

*From the office of David Nicholson CBE
Chief Executive of the NHS in England*



*Richmond House
79 Whitehall
London
SW1A 2NS
Tel: 020 7210 5142
Fax: 020 7210 5409
david.nicholson@dh.gsi.gov.uk*

- 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 Authorities
Monitor – Independent Regulator of NHS Foundation Trusts

Gateway Reference Number: 9912

20 May 2008

Dear Chief Executive

Information Governance Assurance Programme

Further to my letter of 4 December 2007 and follow-up note of 15 January 2008 to SHAs. Thank you for your efforts to date in delivering improved information governance processes as evidenced through your IG Toolkit annual returns. However, we cannot be complacent and continued action is necessary to ensure the adequacy of our systems, procedures and working practices. The purpose of this note is to set out the further actions required.

Actions Required by SHAs

- i. The data from the IG Toolkit annual returns has now been supplied to SHAs. All SHAs must review the consequential action plans of all organisations for which they are responsible. Progress on these plans will be an agenda item for the mid year and end of year reviews I have with SHA CEOs.

- ii. All SHAs should consider independent audit of their PCTs and Trusts on the information governance standards associated with the NHS CFH Information Governance Statement of Compliance (as detailed in the version 6 release of the NHS Information Governance Toolkit, to be issued in June 2008).
- iii. All SHAs should ensure that all organisations for which they are responsible have appropriate access to Information Governance Subject Matter Experts.

Actions Required by all NHS Organisations

- iv. All NHS organisations must now include details of Serious Untoward Incidents involving data loss or confidentiality breach in their annual reports for 2007/8 onwards (see Annex A for details).
- v. All NHS organisations must now make specific reference to information governance in terms of identifying and managing information risks in their annual Statement of Internal Controls from 2007/8 onwards (see Annex B).
- vi. All NHS organisations must identify a Senior Information Risk Owner; at Board level (guidance on this role will be provided in version 6 of the NHS Information Governance Toolkit).

Future Actions

In the context of recent Cabinet Office guidance, there is work underway to determine whether and how confidentiality policies and disciplinary procedures should be amended to ensure that all NHS staff are fully aware of their obligations in respect of Information Governance. This of course needs to be supported by adequate training for staff. You can expect further correspondence and information on this by the end of June.

I recognise that all of the above requires a significant investment of time and energy but we must ensure that the public has, and can continue to have, confidence in our systems, procedures and working practices.

Yours sincerely



DAVID NICHOLSON CBE
NHS CHIEF EXECUTIVE

Reporting of Personal Data Related Incidents

Principles

The reporting of personal data related incidents in the Annual Report should observe the principles listed below. The principles support consistency in reporting standards across NHS Organisations while allowing for existing commitments in individual cases.

- a) You must ensure that information provided on personal data related incidents is complete, reliable and accurate.
- b) You should review all public statements you have made, particularly in response to requests under the Freedom of Information Act 2000, to ensure that coverage of personal data related incidents in your report is consistent with any assurances given.
- c) You should consider whether the exemptions in the Freedom of Information Act 2000 or any other UK information legislation apply to any details of a reported incident **or** whether the incident is unsuitable for inclusion in the report for any other reason (for example, the incident is *sub judice* and therefore cannot be reported publicly pending the outcome of legal proceedings).
- d) Please note that the loss or theft of removable media (including laptops, removable discs, CDs, USB memory sticks, PDAs and media card formats) upon which data has been encrypted to the approved standard, is not a Serious Untoward Incident unless you have reason to believe that the protections have been broken or were improperly applied.

Content to be included in Annual Reports

Recently issued guidance on Serious Untoward Incidents involving data, classified incidents in terms of severity on a scale of 0-5 in terms of either/both risk to reputation and risk to individuals. Figure 1 is reproduced from that guidance

Figure 1

0	1	2	3	4	5
No significant reflection on any individual or body Media interest very unlikely	Damage to an individual's reputation. Possible media interest, e.g. celebrity involved	Damage to a team's reputation. Some local media interest that may not go public	Damage to a services reputation/ Low key local media coverage.	Damage to an organisation's reputation/ Local media coverage.	Damage to NHS reputation/ National media coverage.
Minor breach of confidentiality. Only a single individual affected	Potentially serious breach. Less than 5 people affected or risk assessed as low, e.g. files were encrypted	Serious potential breach & risk assessed high e.g. unencrypted clinical records lost. Up to 20 people affected	Serious breach of confidentiality e.g. up to 100 people affected	Serious breach with either particular sensitivity e.g. sexual health details, or up to 1000 people affected	Serious breach with potential for ID theft or over 1000 people affected

Incidents classified at a severity rating of 3-5 are those that should be captured as Serious Untoward Incidents and should be reported to SHAs and to the Information Commissioner. These incidents need to be detailed individually in the annual report in the format provided as Table 1 below.

