

Information Governance

2014 Review of Activity

Author: Christina Munns

Date: March 2015

Contents

Contents	2
Purpose	3
Background & Overview	3
Workstream 1: Assuring the HSCIC's Handling of Information	5
Workstream 2: HSCIC's Internal Compliance & Assurance	6
Workstream 3: National Infrastructure Assurance	7
Workstream 4: System-wide Support	8
Action Required of the Board	11

Purpose

The purpose of this paper is to:

- a. update the Board on strategically significant Information Governance (IG) activities undertaken in 2014, and
- b. propose that, following a year of responding to the new legislative framework now is an opportune time to develop an IG Strategy to ensure that IG is used to transparently drive continual improvement, reinforcing the HSCIC's key value of trustworthiness.

The Board is asked to note progress to date and to comment on proposed future activities.

Background & Overview

“Over the past year, the subject of IG has moved from the backwaters of organisational management into the mainstream of public discussion.”¹ The Health and Social Care Act 2012 set the scene for this change. The HSCIC has acted with appropriate urgency in response. The Health Select Committees and *Partridge Review*² provided further opportunities to respond. Following this period of stabilisation, the HSCIC is now in a position where it can be proactive in order to improve IG's contribution to the business, both internally and externally. The December 2014 publication of the Code of Practice on Handling Confidential Information³ signalled this readiness, outlining good practice for which the system must have regard when collecting, analysing, publishing and disseminating confidential information.

The HSCIC has acted internally to show significant progress in areas such as data dissemination, as recognised by Sir Nick Partridge's report⁴. Following the publication of strategic drivers such as Dame Fiona Caldicott's reports⁵ and the National Information Board's (NIB) *Framework for Action*⁶ the HSCIC has been entrusted with system-wide roles in the areas of Cyber Security, IG Toolkit re-launch and development of the Information Governance Alliance (IGA). In parallel, IG has become more prominent within the broader informatics sphere. Following the Informatics Governance and Accountability Review (IGAR)⁷ a system-wide backdrop was created, providing a governance structure for handling system-wide IG issues.

A three-pillar model for handling system-wide IG issues emerged. It comprised of a strategy, delivery and oversight pillar. The key players within each were the National Information Board, the IGA and Dame Fiona Caldicott's Independent IG Oversight Panel (IIGOP), respectively. The HSCIC IG function is actively involved within each pillar, particularly within the delivery pillar, as host to the IGA.

The HSCIC was also host to the Caldicott Implementation Monitoring Team, which submitted evidence to Dame Fiona Caldicott's IIGOP to inform her *The First Year Report* to the Secretary of State for Health. There were three firm recommendations in this report which concluded that the health and social care landscape “could do better” when implementing the recommendations; that the focus should be on fair processing, consent management and leadership.

It is the IIGOP's three recommendations and the NIB's *Framework for Action* which has formed the basis of the IGA work plan. The IGA is committed to working in partnership to provide authoritative point of IG guidance for the health and social care system.

Each of the roles that the HSCIC play in support of the whole system is also undertaken internally - both in support of its internal compliance and assurance responsibilities and in assuring the HSCIC's information handling activities. Similarly the HSCIC provides assurance, advice and guidance to protect the national infrastructure it delivers.

¹ Dame Fiona Caldicott The Independent IG Oversight Panel Report: The First Year, December 2014
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/391533/iigop-annual-report.pdf

² <https://www.gov.uk/government/publications/review-of-data-releases-made-by-the-nhs-information-centre>

³ <https://systems.hscic.gov.uk/infogov/codes/cop>

⁴ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/380042/HSCIC_Report_Summary_of_progress_261114_FINAL.pdf

⁵ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf and

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/391533/iigop-annual-report.pdf

⁶ <https://www.gov.uk/government/news/introducing-personalised-health-and-care-2020-a-framework-for-action>

⁷ <http://www.england.nhs.uk/iscg/wp-content/uploads/sites/4/2014/02/ISCG-009-006.pdf>

Information Governance: 2014 Review of Activity

There are, therefore, four streams of interrelated work at the core of the IG programme which aim to facilitate the delivery of HSCIC's core values:

1. Assuring the HSCIC's 'handling' of information;
2. HSCIC's internal compliance and assurance;
3. National infrastructure assurance;
4. System-wide support.

