

Document filename: ITK 2.0 TOM – IG Control Implementation Patterns			
Directorate / Programme :	HSCIC - Architecture	Project	Interoperability
Document Reference :		HSCIC-ITK-ARCH-500	
Project Manager :	Shaun Fletcher	Status :	Final
Owner :	George Hope	Document Version :	1.0
Author :	George Hope	Version issue date :	01/06/2016

ITK – Resources – Target Operating Model IG Control Implementation Patterns

Document Management

Revision History

Version	Date	Summary of Changes
1.0	01/06/2016	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	01/06/2016	1.0
Richard Dobson	ITK Accreditation Manager	01/06/2016	1.0
Nigel Saville	ITK Accreditation	01/06/2016	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

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	Document Purpose	4
1.2	TOM Documentation Set	4
1.3	Audience	4
1.4	Document Scope	5
1.5	Document Overview	5
2	Overview of the Control Implementation Patterns	6
3	IG Controls Baseline	9
3.1	Authentication	9
3.2	RBAC	10
3.3	Patient Shielding	11
3.4	Audit	12
3.5	Data Retention	14
4	IG Controls Clinical Data	15
4.1	Legitimate Relationships	15
4.2	Sealed Envelopes	16
5	IG Controls Cross Organisational Clinical Data	19
5.1	DCR Consent to Share	19
6	Technical Security Controls	21
6.1	Content Commitment (Digital Signatures)	21
6.2	Secure Communications	21
6.3	Storage	21
6.4	Time Stamping	22
6.5	Network Access Controls	22
6.6	Workstation Access Controls	23
6.7	Security Testing	23
7	Security Management Process	24

1 Introduction

1.1 Document Purpose

This document is an additional resource provided as part of the Interoperability Toolkit. It provides a detailed catalogue of implementation patterns for Information Governance Controls relevant to Locally Assured Systems.

The “IG Guidance” document describes the overall framework within which Information Governance is applied to Locally Assured systems. This document provides supporting information, in terms of a detailed (and potentially more volatile) catalogue of specific control implementation patterns.

