

Implementing the responsibilities of the
Senior Information Risk Owner (SIRO)
together with those of
Information Asset Owners (IAO)
Information Asset Administrators (IAA)
and the inter-relationship with
Information Governance

11th March 2010

Chris Linacre
SIRO
Director of Service Development
Sheffield Teaching Hospitals FT

Peter Wilson
Information Governance, Caldicott
& SIRO Support Manager
Sheffield Teaching Hospitals FT

Introduction

This is a joint presentation to give an overview of the approach taken by Sheffield Teaching Hospitals in:

- v Contextualising the SIRO role to information risk and information governance responsibilities within an NHS Trust
- v Briefing, supporting and training for the SIRO role from an information governance and assurance viewpoint
- v Engaging other board members to increase their knowledge, appreciation and understanding of the SIRO responsibilities for information security and assurance

Following the HMRC data losses

- Ø Cabinet Office asked Robert Hannigan, Head of Security, Intelligence and Resilience to assess data handling procedures in government departments
- Ø December 2007: Interim report “Data Handling Procedures in Government”
- Ø In parallel, Poynter Investigation and Report into the specific circumstances in HMRC data loss
- Ø Thomas/Walport Review of the security of personal data in both the public and private sector.
- Ø Data Handling Procedures: Final Report, delivered in July 2008
 - v Section 3 Implementation
 - v 3.14. The work underway by some central Government Departments will influence some practices in the wider public sector

The NHS approach

Following the Government directive of November 2007 (before the interim Cabinet Office report), David Nicholson initiated the Information Governance Assurance Programme (IGAP) for the NHS. Its remit was:

- v to provide assurances regarding the current processing of person identifiable information in line with the requirements of the Data Handling Report and,
- v to produce an Information Governance Assurance Framework for the healthcare sector to provide continuing assurance that sensitive person identifiable information is managed securely and confidentially.

The Programme recognised that NHS organisations were already providing some forms of assurance through their submission of the Information Governance Toolkit assessment to the Department of Health. This also included reporting to the Healthcare Commission on standards C9 and C13 of the Standards for Better Health.

The NHS approach

- v HMRC loss, November 2007
- v David Nicholson letter, December 2007
- v Cabinet Office Interim Report, December 2007
- v David Nicholson letter, January 2008
- v Further 2 letters from Matthew Swindells of the DH
- v David Nicholson letter, May 2008
 - § Information Governance Assurance Programme
 - § Reporting of Personal Data Related Incidents
 - § Serious Untoward Incidents (SUIs)
 - § Based on the DHR final report
- v Cabinet Office Final Report, June 2008
- v David Nicholson letter, September 2008
- v IGAP closure document August 2008

IGAP

- v introduced new rules on the use of protective measures, such as encryption and penetration testing of systems.
- v standardising and enhancing the processes by which organisations understand and manage their information risk, identifying the key individuals responsible for information assets and setting out their responsibilities.
- v requiring quarterly risk assessment within each organisation of the confidentiality, integrity and availability of information.
- v introduced mandatory training for all staff involved in handling personal data, with training taking place on appointment and reinforced on an annual basis.
- v requiring the use of Privacy Impact Assessments when introducing new policy or processes that involve personal data.
- v introduced greater scrutiny and monitoring through the inclusion of information risk in Statements on Internal Control, which are scrutinised by the SHAs/Monitor
- v The formal reporting of Serious Untoward Incidents (SUI) at level 3 or above

Introduction of the SIRO

- v In setting up the IGAP the DH mandated a SIRO at Board level in all NHS organisations
- v The SIRO was further embedded into the NHS by the introduction of Control 121 in the CfH Information Governance Toolkit v.6 2008/09
- v This meant that there had to be a board level executive with the role.
- v Many NHS Trusts considered amalgamating the role into that of the Caldicott Guardian, but there are major differences in responsibilities, which have been detailed in CfH guidance, namely:

