

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

Cc: Chief Information Officers of all Strategic Health Authorities
Monitor – Independent Regulator of all NHS Foundation Trusts

Gateway ref: 10509

September 2008

Dear Chief Executive

DATA SECURITY

Further to my letter of 20 May 2008 I am writing to ask you to conduct a review to ensure that your organisation has fully implemented the policy that all removable data must be encrypted. I would also like to draw your attention to the report of the Cabinet Office Data Handling Review that was published on 30 June 2008, which contains mandatory security standards for the public sector. A second report, the Thomas/Walport Data Sharing Review, is also relevant and whilst the government response to the recommendations in this report has not yet been finalised, it is likely that all will be accepted.

Data Handling Review

The government's Data Handling Review report contains a number of recommendations that are mandatory to government and, with some exceptions, the wider public sector. The Information Governance Assurance Programme (IGAP) has ensured that the NHS is already able to apply many of the recommendations and further guidance on the remainder will be published later in the year, but part of the solution to reducing risk lies in ongoing culture change to ensure that information risk management is high on the agenda. You should review your arrangements against the recommendations (summarised in Annex 1). The Report is at <http://www.cabinetoffice.gov.uk/csia>

Data Sharing Review

The Prime Minister asked the Information Commissioner, Richard Thomas and the Director of the Wellcome Trust, Mark Walpole, to jointly review data sharing in the UK. Their Report and its annexes contain a lot of examples from the health sector and makes a number of recommendations that the government is current considering. A summary of the recommendations is at Annex 2, and you should note the strengthened powers of the Information Commissioner as a regulator. This builds upon new powers provided to the Commissioner in the Criminal Justice Act 2008 which allow fines of up to £500,000 to be imposed on bodies or individuals who are aware of information risks but have not taken reasonable and appropriate steps to mitigate against those risks. The Report is at <http://www.justice.gov.uk/reviews/datasharing-intro.htm>

GP Practices

The Information Commissioner has written to me to draw attention to a risk identified during the IGAP work relating to the dispersed nature of GPs and their independent status. Each Practice is legally responsible for holding data securely and we are looking at the national contract and considering how best to secure compliance with standards through contractual means in the future.

PCTs should be reminded of the requirement to conduct a risk assessment for the transport of patient identifiable data in General Practice. Back up tape encryption to NHS CFH standards will provide significant protection in the event of the loss of a practice back up tape. NHS CFH has negotiated significant reductions on licence and installation prices under the GP Systems of Choice (GPSoC) Framework. Pricing for the back up tape encryption services can be found at www.connectingforhealth.nhs.uk/gpsoc/news.

PCTs that plan to order the back up tape encryption service from GPSoC suppliers are encouraged to do so by the end of September 2008 so that volumes can be confirmed and a deadline set for installation across all PCTs that require this service.

In addition:

- all Practices should be asked to sign a statement of compliance in respect of key security requirements (aligned with the Data Handling Review requirements)
- all Practices should be using the NHS Information Governance Toolkit
- an on-line training package including targeted GP modules is provided free to users and meets the current contractual requirement for each Practice to have a trained IG lead. 80 workshops for Practices and PCTs are being provided this autumn
- all practices should be aware that free encryption software is available for removable data and should be supported by PCTs in its use
- all practices should be aware that NHSmail provides a secure e-mail transfer solution and should be encouraged to migrate to NHSmail
- all practices should be aware that the N3 network provides a secure environment for data transfer
- all practices should be aware that GP2GP secure transfer increasingly means that patient records can move securely between Practices

Encryption software

You are aware that there is a mandatory requirement that all removable data, including laptops, CDs, USB Pens etc must be encrypted. A central procurement has made MacAfee SafeBoot encryption software widely available at no cost to individual trusts. However, there are still over 200 NHS trusts that have not yet taken advantage of the software. It may be that other, locally procured software is being used but you will wish to check that all trusts are using encryption appropriately.

There is also some evidence that trusts who are using the software have over-ordered eg rounding up to 4,000 licences when only 3,200 are needed. Any unused licences will need to be returned.

PACS encryption

The encryption mandate applies equally to PACS images whether on CD or back-up tapes. There could be occasional exceptions on patient safety grounds such as a severely ill patient being transferred to another hospital where the time to encrypt could cause a danger to the patient and a risk assessment will need to be made.

However, there are some myths at large eg that encryption and subsequent decryption can alter images. We have established that encryption does not and cannot reduce the quality of PACS studies. Another myth is that it takes too long to encrypt PACS images on a CD. The average PACS study is 26Mb, and this takes approximately 26 seconds to encrypt on a standard PC.

At present, it is typically a three or four step process to encrypt images onto a CD from a PACS system:

1. PACS burns an unencrypted CD which is then loaded into a PC.
2. SafeBoot (the centrally procured software) encrypts the files on the PC.
3. The PC burns a new CD with the encrypted files. The unencrypted CD should then be destroyed in line with the guidance at Annex 3.
4. A PACS viewer can be incorporated with the CD to enable the image to be opened on any PC – information regarding this will be made available to trusts shortly.

The CD and the password MUST be transferred by different routes.

If compression is used to reduce the size of a PACS image, it must be “Lossless compression”, otherwise image quality may be affected (some applications combine encryption and compression which may have created the myth about encryption).

It may be that other, locally procured software is being used but you will wish to check that all trusts are using encryption appropriately.

NHS CFH is working with PACS suppliers and McAfee to make changes to PACS systems to enable encrypted CDs to be burned directly from the PACS systems. In addition, following a successful pilot, it is intended to rollout a nationally scaled solution for bulk secure file transfer by January 2009. This will allow any file between 20MB and 1GB to be transferred securely across N3 (smaller files can be transferred via NHSmail).