1.2 TOM Documentation Set

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

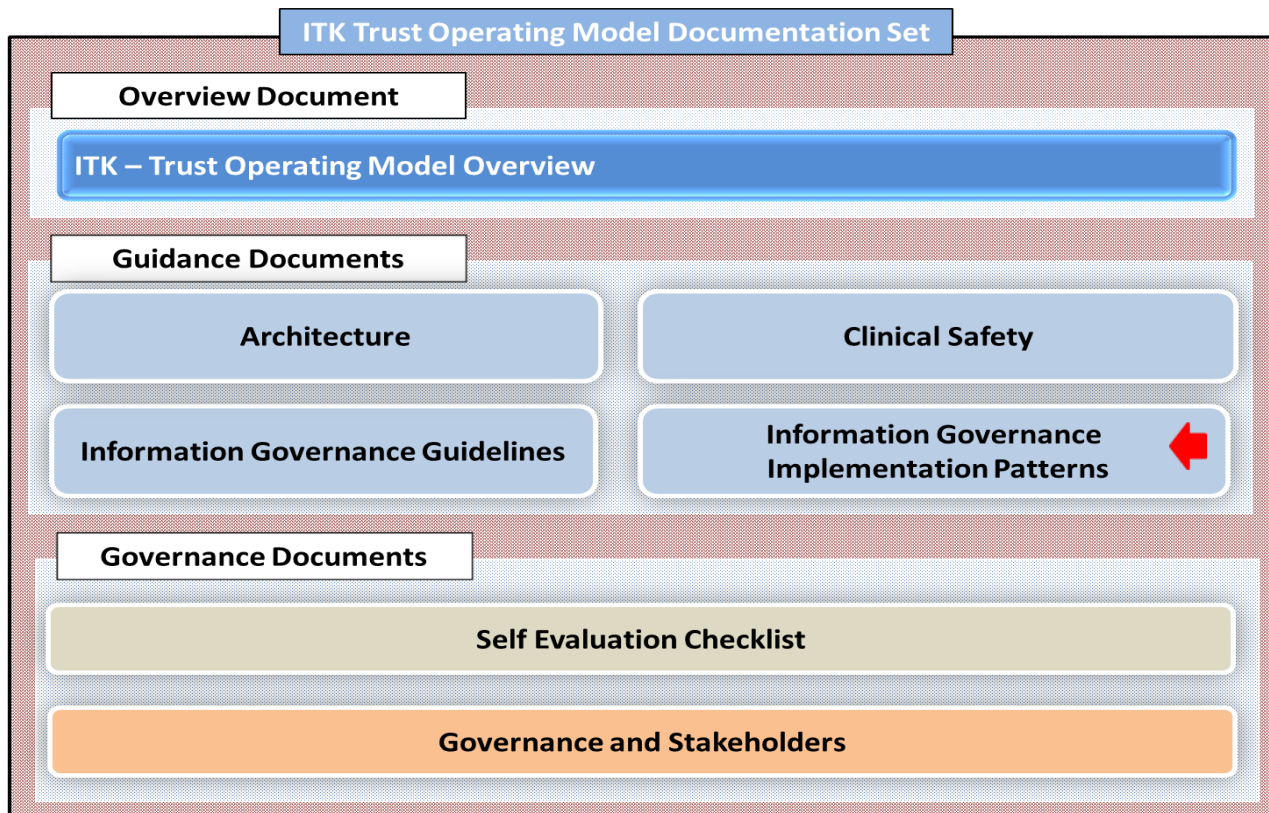


Figure 1 - The ITK Trust Operating Model Document Set

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 architects and technical members of the project team.

Secondary audiences may include 3rd parties such as supplier 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.

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 (eg training, communications, service management etc) are not covered.

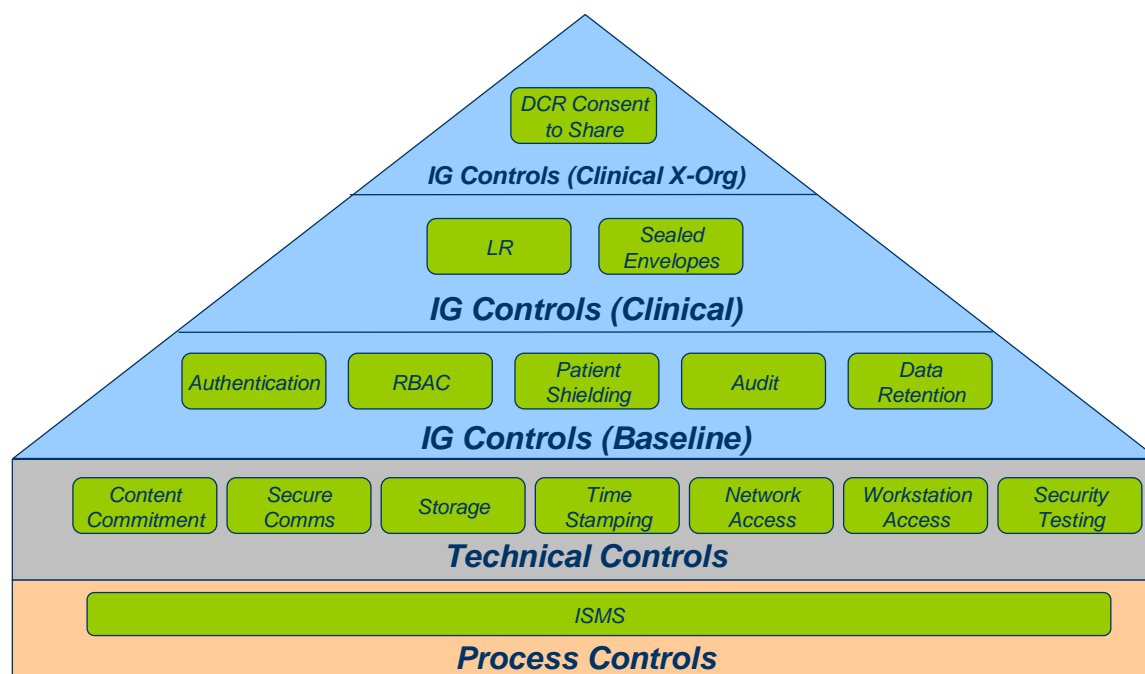
This document is not intended in any way to replace the requirements set by the NHS Information Governance Toolkit (IGToolkit). Further information and requirements for organisations on the IGToolkit can be found at:
<https://www.igt.connectingforhealth.nhs.uk/>

1.5 Document Overview

This document gives an overview of the approach to categorising the Control Implementation Patterns. The rest of the document then works through each of the categories of control in turn, explaining in more detail the controls in each category and known implementation patterns for each one.