The SIRO and Caldicott Guardian roles

The SIRO

- v Is accountable
- v Fosters a culture for protecting and using data
- v Provides a focal point for managing information risks and incidents
- v Is concerned with the management of all information assets

The Caldicott Guardian

- v Is advisory
- v Is the conscience of the organisation
- v Provides a focal point for patient confidentiality & information sharing issues
- v Is concerned with the management of patient information

The IG Toolkit v.6 2008/09

- v **Released 1st July 2008**
- v **Control 121**

Does the Trust have a Board level Senior Information Risk Owner (SIRO) who takes ownership of the Trust's information risk policy, acts as advocate for information risk on the board and provides written advice to the accounting officer on the content of their Statement of Internal Control in regard to information risk?
- v No other controls really referred other than the continuing requirement within the "300" series for asset registers and general ownership of "major" assets within the organisation.
- v If the organisation is following an ISO/IEC 27001 Information Security Management Systems (ISMS) approach that would be a standard requirement.

SIRO requirements IGT v.6 Control 121

Level 1

The Trust should nominate an Executive Director or Senior Manager Board member to be responsible for ownership of information risk across the Trust and to act as the Trust's Senior Information Risk Officer (SIRO).

Level 2

An assessment of any gaps in knowledge or skills should be undertaken and training provided to ensure that the Board member assigned responsibility for information risk has the necessary skills and knowledge to be effective in their role. The Trust should also ensure that the support infrastructure for the SIRO is in place.

Level 3

The Trust should ensure the role and responsibilities of the SIRO and the infrastructure to support the SIRO is kept under review. The Board member assigned to the role should undertake and pass the strategic information

Appointing the SIRO

Important requirements

- v Board member - limited numbers available – also busy!
- v Thorough briefing note to the Board covering
 - § The role and responsibilities – JD helps
 - § How the role sits within IGAF
 - § The formal inter-relationship with Information Asset Owners and Information Asset Administrators
 - § Workable risk assessment and reporting structures
 - § The support structure provided to the role by Information Governance, especially around risk assessment , management and controls
 - § Reporting mechanisms
 - § Handling SUIs
- v Preferably someone who wants to do it

STHFT SIRO

- v Is the Director of Service Development
- v Executive Board Member
- v Member of IG Committee
- v Role presented to the Board
- v Responsibilities identified and publicised within the Trust
- v Is a focal point for resolution and/or discussion of information risk issues
- v Is supported by the IG Department
- v Is a figurehead for all major information security developments within the Trust
- v Understands the responsibilities of the role as detailed on the previous slides

[SIRO Slides](#)

The SIRO & Information Governance

With the development of the role and responsibilities of the SIRO as initially determined by the DHR, the DH and the CfH mandate through the IG Toolkit v.6 control 121, changes to the IG reporting structure were inevitable.

Whilst working practices vary from Trust to Trust, after some discussion it was decided:

