KPMG
cutting through complexity

Information Governance in Health and Social Care

> Instilling a central, corporate outlook on Information Governance through the adoption of a tailored IG Toolkit designed by local government organisations, with the support of major stakeholders such as HSCIC and DH, is essential to build the necessary trust to enable the improvements in services envisaged by the Health and Social Care Act to be achieved.

The 21st century is all about technology and communication.

As the global village becomes smaller and people become better connected and more knowledgeable, organisations find that they are challenged daily by the need to ensure that confidential data will not leak, either due to intentional or unintentional activities. Public sector organisations that use a wide variety of personal data in the form of patient information and identifiers are particularly affected. In the wake of the Health and Social Care Act 2012, shifting services mean that local authorities are subject to a greater variety of different information governance requirements, chiefly with respect to the provision of Public Health and Adult Social Care.

The profile of Information Governance (IG) in the public sector has risen significantly in recent years and public and media interest remains high. For example, the Information Commissioner's Office (ICO) issued a dedicated press release in May 2014 that criticised the Student Loans Company, due to multiple incidents where personal information that included medical details and a psychological assessment were sent to the wrong people.

The ICO also has the power to impose fines of up to £500,000 for serious breaches of the Data Protection Act 1998. Several substantial fines have been issued in the past year: for example, Aberdeen City Council was fined £100,000 after 'inadequate' home working arrangements resulted in the upload of 39 pages of personal data to the internet; and a fine of £80,000 was imposed on North East Lincolnshire Council after an unencrypted USB containing the (sensitive) personal information of 286 children was lost.

The increasing integration of health and social care means that communication between local authorities and healthcare organisations is increasing in volume and significance. In this technological age, it is possible to vastly improve services through communication and information transfer. The eventual benefits are clear: consider the utility of a single record for an individual that contains essential information from health, police, social care and housing, accessible via a single identifying reference number.

But when personal data is involved and perhaps even held in one repository, the barriers are evident. One response to these challenges is the NHS Information Governance (IG) Toolkit. All Health and Social Care service providers should complete a NHS IG Toolkit, as a best practice IG framework that forms the bedrock of information processing by NHS organisations. The NHS IG Toolkit sets out a number of requirements that define how information should be handled and protected from unauthorised access, loss, damage and destruction.

This self-assessment toolkit allows organisations like Commissioning Support Units (CSUs), many of whom provide data analytics services to Clinical Commissioning Groups (CCGs), to determine the extent to which they comply with legal and DH guidance and to take corrective action where necessary. Moreover, the NHS IG Toolkit enables these organisations to put in place a wider framework that provides the tools necessary to instil a culture of robust information governance throughout the entire organisation:

Information Governance Management	■ IG policies are being meaningfully applied to the organisation through strategies and improvement plans ■ Employee, contractor and supplier contracts are in line with IG policies
Confidentiality and Data Protection Assurance	■ The organisational and individual staff have sufficient skills and knowledge to be able to keep personal information secure ■ Personal information is only used lawfully when it does not directly contribute to the delivery of care and that all new processes, services and IT systems conform to those standards ■ Individuals are aware of how their information is used and that they are able to request access to their personal data
Information Security Assurance	■ All IT systems have managed access rights and all transfers of hardcopy and digital person identifiable and sensitive information have been identified and risk assessed ■ IT networks operate securely; processes are in place to ensure that malicious code can be rapidly detected and removed; and all information assets are protected
Clinical Information Assurance	■ There are processes in place to ensure clinical information accuracy and the consistent use of the NHS number ■ Regular monitoring and audits are undertaken to measure the quality of clinical information
Secondary Use Assurance	■ Tools such as external data quality reports, local and national benchmarking and data quality audits are used to evaluate data quality ■ National data definitions, standards and values should be regularly incorporated locally
Corporate Information Assurance	■ There is effective management of corporate records ■ The organisation complies with Freedom of Information Act 2000 ■ The organisation undertakes audit of the records in line with information lifecycle management

Source: HSCIC, via https://www.igt.hscic.gov.uk/ ; July 2014)

In the NHS, the IG Toolkit has been successful in driving improvements across complex organisations. For example, the toolkit enables organisations such as Acute Trusts, with decentralised working practices and essentially dispersed services, to manage IG and data security consistently as a central service on a corporate level.