2 Overview of the Control Implementation Patterns


The diagram below reprises the range and categorisation of IG Controls identified as relevant in the “IG Guidance” document of the Trust Operating Model. Please refer to that document for more details.



The rest of this document summarises the range of concrete Implementation Patterns that have been identified as options for Locally Assured systems to use in implementing each IG Control.

This list can never be considered exhaustive as there is always the potential for new implementation approaches to be devised. In addition the maturity of the various Implementation Patterns varies, with the following ratings being used:

Rating	Description
LEVEL 1	The implementation pattern is fully endorsed and defined in detailed formal documentation. It is a preferred approach, which Trusts are encouraged to adopt. <i>Typically this is the same approach as is used by fully Spine Compliant systems</i>
LEVEL 2	The implementation pattern is recognised as acceptable
LEVEL 3	The implementation pattern is a potential candidate which is not yet fully proven. <i>The “Level 3” Implementation Patterns are included to</i>

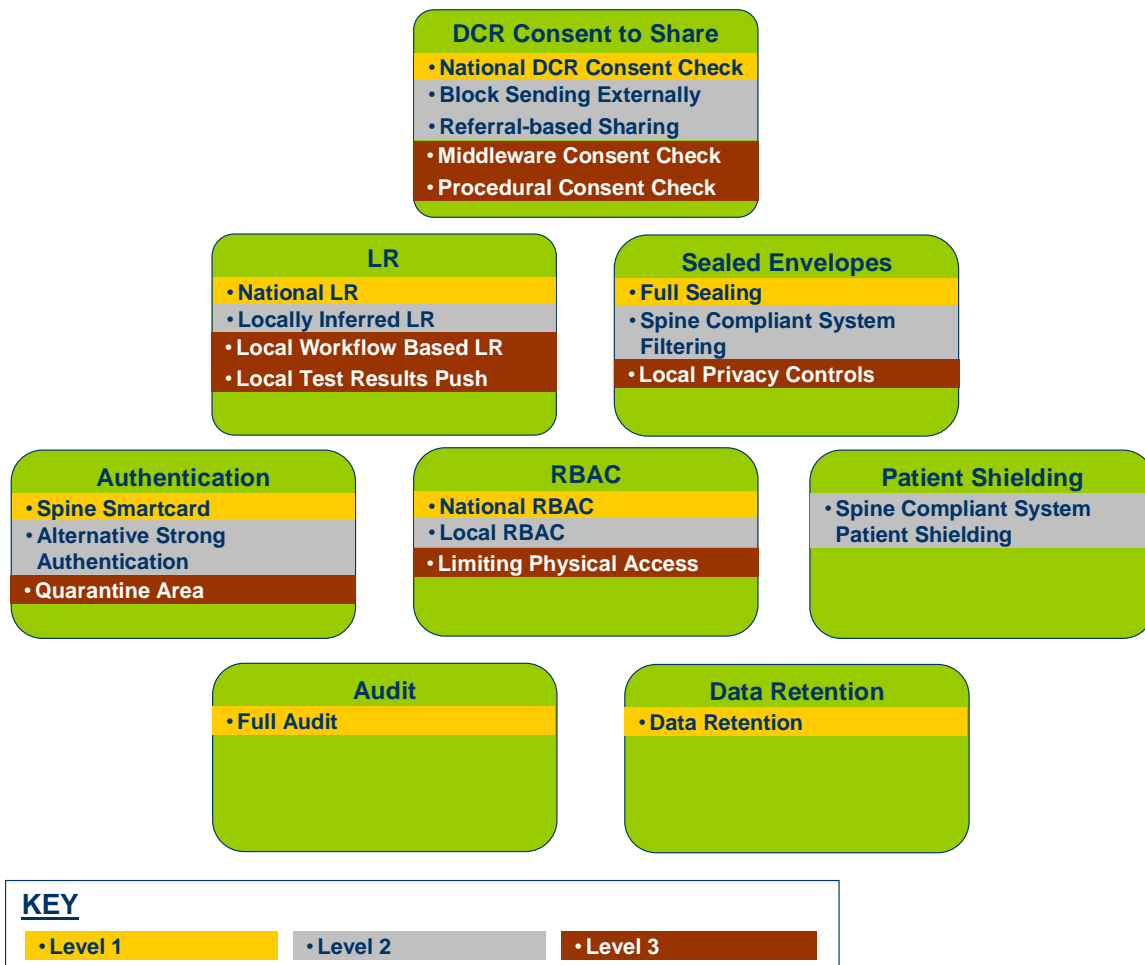


provide maximum assistance to Trusts in terms of listing possible mechanisms for meeting IG requirements. However they are not yet fully documented and require more investigation and proving in practice.