These work streams not only have important relationships and overlaps with the broader care system as described above but also with each area of the HSCIC. After a year of focussed improvement activities it is suggested that the intelligence and learning from these work streams could drive organisation-wide efficiency and continual improvement (see Figure1), positioning IG as a positive enabler as opposed to being perceived as a 'blocker'. It is for this reason that we suggest that in 2015 the HSCIC develops an organisation-wide strategy for IG and a Strategy Delivery Group which monitors the implementation of the strategy and the policy framework underpinning it.

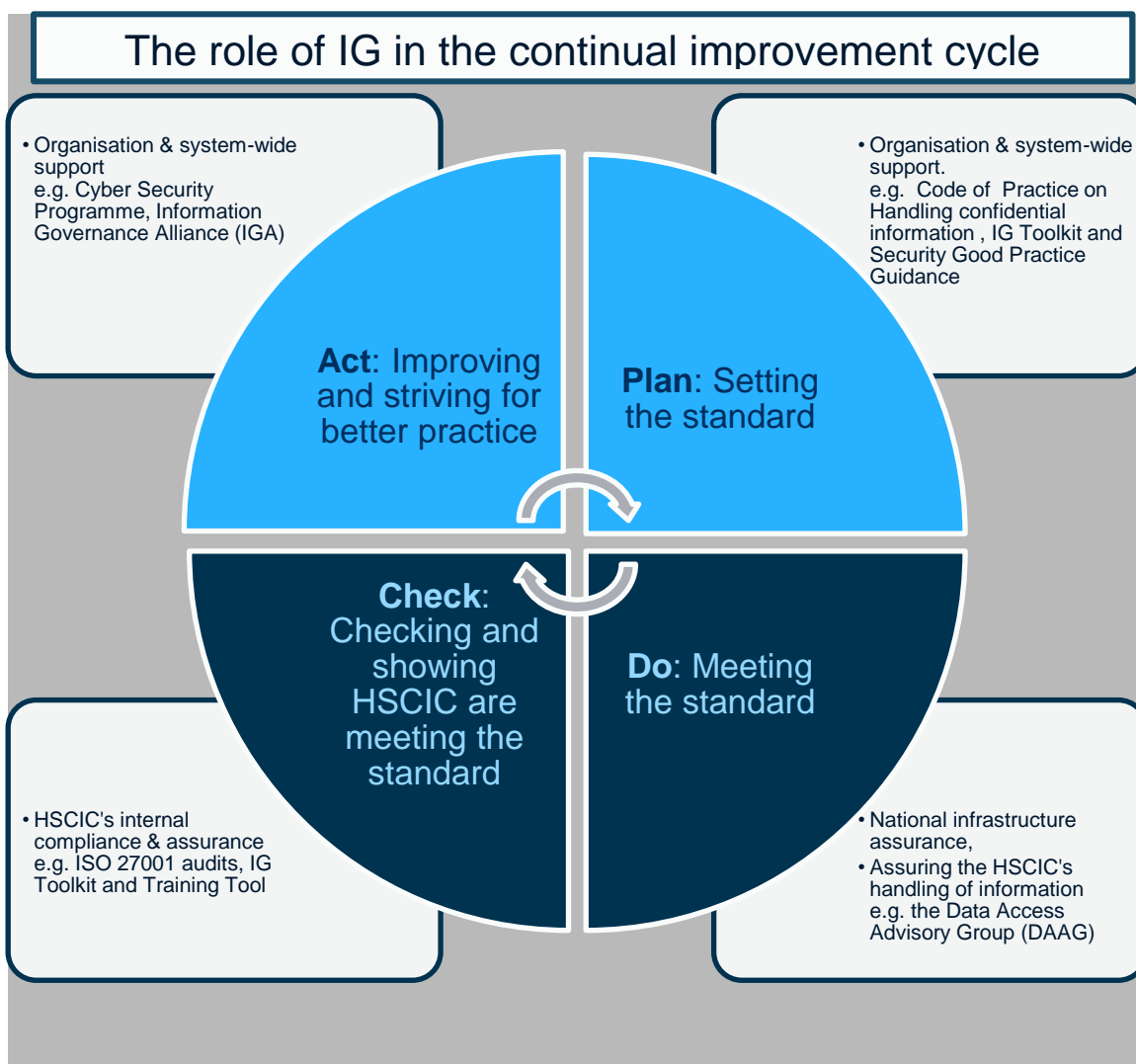


Figure 1: How the IG function can implement the continual improvement cycle for information risk management for the benefit of both the HSCIC and the broader health and social care system.

