Approved July 2015

NHSS Information Security Policy Framework

Introduction

1) Antecedents and reason for change

The NHSS Information Security Policy Framework commences June 2015 to replace both the NHSS Information Security Policy (2006) and the NHSS Information Assurance Strategy (2011-2015).

The new framework differs from the former policy in terms of purpose, scope and construction in the following ways:

- For the first time there is a commitment to conforming to the International Standard ISO-27001 (2013) across all Boards as closely as possible (though it is not a requirement to be formally certified). The reason for this is two-fold. Firstly, the standard reflects best practice in information security management. Secondly, because it is an internationally recognised standard and used by organisations in different sectors it makes it easier for NHSS to convince the increasing number of information sharing partners that it is basically equivalent (even if specific controls differ from central or local government for example).
- It should so be noted that as of February 2015 the Information Commissioner Office (UK) has statutory powers to audit any NHSS Health Board. It has been agreed that where such as audit is to occur, the NHSS Information Security Policy Framework and associated controls will be used as a starting point to establish conformance to NHSS policy and adherence to the provisions of the Data Protection Act (1998) (especially but not exclusively seventh principle).
- There is a clear differentiation between the information risks (most) which are owned and managed at Board level by the Chief Executive Officer and the risks that need to be managed at national level.

- In order to achieve these ends it is not possible to have a single standalone information security policy as in the past. Instead, each Board is responsible for its own information security policy and information security objectives but must include a number of national mandatory 'components' that are agreed by eHealth Governance structures (e.g. eHealth Strategy Board).
- These components include the need to formally plan, build and implement an information security management system (ISMS), to make leadership and resource commitments between 2015 and 2017.
- Some of the mandatory components are the national controls, standards and guidance which featured prominently in the previous Information Security Policy (2006). The national control set/standards/guidance need to be constantly updated (e.g. email, encryption, online tools).
- For the first time explicit reference is made to national accreditation required for systems/services which are deemed to be of national significance in NHSS and of the university-led 'safe havens' to be used for purposes such as research. In such cases it needs to be clear that the Board or other organisations commissioning a new (or reviewing an old) service are responsible for carrying out the risk management documentation and the national accreditor for carrying out the formal process that leads to it being officially 'signed off'.

2) How does is differ from the NHSS Information Assurance Strategy 2011-2015 and the Information Security Policy (2006)?

The IA Strategy has served its purpose and the specific activities that needed to be carried out by Boards have been achieved. But many of the broader issues relating to leadership and risk management still need to be addressed.

The logic of the Information Security Policy Framework is that there needs to be a re-think about the 'engine' that is in place to deliver improvements in information security in Boards. Simply asking more and more specific activities to take place in Boards (e.g. putting in privacy breach detection tool, considering IA opportunities for Single Sign On etc.) will not necessarily lead to the level improvement required without dealing with how the entire security function is managed.

The revised IA Strategy will have as its centre-piece the need to plan, design and implement an information security management system in each Board. A great deal of effort, time and

resources is likely to be needed to put in place an ISO-27001 conformant ISMS (or improving an existing one). A two year action plan is required.

The Information Security Policy Framework is a vital part of a wider package of measures in the Information Governance Improvement Plan 2015-2017 (ranging from improvements to national scrutiny to developing better guidance for information sharing). In turn, the total package of information governance work underpins all the NHSS strategies (i.e. eHealth, Health Informatics and Research etc.).

What action is required by Boards?

The policy framework includes many things which Boards are already doing (e.g. incident management process, risk assessment, treatment plans, internal audit and following national standards etc.). But there are a number of new things to be undertaken which will require varying amounts of time, budget and change management. It is for this reason that a two-year action plan is required.

Reading across the whole framework a number of things stand out:

What is new?	**Resource/change implications for Boards**
SIRO	Assigning role to executive level person, and putting information risk high on agenda
Information Security Objectives	Written product
Information Security Policy	Written product
Determining scope	Resource to do analysis of business partnerships; and knowing where Board operations begin and end
Planning	Resource to do planning for setting up ISMS
Information Security Manager	Re-configuring post, if necessary re-grading, re-training
Participation in national groups	For Information Security Manager and/or assistants to participate in national accreditation, national public benefit and privacy panel and SWAN IA assurance so that burden of national information risk management is applied as equally as possible and not duplicated.
Communications/staff awareness	If not there already, then need to be created. Similarly, a form of mandatory information security induction