LEVEL 3 implementation patterns are not, as yet, approved nor endorsed by CFH

Note that these ratings apply to the maturity of the pattern, and not to the quality of the solution that may be possible. So, for example, a “Level 3” approach could provide equivalent security to one rated as “Level 1” – the difference being that this would need to be confirmed on a case-by-case basis.

Based on these ratings, the diagram below summarises the available Implementation Patterns. Each box corresponds to a particular IG control, and the bullet points within show candidate implementation patterns for that control.



The remainder of this document describes each IG Control and its Implementation Patterns in more detail

3 IG Controls Baseline

This chapter describes in detail the baseline IG Controls which every Locally Assured system wishing to satisfy the assurance criteria must implement

3.1 Authentication

3.1.1 Requirement

The organisation is able to verify the identity of a user accessing the system.

3.1.2 Implementation Patterns

- **Spine Smartcard Authentication (LEVEL 1)**

NHS CRS Smartcards help control who accesses the NHS CRS and what level of access that they can have. A user's smartcard is printed with their name, photograph and unique identity number.

To register for a Smartcard, Registration Authorities are required to ask applicants for identification which satisfies the government recommended standard 'e-GIF Level 3', providing at least three forms of ID (photo and non-photo), including proof of address.

<http://www.connectingforhealth.nhs.uk/systemsandservices/rasmartcards>

- **Alternative strong authentication (LEVEL 2)**

Where use of the Spine Smartcard is not possible, other types of two-factor authentication may be considered e.g. SecurID.

In a small number of cases two factor authentication may not be appropriate and in these cases single factor authentication is acceptable. An effective password policy must be part of the security measures that together provide a co-ordinated and effective response to all the threats to the system.

Minimum requirements for an effective single factor authentication policy can be found in:

NPFIT-FNT-TO-IG-IGCOM-0066.03 – Single Factor authentication Policy

In terms of the registration process, Registration Authorities are required to ask applicants for identification which satisfies the government recommended standard 'e-GIF Level 2'.

Adhering to level 2 for registration requires a Personal statement (as for level 1), including information that may be crosschecked against supplied documentary/third party evidence. In support are required one piece of documentary evidence that contains the registrant's signature and photograph (ideally a passport or National Identity Document) and one piece of evidence of activity in the community, such as a bank statement (two if the evidence of personal identity does not contain a photograph and signature). An item of third party corroboration may be substituted for one of the above pieces of evidence.

Cabinet Office, Office of e-Envoy: Registration and Authentication, e-government Strategy Framework and Policy and Guidelines. Ver 3.0.

In all cases the authentication mechanism must make use of individual authentication credentials, i.e. there must be no shared user credentials

- **Quarantine Area (LEVEL 3)**

It may be that in some circumstances the above cannot be achieved (eg anonymous patient using a kiosk or multiple users using the same login credentials). In that case it may be possible to submit updates to a “quarantine” area initially. The solution is completed by putting in place an administrative process for a properly authenticated user (as above) to take responsibility for checking and releasing the updates later - to ensure that the updates are attributable to a uniquely identifiable individual.

This is a “Level 3” implementation pattern, and therefore not yet fully documented or endorsed

3.2 RBAC

3.2.1 Requirement

Access to information and functions is limited to those needing it to fulfil their Organisational role.

3.2.2 Implementation Patterns

- **National RBAC (LEVEL 1)**

The National RBAC implementation determines the full set of access rights for a user based on the set of Activities that accrue through the National Baseline Policy plus any additional Activities allocated explicitly at a local level.

(The National Baseline Policy is the minimum set of things someone with a specific Job Role should be able to do either in its own right or in conjunction with any Areas of Work specified).

The following document provides full details:

NPFIT-FNT-TO-IG-DES-0093.07 - National RBAC Database User Guide

- **Local RBAC (LEVEL 2)**

The fundamental requirement is to restrict access to data or functions to those whose job functions demand it. Local implementations of RBAC must ensure that their solution satisfactorily meets this requirement. RBAC privileges must be strictly controlled and should allow for clear separation of access rights in the system. Evidence of RBAC controls and policy will need to be provided.

