

---

<b>Document filename:</b> ITK 2.0 Trust Operating Model IG Guidance v1.0.docx			
<b>Directorate / Programme :</b>	HSCIC - Architecture	<b>Project</b>	Interoperability
<b>Document Reference :</b>		HSCIC-ITK-ARCH-202	
<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 IG 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.	NPFIT-ELIBR-AREL-DST-0367.06	Interoperability Toolkit - Resources IG Control Implementation Patterns	2.0
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	5
1.3	Audience	5
1.4	Document Scope	5
1.5	Document Overview	6
<b>2</b>	<b>Principles</b>	<b>7</b>
<b>3</b>	<b>Security Domains and Risks</b>	<b>9</b>
3.1	Security Domains	9
3.2	Domain Boundary Risks	10
3.3	Risk Ownership	11
<b>4</b>	<b>Categorisation of Controls</b>	<b>13</b>
4.1	Overview	13
4.2	Categorisation of controls	13
4.3	Business Scenarios	14
4.4	Controls to Business Scenarios Mapping	16
<b>5</b>	<b>Control Implementation Approaches</b>	<b>18</b>
5.1	Overview	18
5.2	Control Implementation Strategies	18
5.3	Control Implementation Patterns	20
<b>6</b>	<b>End to End Information Flows</b>	<b>21</b>
<b>7</b>	<b>Appendix A - Legal Obligations</b>	<b>23</b>
<b>8</b>	<b>Appendix B – Considerations for Bulk Reporting Data Extract / Transfer</b>	<b>24</b>
<b>9</b>	<b>Appendix C – Additional Controls</b>	<b>26</b>

---

# 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 provides guidance and details best practice on the Information Governance issues relevant to integration of systems within a Local Application Integration environment. It does this by introducing a framework for self-evaluation of systems against a set of Information Governance criteria which qualify them as “Locally Assured”.

Systems meeting these criteria alone will not be permitted to connect directly to the Spine. However they will be considered as having implemented a well defined and appropriate set of IG Controls. This makes them suitable for the handling of patient data within a Trust or Local Health Community (LHC) environment, and more specifically means that they may interface with Spine Compliant systems without invalidating the HSCIC Assurance conducted on these.

In this context then “appropriate” IG controls means:

- **Sufficient** - to ensure that patient data is protected and the Care Record Guarantee<sup>1</sup> is honoured
- **Proportionate** – based on the level of risk. Thus ensuring that opportunities to deploy and link systems are assessed with the appropriate balance of clinical safety and confidentiality risks

The document explains the controls that are required and identifies possible technical mechanisms that can be used to implement these controls. References are included to more detailed documentation and specifications where appropriate.



It remains the responsibility of the organisation(s) involved to assess the risk of applying and/or overriding any of the guidance given in this document



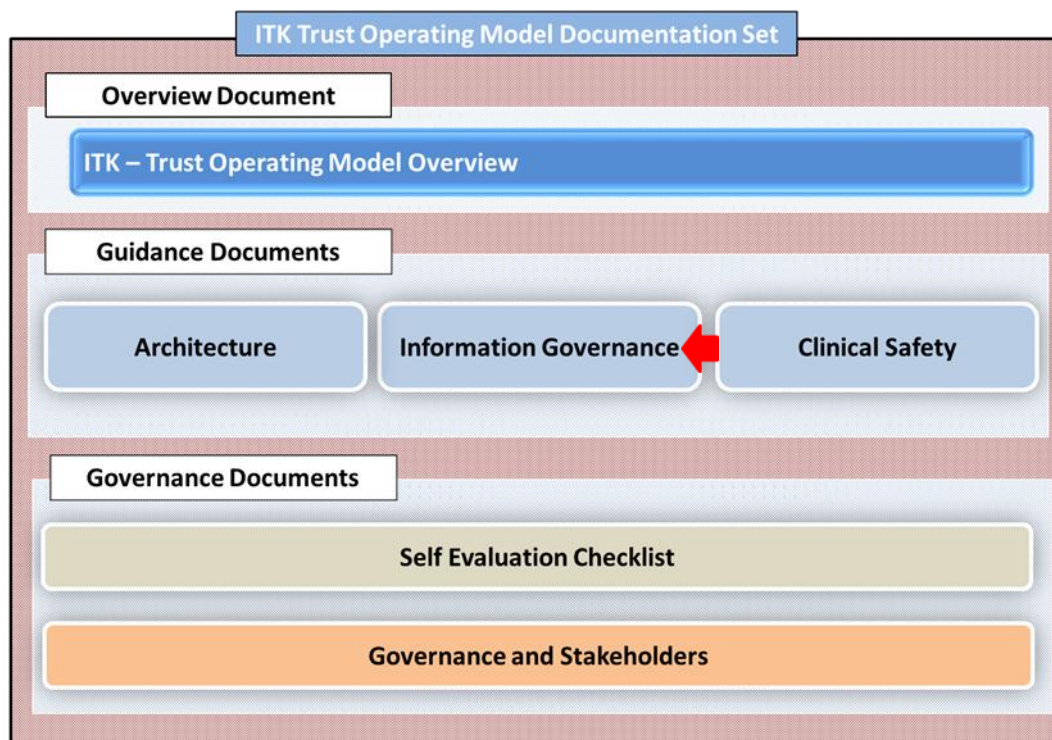
This document is intended to provide information to support the “IG” tab of the Self-Evaluation Checklist. Having read this document, the IG tab should be completed.

