

BUSINESS CASE FOR IMPLEMENTATION OF THE SIRO AND IAO FRAMEWORK FOR INFORMATION ASSURANCE

Introduction

It is essential that NHS Trusts and other NHS bodies implement the SIRO and IAO framework. This briefing has been prepared in order to set out the business case for accomplishing this. The HMRC major data loss in 2007 resulted in minimum mandatory actions being required in the public sector. This was sent to all NHS Chief Executives via the Department of Health. David Nicholson, the NHS Chief Executive, sent a letter to the NHS in September 2008, telling CEs of Trusts that they had to implement the mandated minimum actions from the Data Handling Review (see Page 2). There are also a number of other key imperatives which are outlined below. These include the financial and reputational impact of non-compliance. Being able to assure stakeholders of information security is a pre-requisite for world class commissioning. There is also a corporate liability risk in relation to non-compliance with the Data Protection Act 1998

Key Issues

Key Issues for the NHS include:

- Loss of unencrypted portable media with personal data
- FOI/ poor records management
- Unlawful access to personal information via blagging
- Disposal of old IT equipment such as desk top and lap top computers
- The NHS has been involved in over 100 major losses in the last year; many Trusts have had enforcement action taken against them or undertakings by the Information Commissioner
- Lack of investment will lead to poor reputation, complaints, inability to provide good services and criticism from a number of bodies
- Impact on clinical and managerial careers at all, including the highest levels

New Fines

- There is a new power for the Information Commissioner (Criminal Justice and Immigration Act 2008) which allow fines to be levied on organisations which lose or misuse personal information. The fine is likely to come into power early next year and is likely to be up to £500,000. However, the consultation document from the Ministry of Justice is seeking 'unlimited fines'
- The courts will also have the power to impose custodial sentences

The expected standards have been set out very clearly for the NHS in David Nicholson's letter below and thereafter in the Information Governance Toolkit which is required for each NHS organisation (and its partners). It is partly against these standards that fines will be levied, and inspection's conclusions drawn.

DATA HANDLING REVIEW: Recommendations

The recommendations coloured orange are to be applied by 2009/10 and guidance on these is in preparation. The other recommendations are already mandatory.

Stronger Accountability
1. Accounting officers to cover information risks in Statements of Internal Controls
2. Board level Senior Information Risk Officers (SIRO) to be appointed
3. Information asset owners to be identified
4. Information Risk Policy
5. Annual assessment of risk and performance
6. Regular assessment of risk
7. Standard contract clauses for all contracted services
Mandated Security Standards
8. Shared definition of minimum personal data requiring protection
9. Secure access to, rather than transfer of, data wherever practicable
10. Encryption to become the norm for all portable electronic media
11. Secure disposal of data and hardware when disposal is required
12. Penetration testing on systems holding data on large numbers of individuals
13. Strong access controls in new systems as they are brought on line
14. Audit trails and monitoring of user activity
15. Forensic readiness policies
16. Regular audit of compliance with policies by managers
17. Accreditation of new systems
Culture Change
18. Use of Privacy Impact Assessments for all new projects *
19. All Departments to have plans to enhance culture and to monitor progress through surveys etc
20. Mandated training for all users of personal data and those in key roles
21. HR processes to ensure appropriate disciplinary action is taken
Greater Scrutiny
22. Coverage of information risks in annual reports
23. All Departments to issue an information charter (Care Record Guarantee for the NHS)
24. Reporting process for serious incidents
25. Encouraging staff to report concerns about information risk

*where appropriate

Cost of an Information Loss

96% of large businesses/organisations (with over 500 employees) suffered a security incident last year (2008). The average cost of the worst incident for large businesses/ organisation was £1million-£2 million.

The average cost of for those organisations with less than 250 employees was £90k-£170k.

Source: Department for Business, Enterprise and Regulatory Reform

http://www.pwc.co.uk/pdf/BERR_2008_Executive_summary.pdf

The costs would include :

- informing people of loss or misuse of their information,
- the management of the media interest,
- the management of liaison with statutory bodies
- the management of the investigation the breach,
- putting in place mitigating actions,
- paying fines and costs etc
- there is also a cost to organisation reputation.

Report by the Care Quality Commission

The Care Quality Commission is working with the Information Commissioner to improve management of personal information in the NHS. The CQC has recently published a report on information management in the NHS 'The Right Information, in the Right Place, at the Right Time':

http://www.cqc.org.uk/newsandevents/newsstories.cfm?cit_id=35295&FAArea1=customWidgets.content_view_1&usecache=false

Litigation

Research by the Information Commissioner (www.ico.gov.uk) shows that the public is becoming increasingly concerned about the way in which their personal information is managed. It is also becoming an area in which litigation is likely to increase. It is likely that the legal profession will take note of the recent Max Mosley case and use privacy invasion as a case for compensation for subjects of data loss (this would result in potentially larger sums for subjects than via other routes).

Mandatory Information Governance Training

One of the actions on David Nicholson's list on Page 2 is number 20. This states that from 2009/10, there should be mandatory IG training for all users of personal information and for those in key roles. Most Trusts have decided to do this annually or every two years. For a list of useful training tools, including a mandatory training DVD, visit:

<http://www.dilysjones.co.uk/products.aspx>

Conclusions

The requirement to implement the SIRO/IAO framework is a sensible one, as it is imperative for organisations to be able to demonstrate information assurance at the highest level to inspection bodies, to the public and it is a statutory requirement for example, as enshrined within the Data Protection Act 1998 for personal information.

The cost of an information loss is considerable, financially, in workforce terms, and in terms of reputation loss.

The 'front end' implementation costs are minimal in respect of the likely costs of managing a serious incident and being fined (particularly when the new fines come into force in 2010). Many NHS organisations have achieved implementation of the framework for costs of £30k-£50k depending on size. This includes training, awareness raising and information asset identification, logging and risk assessing.

For further information on consultancy services, tools, open and bespoke courses please contact:

Katie Fairman
Dilys Jones Associates Ltd
Index House,
St George's Lane,
Ascot,
Berkshire
SL5 7ET

Tel: 01753 621961/ 01344 636388
Fax: 01753 830911

Katie@dilysjones.co.uk
www.dilysjones.co.uk and www.drfoi.co.uk

The Knowledge Leader in Information Governance