- **Limiting physical access to the system (LEVEL 3)**

This approach is based on limiting physical access to the system, based on manual and procedural controls. For example, by ensuring that access to the system is only granted for users who require access to the full extent of information available. This is only likely to be appropriate for smaller systems with limited capabilities.

This is a “Level 3” implementation pattern, and therefore not yet fully documented or endorsed

3.3 Patient Shielding

3.3.1 Requirement

The underlying requirement is that extra protection is provided from unauthorised access for personal demographic details of those patients flagged as requiring this.

There are four aspects to this requirement:

1. Identification of such patient records
2. Ensuring that personal demographic details cannot be inappropriately accessed for these patients
3. Ensuring that personal demographic details cannot be inappropriately updated for these patients
4. Ensuring that the shielding status itself cannot be inappropriately changed

In terms of Spine systems, PDS provides a full implementation of all four aspects:

1. PDS records are identified by an “S-Flag” if access to demographics must be restricted
2. PDS will only return the patient's name, sex, date of birth and death for S-Flagged records.
3. S-Flagged PDS records can only be updated directly by the National Back Office
4. The S-Flag itself can only be updated directly by the National Back Office

The Spine is therefore completely self-protecting in this regard.

Spine Compliant systems must also have, in addition, their own mechanisms for flagging of patients whose locally maintained demographic details need to be shielded. Therefore these local shielding mechanisms should also take account of the four requirements listed above - and should ensure that these cannot be compromised by integration with other Non-Spine Compliant systems.

Finally, note that there is currently a mandated link between the Spine S-Flag and the local shielding mechanism. Thus a Spine Compliant system must always ensure that its local shielding mechanism is applied to any patients marked with an S-Flag on PDS.

3.3.2 Implementation Patterns

- **Spine Compliant System Patient Shielding (LEVEL 2)**

Before connecting any integration solutions to a Spine Compliant system it should be ensured that the Spine Compliant system's shielding implementation is robust enough to ensure that it cannot be compromised by the new interface. (Typically it might do this by using a local alias e.g. MRN for a patient with sensitive demographics, in order to maintain information flows and to avoid compromising patient care or creating a clinical safety issue).

3.4 Audit

3.4.1 Requirement

Typically, IG Officers, Privacy Officers and Caldicott Guardians need functionality to record and retain audit data that provides for reporting on system use, investigation of incidents and fulfilment of Care Record Guarantee commitments.

<http://www.connectingforhealth.nhs.uk/systemsandservices/scr/staff/impguidpm/ig/igcontrols>

Four high level use scenarios demonstrate how the audit functions will be used¹;

1. Investigation of reported incidents of misuse of systems
2. Investigation of IG alerts
3. Responding to requests for information from the public
4. Fulfil Care Record Guarantee commitments

Different business environments, systems and use scenarios will determine the applicability of audit functionality based on satisfying these business requirements. For example; it will not be necessary for a system to generate IG alerts for self claimed Legitimate Relationship if the system itself does not use a Legitimate Relationship Service.

¹ For CFH architects, the internal document "IG Audit and Alerts Gold Standard" provides more information on each of these Use Cases.

3.4.2 Implementation Patterns

- **Full Audit (LEVEL 1)**

System audits must keep data appropriate to identify:

1. Who carried out particular system activity (identified by their unique user role profile, for example)
2. What events occurred in the system (such as changes to clinical records or system configuration, etc.)
3. Where events occurred (network access point, for example)
4. When events occurred (time / date).

Systems must provide audit functionality to record, retain and report on system use, that:

- Provides the capabilities to carry out analysis of audit trail data.
- Allows users to trace events through all relevant systems
- Are of a standard of integrity that is acceptable for use as evidence in legal proceedings
- Covers all service events defined by the acronym *CRUD*
 - C – Create;
 - R – Read, View, Print;
 - U – Update
 - D – Delete
- Provides facilities for approved users to retrieve audit data and produce reports that identify system use.

Once the audit data is captured and retained standards must be met to ensure it can not be altered or deleted. Audit data will be used as evidence in legal proceedings and must meet strict tests of integrity to be of value.

It must be retained in accordance with Data Retention periods specified by Department of Health (see Section 3.5, Data Retention) and it must be capable of being searched and output, but only by users authorised to do so (see Section 3.2, RBAC).