Incidents classified at a severity rating of 1-2 should be aggregated and reported in the annual report in the format provided as Table 2 below.

Incidents rated at a severity rating of 0 need not be reflected in annual reports.

Table 1

SUMMARY OF SERIOUS UNTOWARD INCIDENTS INVOLVING PERSONAL DATA AS REPORTED TO THE INFORMATION COMMISSIONER'S OFFICE IN 2007-08				
Date of incident (month)	Nature of incident	Nature of data involved	Number of people potentially affected	Notification steps
Jan	Loss of inadequately protected electronic storage device	Name; address; NHS No	1,500	Individuals notified by post
Further action on information risk	The [organisation] will continue to monitor and assess its information risks, in light of the events noted above, in order to identify and address any weaknesses and ensure continuous improvement of its systems. Planned steps for the coming year include ...			

Notes to producing Table 1

Nature of the incident

Select one of :

- a) Loss of (*insert from category list below*) from secured NHS premises
- b) Loss of (*insert from category list below*) from outside secured NHS premises (*including, for example, post, courier, theft from employee home or car; loss by a contractor or third party supplier*)
- c) Insecure disposal of (*insert from category list below*) (*including, for example, sale of computers with unwiped hard drives, disposal of unshredded paper documents*)
- d) Unauthorised disclosure (*including, for example, criminal, negligent or inappropriate use of an information system or information asset by a staff member, contractor or third party supplier, resulting in disclosure; disclosure as a result of software or systems failure*)
- e) Other

Category List

- i) inadequately protected PC(s), laptop(s) and remote device(s) *(including, for example, PDAs, mobile telephones, Blackberrys)*
- ii. inadequately protected electronic storage device(s) *(including, for example, USB devices, discs, CD ROM, microfilm)*
- iii. inadequately protected electronic back-up device(s) *(including, for example, tapes)*
- iv. paper document(s)

Nature of data involved

A list of data elements (e.g. name, address, NHS number).

Number of people potentially affected

An estimate should be provided if no precise figure can be given.

Notification steps

Individuals notified by post* / email* / telephone* *(*delete as appropriate)*

Police* / law enforcement agencies* notified *(*delete as appropriate)*

Media release

Further action on information risk

A summary of any disciplinary action taken as a result of the incidents should also be included.

Table 2

SUMMARY OF OTHER PERSONAL DATA RELATED INCIDENTS IN 2007-08		
Category	Nature of incident	Total
I	Loss of inadequately protected electronic equipment, devices or paper documents from secured NHS premises	
II	Loss of inadequately protected electronic equipment, devices or paper documents from outside secured NHS premises	
III	Insecure disposal of inadequately protected electronic equipment, devices or paper documents	
IV	Unauthorised disclosure	
V	Other	

Annex B - SIC Guidance

It is important to remember that an organisation's assets include information as well as more tangible parts of the estate. Information may have limited financial value on the balance sheet but it must be managed appropriately and securely. All information used for operational purposes and financial reporting purposes needs to be encompassed and evidence maintained of effective information governance processes and procedures with risk based and proportionate safeguards. Personal and other sensitive information clearly require particularly strong safeguards. The Accountable Officer and the board need comprehensive and reliable assurance from managers, internal audit and other assurance providers that appropriate controls are in place and that risks, including information and reporting risks, are being managed effectively.

The SIC should, in the description of the risk and control framework, explicitly include how risks to information are being managed and controlled as part of this process. This can be done for example by referencing the work undertaken by your organisation between December and January as part of the first phase of the IGAP and by reference to your organisation's use of the Information Governance Toolkit. The SIC will then be reflected formally in your Annual report.

Any incidence of a Serious Untoward Incident (as described in Annex A) should be reported in the SIC as a significant control issue. For the avoidance of doubt these are those incidents with a severity rating of 3, 4 or 5.