Documentation	Review and put in place better ways to manage documentation required for ISMS to run (and its business continuity). If Board decides to get formal ISO accreditation then it will not succeed without effective records management.
Information Asset Register	Even at a high level this can be labour-intensive to set up.
Change over to information risk assessment template	To ensure that Board employees and third parties use the NHSS standard template, and make reference to the national control set. And to routinely use the national impact levels.
National accreditation	Requirement to do risk assessment following national template prior to accreditation work.
National controls	Requirement to take on many more controls at national level in the light of cross-Board risks such as updating software, hardware, authentication for patients to online services etc.
National reporting	Requirement to do national level reporting of significant incidents
Performance and audit	Requirement to beef-up internal audit function so that it can deal with auditing on information security management system at regular junctures. If not already to have robust processes in place for incident analysis and evaluation.
Management review	For executive sponsored reviews of the ISMS, for incorporation of progress (and mitigation of risks following significant incidents) to be covered in management board meetings, in annual reports etc.

Government

What is new?	**Resource/change implications for SG?**
SG review high level review of progress against framework	Information Security should already be discussed in general terms as part of mid-year and annual eHealth Plan reviews. Should also be a formal external review of progress specifically against information security policy framework. ICO to conduct own audits as and when required. It will use the policy framework as starting point for discussions around conformance.

Accreditation of significant systems/services including Safe Havens	Qualified persons able to carry out the accreditation to the satisfaction of governance structures (especially Public Benefit and Privacy Panel).
National Risk Register and risk acceptance criteria	Information gathered as part SG reviews, ICO enforcement, incidents and other sources.

ANNEX A: Case studies for implementation of framework

1) Leadership

The Board has a Caldicott Guardian who is responsible for advising on how patient data is handled and the purposes to which it is used internally and whether shared externally. The CEO recognised that this function needed to continue, but also assigned the role of SIRO to the Director of Corporate Services who sits on the executive management board so that the whole information risk landscape (not just patient identifiable information) could be considered and to report on the performance of the ISMS in line with the NHSS information security policy framework. Neighbouring Board Y took a slightly different approach and asked the Caldicott Guardian, who already sits on the executive board as Clinical Director to also take on the role of SIRO (with additional training relating to corporate information risks). The outcome is the same in both cases: information risks – relating to patient, employee and corporate information - are being managed in a more holistic way across the organisation and high level management reviews are taking place of the entire ISMS (not just getting a report from a head of ICT).

2) Information Security Objectives

The Board already has its own information security policy and there has been an ongoing programme of work relating to security (some of which stems from the NHSS Information Assurance strategy 2011-15). But given the significant new demands on the security function (new services, new applications and new cyber threats etc.) and a pattern of security incidents, it was important that a set of objectives were set out by the CEO and for progress to be covered in the annual report.

3) Information Security Policy

The Board high level security objectives, along with results of recent evaluation, audit and management review led to the existing policy being revised. New national-level controls and standards (e.g. encryption of portable devices and national reporting process) were included along with Board-specific policies (e.g. use of social media and use of staff ID cards). The policy used the same format as the national framework. This meant that external auditors such as the ICO could compare Boards more easily.

4) Information Security Management System

4.1 Scope

The Board works increasingly closely with a local authority and shares the IT network (SWAN) and many services. But an emerging problem is that employees are not always clear which organisation's security policy they should be following and who is responsible for managing the security function. After a review it was made clear that the Board ISMS was separate from the local authority ISMS (with staff following policy of their respective organisations). There were some differences in the two organisations' overall information security policy (though both followed basic elements of IS0-27001), but the information sharing agreement and guidance for the particular shared services ironed these out (i.e. the 'rules' that both sets of staff needed to follow when accessing a particular IT application.

4.2 Planning

The Board has experienced several organisational structure changes in recent years and the information security team has moved from IT division to Information Governance to corporate services and back again. When planning for the ISMS it was decided that the dotted lines and business processes which criss-crossed the whole Board were more important than where the information security function was physically based. It was decided that the information security manager could be located close to IT personnel but should report directly to the Head of Information Governance (who in turn reports to the SIRO) to ensure there was candour in relation to problems with IT and ensure that there was no artificial separation between 'IT security' and the other wider information risks that the ISMS needs to address (e.g. paper files, legislative compliance).

4.3 Resources

The Board had a longstanding IT Security Officer role. Subsequent to the creation of the SIRO, security objectives and commitment to having ISO-27001 conformant ISMS, a review was made of resources. It was agreed that the role needed to be re-configured into an 'Information Security Manager' and for the grade to reflect the new responsibilities and standing. The current post-holder needed to undergo further training and accreditation (e.g. information risk management and Information Security Management Principles exam) and thereafter it was clear that a future post-holder needed to have the appropriate skills and experience for this specialist (not general administrative) post.

