Director-General Health & Social Care and
Chief Executive NHS Scotland
Derek Feeley

The Scottish Government

Dear Colleague

NHSSCOTLAND INFORMATION ASSURANCE STRATEGY

CEL 26 (2011)

15 November 2011

Addresses

For action:
NHS Board Chief Executives

For information:
eHealth Leads
Information Governance Leads
Caldicott Guardians

Summary

1. The NHSScotland Information Assurance Strategy (IA) sets out the strategic direction for further developing our IA capability and effectively embedding an IA culture across NHSScotland.

Background

2. The Strategy reflects a commitment within the eHealth Strategy. It builds upon agreement with the CEOs and the eHealth Strategy Board that it should be developed and its contents reflects the outcome of significant consultation with NHSScotland Boards.

3. NHSScotland is transforming the way it uses information, sharing considerable amounts of data and joining up services and IT systems on an unprecedented scale. These changes are key underpinnings of the Quality Strategy. The IA Strategy emphasises that Boards need to focus in using the information they hold, wisely and well as well as responsibly and with care. In this context Boards recognise the importance of the availability, integrity and confidentialty of information and its duty of care in relation to the information it uses.

4. NHS Boards continue to make improvements around the security and confidentialty of information. However Boards also agree on the need to focus more effort on changing the culture, behaviours and the key strands of Integrity and Availability of information as services become more reliant on IT for the delivery of care. The IA Strategy and its associated Scottish Government-supported improvement programme addresses each of these aspects.

Action

CEOs are asked to:

1. Continue to assure themselves that robust mechanisms are in place to demonstrate information assurance maturity within their Board.

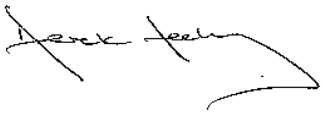
2. Disseminate the strategy to those responsible for implementing the information assurance strategy locally.

Enquiries to:
eHealth Information Assurance Team
eHealth Division
St Andrew's House
Regent Road
Edinburgh EH1 3DG

Tel: 0131-244 -2351
Email:
eHealthInformationAssurance@scotland.gsi.gov.uk

Further copies of this CEL can be downloaded from:
http://www.show.scot.nhs.uk/

Yours sincerely



Derek Feeley
Director General Health & Social Care and Chief Executive NHS Scotland

NHSScotland

INFORMATION ASSURANCE STRATEGY

2011 – 2015

INTRODUCTION

1. Information is a vital tool for NHSScotland. The effectiveness and safety of care and the efficient management of healthcare services depend on information.

2. We have a duty to use personal and business information *Wisely and Well* as well as *Responsibly and with Care. Wisely and well* ensures that the right information is available to the right people at the right time. If it is in the interests of a patient that information is available we must commit to finding ways to ensure it is made available.

3. *Responsibly and with care* reflects the sensitivity of much of the information that NHSScotland needs to do its job. This is reflected in the legal and professional duties about confidentiality that guide our actions. This care is about the whole organisation and is as much about the appropriateness of the conversation in the corridor or over the telephone as it is to a paper document or an electronic message. It is everyone's job not just the job of IT or of Medical Records.

4. NHSScotland recognises the importance of the availability, integrity and confidentialty of information and its duty of care in relation to the information it uses. NHS Boards have invested in improvements in these areas and will continue to do so, to meet rising UK and European legislative requirements. The Information Assurance Strategy reflects the increasing value of information to the Scottish NHS and the collaborative way in which it is used and shared.

5. NHSScotland is transforming the way it uses information, sharing considerable amounts of data and joining up services and systems on an unprecedented scale. In addition, the UK Government is demanding greater openness and transparency from public sector bodies at a time when the public are more anxious about the ubiquitous use of their data. Against this rapidly advancing and changing environment, Boards need to deliver confidence that their information is held securely, appropriately, maintained accurately and is available when necessary. These requirements reflect what is defined as Information Assurance (IA).

PURPOSE

6. The purpose of this strategy is to set out the strategic direction for further developing information assurance capability and effectively embedding an IA culture across NHSScotland.