3.5 Data Retention

3.5.1 Requirement

Minimum periods for which the various records created within the NHS should be retained, either due to their ongoing administrative value or as a result of statutory requirement, are contained in the Records Management: NHS Code of Practice (Part 2), Annex D.

http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4131747

The retention schedules apply to all the records concerned, irrespective of the format (eg paper, databases, e-mails, X-rays, photographs, CD-ROMs) in which they are created or held.

3.5.2 Implementation Patterns

- **Data Retention (LEVEL 1)**

Implementation of data retention, in line with the minimum periods specified above.

4 IG Controls Clinical Data

This chapter describes in detail the additional IG Controls which any Locally Assured system handling clinical data must implement.

4.1 Legitimate Relationships

4.1.1 Requirement

Only those users with a “legitimate relationship” (LR) with a patient are able to access sensitive personal data about that patient.

'NPFIT-FNT-TO-IG-DES-0124.04 - 'Legitimate Relationships Requirements - Guidance to NPfIT suppliers (Logicalised and Prioritised)

4.1.2 Implementation Patterns

- **National LR (LEVEL 1)**

The document above details a number of business rules that underpin the application of LRs within systems.

These are separated into sub-sections, each of which deals with a particular aspect of LRs. These contain a list of business rules and requirements, supported by explanatory notes where applicable. These sub-sections are:

- Legitimate Relationships and their Changing States
- Workgroups
- Legitimate Relationships between Patients and Workgroups

Details of the business requirements for each of these sections can be found in:

NPFIT-FNT-TO-IG-DES-0124.04 - Legitimate Relationships Requirements - Guidance to NPfIT suppliers (Logicalised and Prioritised)

- **Locally inferred LR (LEVEL 2)**

In this case the local system maintains a record of any LRs it has itself created on Spine. Thus it is able to infer the Spine LR's existence without actually incurring the overhead of sending / receiving messages to the Spine LR service.

NPFIT-FNT-TO-IG-DES-0160.06 (or NPFIT-ELIBR-AREL-EXLC-EXTIG-0039.01) LR Inference Rules for NCRS and ESP Applications

Checks would need to be made that these 'inference rules' were being applied consistently and correctly.

- **Local Workflow-Based LR (LEVEL 3)**

In this approach the local system does not use LRs directly, but instead provides an equivalent control over access to clinical data based on the business workflow. Typical examples might be allowing access to medical records when it is known that the patient is checked into a clinic or ward and the user in question works there.

Another example might be for a worklist based process. In this case the fact that a patient has been placed in a user's worklist clearly indicates that they have a legitimate need to view their records.

Such mechanisms can provide a robust and acceptable alternative to National or Locally Inferred LRs. However it is necessary to be sure that the workflow-based access is sufficiently constrained, and that there are no "loopholes" (e.g. search facilities) which allow the workflow controls to be bypassed. Thus each implementation must be examined on its merits.

This is a "Level 3" implementation pattern, and therefore not yet fully documented or endorsed

- **Local test results "push" (LEVEL 3)**

This implementation pattern is a variant of the workflow-based approach, and covers the specific scenario where an Spine Compliant system "pushes" test results to other systems within the same trust. Thus the Non-Spine Compliant system cannot freely access clinical data – it is "pushed only" specific results that the Spine Compliant system decides are relevant. In this case, the range of data available is limited, and would ideally be linked by some order reference to the relevant patient records in the recipient system, so that the local controls are then appropriately applied.

While it remains best practice that the Non-Spine Compliant system SHOULD also implement one of the above LR mechanisms to further restrict access, in this specific scenario it is not mandatory, but the solution would need to be risk-assessed by the NHS organisation as being suitable for deployment.

This is a "Level 3" implementation pattern, and therefore not yet fully documented or endorsed

4.2 Sealed Envelopes

4.2.1 Requirement

Patients are able to restrict access to identified pieces of information within their Care record.

4.2.2 Implementation Patterns

- **Full Sealing (LEVEL 1)**

Patients, and/or their authorised representative(s), in consultation with their clinician(s), will be able to:

- Identify one or more sets of sensitive information which should be sealed from everyone other than the author and, for information sealed locally, people in the same workgroup as the sealer (for spine documents only the author applies);
- Request, for each set of sealed information, whether people other than the author and those in the same workgroup as the sealer can ever gain access:
 - if “sealed”, the local information can be made available to users outside the workgroup with the patient’s express permission, or through override in exceptional circumstances (e.g. public interest); or
 - if “sealed and locked”, users from outside the workgroup will be unaware that the sealed information exists;
- Change their minds at any time and change or remove one or more of the restrictions.

