



**Information Commissioner's Office**  
Promoting public access to official information  
and protecting your personal information

**Press Release**  
**14 July 2009**

### **NHS puts over 20,000 records at risk**

The Information Commissioner's Office (ICO) is issuing further warnings to NHS bodies about the importance of data security, after finding five more NHS organisations in breach of the Data Protection Act. In one case, a ward hand-over sheet containing notes about patients' health was left on a bus.

The Royal Free Hampstead NHS Trust reported the loss of an unencrypted compact disk containing medical treatment details of 20,000 patients from the hospital's cardiology department.

Chelsea and Westminster Hospital Foundation Trust reported the theft of an unencrypted memory stick containing 143 patient details including sensitive medical information. The Trust believes that the information was stolen from an unlocked office that was being used as a walk-in clinic. The memory stick was not password protected or encrypted, and an employee had been taking it home for use on his personal computer.

It emerged that Epsom and St Helier University Hospital NHS Foundation Trust was storing hospital records insecurely for nearly two years following data being transferred between hospitals.

A ward handover sheet, containing information relating to 23 patients in the care of Surrey and Sussex NHS Trust, was found on a bus. The Trust also reported the theft of two laptop computers. Although they were kept behind three locked doors, they were not encrypted.

Hampshire Partnership NHS Trust informed the ICO about the theft of an unencrypted laptop computer holding the personal data of 349 patients and 258 staff. The laptop was stolen from an employee attending a health conference.

Some of the information was classified as sensitive personal data as defined in Section 2 of the Act. The NHS bodies have agreed to implement the appropriate security measures to ensure that personal details are properly protected by establishing physical safeguards, such as locking an office. Staff will be appropriately trained on the policy for storage and how to follow that policy. Laptops, mobile and portable devices held by The Royal Free Hampstead NHS Trust, Chelsea and Westminster Hospital NHS Foundation Trust and Hampshire Partnership Trust will be password protected and encrypted.

Sally-anne Poole, Head of Enforcement and Investigations at the ICO, said: “These five cases serve as a reminder to all NHS organisations that sensitive patient information is not always being handled with adequate security. It is important that staff adhere to policies designed to protect individuals’ sensitive information.

“Data protection must be a matter of good corporate governance and executive teams must ensure they have the right procedures in place to properly protect the personal information entrusted to them. Failure to do so could result in patient information, including sensitive medical records and treatment details falling into the wrong hands.

“The Data Protection Act clearly states that organisations must take appropriate measures to ensure that personal data is kept secure. These five organisations recognise the seriousness of these data losses and have agreed to take immediate remedial action.”

Failure to meet the terms of an Undertaking is likely to lead to enforcement action by the ICO. A copy of the Undertakings can be downloaded from

[http://www.ico.gov.uk/what we cover/data protection/enforcement.aspx](http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx)

## 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](http://www.ico.gov.uk)

### Notes to Editors

1. The Information Commissioner's Office promotes public access to official information and protects personal information. The ICO is the UK's independent influential and practical authority on information rights and responsibilities, making a difference to people.
2. The Royal Free Hampstead NHS Trust, Chelsea and Westminster Hospital NHS Foundation Trust, Epsom & St Helier University Hospitals NHS Trust, Surrey and Sussex Healthcare NHS Trust and Hampshire Partnership NHS Trust have all signed formal Undertakings outlining that they will process personal information in line with the Data Protection Act.
3. 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.
4. 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](http://www.ico.gov.uk)
5. For more information about the Information Commissioner's Office subscribe to our e-newsletter at [www.ico.gov.uk](http://www.ico.gov.uk)
6. 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