Work stream 1: Assuring the HSCIC's Handling of Information

Improvements to the process for obtaining data

Since the Partridge Review, over 800 data requests have been actioned using appropriate governance controls and quality checks. A single point of contact, the Data Access Request Service has been established for the consistent management of data access applications, ensuring activity is centrally logged, monitored and audited.

The end-to-end process for obtaining data has improved significantly. A single application form, the Data Sharing Framework Contract and Data Sharing Agreement, has been developed and Service Level Agreements for applications have been introduced. Although this has reduced the bureaucracy to minimise unnecessary delays when data is required, further safeguards have been put in place to ensure that recipients handle any data received respectfully and appropriately, inline with the law. Data is now only shared with organisations with which the HSCIC has a contractual relationship, enacted through a binding Data Sharing Contract. Therefore if any organisation receiving data does not sign the Data Sharing Contract, the sharing of data will cease and existing data must be deleted (unless another legal basis exists, e.g. a statutory responsibility to share the data).

The Data Access Advisory Group (DAAG) helps to ensure that the use of patient data for research purposes and for improving patient care is done in a controlled environment where any risk of disclosure is minimised. It has therefore benefitted greatly from the addition of three independent members. DAAG has taken on additional responsibilities to look at the legal basis of collections during its end-to-end review of data disseminations and is working to continually improve its processes. There is good cross-directorate working and a revised process to improve the quality of applications. Figure 2 shows the ratio of applications for Data Sharing Agreements being approved (with and without caveats) to those not recommended for approval.

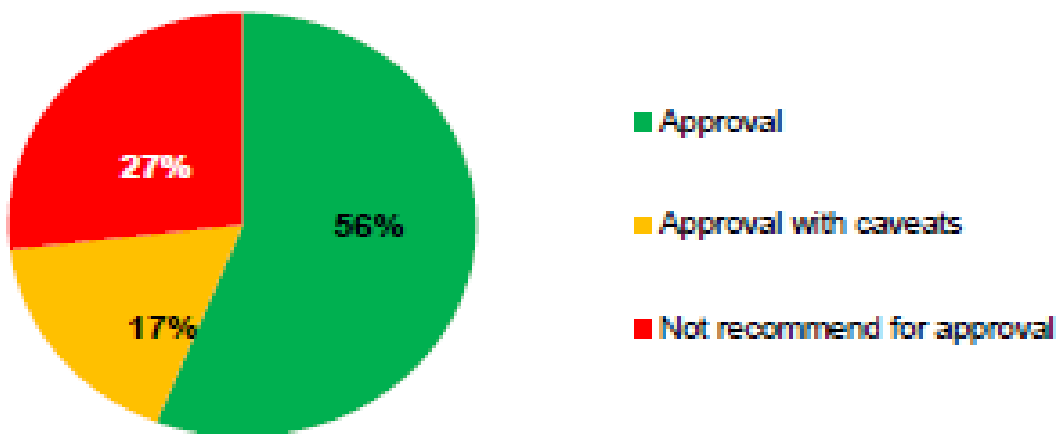


Figure 2: Proportion of DAAG applications for Data Sharing Agreements approved, approved with caveats and not recommended for approval between Sept 2014 and March 2015

To continue this improvement, the HSCIC intends to consult on the formation of a new independent Data Dissemination Advisory Group (DDAG) to replace DAAG and which may incorporate the data dissemination function of the GPES Independent Advisory Group (GPES IAG). GPES IAG's role was to consider requests for information that could be collected and provided by GPES, and to recommend a course of action to the HSCIC. The DDAG proposals underpin the *NIB Framework for Action* (and in particular the theme of 'building and sustaining public confidence') and will play a crucial role to underpin objectives 3, 4 and 5 of the *HSCIC Strategy 2015-2020*.⁸

⁸ <http://www.hscic.gov.uk/article/3887/HSCIC-publishes-strategy-for-2013-2015>

Transparency and auditing data releases

To further improve transparency a list of all data released under active Data Sharing Agreements is now published via the HSCIC Quarterly Register, including receiving organisations, type of data and legal basis. A Data Sharing Agreement template has also been published.

