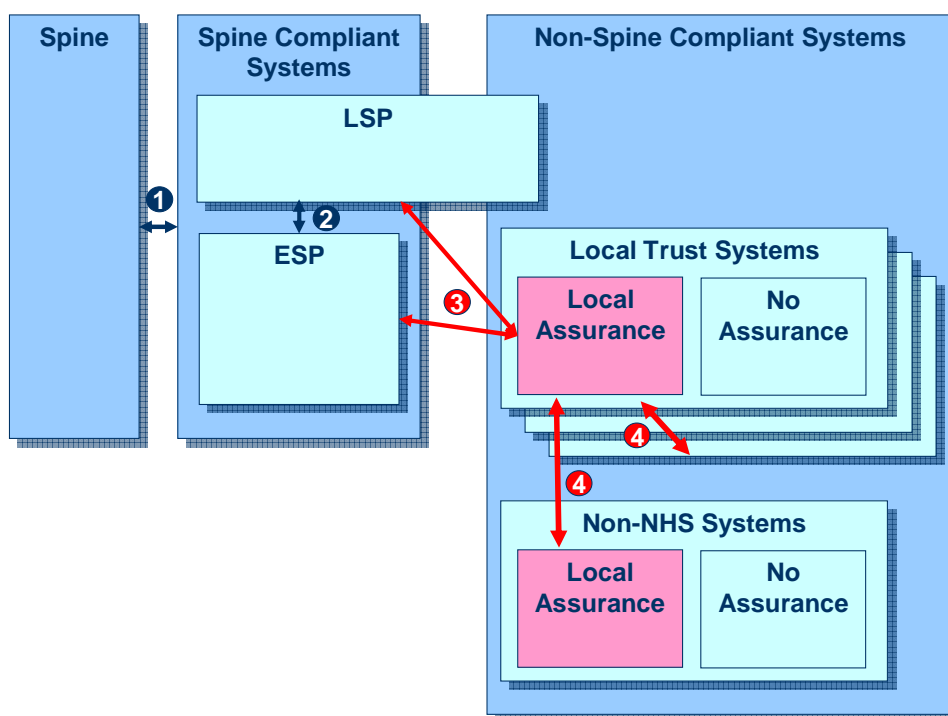
- **Overview of the Trust Operating Model**  
A brief overview of the background to the Trust Operating Model and its key principles.
- **Overview of Guidance Documents**  
An overview of the Guidance Documents contained in the Trust Operating Model. These include the Architecture, Information Governance, and Clinical Safety Guidance.
- **Overview of Governance Documents**  
An overview of the Governance Documents contained in the Trust Operating Model. These include a Self-Evaluation Checklist and a definition of the Governance structures appropriate for decision making and sign-off.

## 2 Overview of the Trust Operating Model

### 2.1 Background

The purpose of the Trust Operating Model is to assist Trusts with the implementation of integrated systems within their local environment. In particular, it provides guidance on their responsibilities in terms of ensuring that local systems do not compromise any core Spine Compliant systems to which they connect.

The diagram below shows an overview of the relevant systems landscape, with key points described in the text which follows.



**Figure 2 - Schematic diagram of Systems Landscape**

On the left of the diagram is the **Spine**, and connected to it are a range of **Spine Compliant Systems**. These systems may be provided either by the Local Service Providers (**LSP**) or under Existing System Provider (**ESP**) arrangements. Typical examples would include the core Patient Administration Systems (PAS) and Electronic Patient Record systems (EPR) used by a Trust. Certain Departmental Systems may also be Spine Compliant.

In the case of these Spine Compliant Systems, the pre-requisites for connection to the Spine **(1)** are governed by existing CFH Compliance documentation and processes. It is not the purpose of this document set to propose any changes in this area.

Within a local environment there may also be connectivity between Spine Compliant LSP and ESP provided systems which are covered under the terms of existing contracts or

migration activities **(2)**. Again, it is not the purpose of this document set to propose any changes in this area.

The focus of this document set is rather on the **Non-Spine Compliant Systems** shown on the right of the diagram.

These are generally **Local Trust Systems** - for example Departmental Systems deployed to meet the needs of a particular department or clinic within a Trust.

They may also be **Non-NHS Systems** – for example systems belonging to private healthcare providers, or Social Care or Local Authority based applications.

These Non-Spine Compliant Systems can be further categorised based on the concept of “**Local Assurance**”. This describes Local Trust Systems or Non-NHS Systems which meet the criteria defined in this Operating Model – including having been through a local process of assurance to ensure this. They are thus suitable for connection to Spine Compliant systems **(3)** - although not for direct connection to the Spine itself.

The criteria for Local Assurance are also intended to cover suitability for connecting to similar systems in other organisations, for example as part of a Local Health Community **(4)**.

This is in contrast to Non-Spine Compliant Systems classified as “**No Assurance**”. While these systems may well have been through a form of assurance appropriate to their standalone role, the term is specifically intended to signify systems that have not been through any CFH recognised process to assure them as suitable for participating in integrated solutions which handle patient identifiable data.