---

<sup>1</sup> [http://www.nigb.nhs.uk/guarantee/crs\\_guarantee.pdf](http://www.nigb.nhs.uk/guarantee/crs_guarantee.pdf)

## 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 with Information Governance responsibilities within a Trust.

Secondary audiences may include 3<sup>rd</sup> parties such as suppliers.

## 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.



This document is not intended in any way to replace the requirements set by the NHS Information Governance Toolkit (IGToolkit). Further information and requirements for organisations on the IGToolkit can be found at:

<https://www.igt.connectingforhealth.nhs.uk/>

## 1.5 Document Overview

The rest of this document introduces the fundamental concepts underlying this IG Framework. These include:

- **Principles**  
Underlying Principles which have shaped the approach
- **Security Domains and Risks**  
Introduces the concept of an intermediate level of systems - consisting of Locally Assured systems which have been through an assurance process based upon this Framework. These systems sit between fully Spine Compliant systems and systems that have not been through any form of HSCIC recognised assurance process. The implications of sharing data across these domains are considered.
- **Categorisation of Controls**  
Explains the approach to categorising security controls into groups, and outlines a categorisation model to assist with this. The controls are then mapped to Business Scenarios, with the purpose of indicating which controls are necessary in each case.
- **Control Implementation Approaches**  
Advocates a rigorous but flexible approach to implementing controls in practice, and outlines potential strategies and patterns that can be used.  
  
Note that the supporting document “ITK Resources - IG Control Implementation Patterns” provides a detailed catalogue of specific control Implementation Patterns
- **End-to-End Information flows**  
Looks at the wider issues regarding the end-to-end information flows that a new interface may open up.

## 2 Principles

The following principles underlie the more detailed guidance given in the rest of this document:

### **Trust responsibility (from Overview)**

This document provides detailed guidance to assist Trusts in taking responsibility for selecting an appropriate set of IG controls for Local Application Integration initiatives.

### **Risk-based approach (from Overview)**

As described in the Overview document, balancing risks and benefits is central to the approach. Chapter 3 describes specific IG related risks in more detail, and the remaining chapters detail controls which will be relevant to different scenarios.

The implication of this risk-based approach is that a “one size fits all” approach to IG is not appropriate to Local Application Integration. Rather it is necessary to take a granular approach whereby Information Governance controls are tailored to the business scenario

### **Consideration of external implications (from Overview)**

Again, this principle is described in the Overview document, and returned to in more detail in the Governance document. In this document it is also covered explicitly in Section 3.3 on “Risk Ownership”.

### **Importance of both technical and procedural aspects of IG**

It is important to ensure that organisational processes and procedures are treated at least as seriously as technical system capabilities and system assurance activities.

It is the strength of the overall “system” – both technical and procedural which matters. Complex and expensive technical controls can easily be nullified by lax user and administrative processes. Conversely, there may be situations where a simpler technical approach may be acceptable when reinforced by robust procedural controls.

The process aspects of IG are also important in terms of project lifecycle – from initial risk assessment, through to assurance of the design and implementation (including 3<sup>rd</sup> party external scrutiny where relevant), and

continuing in ongoing reassessment of the benefits gained and risks incurred.

### **Clear documentation and justification of decisions**

Understand the controls defined by NHS HSCIC that are required for systems that connect directly to the Spine; treat those as an ideal whilst coming to a proportionate view for other systems. Be able to justify all decisions where a different approach is applied. (Whether on a permanent or temporary basis).



## 3 Security Domains and Risks

This chapter explains how systems in a Local Application Integration environment can be considered in terms of three Security Domains - with this Operating Model effectively defining a new intermediate domain based on the concept of Local Assurance. The chapter also considers the key risks to be mitigated due to interactions between these domains.

