Information Governance summary in NHSS, health and social care 2015-2017

Information Governance (IG) is an essential requirement that enables NHSS and its partners to deliver services within the law, with the right level of security and accountability, and above all with the right level of public trust. IG covers a whole framework of interlinking functions ranging from information and records management, privacy, adherence to access to information and other legislation and risks relating to confidentiality, integrity and availability of information. IG should not be seen as a barrier to health and social care integration and it is essential that the business starts on the premise of "what it needs to do" and then be advised on risks (rather than the other way round). But there is no doubt that the ever widening group of information sharing partners, new data flows, blurred lines between what is direct care, supporting services and research and public anxieties about areas such as 'Big Data' means IG has become far more complex and difficult. The impact of getting the information risk management balance wrong is also higher than ever given the increasing reliance on digital systems in health 24/7, the new global 'cyber' threats and new legal penalties such as Information Commissioner audit, enforcement and fines.

Key work in progress

New NHS Information Security Policy Framework: To be used as a vehicle to improve security in each health board. As it is aligned to ISO-27001 it is hoped to bring health closer to the requirements in local authorities and central government. It is essential that information sharing partners agree on 'equivalency' of security even if they adopt different means/controls to achieve this and agree on a light touch means of accreditation/assurance.

Security controls: Out of the policy framework is a need to develop new national policies/standards/guidance in areas which are becoming more important (e.g. technical vulnerability management, resilience, accreditation of national-level systems and 'safe havens').

Scottish Wide Area Network (SWAN): This is an essential piece of the jig-saw to enable information sharing and work is ongoing to provide maximum technical flexibility and consistent security levels in accordance with SWAN policy and code of connection.

Information Sharing Agreements: SWAN does not by itself allow information sharing. It is the agreements between the parties on the data, its handling and other work that is becoming ever more crucial. Scottish Accord on Sharing Personal Information (SASPI) and toolkit is to be formalised as *de facto* standard for doing this in the Scottish public sector.

Public Benefit & Privacy Panel: A new governance structure – which merges three existing ones – is to be established which deals with scrutiny of requests to use NHSS data-sets. This could in time (subject to agreement of relevant Data Controllers) also consider national level projects using local authority and GP data.

Training and capability: IG is the responsibility of everyone (not just IG Leads) and key persons – such as new Chief Officers - need to be equipped with the knowledge to be able to navigate this area. Special emphasis should be on SIRO and Caldicott-level training materials and on ensuring that senior leaders understand the new risk and regulatory landscape.