Local authorities have been increasingly expected to prove compliance with a variety of disparate IG regimes, which during 2013-14 included assessment against 40 requirements of the health-centred NHS IG Toolkit and various technical certifications, depending on service provision and data sharing arrangements.

> “When it comes to sharing information, a culture of anxiety permeates the health and social care sector. Managers, who are fearful that their organisations may be fined for breaching data protection laws, are inclined to set unduly restrictive rules for information governance. ...There is also a lack of trust between the NHS and local authorities and between public and private providers due to perceived and actual differences in information governance practice. This state of affairs is profoundly unsatisfactory and needs to change.”
>
> *Caldicott2 review: ‘Information: to share or not to share?’*

Such fragmented information governance requirements are unsustainable and make the pursuit of a central IG strategy more challenging. Without central management, there is a risk that local authorities already subject to overlapping IG requirements could experience further fragmentation, as new requirements emerge from future legislation.

To repeat the healthcare successes of the NHS IG Toolkit, a collaboration between HSCIC, DH, local government organisations and other stakeholders has designed a Local Authority IG Toolkit to help consolidate existing IG requirements. Released from June 2014, this toolkit presents a local government perspective on IG and aims to provide local authorities with the means to seed a full corporate IG outlook, rather than focusing on single service requirements. Over time, the intention is to expand this perspective into a complete IG framework for local government organisations and, ultimately, to become a best practice framework for all public services.

Information sharing and collaboration

Although strategic data sharing is likely to lead to a range of positive initiatives, such as a reduction in hospital admissions through collaboration with Adult Social Care services, there is no general legal right that allows local authorities, health trusts, police forces and other public bodies to share information. Implementing data sharing programmes using personal data requires compliance with the Data Protection Act 1998 and the legal duty of confidentiality, as well as the ability to overcome technical and operational obstacles. Technical challenges would include the merging of correct records into a single entity, which may require the cross-referencing of the NHS unique patient identifier and National Insurance numbers. The drive to utilise such integrated digital care records is ongoing. However, common information governance standards and information sharing frameworks incentivise sharing by providing assurance that confidential data is held securely and confidentially, recorded accurately and reliably, and shared and disclosed appropriately and lawfully.

The Health and Social Care Act 2012 has changed the organisational structure of the NHS and its functions, which has led to discussions over the permissible uses of NHS data. It is likely that the Care Act 2014 will also bring further changes to the responsibilities of local authorities with respect to social care. At present, the HSCIC is undertaking a comprehensive review of all policies, processes and governance for the data sharing that may result in more stringent regulation. It is likely, therefore, that additional IG requirements will be introduced that further complicate the position of local authorities.

Case study: Benefits derived from applying the IG Toolkit

As a result of the increased focus upon the security of personal information in the public sector and concerns over compliance with information governance (IG) clauses in supplier contracts, we were approached by a third sector organisation requesting a review of the system of controls in place to assess whether adequate assurance could be provided over IG. We also developed an action plan to address any recommendations arising from the review, taking financial restrictions into consideration. The plan included clear roles and responsibilities, which could be clearly understood by all.

We carried out a high level assessment of the IG framework in place, in line with NHS IG Toolkit 'Voluntary Sector Organisation' requirements as a best practice framework that considers IG management, confidentiality, data protection, information security, care records assurance and corporate information assurance. This assessment against the NHS IG Toolkit resulted in:

- An independent and objective evaluation of the prioritisation and management of information governance across the organisation.
- A better understanding of the roles and responsibilities for managing information and key information governance requirements.
- A high level understanding of staff's knowledge of information governance policies and procedures, through a staff survey, which identified where policies and procedures may be unknown or open to interpretation.
- An independent assessment on the culture of information governance embedded in the organisation and the oversight of organisational compliance with information governance requirements.
- Maximising the value of organisational assets by ensuring data is held securely and confidentially; recorded accurately and reliably; and is shared appropriately and lawfully.

This highlights the potential of applying a tailored IG Toolkit framework in non-NHS organisations.

Contact us

Andrew C North
Technology Risk – Sectors PS
Director
T: +44 (0) 113 254 2839
E: andrew.c.north@kpmg.co.uk

Laura Buckles
Technology Risk – Sectors PS
Analyst
T: +44 (0) 788 005 3469
E: laura.buckles@kpmg.co.uk

www.kpmg.co.uk

Produced by Create Graphics | Document number: CRT019331