### 3.1 Security Domains

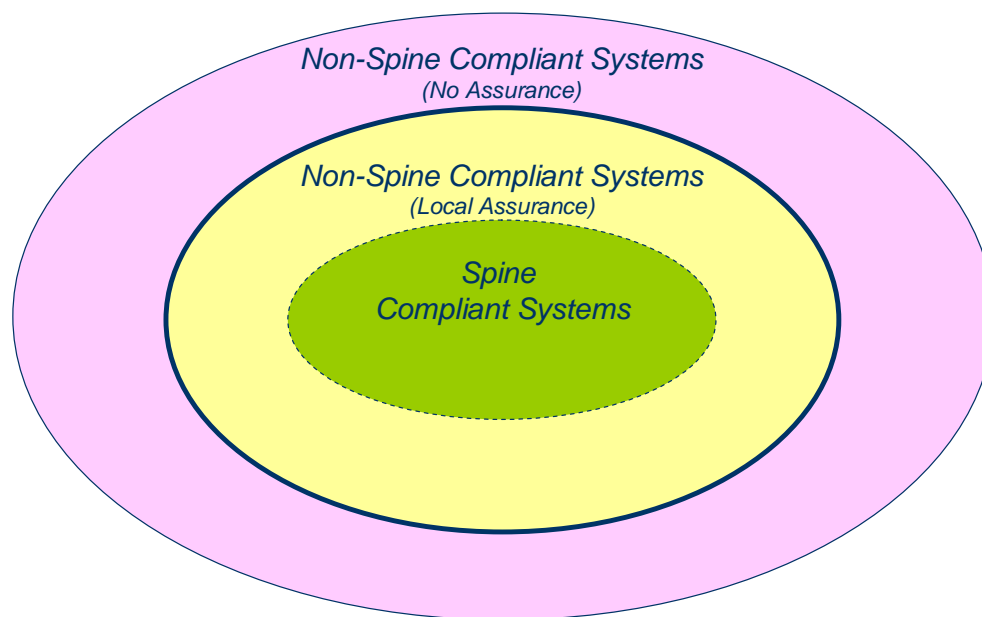


Figure 2 - The ITK Security Domain

The diagram shows three IG domains, with all of these typically being relevant to a Trust Integration landscape:

- **Spine Compliant Systems<sup>2</sup>**

Systems in this domain achieve the highest level of Information Governance assurance. Both the IG Controls and the approach to implementing these controls are prescribed in detail via HSCIC Compliance documentation. These are the only category of systems allowed to connect to the National Spine<sup>3</sup>.

- **Non-Spine Compliant Systems<sup>4</sup> (Local Assurance)**

<sup>2</sup> For the purposes of this definition, systems which have passed Choose and Book compliance only need not be considered as Spine Compliant.

<sup>3</sup> Note: The key point here is that the systems have been through a rigorous assurance process, with Spine connectivity being but one consequence of this. For example, other consequences include the acceptance by Trusts of using a shared system instance.

<sup>4</sup> Note: Throughout this document the term “system” is used to mean both the IT system and the associated processes and procedures specific to a particular implementation

Systems in this domain may not meet the standards necessary for Spine connectivity. However they do meet the criteria described in this set of documents for Local Assurance – including having been through a Trust-based process of assurance to ensure this.

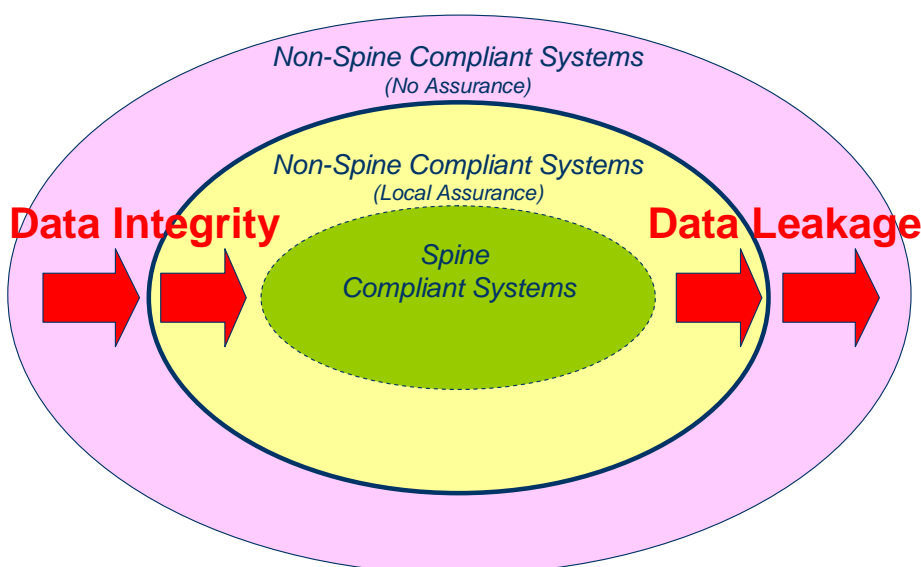


These therefore form an intermediate layer of systems. Although not allowed to connect to the Spine directly, they are able to exchange data with systems assured by HSCIC for Spine Compliance.

- **Non-Spine Compliant Systems (No Assurance)**

These systems have not been through a HSCIC approved process for assurance of their IG Controls. The risks in terms of handling personal-identifiable data are therefore not quantified from the HSCIC point of view.