## 2.2 Principles

A number of principles underlie the approach taken in the remainder of the Trust Operating Model. At this level the principles are broad, and intended to give an insight into the overall direction of and thinking behind the document set. More detailed implications are worked through in the relevant underlying documents.

### Trust Responsibility

An underlying theme of the Operating Model is “Trust Responsibility”. Trusts own and are responsible for both the systems and the data in their local environment. While controls and checkpoints are needed, Trusts must ultimately take responsibility for discharging these obligations. Any other approach stifles local innovation and is not scalable.

By defining a clear and documented set of guidelines and processes, the Operating Model places the responsibility firmly with Trusts in terms of the decision to connect new local systems.

### **Risk-Based Approach**

There is a balance to be struck between (i) the clinical benefit and (ii) the potential risks of any Trust integration activity.

For example, the Information Governance controls applied must be correct and appropriate. Insufficient control introduces unacceptable risks to patient confidentiality and breaks the Care Record Guarantee [1], while too much puts unnecessary limitations on data sharing to improve patient care. The implication is that IG controls must be tailored based on the data, systems, and activities involved.

In a similar way, any Clinical Safety implications of new integration activity need to be evaluated and a balanced judgement made.

In short, it is essential to always be aware of, and assess and manage the risks to, the entire local environment

### **Consideration of External Implications**

It is important to be aware of the possible wider implications of local decisions, and in all cases to avoid making risk-based judgements without fully involving other organisations who may be affected.

For example, it is necessary to give explicit consideration to the implications of shared systems - so that the activities of one Trust cannot affect other Trusts sharing a PAS / EPR

Implications for the Spine also need to be considered, as these might ultimately affect all other organisations nationally. To achieve Spine Compliance, directly Spine connected systems must go through a rigorous process. This ensures a high standard of operational and data integrity. It is essential that this cannot be compromised due to the "rogue" activities of any downstream Local Trust or Non-NHS systems.

The implications of this are in terms of clear Information Governance guidelines to define what Locally Assured systems may or may not do. In addition, the defined governance processes include mandatory escalation points for cases where the implications of a new Locally Assured systems stretch beyond Trust boundaries.



## 2.3 Trust Operating Model Components

The Trust Operating Model comprises a number of documents which may be categorised in terms of two major components:

Guidance
<p>These documents give clear guidance to Trusts on local application integration issues, including:</p> <ul style="list-style-type: none"> <li>○ <b>Architecture</b> – a set of Architecture Principles highlighting the correct approach to key design questions</li> <li>○ <b>Information Governance</b> – a framework for understanding the Information Governance Controls required and the technical implementation mechanisms available to achieve this</li> <li>○ <b>Clinical Safety</b> – a framework for assessing and managing clinical safety risks</li> </ul>

Governance
<p>These documents describe the recommended process for a Trust to follow in order to decide whether a new Locally Assured system is suitable to connect to the LSP / ESP / LHC environment<sup>1</sup>. They consist of</p> <ul style="list-style-type: none"> <li>○ <b>Self Evaluation Checklist</b> - highlights the points that need to be checked before connecting a Locally Assured system</li> <li>○ <b>Governance and Stakeholders</b> - defines the decision making process which, based on the preceding guidance and self-evaluation, must ultimately conclude as to whether or not a new Locally Assured interface can be connected. Also provides further examples of the process steps and stakeholders who may need to be involved.</li> </ul>



The rest of this document provides further summary-level information about each of these documents

<sup>1</sup> Note: This is as opposed to CFH processes (eg CAP) that govern connection to the Spine

## 3 Overview of Guidance Documents

### 3.1 Architecture

Local Application Integration is an area which raises distinct architectural challenges to be addressed. Therefore this aspect of the Operating Model provides a set of Architecture Principles to guide key design decisions. Topics covered by these Principles include:

- Security
- Integration Processing
- Configuration and Management
- Information Architecture

### 3.2 Information Governance

#### 3.2.1 Background

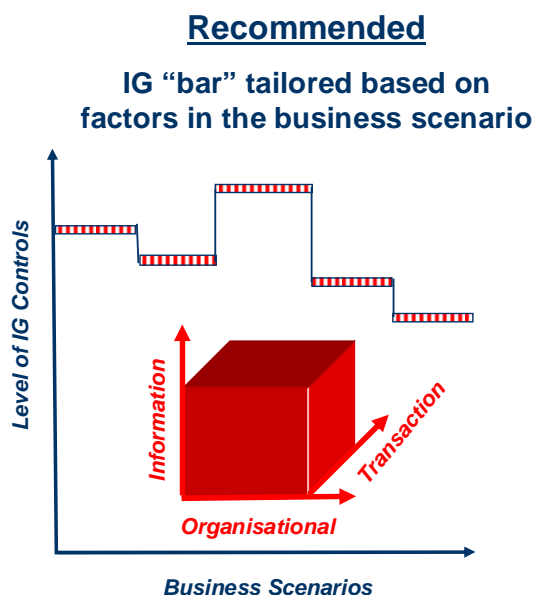
Appropriate Information Governance is an essential aspect of Trust Integration. Therefore this aspect of the Operating Model provides a framework for analysing the controls needed.