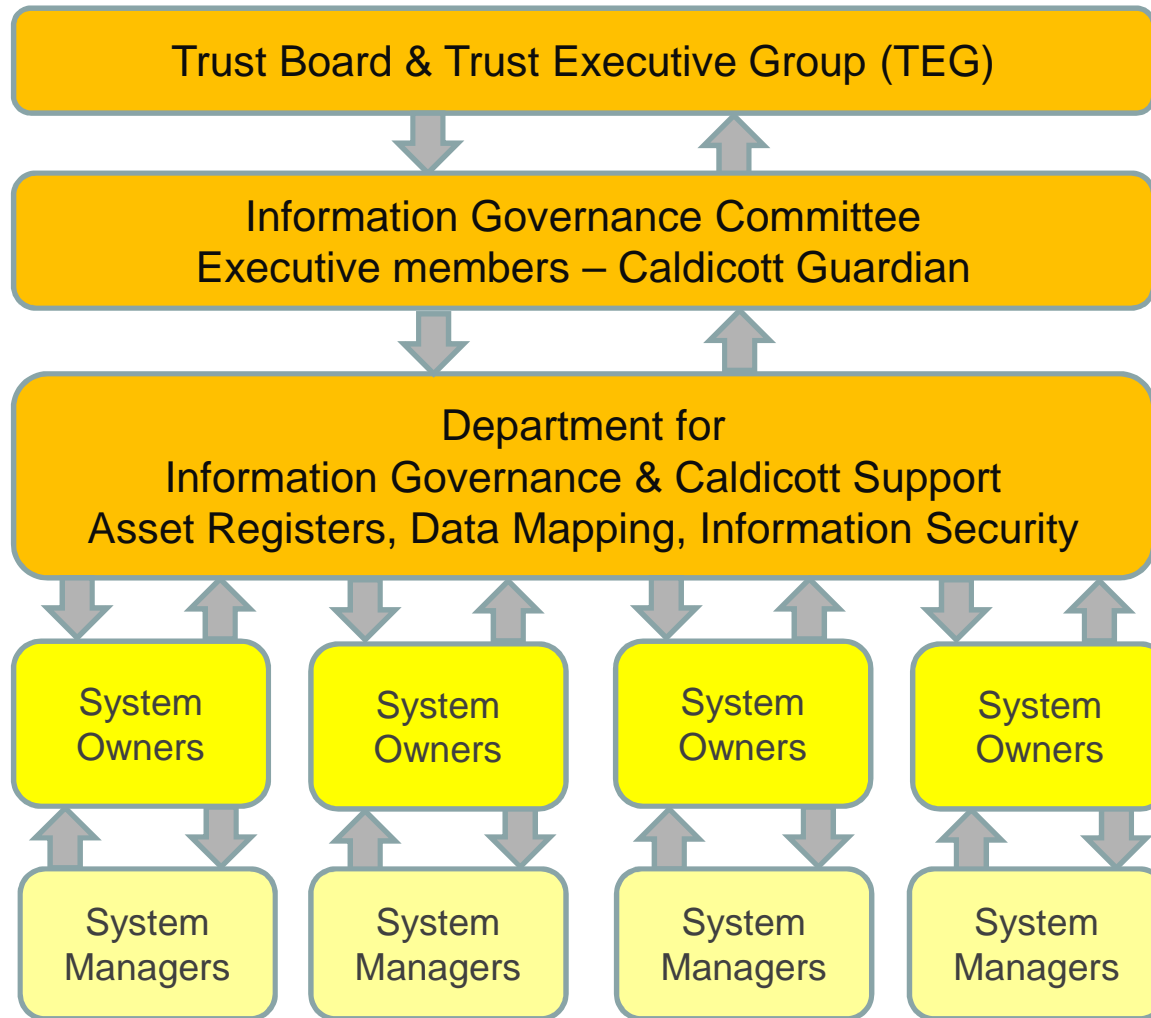
- v The SIRO would become part of the Information Governance Committee, acting as chair when necessary. This was considered important as:
 - § The IG Department has considerable expertise in Risk and Security Management including a specialist IS Manager who, like the IG Manager is ISO/27001 trained
 - § The IG Department has a high profile with regard to information risk throughout the Trust
 - § Support and reporting mechanisms are formalised through the IGC

Publicising the SIRO role

The SIRO role, its responsibilities and the reporting mechanisms, either direct or through a committee structure must be well publicised. Publicity paths include:

- v Agenda items on senior management groups such as:
 - § Trust Board
 - § Trust Executive Group
 - § Clinical Management Board
 - § Patient & Healthcare Governance Committee
 - § Corporate Governance Committee
- v Articles in the Trust Magazine, and electronic news magazines
- v A specialist Information Security broad sheet - DataSafe
- v The Trust Intranet with contact and reporting details
- v Trust induction and IG Training Programmes

The Structure: STHFT 2008/09



The next stage – IAOs and IAAs

With the SIRO responsibilities defined, developed and clarified through the IGT v.6 for the period 2008/09, major definition changes came about in IGT v.7 2008/09

Whilst these changes appeared minor, in real terms they introduced more formal reporting mechanisms and specific job roles that had to be allocated with responsibilities which require resources for training and support.