Further guidance is available to the NHS at the following locations:

- a) The IG Toolkit at <http://nww.igt.connectingforhealth.nhs.uk>
- b) The Good Practice Guides at <http://nww.connectingforhealth.nhs.uk/infrasec/>
- c) The PACS documentation at <http://nww.connectingforhealth.nhs.uk/pacs/>

Serious Untoward Incident reports (SUIs)

There are some recent examples where SUIs related to data loss have not been properly reported to the SHA or to the Department at the time the incident was identified. The Accounting Officer role in reporting such incidents is very important and is re-enforced by the powers of the Information Commissioner outlined in the data Sharing Review. I would be grateful if you would ensure that all Trusts are operating the reporting processes correctly.



David Nicholson CBE
NHS Chief Executive

DATA HANDLING REVIEW: Recommendations

The recommendations coloured orange are to be applied by 2009/10 and guidance on these is in preparation. The other recommendations are already mandatory.

Stronger Accountability
1. Accounting officers to cover information risks in Statements of Internal Controls
2. Board level Senior Information Risk Officers (SIRO) to be appointed
3. Information asset owners to be identified
4. Information Risk Policy
5. Annual assessment of risk and performance
6. Regular assessment of risk
7. Standard contract clauses for all contracted services
Mandated Security Standards
8. Shared definition of minimum personal data requiring protection
9. Secure access to, rather than transfer of, data wherever practicable
10. Encryption to become the norm for all portable electronic media
11. Secure disposal of data and hardware when disposal is required
12. Penetration testing on systems holding data on large numbers of individuals
13. Strong access controls in new systems as they are brought on line
14. Audit trails and monitoring of user activity
15. Forensic readiness policies
16. Regular audit of compliance with policies by managers
17. Accreditation of new systems
Culture Change
18. Use of Privacy Impact Assessments for all new projects
19. All Departments to have plans to enhance culture and to monitor progress through surveys etc
20. Mandated training for all users of personal data and those in key roles
21. HR processes to ensure appropriate disciplinary action is taken
Greater Scrutiny
22. Coverage of information risks in annual reports
23. All Departments to issue an information charter (Care Record Guarantee for the NHS)
24. Reporting process for serious incidents
25. Encouraging staff to report concerns about information risk

DATA SHARING REVIEW: Recommendations

Developing Culture
1. Organisations should clarify senior executive ownership and accountability for the handling of personal information in their corporate governance arrangements
2. Companies should review internal controls over using and sharing personal information at least annually
3. Robust plain English privacy notices should be prominently published, giving details of information use, sharing and how people can access information
4. All organisations routinely using and sharing personal information should provide effective training for staff
5. Organisations should avoid collecting unnecessary personal information
The Legal Framework
6. The Government should assume a leadership role in promoting reform of European law
7. The IC should be required by law to produce a data sharing code of practice and be able to endorse context specific guidance that elaborates on the CoP
8. Primary legislation should provide SofS with power to remove legal barriers to information sharing but all use of such power should be reviewed by the IC
The Regulatory Body
9. Increased penalties for breach of the Data Protection Act
10. The new fine provisions in the Criminal Justice Act to be brought into force by 8 November 2008 (enable organisations including Gov Departments and individuals to be fined for not taking action when they new there was a risk
11. The IC should take into account failure to notify him of a breach when determining penalties
12. The IC to have statutory power to enter premises to carry out inspections
13. A new fee scheme to be introduced to provide more funding for the IC
14. The IC should be reconstituted as a multi-member Information Commission
Research & Statistical Analysis
15. Legislation to introduce 'safe havens' for processing data to support research and analysis
16. Government Departments should work with academic and other partners to set up safe havens
17. NHS to develop a system to resolve 'consent for consent' issues
Safeguarding & Protecting Publicly Available Information
18. Government to commission an enquiry into on-line services that aggregate personal information
19. Government to remove the provision allowing the sale of the edited electoral register

Securely destroying optical media

Context

This statement provides brief guidance on various methods of destroying Optical media¹ safely and securely.

It is believed this statement represents what is regarded as current good practice in this area.

If there are any questions regarding this statement or further assistance is required, please refer to the NHS CFH Infrastructure Security Team "Disposal & Destruction of Sensitive Data" Good Practice Guideline (GPG) document².

Alternatively, please contact the Infrastructure Security Team at:

cfh.infosecteam@nhs.net

Guidance

Methods

- The easiest and safest method of destroying optical media is with sandpaper. This can be done by using fine sandpaper to remove the top of the CD/DVD (the label side) until the clear part of the disk is revealed. If sandpaper is not available, any implement which can scratch into the label side of the media will do (e.g. scissors, pin.)
- Another method is to have the destruction of the optical media performed by a professional 3rd party which has dedicated equipment for this type of destruction. Many companies which destroy confidential paper waste in a secure manner will also provide a service to destroy optical media in a similarly secure fashion.

Devices

- Where there is a need to routinely destroy optical media, it is advisable to use a dedicated device for the media's safe destruction.
- The easiest way to achieve this is through the use of a CD shredder. These shredders generally destroy the media through either cutting the disk, or by scratching the surface. It is recommended to purchase a device capable of shredding the media such as those described at:

<http://www.shreddingmachines.co.uk/shredders.asp?id=1100&cat=Fellowes%20FS-9C%20Shredder>

¹ Optical Media: this includes Write Once (e.g. CD-ROM, DVD-R) and Write Many (e.g. CD-RW, DVD-RW)

² <http://www.connectingforhealth.nhs.uk/infrasec/gpg/index.htm>