## 3.2 Domain Boundary Risks



**Figure 3 – Security Risks : Schematic Diagram**

The potential for IG issues arises when a domain boundary is crossed - for example, due to a systems interface. The key risks are:

- **Data Integrity**

When data moves from a less secure system to a more secure system then there is a risk to data integrity. In other words, the interface may act as a route for unattributable, inaccurate or malicious data to enter the more secure system.

**Example:** A non-authenticated user gains access to an unassured Local Trust System and maliciously changes demographic details. Later this data is uploaded to the PAS, and the PAS then updates PDS. Thus the erroneous details are propagated nationally

without the update being attributable to an individual as the unassured system fails to enforce the use of unique usernames, and/or keep appropriate audit trails.

- **Data Leakage**

When data moves from a more secure system to a less secure system then there is a risk of data leakage. In other words, the interface may act as a “backdoor” for gaining access to sensitive data.

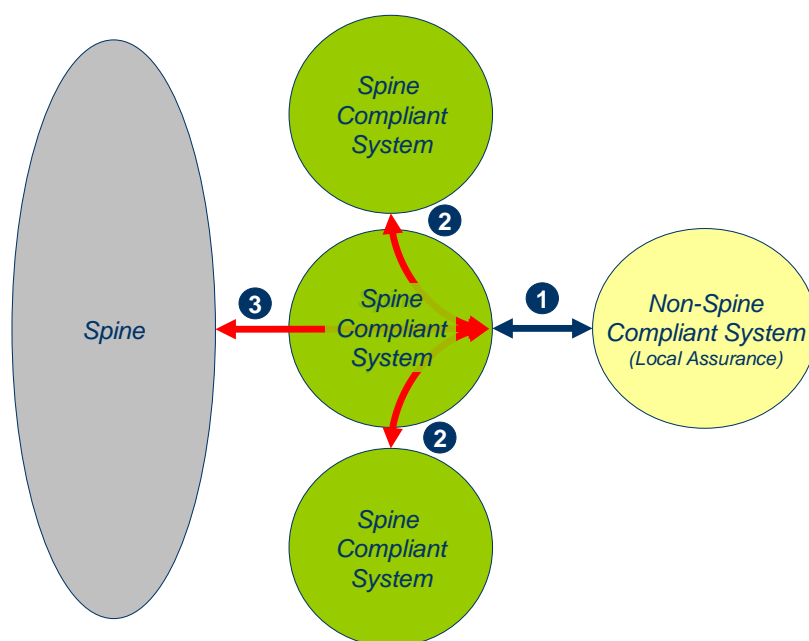
**Example:** Extracts from a patient’s Summary Care Record are downloaded to the local Electronic Patient Record, and then passed on to other departmental systems. Some of these departmental systems are unassured and have weak security controls. A member of the public manages to gain access to one of these unassured systems and views sensitive medical data about a patient that originated from another organisation.



Other sections of this document are concerned with defining a set of controls suitable for mitigating these risks due to interfacing of Non-Spine Compliant Systems to Spine Compliant systems.

### 3.3 Risk Ownership

When assessing a new interface against the controls described in this document, it may be determined that some residual risk remains. In this case the Risk Assessment must document these risks, and a realistic Work Off Plan proposed to make improvements over time. It will then be necessary for those affected by the risk to make a decision as to whether or not to accept the risk and proceed, however overall acceptance rests with the Senior Information Risk Owner (SIRO) within the Trust(s) involved. The diagram below illustrates the implications in terms of risk ownership.



**Figure 4 – Risk Ownership : Schematic Diagram**

**(1)** shows the new interface itself. Clearly any risks introduced by the new Non-Spine Compliant System being connected will impact the Spine Compliant System belonging to that same Trust. Therefore the Trust will need to make a risk-based decision as to whether to proceed with the connection.

**(2)** shows links to Spine Compliant systems belonging to other Trusts. The risk analysis must determine whether there is any possibility of the new interface having an impact on these other Trusts' systems. For example, it may be that data uploaded by one Trust is stored in a shared database and/or otherwise propagated to other Trusts. If there is a potential impact on other Trusts, then the relevant Trusts must also be involved in the risk decision, with acceptance from their Senior Information Risk Owner(s).

**Note:** an important and common example of this will be where several Trusts are sharing a single PAS / EPR instance.

**(3)** shows links to Spine. Again the risk analysis must determine whether there is any possibility of the new interface introduced in (1) having an impact on the Spine. This might be through the propagation of data, even though the new interface does not itself connect directly to the Spine. If there is potential impact on Spine, then HSCIC must also be involved in the risk decision.

The "Self Evaluation Checklist" provides more detail on evaluating and assessing any potential risks. The "Governance and Stakeholders" document then defines in detail the consultation and decision making process.