A new, strengthened audit function is being developed to monitor adherence to Data Sharing Agreements and Data Sharing Contracts. Failure to abide by Data Sharing Agreements and Contracts will result in the data dissemination being stopped and the deletion of any existing data.

Four audits have been completed so far and the audit reports have been published (PA Consulting, Methods Consulting, University Hospitals Birmingham and NHIS).⁹ Further audits are being undertaken and a forward programme is being established for 2015/16 where it is anticipated that 25 or more audits will be undertaken.

Work stream 2: HSCIC’s Internal Compliance & Assurance

Compliance & Assurance

The HSCIC continues to meet its legal requirements under the Data Protection Act (DPA) and Freedom of Information (Fol) Act. Figure 3 shows the number of requests handled under these Acts, showing a significant increase in DPA requests. Throughout 2014 the HSCIC has also been developing its fair processing portal, in line with data protection principles.¹⁰

Year	Freedom of Information Requests (Fols) - requests for access to recorded information held by the HSCIC as a public sector organisation	Data Protection Act (DPA) requests	
		‘Subject Access’ – requests for access to one’s own data by a data subject	‘Preventing Use’ – requests from individuals wishing to prevent processing of their data for secondary use purposes
2013-4	771	30	5
2014-5	828*	59*	50*

Figure 3: A comparison between the 2014-5 and the 2013-14 statistics for Fol and DPA requests. *Please note that these figures are correct at the time of writing (13/03/15) but are expected to increase slightly until the end of the financial year. The 2013-4 figure represents the full financial year.

The HSCIC IG Toolkit submission is facilitated by an internal working group. For March 2014–15 it achieved a score of 93% and evidence is currently being collated for the 2014-15 submission. Over and above the requirements of the IG Toolkit, the HSCIC is working, where appropriate, towards the externally assessed, highest industry standards of ISO27001 for information security.

Security

Corporate technical security has also been improved throughout 2014. To improve physical security, information and analytics services which were housed within Trevelyan Square, Leeds have been successfully migrated to the secure HSCIC Data Centres in Plymouth.

Similarly to increase technical security, the HSCIC has also now completed the migration from the Windows XP operating system. There are approximately 5-10 machines that have had to remain on Windows XP to allow testing of applications and for regression testing to be completed in relation to NHS systems. The remaining machines are fully encrypted and locked down with no access to other applications or the network. Furthermore, they are all protected using an application control system which blocks items before they can be run, to avoid the possibility of infection or compromise.

⁹ <http://www.hscic.gov.uk/dsa>

¹⁰ <http://www.hscic.gov.uk/patientconf>

Work stream 3: National Infrastructure Assurance

HSCIC Cyber Security Programme: Protecting the National Infrastructure

A cyber security programme has been developed, providing an enhanced set of information assurance and cyber security capabilities. The foundations have been put in place in 2014 - a cyber threat assessment has delivered a statement of information security and cyber threats and a statement of information security risk appetite has been developed. A 24 by 7 incident reporting and handling service is up and running and is being expanded to meet the perceived cyber threat.

The Information Assurance and Cyber Security Committee (IACSC) has been established as a sub-committee of the board chaired by Sir Ian Andrews. It reviews and monitors the effectiveness of the system of integrated governance, risk management and internal control relating to information assurance, information governance, cyber and security issues.

IG and security support, advice and guidance for the national programmes continues, with technical security specialist representation on the HSCIC's Architecture Governance Group. In particular, the Infrastructure Security Team has been working closely with the Spine2 Programme, providing technical assurance, advice and guidance on core messaging, identity and access management based on the identification and analysis of risk.