The local integration environment offers opportunities for applications to benefit from data sharing – both within and across organisational boundaries. However clearly patient confidentiality and the Care Record Guarantee must be respected and local applications must not be able to compromise this in any way. The situation is further complicated as Local Trust Systems and Non-NHS Systems may not always implement the same level of IG controls as those which are Spine Compliant. It is thus important to protect Spine Compliant systems from any less tightly controlled “downstream” systems.

In considering any integration solution therefore, a balance needs to be struck between the risks involved and the benefits available due to improvements in patient care. The IG Framework proposes an approach to achieving this balance by focusing on three key areas.

#### 3.2.2 Categorisation of Controls

The key point here is to avoid a “One-Size-FitS-All”, “worst case” approach to IG, and instead to take a more granular approach based on controls tailored to the specific Business Scenario. The diagram below illustrates the recommended approach:



**Figure 3 – Categorisation of Controls**

Specifically, the IG Framework applies the following three steps:

1. To list the relevant IG Controls and organise them into categories for easier reference
2. To define a set of Business Scenarios – based (as shown in the diagram) on the informational (demographic, clinical), transactional (read, update) and organisational (within Trust, Cross-Organisation) characteristics of the interface in question
3. To map the IG Controls to the Business Scenarios, indicating which ones are relevant and required in each case.

### 3.2.3 Control Implementation Approaches

Having identified the Controls required for each Business Scenario, the IG Framework next considers the implementation mechanisms available for each Control. The key point here is to focus on ensuring that the business requirement behind the control is met - whilst allowing some flexibility in the actual technical implementation mechanism used.

Therefore the IG Framework refers to a catalogue describing a number of potential implementation approaches for each control.

### 3.2.4 End-to-End Information Flows

Finally the IG Framework draws attention to the importance of considering end-to-end information flows. Interfaces rarely operate in isolation – more often they form part of a “chain” of interconnected systems.

Therefore this aspect of the IG Framework explains what needs to be considered when moving data between systems subject to different assurance regimes. It outlines the points to consider and what is acceptable from an end-to-end perspective.



Further information on each of these topics can be found in the supporting document “Trust Operating Model - IG Guidance”

## 3.3 Clinical Safety

### 3.3.1 Background

Consideration of Clinical Safety implications is another essential aspect of Local Application Integration. In many ways the topic is similar to IG, in that it relates to the management of risk. Thus once again a balance must be struck – ensuring the paramount importance of patient safety is considered at all times, while at the same time making sure that this does not become an unnecessary barrier to innovation.

### 3.3.2 Clinical Safety Signoff Levels

The Clinical Safety Framework addresses this by defining a simple graded model for risk assessment and engagement with appropriate clinical safety experts. It describes a five level model for signoff of local systems from a clinical safety perspective. The approach is based on an initial self-assessment of risk - with increasing levels of clinical safety involvement being recommended based on the outcome.



**Figure 4 – Clinical Safety Framework**



Further information can be found in the supporting document "Trust Operating Model – Clinical Safety Guidance"

## 4 Overview of Governance Documents

### 4.1 Self-Evaluation Checklist

It is important to ensure that any Locally Assured system meets the required level of assurance before connecting it to the wider environment of Spine Compliant or Local Health Community systems. A rigorous process in this area has many benefits including:

- Reassurance for the LSP - that their core application such as the PAS / EPR will not be compromised by “rogue” Local Trust Systems
- Reassurance for other Trusts sharing a PAS / EPR – that the shared systems will not be impacted by ill-considered activities of other Trusts
- Reassurance for CFH – that the integrity of National Spine systems will not be compromised by downstream connected applications
- Reassurance for patients – that their personal data is safe
- Clarity for Trusts – about the process to go through and the steps that are required.
- Confidence for application and integration vendors – that by following the process it is possible to connect to LSP solutions

Therefore this component of this Operating Model summarises all of the preceding guidance into a self-evaluation checklist for Trusts.

The checklist is the basis for a formal self-evaluation exercise by each Trust - with documented steps to follow and automated built-in logic to highlight potential risks and escalation points.

The Self-Evaluation Checklist therefore helps to drive a Trust's assurance process by providing specific details of the checks and tests recommended. The completed checklist becomes a formal artefact - to be retained as evidence of the activity.



Further information on the Self-Evaluation Checklist can be found in the supporting document “Trust Operating Model – Self Evaluation Checklist”

### 4.2 Governance and Stakeholders

The Guidance documents and the Self-Evaluation checklist will assist a Trust in understanding and applying best-practice, and thus in determining the suitability of their proposed integration for connection to the wider environment of Spine Compliant or Local Health Community systems. However ultimately this evidence will need to be used as the basis of a Go / No Go decision about deployment of the new solution. Therefore this component of the Operating Model defines the governance structure appropriate to these decisions.

An example stakeholder RACI is also provided - with the aim of further clarifying roles and responsibilities, and of providing a starting point for a Trust Project Manager in considering the project tasks and stakeholders who will need to be involved.



Further information on the Governance and Stakeholders can be found in the supporting document "Trust Operating Model – Governance and Stakeholders"

\*\*\* End of Document \*\*\*