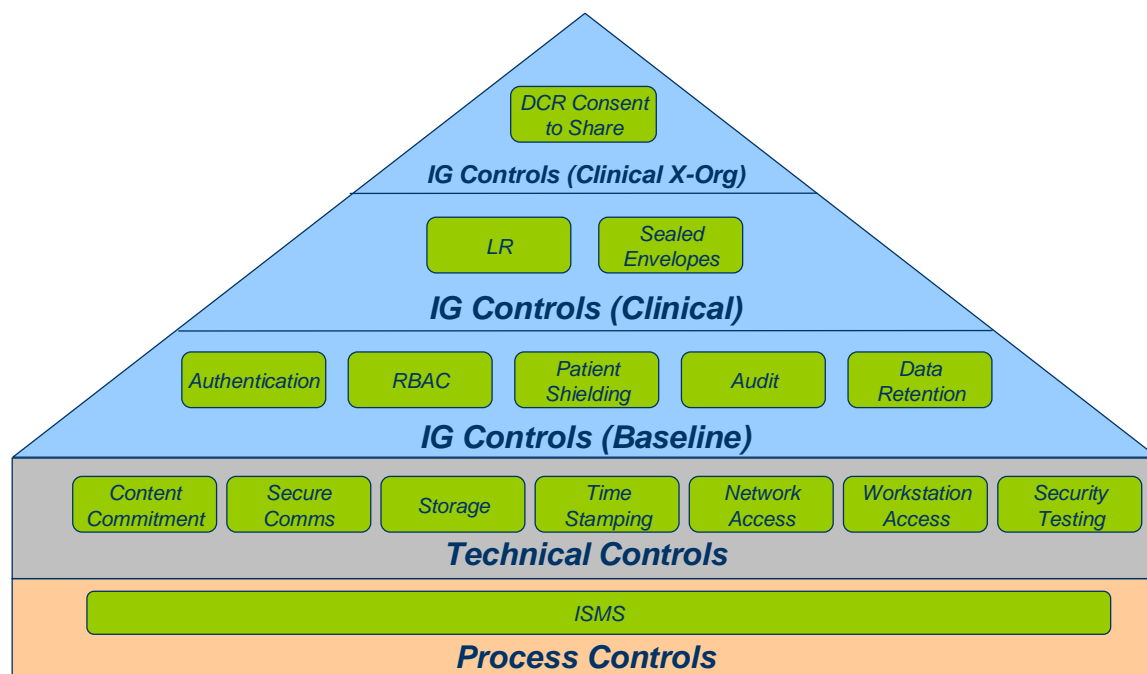
## 4 Categorisation of Controls

### 4.1 Overview

A “one size fits all” approach to IG controls is not appropriate or practical. Rather IG Controls must be tailored based on the business scenario. This enables system suppliers and deploying organisations to concentrate on implementing an adequate set of controls that are relevant to the task in hand.

In order to manage the potential complexity of this approach, controls are categorised. This means organising the large number of IG Controls into a much smaller number of categories. These categories can then be used to more easily specify which IG Controls apply in which business scenarios.

### 4.2 Categorisation of controls



**Figure 5 - The ITK Trust Operating Model Control Categories**

The diagram shows the full range of controls relevant to Local Application Integration. They are grouped into categories as follows:

#### 4.2.1 Foundational Controls

Controls that need to be considered as a basis for any systems implementation

- **Process Controls**  
Sound information security processes form the basis for all other technical and systems controls.
- **Technical Controls**

There are a set of technical controls which are best-practice for any system handling patient data. These cover infrastructure issues such, for example, as network and workstation security

### 4.2.2 Application Controls

These controls relate to features of the system, and need to be applied on a transaction-by-transaction basis

- **IG Controls (Baseline)**

These basic controls are best-practice for all processing of patient data (ie both demographic and clinical data)

- **IG Controls (Clinical)**

These additional controls are best-practice which is relevant only to processing of patient clinical data

- **IG Controls (Clinical Cross Organisation)**

These additional controls are best practice which is relevant only to processes which handle patient clinical data and share it across organisational boundaries



A more detailed description of each control is given in the supporting document “Interoperability Toolkit – Resources IG Control Implementation Patterns”.

## 4.3 Business Scenarios

Having categorised the Controls, the implications of different Business Scenarios must also be considered. The scenario will influence the business impact should the organisation suffer a security breach, for example unauthorised disclosure. The following Business Scenarios have been defined:

- **Demographic Feed**

A Spine Compliant system transmits a feed of demographic data to a Non-Spine Compliant system within the same Trust. In this scenario it is the Spine Compliant system which is in control of selecting the demographic data to expose. (Example: PAS outbound ADT messaging)

- **Demographic Query**

A Non-Spine Compliant System makes a query against a Spine Compliant system within the same Trust for demographic information. In this scenario it is the Non-Spine Compliant system which is in control of selecting the demographic data to expose.