7. The Strategy supports the new eHealth Strategy 2011-2017 (Annex A) and aims to guide improvement in three broad areas: availability, integrity and confidentiality.

Information Assurance		
Confidentiality We protect information from unauthorised disclosure and ensure that we only hold information that we need and have a right to retain	**Integrity** We ensure that the data we hold is correct, current, & can only be modified by authorised users with clear audit trails	**Availability** We ensure that the data needed is there when its needed
Board Governance of IA Clear lines of accountability & roles and responsibilities Awareness & Education of all employees Codes of Practice: confidentiality , Health records management, HR, IG & acceptable use policies Information sharing protocols Fair processing Privacy impact assessment Identity & access management	Development & implementation of Clinical & Administrative systems & workflows Data Quality Classification of Information & application of applicable security controls System Audit & monitoring Software & hardware-based solutions to protect information systems Corporate records management	Development & implementation of Clinical & Administrative systems & workflows Risk Management Business continuity Incident reporting & response procedures Service & operational level agreements. DR plans and wider IA activity are clearly articulated Technical system performance. IT operational environment maintenance FOISA Compliance procedures

This Information Assurance strategy sets out a coherent approach to managing information by making it an integral and effective part of normal business processes.

VISION

That the NHS in Scotland gets the best out if its information, moves forward and develops its use, confident that the risks associated with collecting, holding, using and sharing information are well managed. NHSScotland arrangements carry the trust and confidence of both patients and NHSS employees.

PRINCIPLES

NHSScotland believes that accurate, timely and relevant information is essential to deliver the highest quality healthcare. As such, it is the responsibility of all NHS employees to ensure and promote the quality of information and to actively use information in decision making processes.

NHSScotland aims to strike a balance between principles of corporate governance and public accountability, placing importance on confidentiality and security arrangements to safeguard both personal and business information.

NHSScotland recognises the need to share patient information internally, across NHS Boards and with key partners in a controlled manner consistent with the interests of the individual(s) or in the public interest to protect an individual(s) or society from risks of serious harm such as child/adult protection, serious communicable diseases or the prevention and/or detection of a crime.

STRATEGIC ACTION

The following four areas are consistently[1,2] seen as key to delivering successful information assurance:

1. Leadership and Governance
2. Information Risk Management
3. Policy and Operations
4. Monitoring and Compliance.

The table below illustrates the key areas of activity:

Key Areas and elements for Success in Information Assurance				
	Leadership & Governance	**Information Risk Management**	**Policy & Operations**	**Monitoring & Compliance**
Human Factors	Strategy, Vision & Direction Clear lines of accountability	Board governance of IA	Awareness & Education of all staff Structure, Roles, Responsibilities Skills & expertise	Internal & External Audit
Policy /Practices	Information to public e.g. HRIS Clear & Robust methods for communicating & enforcing policies & procedures	Incident reporting Classification of Information & application of applicable security controls Information Risk Management Disaster Recovery Business Continuity Privacy Impact Assessment	Business Continuity Identity & access management HR, IG & Acceptable Use policies Service & operational level agreements DR plans & wider IA activity are clearly articulated within contracts with suppliers.	Statement of Internal Controls IG walk rounds IG standards Breach detection & reporting
Technology	Key strand of IT strategy	IT security risk assessment	System Audit & monitoring Software & hardware-based solutions - to protect information systems IT infrastructure maturity model IT operational environment maintenance (virus & malware protection)	IG toolkit Verification & Testing

The actions under each area where delivery can be strengthened are:

[1] Information Assurance Maturity Model: CESG
[2] The Coleman Report: Independent Review of Government Information Assurance: June 2008

1. Leadership and Governance

Outcomes: Information assurance responsibilities are assigned from the Board downwards to ensure information as a business asset is balanced with other business drivers at every level of the organisation.

Information Assurance will be **understood**, **visible** and **accessible** to all NHSS employees and will be embedded in the culture of NHSScotland both nationally and locally, aligned across NHSS Boundaries.