Protecting the national infrastructure also includes the efficient handling of any incidents which may occur. Dame Fiona Caldicott highlighted and commended the HSCIC's handling of incidents in her *IIGOP: The First Year* report. The report stated that:

"The HSCIC, tasked by the Health Secretary to support the NHS in improving its data security and information handling generally, began dealing with a Hospital Episodes Statistics (HES) breach in June 2014. New inspection procedures introduced by the HSCIC had uncovered a number of organisations which were sending HES data and failing to follow data dictionary standards. This meant they were inadvertently enabling personal confidential data to enter the data base. Following an alert to the Information Commissioners' Office this was understood as a large scale problem, although having a low level potential impact, as the affected data fields were unknown to either senders or receivers of HES data. The relevant organisations were contacted to gain their cooperation in closing the breach, without alerting any unfriendly observer to the location of the confidential details. This was important to preserve the general ignorance of the detail of the breach and continue to protect individuals' privacy. Trusts and others were encouraged to provide named contacts who would then start cleaning up their data flows to the HSCIC. In order to manage any untoward reporting in the media, trade titles were informed and briefed about the importance of restricting their reporting to avoid any risk of leading people towards this confidential data. The organisations concerned are now following data dictionary standards and the specialist press reported the breach responsibly."¹¹

¹¹ https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/391533/iigop-annual-report.pdf

Work stream 4: System-wide Support

Compliance & assurance: IG Toolkit re-launching a fit-for purpose framework for IG policy delivery

The HSCIC is also responsible for the maintenance and development of the IG Toolkit (IGT), the single reporting tool for serious IG incidents (SIRI) and the IG Training Tool. Each of them provides an important service to the wider health and social care service, as well as to the HSCIC itself. The value of such tools to the service is illustrated by the significant number of incidents reported since the single SIRI tool went live on 1st June 2013, totally 2067 to date. Three of these were reported by the HSCIC. The intelligence gained from the analysis of trends reported is invaluable for the system, providing lessons learned and facilitating continual improvement.

To ensure the IGT is continually improved, its re-launch was initiated in 2014 and this features as a commitment in the NIB *Framework for Action*. The project team has consulted widely, aiming to understand the strengths and weaknesses of the current IGT in light of the first major objective, to re-launch the IGT by October 2015. By October 2015 there will be a new look and feel to the IGT website and modules will be added on cyber security and Caldicott2 implementation. A module for large organisations, small organisations and education, training and development will also be added.

In the long-term the project will:

- create and launch a revised, updated and reinvigorated information governance assurance framework across the health and care system, which is suitable to be extended more widely into the public sector at the appropriate time;
- ask users about their experiences of the IGT and respond to the feedback, ensuring the toolkit is fit for purpose and does not impose an unnecessary burden on its customers;
- ensure that the IGT is suitable for use across health, public health & social care and
- update the IGT and its associated guidance to be easy to understand by clinicians, patients and administration staff.

Infrastructure assurance: Enhancing care system cyber security capabilities

The HSCIC has been asked to be the DH delivery arm of cyber security. The HSCIC is also leading the bid for £2.5m National Cyber Security Programme funding through the Office of Cyber Security and Information Assurance (OCSIA), developing several innovative products to enhance care system cyber security capabilities. Nationally, it will encourage innovation and help align to wider Government emergency response teams.

Projects include:

- working with the Office of Cyber Security & Information Assurance (OCSIA), Communications-Electronics Security Group (CESG) and the Centre for the Protection of National Infrastructure (CPNI) to establish a national focal point and governance model for care system cyber security guidance and incident support. This will provide a form of CareWARP (Warning, Advice & Reporting Point) and CareCERT (Computer Emergency Response Team) service which will also protect against the internal threat.

Information Governance: 2014 Review of Activity

- development of a 'scenario assist' package that will be made available to all care organisations and business partners to help guide their actions for cyber preparation, assurance and incident response and
- working with others across the system, including other Arm's Length Bodies, to manage potential and emerging risk.

Handling Information: The Code of Practice on Handling Confidential Information: Promoting good practice

To complement the policy deliver framework and cyber security capabilities, the Code of Practice on Handling Confidential Information, published in 2014, describes good practice to those responsible for setting and meeting policy relating to the handling of confidential health and care information (e.g. board members). It applies to any organisation that collects, analyses, publishes or disseminates confidential information, including the HSCIC. It is built around the information handling lifecycle, outlining seven simple steps (Figure 4). The objective is to increase transparency, consistency in good practice and public trust and confidence. Organisations must have regard to it by law, as per s. 263 of the Health and Social Care Act 2012. It will be built iteratively as good practice is identified and legislative changes emerge.