**The Information Asset Owner and
The Information Asset Manager**

IAOs in short

- v Senior individuals within the organisation.
- v Role is to understand what information is:
 - Ø held,
 - Ø added,
 - Ø removed,
 - Ø how information is moved, and
 - Ø who has access and why.
- v Consequently they are able to understand and address risks to the information assets which they 'own' and provide assurance on security and use of information.

Practicalities

Is the foregoing workable?

Does it fit with the structure of the organisation?

Does it duplicate existing systems and working practices?

Are the outcomes already achieved?

Will senior management be prepared for:

- a. Additional formalised responsibility of an IAO? JDs
- b. The training required?
- c. The knowledge base required?

Does the SIRO set up a formal reporting mechanism, or does one currently exist?

What size is a “major asset”

Who supports the proposed structure that is supporting and reporting to the SIRO?

Support for the SIRO, IAOs and IAAs

These key roles don't work in isolation. They should fit into the wider Trust structure, i.e. everybody needs to be aware of Information Governance and play their part.

Information Risk Management is a component of Information Governance but the introduction of an accountable hierarchy that sits with business/divisional managers rather than specialist staff requires a new approach within the Trust.

Among those who can provide support in identifying and mitigating information risk are the IG specialists in the organisation who are already carrying out those functions as required by the IG Toolkit

Their support should include staff training and support, advising on IAO risk assessments, advising and assisting with the delivery of controls and mitigating actions, so ensuring that the organisations approach to managing information risk is accurately reflected in the IG Toolkit assessment.

This should be a two way process, which both feeds information up through the Trust to help strategic planning and underpin corporate assurance, but also downwards to help manage risks by supporting employees and providing the necessary guidance and resources.

