From the office of Christopher Graham
Information Commissioner
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF
christopher.graham@ico.gsi.gov.uk

From the Office of Sir David Nicholson KCB CBE
Chief Executive of the NHS in England
Richmond House
79 Whitehall
London
SW1A 2NS
david.nicholson@dh.gsi.gov.uk

5 September 2011

To: Chief Executives of all Strategic Health Authorities
Chief Executives of all NHS Trusts
Chief Executives of all Primary Care Trusts

cc. Directors of Finance of all Strategic Health Authorities
Directors of Finance of all NHS Trusts
Directors of Finance of all Primary Care Trusts
Chief Information Officers of all Strategic Health Authorit
Monitor – Independent Regulator of NHS Foundation tru
CQC
Chair of NIGB

Gateway Reference Number : 16607

Dear Colleagues,

Information Governance Assurance

The protection of sensitive patient information has always been a priority for us in the NHS. With changes planned to commissioning structures and with increasingly diverse care providers, we need to ensure that we continue to give information governance the priority and attention it needs. This joint letter signals the intention of the NHS and the Information Commissioner's Office (ICO) to work together in supporting you to deliver good information governance.

We would like first of all to acknowledge your efforts to deliver improved information governance processes across the service. We know how hard it is to sustain momentum for work of this kind while delivering high levels of care, maintaining financial control, and helping to deliver service reform. It is essential however that momentum is sustained.

Incidents of data loss continue to occur and in some cases these are both significant and clearly in breach of national guidelines, e.g. encryption of mobile devices. While we have to accept that some incidents will always occur, it is not acceptable where adherence to national policies would have prevented the breach.

We want to call your attention again to a significant change that came into force on 6 April 2010, which enables the ICO to order organisations to pay up to £500,000 as a penalty for serious breaches of the Data Protection Act 1998. Obviously we are all hoping that it will not be necessary for the enhanced powers to be exercised, but at present a significant percentage of all data breaches reported to the ICO relate to NHS organisations. The purpose of this letter is to outline the actions that we jointly recommend to ensure your systems and practices deliver adequate information governance and that commissioning criteria adequately reflect its importance.
All NHS organisations (and others with access to NHS patient information) should:

a. be using the **NHS Information Governance Toolkit** https://www.igt.connectingforhealth.nhs.uk/ to assess and publish details of performance

b. ensure all staff undertake appropriate **information governance training annually** as identified in the NHS Information Governance Toolkit https://www.igte-learning.connectingforhealth.nhs.uk/igte/index.cfm

c. have identified and trained a **Board level individual to act as the Senior Information Risk Owner** (SIRO) for the organisation. Guidance on information governance considerations for all NHS Board members is available at https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Guidance%20for%20Boards.pdf

d. **make staff aware continuously** of the existing information governance policies and guidelines, the fact that they must be followed in practice, and that a breach of policy will be regarded as a disciplinary matter

e. **assist the Information Governance Policy Team in its current risk assessment of all centrally hosted teams** such as Public Health Observatories. Advice on this can be obtained by contacting exeter.helpdesk@nhs.net.

Cluster Arrangements

Both the NHS and the ICO are particularly concerned to ensure that there are no gaps in the information governance assurance provided by SHAs and PCTs during NHS reorganisation. To that end we are asking each PCT cluster to conduct and publish an assessment that covers all constituent PCTs by 31 March 2012.

ICO Audits and Data Sharing Code of Practice

We want to call your attention to the ability of the ICO to carry out a data protection audit where invited to do so. We would encourage any organisation who would find this useful, including those newly providing NHS services. See http://www.ico.gov.uk/for_organisations/data_protection/audit.aspx for more information. The ICO has recently published a Data Sharing Code of Practice that can be found at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/data_sharing.aspx.

Information is at the heart of major reforms to the provision of health and social care. Both the NHS and the ICO want to ensure that good information governance enables the improvements these reforms will bring for patients and service users. We are therefore undertaking a number of joint initiatives on reporting, training, awareness of accountabilities, and an information governance strategy.

Where, despite our efforts, data protection obligations are not met, the ICO will exercise enhanced powers to take whatever action is appropriate.

Yours sincerely,

Christopher Graham
Information Commissioner

Sir David Nicholson KCB CBE
NHS Chief Executive