- **Demographic Update**

A Non-Spine Compliant System transmits demographic data to a Spine Compliant system within the same Trust, for the purpose of updating patient demographic details. In this case it is the Non-Spine Compliant system which is control of “pushing” the data to be updated.

- **Clinical Feed**

A Spine Compliant system transmits a feed of clinical data to a Non-Spine Compliant System within the same Trust. In this scenario it is the Spine Compliant system which is in control of selecting the clinical data to expose.

- **Clinical Query**

A Non-Spine Compliant System makes a query against a Spine Compliant system within the same Trust for clinical information. In this scenario it is the Non-Spine Compliant system which is in control of selecting the clinical data to expose.

- **Clinical Update**

A Non-Spine Compliant System transmits clinical data to a Spine Compliant system within the same Trust, for the purpose of updating patient clinical details. In this case it is the Non-Spine Compliant system which is control of “pushing” the data to be updated.

- **Clinical Cross Organisation**

A Non-Spine Compliant system shares clinical data for any purpose across organisational boundaries

## 4.4 Controls to Business Scenarios Mapping

The matrix below builds on the discussion so far by mapping Control Categories to Business Scenarios.

<div><div>Control Category</div><div>Business Scenario</div></div>	Process Controls	Technical Controls							IG Controls (Baseline)				IG Controls (Clinical)		IG Controls (Clinical Cross-Org)	
	Process Controls	Content Commitment	Secure Comms	Storage	Time Stamping	Network Access	Workstation Access	Security Testing	Authentication	RBAC	Patient Shielding	Audit	Data Retention	LR	Sealed Envelopes	DCR Consent to Share
Demographic Feed	S	S							S				n/a		n/a	
Demographic Query	S	S							S				n/a		n/a	
Demographic Update	M	M							M				n/a		n/a	
Clinical Feed	M	M							M				S		n/a	
Clinical Query	M	M							M				M		n/a	
Clinical Update	M	M							M				S		n/a	
Clinical Cross-Org	M	M							M				M		M	

KEY

S

SHOULD

M

MUST

**Table 1: Control to Business Scenario Map**

Given the principles of “Trust Responsibility” and “Risk Based Approach” (see Chapter 2), the use of “MUST” and “SHOULD” in the matrix refer not so much to the need for the control as to the governance processes to be followed in relation to it.

Items marked as “**SHOULD**” are strongly recommended and Trusts not implementing such controls do so at their own risk. A risk assessment SHOULD be documented and other affected organisations consulted. However the nature of this risk is such that Trusts may ultimately make their own assessment as to whether or not to accept it.

Items marked as “**MUST**” have potential implications wider than just the individual Trust in question, and thus it is not appropriate for a Trust to make unilateral decisions about accepting risks which may affect others. In this case the escalation routes described in the “Governance and Stakeholders” document are mandatory. Specifically a risk assessment MUST be documented, and all other affected organisations consulted for sign off. Examples include:

- **Demographic Update** – where the risk is of compromising the integrity of demographic data held in local shared patient indexes and/or National systems.



- **All Clinical Scenarios<sup>5</sup>** – where the risk is of violating the Care Record Guarantee, by exposing or corrupting clinical data originated from other organisations. (Either via Spine, or via a shared Electronic Patient Record in a Spine Compliant system)
- **All Cross-Organisational Scenarios** – where any risk-acceptance decisions may have implications for connected organisations outside of the individual Trust in question.

---

<sup>5</sup> Note that “IG Controls – Clinical” (e.g. Legitimate Relationships) are a SHOULD best-practice in all clinical scenarios, but they are classified as a MUST for the Clinical Query scenario. The reason is that in this scenario the Local Trust system has control over querying any clinical data in the Spine Compliant system.

## 5 Control Implementation Approaches

### 5.1 Overview

It is important that the IG controls are specified in terms of a business-level security objective to be achieved. In this format the requirement is unambiguous and independent of the technical approach.

However for Locally Assured systems the precise mechanism for implementing the controls is NOT prescribed. Rather a range of technical (and process) implementations are envisaged. This is a key concept as it provides the flexibility to implement the necessary controls whilst minimising the impact and overhead for what are typically existing systems.

Having established the approach, this document develops it further by collating examples to illustrate the range of options that may actually be considered in practice. This further guidance takes two forms:

- **Control Implementation Strategies**  
These illustrate the type and range of approaches that might be considered when implementing a given control.
- **Control Implementation Patterns**  
These illustrate concrete examples of implementation approaches that can be considered for each individual control.

### 5.2 Control Implementation Strategies

Whilst the need for a particular IG Control is pre-defined, for Locally Assured systems there is flexibility in the technical approach used to achieve this. The details will vary for each specific control, but experience reveals some common themes and underlying strategies:

#### 5.2.1 Fully Spine Compliant Implementation

This is the most “obvious” approach – implementing the control based on the full Spine Compliance criteria. This is clearly always acceptable and a preferred approach. However there are many cases where, for existing systems, it may not be either practical or cost-effective.