NPFIT-FNT-TO-REQ-DEL-0142.30 Sealed Envelopes Supplier Requirements Documentation

- **Spine Compliant system Sealed Envelope filtering (LEVEL 2)**

In this implementation approach, the Spine Compliant system filters out any Sealed data and never allows it to be passed to a Non-Spine Compliant system. Therefore the Non-Spine Compliant system can be guaranteed to never see any Sealed data - and thus does not have to implement any further controls in this regard.

- **Local Privacy Controls (LEVEL 3)**

It may be that Non-Spine Compliant systems implement their own existing Privacy Controls which are broadly similar to the Spine concept of sealing. Depending on the precise circumstances then these Privacy Controls may be proven to provide an equivalent (or greater) level of protection. This would, however, need to be proven on a case-by-case basis.

This is a “Level 3” implementation pattern, and therefore not yet fully documented or endorsed

- **Procedural Controls (LEVEL 3)**

It may be that Trusts are able to implement a system of procedural controls - for example making sure that sealed data is never entered to the system. This would, however, need to be proven on a case-by-case basis.

This is a “Level 3” implementation pattern, and therefore not yet fully documented or endorsed

5 IG Controls Cross Organisational Clinical Data

This chapter describes in detail the additional IG Controls that any Locally Assured System passing clinical data across organisational boundaries must implement.

5.1 DCR Consent to Share

5.1.1 Requirement

Confidential information from a patient's Detailed Care Record (DCR) should normally only be shared across organisational boundaries with the consent of the individual concerned.

Security measures should reflect the sensitivity and other relevant risk management issues of the information concerned.

5.1.2 Implementation Patterns

- **National DCR Consent Check (LEVEL 1)**

This approach involves the local system checking against the relevant PDS Consent flag before allowing any data sharing across organisational boundaries.

NPFIT-FNT-TO-IG-DES-0135.06 NHS CRS Consent to Share: Access Rules

- **Block sending clinical data externally (LEVEL 2)**

This approach consists of ensuring that Non-Spine Compliant systems are restricted and can only send data within the Trust. If they are not connected to external organisations, then there is no need to implement controls relating to the PDS consent to share flag.

- **Referral-based data sharing (LEVEL 2)**

In the case of a referral it is an accepted practice to infer that, by agreeing to the referral, the patient has consented to sharing of whatever information is necessary to directly support that referral. Thus as long as the dataset can be shown to be restricted to only that information specifically relevant to the referral in question, this sharing is permitted. A further constraint of this approach is that the receiving system must have the ability restrict access to this data - such that, in the absence of consent, it can only be viewed in circumstances directly relevant to the referral in question.

- **National Consent checking in middleware (LEVEL 3)**

In this implementation pattern, all external data transfers are routed via a middleware integration engine. The middleware does the consent checks, and requests an override and / or refuses to send the data out if they fail.

This is a “Level 3” implementation pattern, and therefore not yet fully documented or endorsed

- **Local / Procedural consent checks (LEVEL 3)**

In the case where the patient is present then other procedural approaches may be possible. For example, the patient could be asked directly in each case whether they agree to the proposed sharing of their clinical details across organisational boundaries. Clearly this approach may need to be supported by either (a) processes, procedures, paper forms etc to ensure that the check is appropriately made, and/or (b) local system facilities to record the response and, specifically, to ensure that sharing is blocked if the patient expresses dissent.

This is a “Level 3” implementation pattern, and therefore not yet fully documented or endorsed

6 Technical Security Controls

This chapter describes in detail the technical security controls which every Locally Assured system wishing to meet the assurance criteria must put in place.

6.1 Content Commitment (Digital Signatures)

6.1.1 Requirement

There are scenarios when digital signatures are required. The two uses for digital signatures are:

- Content Commitment Signatures – where the signature is used for specific messages to affirm the signer's commitment to selected content in the message – the signer is prompted to confirm that the content should be signed.
- Origin Authentication Signatures – where the signature is included automatically on all messages sent by a user or system, to authenticate the identity of the sender.

6.2 Secure Communications

6.2.1 Requirement

David Nicholson, NHS Chief Executive, has directed that there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. This is the default position to ensure that patient and staff personal data are protected.