Clearly defined and understood roles and responsibilities in which appropriately skilled staff are held accountable for their decisions and actions. Individuals recognise the relevance of information assurance to them and their own responsibilities. Information assurance is seen as an enabler and an integral part of NHS operations, rather than a restriction.

Actions:

Boards to review local arrangements to ensure clearly articulated lines of responsibility and accountability for both clinical and business information.

Simplify the number of IG forums. Establish an SG supported Information Assurance Forum to develop co-ordinated joint working, sharing best practice and establishing information assurance priorities across NHSScotland.

2. Information Risk Management (IRM)

Outcomes: A proportionate risk management approach embedded in the organisation. Information risk managed throughout the Board in a structured way for clear understanding of risks, threats, vulnerabilities and impact on the business. The risk management framework will be aligned to the Boards corporate risk management framework.

Identify, manage, action and learn from the risk experiences of other NHS organisations.

Assess risk continuously and be aware of up and coming risks.

Actions:

Commission a review of current Board risk management mechanisms, identifying best practice and make recommendations. Profile is raised to CEO and Audit Committee level.

3. Policy and Operations

Outcomes: Requirements/minimum acceptable standards, are articulated to employees and supply chain partners through clear polices based on best practice standards. The standards will be clear, well communicated and readily available.

IA standards, policies and processes continue to evolve to remain current with NHSS national and local objectives and priorities.

A range of IA control measures are implemented in a cost effective way to reduce the vulnerability of information systems to compromise throughout their life cycle.

Deal with incidents in a way that reduces the business impact, including:

- putting in place service and operational level agreements for all business critical services.
- embedding security policies and procedures into national and local delivery contracts with suppliers.
- having access to technology that is affordable, secure and reliable. Have re-usable solutions that are built on 'best of breed' and where others already have experience of their effective use.

Access to personal and business information is correctly managed and safeguarded including creation, storage, transmission and destruction.

Key personnel have the knowledge and experience to be able to build, design and deliver information assurance at local level and with key stakeholders.

Actions:

- Continue to support Health Rights Information Scotland to develop and publish awareness material for the public relating to eHealth, confidentialty and access to health records.

- Commission the production of core NHSScotland information assurance foundation level educational material. Boards to consider using Cabinet Office online training modules as interim measure.

- Work with Human Resources to review key documentation including the data protection/confidentialty statements in employee contracts and information retention policies.

- Support further training for appropriate staff in the following areas: investigations, forensic readiness and risk management & Privacy Impact Assessment.

- Work with NHS Boards to develop an information classification scheme reflecting the breadth of the information processed by NHSScotland that aligns with key partners such as Police and Local Authorities and enables the application of appropriate security controls.

- Work collaboratively to simplify, standardise and document working practices required to support the shared services agenda.

- Acquire and implement specialist Single Sign On software to better manage user identity and system access.

- Acquire and implement privacy and security breach protection software to enable NHS Boards to strengthen their existing privacy surveillance and breach detection and audit capabilities.

4. Monitoring and Compliance

Outcome: Effective compliance mechanisms provide positive assurance that Board policy is being implemented in an effective way to achieve the desired outcomes.

Actions:

Review of the current IG standards and toolkit and their fit with board level compliance IA activity.

Annex A

CONTRIBUTION OF INFORMATION ASSURANCE TO THE NEW EHEALTH STRATEGY

eHealth Strategy Objectives[3]	How does Information Assurance contribute to eHealth Strategy?
1. Maximise efficient working practices, minimise wasteful variation, bring about measurable savings and ensure value for money	IA is not solely about compliance; there is also a strong efficiency element to it; e.g. cost avoidance through continuity planning, avoiding duplication of processes, improving data quality brings clinical benefits as well as increased security.
2. Support people to communicate with the NHSS, manage their own health and wellbeing, and to become more active participants in the care and services they receive	Raising awareness of eHealth and the benefits it can bring. Individuals will make greater use of technology if they are confident that the mechanisms used to share data are safe and secure.
3. Contribute to care integration and to support people with long term conditions	Greater utilisation of new digital methods for self-management (e.g. social media via broadband); and that if used in a secure and controlled manner they can empower patients for example online appointment bookings which are cheaper than traditional methods.
4. Improve the availability of appropriate information for healthcare workers[4] and the tools to use and communicate that information effectively to improve quality	Information Assurance enables data sharing to take place regardless of physical boundaries based on the data protection and Caldicott principles.
5. Improve the safety of people taking medicines and their effective use	Making the right information available to the right people at the right time irrespective of physical boundaries and taking into account the data protection and Caldicott principles.