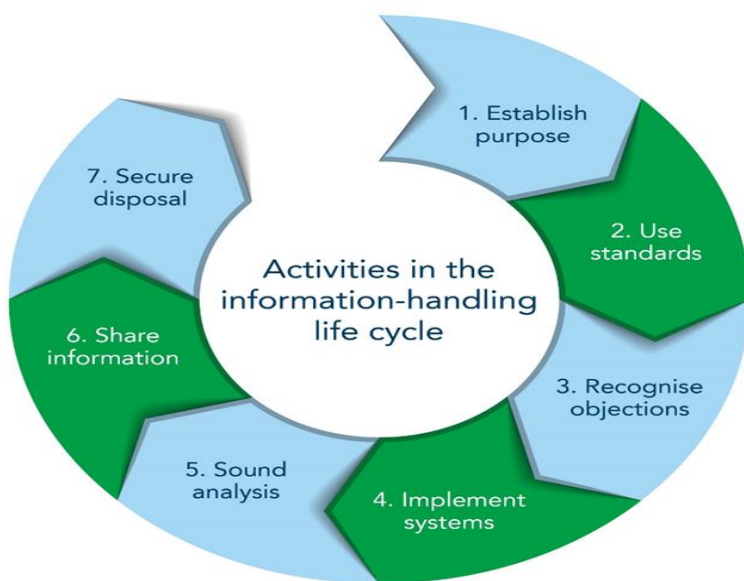


Figure 4: The 7 activities in the information handling lifecycle which underpin the Code of Practice on Handling Confidential Information

IGA: The authoritative system-wide source of advice and guidance

The IGA, which came into existence in 2014, is helping to develop good practice for inclusion within the Code of Practice on Handling Confidential Information. It aims to enhance the quality of health and care services, including people's experience of using those services, by improving information governance. The IGA aim to improve information governance in health and care by:

- becoming the authoritative source of advice and guidance;
- providing support to organisations to help them and their staff handle personal information confidently and in the best interests of people who use their services;

Information Governance: 2014 Review of Activity

- developing the leadership and culture of health and care services to promote legal and secure information sharing and
- developing the capacity and capability of information governance professionals by providing expert advice and supporting knowledge sharing networks.

The IGA partner with the HSCIC, NHS England, Public Health England and Department of Health and have close working relationships with the Independent Information Governance Oversight Panel (IIGOP), the National Data Guardian, the Information Commissioner's Office, the Health Research Authority, Monitor and other leading national organisations.

The IGA has contributed IG expertise to national guidance published by partner organisations and has published documents for consultation on sharing information with voluntary sector organisations. The IGA has also re-established local and national networks of IG Leads.

The Caldicott Implementation Monitoring Team was also hosted by the HSCIC in 2014 and has informed the Independent IG Oversight Panel's (IIGOP) "*The First Year*" Report to the Secretary of State for Health, from Dame Fiona Caldicott. This Report concluded that effort needs to focus on the areas of leadership, fair processing and consent management. It is upon these three themes that the IGA has built their work plan.

Consent management/objections: Honouring the information sharing preferences of the public

Consent management is in itself the subject of a programme of work. The HSCIC Caldicott Guardian and Clinical Lead accepted a request from the NIB to co-chair a programme of work which will:

- implement and develop the role of the National Data Guardian (Dame Fiona Caldicott);
- create a dialogue with the public to help to understand the ethical issues relating to the use of individuals' data in the health and care system and to build public understanding of the importance of individual data to support better health and care;
- develop a system of consent, whereby citizens can, where appropriate, choose what use is made of their data and
- develop systems of information governance and security which will ensure that the health and care system safeguards individuals' information.

Looking forward

This report shows how the HSCIC has reacted quickly over the past year to continually improve processes in response to the *Partridge Review* and others. Going forward, HSCIC will aim to proactively use IG to its full potential as an enabler for continual improvement. This will be beneficial both within the HSCIC and throughout the wider health and social care system, and in turn will be a mechanism for delivery of the HSCIC's values, particularly trustworthiness.

The system-wide support work of the HSCIC has contributed to continual improvement and good practice throughout the system. Good practice and learning from the internal work is reflected within the system-wide work and vice versa so that the benefits of the outcomes are shared. It is upon this premise of "do once and share" that initiatives such as the IGA are built.

Action Required of the Board

Looking forward to 2015 and beyond, it is proposed that the Board support the development of an IG Strategy and IG Strategy Group which ensure that the Strategy is implemented proactively throughout the HSCIC and that the policy framework underpinning it continues to be fit for purpose.