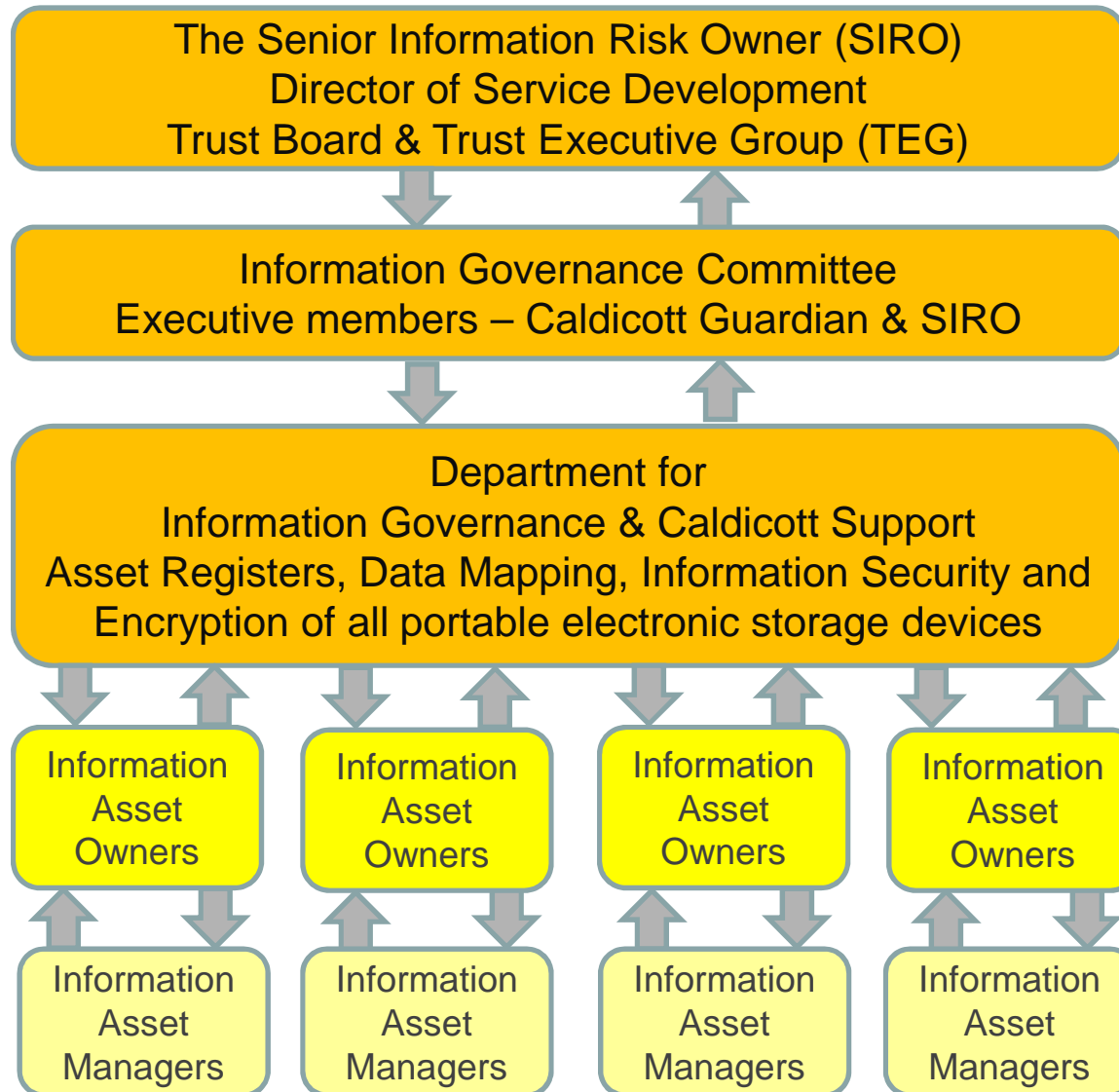
STHFT model

Based on a centralised organisation spread over two campuses

- v 5 Hospitals
- v 8 Clinical Directorates
- v 23 Clinical Specialities
- v 4 non clinical Directorates
- v 14,000 staff
- v 1 million elective admissions a year
- v A & E
- v Minor Injuries Clinic
- v Turn over circa £800 million

- v SIRO sees role as magisterial
- v IAOs at Director Level
- v Reporting and support mechanisms via Information Governance
- v Information Governance Manager is Deputy Caldicott Guardian and *de facto* Deputy SIRO

The Structure: STHFT 2009/10



In short: SIRO, IAOs, IAAs and IG

The relationship with Information Governance

- v Information Risk Management is a major component of Information Governance
- v The role of the Information Governance Department is to supply a resource to mitigate that risk by supplying:
 - Ø Advice
 - Ø Support
 - Ø Training
 - Ø Reporting mechanisms
 - Ø Risk assessment using an ISO27001 approach
 - Ø Data flow mapping
 - Ø Encryption methodology

Alternatives

Organisations may have a different approach to reach the same result

- v Decentralised organisations
- v Geographically diverse
- v Smaller
- v Specialist

There is nowhere in the guidance that mandates a method to reach compliance with IGAF or the requirements of the IG Toolkit

Training

As stated previously the Information Governance function should be able to supply training for both the SIRO and the IAOs.

The SIRO must understand his responsibilities:

- v Lead and foster a culture that values, protects and uses information for the success of the organisation and benefit of its patients
- v To own the organisation's overall information risk policy and risk assessment process, test its outcome, and ensure it is used
- v Advise the Chief Executive or relevant accounting officer on the information risk aspects of his/her statement on internal control
- v Own the organisations information incident management framework

As part of that support I consider it incumbent on the IG function to prepare an overview training package that covers the major areas of SIRO responsibility. These would include assets, risk (through threat and impact analysis), reporting mechanisms and SUIs, information risk policies and procedures.