[3] eHealth Strategy 2011-2017: http://www.scotland.gov.uk/Publications/2011/09/09103110/0

[4] The World Health Organisation defines a healthcare worker as anyone whose focus or activity is to improve health. The definition includes doctors, nurses, midwives as well as technicians and managers.

Annex B

NHSS INFORMATION ASSURANCE CURRENT AND PROPOSED IMPROVEMENT ACTIVITY

Area key to success	Areas identified by Boards for focused improvement activity	Current national improvement activity	Proposed future improvement activity
Leadership/ Governance	Acknowledgement that strong visible leadership at board level is essential. However, others also have a role to play such as the Caldicott Guardian custodian of patient identifiable data or Information Asset Owner (Staff with service based responsibility for information assets.) Skilled and competent IG practitioners[5] are essential to providing assurance to CEO`s. Greater collaboration between IG practitioners, infrastructure and eHealth leads to drive forward IA agenda at local and national level.	NHSS Caldicott Guardian Forum established to facilitate the legitimate sharing of the patient identifiable information intra NHSScotland and with key partners. SG continues to support the IG Practitioners through the provision of specific guidance e.g. NHSScotland Caldicott Guardian Manual and new website.	Boards to review local arrangements to ensure there are clearly articulated lines of responsibility and accountability for both clinical and business information**.** Establish an SG supported Information Assurance Forum to develop co-ordinated joint working, for sharing best practice and establishing Information assurance priorities across the NHSS.
Information risk management	Greater focus needs to be placed on the approach to identification, reporting and management of risks and sharing collective learning from incidents.		Boards to ensure robust risk management frameworks in place, which feed into service plans and the development of appropriate controls. Profile is raised to CEO and Audit Committee level. It is recommended that the Strategy Board supports further discussion with CEO`s regarding the mechanisms for central incident reporting.
Training, Education and Awareness - Public	Important to raise public awareness of development and benefits of eHealth. Health Rights Information Scotland public information leaflets were seen as a valuable vehicle for promoting a consistent public message.	SGHD commissioned Health Rights Information Scotland to develop a leaflet and short animated clip outlining the eHealth agenda. This work is complete.	Existing wider activity seen as sufficient.

[5] Information Governance Practitioner includes: Caldicott Guardian, Data Protection Officers, Information Governance Managers, IT Security Officers, Health Records & Freedom of Information Leads

Area key to success	Areas identified by Boards for focused improvement activity	Current national improvement activity	Proposed future improvement activity
Training, Education and Awareness - Staff	Beyond the Board it was recognised that every member of staff has a personal responsibility to adhere to their professional codes of conduct and/or practice in respect of good information management including participation in information governance training relevant to their job role. Future work should challenge 'custom and practice'. This could be achieved by NHS specific package which: • clearly articulate NHS expectations • reads across to existing material such as NHSScotland Code of Practice on Confidentiality. • case study based and capable of being delivered in a range of formats. • dovetailed with the existing mandatory learning packages for junior medical and nursing staff. • capable of being used by Higher Education Institutions, to influence practice from the outset. Continue to extend NHS Board staff skills in the following areas: • investigations • forensic readiness • risk management & Privacy Impact Assessment Enhance skills of Band 2 AfC Health Records staff.	Approaches currently vary across Boards depending on the resources available. A small number of Boards have purchased commercial generic online packages, however their content and success is unknown. SG has commissioned NES to develop core NHSScotland information assurance foundation level educational material. This work is now underway and is anticipated to be complete by Nov 2011 A revised Code of Practice on Confidentiality is in the final stages of preparation. NHS Education Scotland has completed work to extent the existing IA material within DOTS. It will be launched in August 2011. NHSS IG Team have facilitated training days held for risk management & Privacy Impact Assessment (PIA). The certificate of technical competence training programme for health records staff is currently being rolled out across NHS Boards.	Boards to consider using Cabinet Office online training modules as interim measure. SG will continue to work with NES & key stakeholders to review and update the IA material within "Flying Start". It is recommended that Strategy Board supports further training for appropriate staff in the following areas: investigations, forensic readiness and risk management & Privacy Impact Assessment.