NHS bodies will need to make a local judgement on the balance of risk to patient care against risk to personal data security in determining whether use of unencrypted devices should continue as an interim measure. Where it is felt that continued reliance upon unencrypted data is necessary for the benefit of patients, the outcome of the risk assessment must be reported to the organisation's Board, so that the Board is appropriately accountable for the decision to accept data vulnerability or to curtail working practices in the interests of data security.

<https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption%20Guidance%2031.1.2008.doc>

6.3 Storage

6.3.1 Requirement

All systems should store patient data in an environment that is physically secure and have data storage and media control policies that ensure the protection against data theft or other unauthorised access

Any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted. This is also now a requirement across all public sector organisations set by the Cabinet Secretary.

NHS bodies will need to make a local judgement on the balance of risk to patient care against risk to personal data security in determining whether use of unencrypted devices should continue as an interim measure. Where it is felt that continued reliance upon unencrypted data is necessary for the benefit of patients, the outcome of the risk assessment must be reported to the organisation's Board, so that the Board is appropriately accountable for the decision to accept data vulnerability or to curtail working practices in the interests of data security.

<https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption%20Guidance%2031.1.2008.doc>

6.4 Time Stamping

6.4.1 Requirement

It is important to maintain an accurate time source for all systems. This is essential for incident analysis and important in diagnosing problems from audit logs or when rebuilding and replaying messages

The Network Time Protocol (NTP) is used to ensure audit logs and message stamps are recorded with the same date and time between systems (within 250 milliseconds of the NASP-provided or National Network Time Servers).

The NHS CRS NTP service provided by BT should be used as the recommended source.

6.5 Network Access Controls

6.5.1 Requirement

N3 is a private Wide Area Network (WAN) and access is therefore strictly limited to authorised endpoints. Any organisation wishing to connect to N3 is responsible for ensuring that their N3 connection does not compromise the security measures already in place within the WAN.

The following document provides guidance on the application of network security controls.

NPFIT-FNT-TO-IG-GPG-0031.03 Local Area Network Security – Good Practice Guideline

6.6 Workstation Access Controls

6.6.1 Requirement

Recommendations for workstation controls can be found at the National Institutes of Standards Technology:

A guide to server security can be found at: -

<http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf>

A guide to securing information technology systems can be found at:

<http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>

6.7 Security Testing

6.7.1 Requirement

A IT Security Health Check (ITSHC) affords business owners the requisite information to assess the security risks inherent within a system and provides an assessment of the effectiveness of current controls and countermeasures.

The degree and scope of an ITSHC is dependent on a number of factors, such as the type of development going through the compliance process, and the method of deployment. The following table illustrates the degree to which an ITSHC is required.

<i>Activity</i>			First of Type (FOT)	System update (not FOT)	Common infrastructure component²	Subsequent deployment (subject to specific requirement)³	Subsequent deployment
<i>Security Practices</i>	ITSHC	Application	Y	N	Y	N⁴	N
		Infrastructure	Y⁵	N	Y	Y	N⁶
	Local⁷	Application⁸	Y	Y	Y	N	N
		Infrastructure	Y	Y	Y	Y	Y

² Such as a centralized message-handling service, or a solution deployed from a data-centre

³ Such as might apply to the Independent Sector, or if approval for offshore support was being requested

⁴ Not required here because application-level testing would have taken place at FOT, and application-level testing is only required once

⁵ This may be on a model deployment, or might take place in conjunction on-site at the FOT customer

⁶ The responsibility for ensuring the security of local infrastructures rests with the owners of that local infrastructure, under the obligations associated with connectivity to N3

⁷ These are practices that we would expect to find as part of a supplier's normal development processes, or a Trust's normal deployment processes, but which are not mandated by NHS CFH

⁸ Local security practices as described for example in section 3.3.6

7 Security Management Process

BS ISO/IEC 27001:2005 BS7799-2:2005 replaces the 2002 version of BS7799 part 2 and is used to formulate an Information Security Management System (ISMS) (that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security) for those organisations wishing to fully comply with the standard. Alternatively, it can be used as a mechanism by Trust senior management to formulate a cyclic review of the implementation of IG toolkit action planning.

<https://www.igt.connectingforhealth.nhs.uk/isoiecsummary.aspx?tk=399854829563914&cb=11%3a53%3a40&Inv=20&clnav=YES>

Note: The preceding catalogue of controls detailed within this document is intended to provide a baseline of common controls that must be considered. However, these controls are not exhaustive, and NHS Organisations must consider all available controls in order to manage those risks identified to an acceptable level.

*** End of Document ***