Further Training support

Connecting for Health information Governance Training Tool is an e-learning package covering various areas of the IG spectrum such as:

- v Confidentiality & Caldicott
- v Information Governance and IG Management
- v Information Governance for NHS CFH Staff
- v Information Risk Management, which includes
 - Ø Introductory NHS Information Risk Management for SIROs and IAOs
- v Information Security
- v Records Management

To access the on line training tool you will need to register with an nhs.net or NHS specific log-in to open an account

IG Training Tool

NHS Information Risk Management for SIROs and IAOs

- Ø Completion of the course will enable a minimum score of level 2 in the SIRO control 121 of the IG Toolkit v.7
- Ø As will a certain course tutored by an external provider not a few centimetres from the Ramada Hotel

Other support documentation

It is vitally important that all related IG related policies and procedures are update to reflect the roles and responsibilities of the SIRO and the IAOs. This documentation should at least include:

- v Information Security Policy
- v Information Risk Management Policy
- v Password Policy
- v Network Policy/Secure signup agreements
- v Data Protection Policy
- v E-mail Policy
- v Confidentiality Code of Conduct
- v Records Management Policy/ Code of Practice
- v Digital Forensic Readiness Policy
- v Encryption Policy/Procedures

and where it exists

- v Mandated Procedures for the Transfer of PID and other sensitive Personal Information

The SIRO – and SIRO support

Developing an integrated SIRO support

What fits your organisation:

- § Setting up the support role
- § Who does what, where and at what level?
- § Functional reporting must be organisation wide
- § Appetite for change – is there one?
- § Organisational resistance

And don't forget the IG Department – some of us have been doing it for years!!

And we have already got there:

The Information Governance Department

The IGD has an integrated database which:

- v Records PID and other data storage with:
 - Ø Owners and administrator identity
 - Ø Risk assessment of storage security & use
 - Ø Data flows mapping
 - Ø The issue of Trust encrypted USB sticks
 - Ø Trust laptop and encryption register
 - Ø Portable storage device register
 - Ø The Safehaven register
- v This supplies integrated risk management and assessment for all IAOs and IAAs.

The IGD provides the reporting and supporting function for the SIRO required by the IGT.

In short

The SIRO

- ü **Ensures buy-in and compliance with all Trust information security issues from the Board level to the shop floor by using IAOs and IAAs, but the lynch pin is:**
- ü **that “bit” of help from the Information Governance Department**

And that “bit” includes

Increased data and information security through:

- ü Data flow mapping
- ü Risk assessment
- ü Asset registers, including business laptops
- ü Development of secure hard copy handling
- ü Encryption of all portable media devices
- ü Trust issued encrypted USB Sticks
- ü Training – induction and CPD
- ü Risk mitigation exercises
- ü ISMS – ISO27001 standards approach, and
- ü Port control

Some Statistics

- Ø Since 15/07/08 to 25/11/09, the ICO has taken enforcement action 20 times (14 construction industry in one case) and required 54 undertakings be made,
- Ø Of these 1 enforcement action and 35 undertakings relate to the NHS.
- Ø The majority of NHS failures relate to unencrypted portable media, such as USB sticks and laptops
- Ø In other words loss of personal data – breach of confidentiality
- Ø From 26/11/09 to 01/03/10 there have been 11 undertakings: only 1 relates to the NHS: are we improving?

Remember, complacency can bite

“When anyone asks me how I can best describe my experience in nearly forty years at sea, I merely say, uneventful. I never saw a wreck and never have been wrecked nor was I ever in any predicament that threatened to end in disaster of any sort.”

E.J. Smith, Captain, RMS Titanic
(writing in 1907, five years before the iceberg incident)

Peter Wilson

Contact:

**The Department for
Information Governance, Caldicott & SIRO Support
Sheffield Teaching Hospitals NHS Foundation Trust
Weston Park Hospital
Whitham Road
Sheffield
S10 2SJ**

Tel: 0114 2265151

Fax: 0114 2265152

Email infogov@sth.nhs.uk