Area key to success	Areas identified by Boards for focused improvement activity	Current national improvement activity	Proposed future improvement activity
Policy and Operations	*Policies and procedures:* Consensus that the SG produces clear and concise core policy independently of the implementation (local boards have own which are compatible with the national one) Policies and procedures should: • align with professional bodies codes of practice and guidance • explicitly state "rules of game" • greater collaboration internally with appropriate groups of staff e.g. HR Divided opinion on NHSScotland wide core policies and procedures. If this route were to be pursued this should be done on a collaborative basis. Acknowledgment that the ability to successfully apply sanctions against individuals depends on the robustness of board polices and procedures. Boards have well established mechanisms in place to disseminate information about good information management and incidents. Robust methodology in place to assess the business impact of access to information and apply the correct protection, handling and disclosure instructions. Where possible, exploit 'single sign-on' mechanisms to support management of electronic access to information	eHealth is currently reviewing and rationalising the department circulars relating to information governance. Revised NHSS Records Management Code of Practice and 7 practical guidance notes were published in August 2010. Work with Human Resources to review key documentation including the data protection/confidentialty statements in employee contracts and information retention policies. Work programmes for Caldicott Guardians, Data Protection Officers, IT Security Officers and Health Records Managers have been re-established. Work underway to utilise intelligence from the IAM programme to develop, standards, streamline and improve processes for staff identity and role management. SG is supporting an NHS Board led	Consult on the development of core NHS "rules of the game" Establish an IA Group who are commissioned to carry out discrete pieces of work to rationalise and harmonise board level policies and procedures within a given time frame. NHS Boards may wish to consider utilising a policy compliance software to enhance current methods for communicating and enforcing policy at a local level. Work with Boards to develop an NHSS wide information classification scheme which aligns with key partners such as Police and Local Authority and enables the application of appropriate security controls.

		commission for the procurement of a single sign-on solution, on behalf of all NHS Boards.	
	Infrastructure optimisation workshop to look at current IT infrastructure and operations	Number of propriety areas for improvement identified by Boards. Improvements plans developed by Infrastructure Leads.	Greater focus on simplifying, standardising and documenting working practices is required to support the shared services agenda.
		Work continues to develop an NHSS Infrastructure strategy	Boards to review that Service level Agreements and Operating Level Agreements are established for all business critical services and that these include reference to archive, back up and restore process and recovery times
	Developments in technology and communication technologies. Acknowledgement that employees and boards need to understand and respect the power, limitations and technical controls of mobile devices.	Deliberations of implications of Web2 and "Cloud" underway.	
Policy and Operations	**System Audit and monitoring**: General support for introduction of a software package which could assist with system audit of staff activity. Acknowledged this was not " silver bullet" but was a good deterrent.	SG is supporting an NHS Board led commission of a specialist tool to support audit log analysis, on behalf of all NHS Boards, building on the knowledge gained from those who already have purchased the tool.	Expectation that the audit procured tool will be progressively implemented in tandem with associated people management.
Monitoring & Compliance	Work to date had focused on traditional IG activity. Going forward need to review whether the current IG standards and toolkit remain fit for purpose and the extent to which they are embedded into local IA compliance activity.	Some Boards have introduced information governance walk rounds. These were had been well received by operational staff, leading to changes in practice.	NHS Boards to consider the introduction of a information governance walk rounds, involving other NHS Boards IG practitioners.
		eHealth is participating in the discussions with HIS and SG H&SC Quality & Safety colleagues to develop an integrated, risk-based, proportionate approach to governance for NHSScotland.	It is recommended that Strategy Board supports a review of the current IG standards and toolkit and their fit with board level compliance IA activity.