**Examples:**

- Smartcard Authentication
- Spine LR

#### 5.2.2 Alternative Implementation

This approach achieves essentially the same goal as the Spine Compliant Implementation, but via a different technical mechanism. However the alternative mechanism is typically easier for an existing system to implement.

**Examples:**

- Local RBAC
- Local inferred LR

### 5.2.3 Rely on Spine Compliant Partner

In this approach a Non-Spine Compliant System works together with a “partner” Spine Compliant System. The Spine Compliant System is aware of the capabilities of its partner, and ensures that any weaknesses are never exposed.

**Example:**

- A Spine Compliant System filters out any sealed information, thus ensuring that it is never sent to downstream systems.

### 5.2.4 Delegate to Middleware

This approach is similar to the previous one, but builds the additional controls into middleware.

**Examples:**

- A Non-Spine Compliant System sends all outbound clinical messages via an integration engine. The integration engine checks consent, and blocks any transfers to another Trust if the patient has not consented.

### 5.2.5 Manual Processes

It is possible that some controls may be achieved by manual processes and procedures, or by using manual procedures in conjunction with system controls.

## 5.3 Control Implementation Patterns

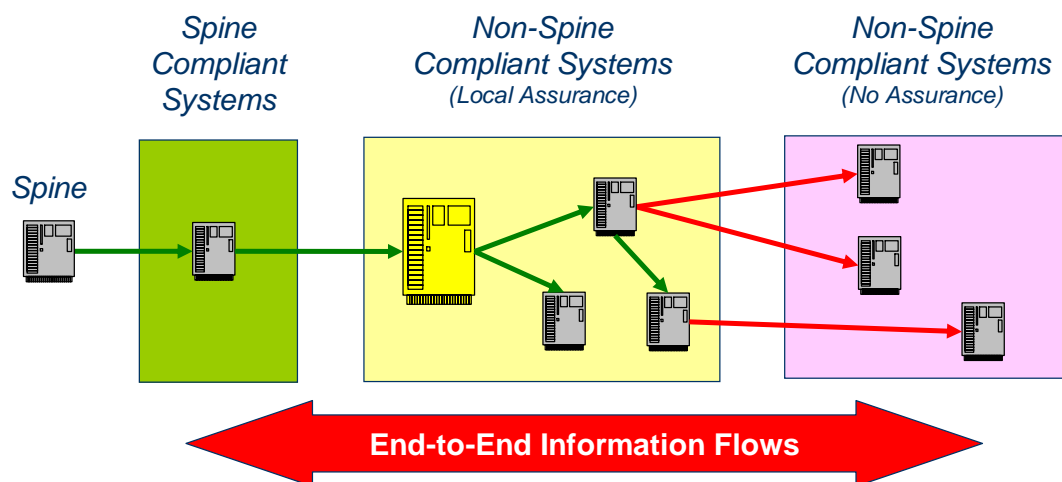
Building on these general strategies, a range of concrete Implementation Patterns that have been identified as options for Locally Assured systems to use in implementing each IG Control.



The supporting document “ITK Resources - IG Control Implementation Patterns” provides a detailed catalogue of these Control Implementation Patterns.

## 6 End to End Information Flows

While the preceding guidance has been focused on the qualities of the interface being assured, the overriding objective is to guard against the data integrity and data leakage issues described in Chapter **Error! Reference source not found.**. Therefore it is essential that the interface is considered in the context of the end-to-end information flows that it enables.



**Figure 6 - The ITK Trust Operating Model Information Flow**

As the diagram shows, there is an issue if the interface undergoing assurance is sound in its own right, but acts as a “gateway” - allowing information to flow between the Spine Compliant system and a network of other Non-Spine Compliant systems which have not been assured to the necessary level.

Therefore these information flows downstream of the interface in question must also be mapped - in order that the assurance process may consider not only the new interface itself, but also the risks of the full end-to-end information flows which will be opened up.

The table below summarises what is acceptable in terms of assurance for data passing between Spine and the full chain of downstream systems.

Downstream Business Scenario	Local Assurance of Downstream interface needed?
Demographic Feed	SHOULD
Demographic Query	SHOULD
Demographic Update	MUST
Clinical Feed	MUST
Clinical Query	MUST
Clinical Update	MUST
Demographic Cross-Org	MUST
Clinical Cross-Org	MUST

**Note:** The “Downstream Business Scenario” needs to be assessed separately for each downstream interface. It may not be the same as the main Business Scenario for the system being assured.

**Example:** A new “Clinical Feed” interface is being assured. Downstream of this is another system which deals with Demographic Data only. Therefore the Downstream Business Scenario is actually a “Demographic Feed”, and a consequentially lower level of assurance is required.