4.4 Staff awareness and training

The Board took the opportunity when putting in place its ISMS to cultivate better relations with the Communications Team and put in place new processes. Apart from having a separate information security area for its content on the corporate Intranet which it could manage itself (such as policies and guidance) like HR, Finance and other functions, it was also agreed that specific targeted messages (on incident status, general news etc.) could be placed on the front page when required in a timely manner. Although it was recognised that clinicians and other professional groups went on various inductions that related to security and Information Governance, the SIRO agreed that all new employees and contingent workers needed to complete the 20 minute online module that outlined the key security policies and procedures. Meta-compliance tools helped to show where such modules were completed by staff. Completion of a basic 'test' is not evidence in itself of compliance to policy so the SIRO asked specifically for analysis during the regular evaluations, audits and management reviews how far this control was working (i.e. leading to less incidents in areas covered by training such as use of mobile devices, data handling etc.)

4.5 Documentation

The Board's series of structured shared drives are designated as the corporate records management system. As part of the planning for the ISMS an opportunity was taken to make clearer how far the ISMS activities translated into the functions, activities and transactions on the file plan. Legacy records were reviewed and disposed of and permissions updated so that only those who needed to access the ISMS documentation was able to do so. An opportunity was also taken to identify and manage vital records relating to the ISMS (e.g. codes, cryptography, contacts for key vendors etc.) so that they could still be accessible should there be a problem with the shared drives.

5) Information Security Risk Assessment

The Board executive was nervous at the prospect of compiling an information asset register given the scale and complexity of the operations over several hospitals, dozens of GPs practices and other sites. The approach was to include only the most significant assets (e.g. data on the Patient Administration System, data held on local and national PACS etc.). But even this high level IAR meant that there could be better prioritisation in terms of when to carry out information risk assessment and put in place treatment plans (i.e. on the higher impact).

When carrying out risk assessment the Board used the standard NHSS template, and used the national 1-5 impact scale. All significant new services/applications were required to have an information security risk assessment at the right juncture in the project life-cycle (and prior to release into the live environment).

6) Information Security Risk Treatment Plan

The Board uses several risk treatment plan formats, but all follow the same basic methodology and use the ISO-27001 generic control objectives and controls, and consideration of the NHSS national level controls and standards. Some of the risk management and accreditation documentation is undertaken by third party specialists. In such cases it was vital to make them aware of relevant NHSS-specific national controls/standards that needed to be implemented and the national guidance that needed to be considered.

7) Performance evaluation

The Board's re-configuring of the Information Security Manager role, the new role of SIRO and the executive commitment to the ISMS, meant that the ongoing evaluation (which had previously taken place but in an ad-hoc manner) was subject to more robust criteria. This included a monthly review of information security incident reports, data from privacy breach detection tools, feed-back from staff and patients and opportunities for the Information

Security Manager and his colleagues to air concerns to senior management at particular junctures (e.g. weekly) and after significant incidents.

8) Audit

The Board has an existing internal audit function. It was decided at an executive level that information security must be an integral part of the annual audits (rather than something which was occasionally picked up on the side lines in the past). The current auditors, from a finance career home, required some re-training so that they could perform the task. The scope was heavily geared towards what ISO-27001 expects in terms of design of ISMS (documented as being in place) and the various metrics that can suggest how well it is working (e.g. incident reports, uptake of staff training and statistics relating to specific controls such as malware detection/removal. One of the many positive aspects for the Information Security Manager was that the issues picked up during regular evaluation were escalated to senior managers by persons seen as truly independent (i.e. gives added weight to argument for changes needed).

Some of the outputs from the audits featured in the Board annual report (in interests of transparency) and could also be used to explain to The Scottish Government progress in regard to national information security objectives in eHealth.

9) Management review and improvement

The Board ISMS, conforming to ISO-27001, was relatively new and periodically the whole system needed to be reviewed to see if it was working as planned. Some recent bad publicity in regard to security incidents and enforcement notices by the Information Commissioner gave impetus to a review that led to a package of measures such as better reporting at executive board level, ensuring that key information security posts were filled when persons retired and doing information risk assessments on some existing legacy systems and not just new services.

Subject to resource, SG would also offer an external review of progress so as to report back to CEOs and the eHealth Strategy Board on progress.