



All Chief Information Officers
Strategic Health Authorities

Gateway Ref 9424

*From Matthew Swindells,
Director General of Information and
Programme Integration*

*Room 430
Richmond House
79 Whitehall
London
SW1A 2NS*

020 7210 5553

matthew.swindells@dh.gsi.gov.uk

30 January 2008

Dear Colleague

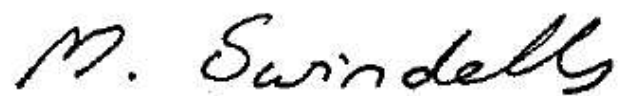
I am writing, further to the recent letter from David Nicholson, to formally confirm that the movement of unencrypted person identifiable data held in electronic format should not be allowed in the NHS. This is the default position to ensure that patient and staff personal data is protected. Any data to be stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should be encrypted. This is also now a requirement across all public sector organisations from the Cabinet Secretary.

As part of the review that you are undertaking of your own organisation and those other NHS organisations within the area of your SHA responsibilities, I would be grateful if you would pay particular attention to this aspect. Wherever possible, person identifiable data should always be stored on a secure server. Where this is not possible and preventing the movement of unencrypted data will adversely affect patient care, there should be a risk assessment of the storage of data locally and on removable devices.

Trusts will need to make a local judgement on the balance of risk to patient care against risk to personal data security in determining whether use of unencrypted devices should continue as an interim measure. Where it is decided that unencrypted data is necessary for the benefit of patients, the mechanism of reporting to the Trust Board that David Nicholson explained in his recent letter should be used. This ensures that, for governance purposes, the outcome of the risk assessment has been reported to the Board where accountability lies, so that they can approve a situation where data vulnerability exists and where working practices have been curtailed in the interests of data security.

NHS Connecting for Health will provide the technical guidance on encryption and they are also putting arrangements in place to ensure that bulk records can be encrypted when their transfer is essential for patient care or for business continuity purposes.

Yours sincerely

A handwritten signature in black ink that reads "M. Swindells". The signature is written in a cursive style with a large, prominent initial "M".

Matthew Swindells
Director General (Information and Programme Integration)