

Press Release

For immediate release

Date: 15 June 2010

Poor data security in the NHS

The Information Commissioner's Office (ICO) remains highly concerned that data breaches involving people's personal information are continuing to occur in NHS organisations. Today NHS Stoke-on-Trent and Basingstoke and North Hampshire NHS Foundation Trust are the latest NHS bodies found to have breached the Data Protection Act (DPA). Both NHS organisations' chief executives have signed [formal Undertakings](#) outlining that they will process personal information in line with the DPA. A quarter (250) of all data breaches reported to the ICO are from the NHS.

Mick Gorrill, Head of Enforcement at the ICO, said: "Everyone makes mistakes, but regrettably there are far too many within the NHS. Health bodies must implement the appropriate procedures when storing and transferring patients' sensitive personal information. We have taken a number of steps to explain the importance of personal data to NHS bodies and help them comply with the law. We will continue to do so."

2,000 paper physiotherapy records were not filed within [NHS Stoke-on-Trent](#)'s archive system and may have accidentally been destroyed or misfiled. At [Basingstoke and North Hampshire NHS Trust](#) an excel spreadsheet, containing 917 patients' pathology results, was emailed via an unsecure address to another department. The spreadsheet was not

password protected and the receiving department had no business need to have access to the excessive amount of clinical records.

The NHS organisations have agreed to implement a number of security measures to protect personal information more effectively. All staff will be made aware of the organisations' policies for the retention and use of personal data and will receive training on how to follow those policies.

NHS Stoke-on-Trent will also apply physical security measures in respect of paper medical records, particularly when they are in transit.

Basingstoke and North Hampshire NHS Trust will only extract and transfer the minimum amount of personal information necessary for any processing requirement. With immediate effect, it will encrypt all portable and mobile devices used to store and transmit personal data.

The ICO can issue a monetary penalty for serious breaches of the Data Protection Act. Monetary penalties are reserved for the most serious cases and this power can only be exercised in limited circumstances. The ICO has made full use of the most appropriate regulatory powers in the two cases highlighted here.

A full copy of the Undertakings can be viewed here:

http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx

Please see below for a link to the latest data breach table

http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/breach_notification_spreadsheet_may2010.pdf

Please see below for a link to the ICO's Guide to Data Protection

http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/the_guide_to_data_protection.pdf

ENDS

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at: www.ico.gov.uk

Notes to Editors

Basingstoke and North Hampshire NHS Foundation Trust

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Third and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

- Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software which meets the current standard or equivalent;
- Only the minimum data necessary for the intended purpose is extracted and/or transferred for any processing requirement;
- Physical security measures are adequate to prevent unauthorised access to personal data, in particular data must be subject to password and/or encryption protection where appropriate;
- Staff are aware of the data controller's policy for the retention, storage, transfer and use of personal data and are appropriately trained how to follow that policy;
- The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

NHS Stoke-on-Trent

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

- Physical security measures in respect of paper medical records are sufficiently adequate to prevent unauthorised access to, accidental loss or destruction of, or damage to personal data, particularly when records are in transit;
- Staff are aware of the data controller's policy for the retention, archiving, storage and use of personal data and are appropriately trained how to follow that policy;
- The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

1. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
2. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003
3. Organisations can now sign the Personal Information Promise to demonstrate their commitment to protecting people's personal information by visiting the website at www.ico.gov.uk
4. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk. Alternatively, you can find us on Twitter at www.twitter.com/ICOnews
5. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
 - Fairly and lawfully processed
 - Processed for limited purposes
 - Adequate, relevant and not excessive
 - Accurate and up to date
 - Not kept for longer than is necessary
 - Processed in line with your rights
 - Secure
 - Not transferred to other countries without adequate protection