The Scottish Government
Directorate of Finance, eHealth & Analytics

24 June 2015

Dear Colleague

Information Governance and Security Improvement Measures 2015-2017

Summary

Board Chief Executive Officers, Caldicott Guardians, Information Governance (IG) Leads, ICT professionals and others will by now have had the opportunity to comment and contribute to a whole package of measures being launched to improve Information Governance and Information Security.

Background

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 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 Office audits, enforcement and fines.

It is for this reason the new measures below should be adopted.

Action

The key requirements I would like to highlight in particular are:

- The new NHSS Information Security Policy Framework and the need for the Board Chief Executives to assign the role of Senior Information Risk Owner (SIRO) and to take steps to ensure that over the next two years each Board has an operational Information Security Management System that

DL (2015) 17

Addresses

For action

Chief Executive Officers
eHealth Leads
Caldicott Guardians
IG Leads
Information Security

For information

Enquires to:

Head of Information Assurance & Governance (NHSS, health and care)
The Scottish Government

Tel: 01312442373

conforms to the policy framework (this replaces NHSS Information Assurance Strategy 2011-15 and the NHSS Information Security Policy 2006) as of 1 July 2015.

- To ensure that plans are made to implement the necessary security controls incrementally to safeguard the confidentiality, integrity and availability of information necessary for the delivery of health and care.

- The new Public Benefit and Privacy Panel for Health and Social Care is set up to scrutinise requests to use NHSS-originated data for national-level projects. I am delighted that Mr Brian Houston (Chair to NHS Lothian) has agreed to Chair and that the IG community across Scotland must pool their efforts and contribute to its success.

- Board eHealth Plans and IG business plans will need to show steady incremental progress in conforming to the new information security policy framework. This should be reflected in Board internal audit reports. The Information Commissioner's Office has agreed to use the new framework as a starting point for any compulsory external audits.

Yours sincerely

John Matheson CBE
Director of Finance, eHealth & Analytics