## 7 Appendix A - Legal Obligations

Before proceeding with any integration exercise, a Trust must satisfy itself that all legal requirements are met. The following documents give guidance on the legal obligations to be considered:

Confidentiality Code of Practice

[www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_4069253?IdcService=GET\\_FILE&dID=9722&Rendition=Web](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253?IdcService=GET_FILE&dID=9722&Rendition=Web)

NHS information governance – guidance on legal and professional obligations

[www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH\\_079616?IdcService=GET\\_FILE&dID=151798&Rendition=Web](http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_079616?IdcService=GET_FILE&dID=151798&Rendition=Web)

In addition, the following document can be used as guidance on the relevant legal issues involved with Data Sharing:

<http://www.dca.gov.uk/foi/sharing/index.htm>

An example of an information sharing protocol used within the NHS can be found at:

<https://www.igt.connectingforhealth.nhs.uk/KnowledgeBaseNew/Surrey%20Overarching%20ISP%20Version%201.7%20Jan%202006.pdf>

It is the Trust's responsibility to consider any regulatory requirements which may apply depending on the scale and nature of the deployment. This may include activities such as, for example, conducting an Information Commissioner's Privacy Impact Assessment (PIA) at the start of the project. See

[http://www.ico.gov.uk/for\\_organisations/topic\\_specific\\_guides/pia\\_handbook.aspx](http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx)



Information within this document is for guidance purposes and not for the purpose of providing legal advice. For specific legal advice pertaining to a particular legal issue or problem, legal counsel should be sought.

## 8 Appendix B – Considerations for Bulk Reporting Data Extract / Transfer

There are a number of circumstances where bulk extracts of data are to be passed to another system for reporting purposes – perhaps to provide more flexible reporting facilities or for specific analysis purposes (e.g. 18-week performance).

Where the receiving system is a Spine Compliant system, then it will be responsible for the application of NHS CRS controls. The transmitting system should, however, still only send the minimum level of detail required to fulfil the necessary business purpose.

Where the receiving system is not Spine Compliant, then the following considerations apply:

- the data provided must be the minimum necessary to meet the essential purpose
- wherever possible, the data should be anonymised.
- the receiving system should only output aggregate statistics
- where outputs include exception reporting which will need to identify individual cases, then these should output the minimum patient identifying data possible, and permit access to such reports to a few key individuals, using RBAC controls, that need to process this information –
- wherever possible, the system should separate exception reports from standard aggregate reports
- standard reporting (covering regularly used reports)
  - o the creation of reports should go through a standard request process, which identifies the business need and any patient data required, which should be vetted to ensure that appropriate controls apply
  - o users with the ability to define reports should not be able to run these reports on live patient data (using synthetic or protected data to validate the reports)
  - o users who can run the reports should not be able to define or modify the reports (except through pre-defined parameter selection)
  - o the process for requesting, creating, testing, and release into production of reports should be subject to auditing and monitoring, both to ensure that patient confidentiality is protected against potential abuse and also to avoid retention of unnecessary report formats
  - o Audit logging of the reports run must be considered
  - o Restriction of low-count report results must be considered
- ad hoc reporting (where a user can define and run a report)
  - o the creation of ad hoc reports should be restricted to a few key individuals for the rare exception where ad hoc reporting is required;
  - o where an ad hoc report is used more frequently, then it should be migrated to standard reporting (see above)
  - o where possible, the output should be restricted to aggregate data only
  - o users should be restricted to specific views or universes relevant to their roles
  - o any use of ad hoc reporting should be monitored (preferably through an alerting mechanism) and audited, which should include a log of the query/filter



- criteria and the fields displayed – where regular use occurs, then this should show the need for a standard report rather than ad hoc facilities to be used.
- for all such transfers, a detailed risk assessment should be made to ensure that there are adequate controls around the access to and use of the data; when performed on a regular basis, the risk assessment should itself be reviewed on a regular basis.

## 9 Appendix C – Additional Controls

The document details a number of controls, and also references the BS ISO/IEC 27001:2005 BS7799-2:2005 standard. However it may be possible for organisations involved in Local Application Integration to implement controls that are not listed in either this document or the standard. These should be taken into consideration when performing a risk assessment.

Below are additional controls that are not included within the document or the standard. Please note that this list is not intended to be exhaustive.

Control
Patient consent to data being processed.
Anonymisation and Pseudonymisation of records
Identification, registration and authentication of professional users and personal users (patients)
Consent to View
Data labelling
Patients restricting access
Clinicians restricting access
Decision-making when patients lack competence
Patient access
Protecting the integrity of data flows during communication
Device identification
Printed document control
Secure storage of data (archived)
Media control
Information security management infrastructure
Systems development and maintenance
Outsourcing
Data Quality and Data Quality Management
Ensuring Data Quality when Registering with a Primary Care Provider
Managing Inconsistencies in Demographic Data
Ensuring Data Quality Despite Change

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