

## **Press Release**

### **For immediate release**

24 August 2010

#### **Sensitive medical records left at bus stop**

The Information Commissioner's Office (ICO) has found Royal Wolverhampton Hospitals NHS Trust in breach of the Data Protection Act (DPA) after the loss of over 100 patient records.

The ICO was alerted to the loss of a CD which contained scans of 112 patient records from the Intensive Care Unit of New Cross Hospital's Heart and Lung Unit. The CD was discovered at a bus stop near the hospital and was unencrypted with no password protection.

Mick Gorrill, Head of Enforcement at the ICO said: "The fact that this information was several years old is of no consequence – patients' personal data should always be handled in accordance with the Data Protection Act. I am pleased that the Trust has agreed to take remedial steps to ensure such an incident does not happen again."

Investigations by the Trust and the ICO were unable to ascertain exactly why or how the CD was ever made, although it was established that there were areas of weakness in the Trust's data protection procedures. This included a lack of timeliness in recalling patients' charts that had been released to consultants.

The Trust has agreed to sign a [formal Undertaking](#) outlining that it will now process personal information in line with the DPA. The Trust will

implement a number of security measures to protect personal information more effectively. These include ensuring that patient charts released to consultants are signed for on receipt and chased for return after just one week. Compliance with the Trust's policies on data protection and records management will also be regularly monitored.

A full copy of the Undertaking can be found here:

[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 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:
  - All staff are aware of the data controller's policies for the storage and use of personal data and the management of patient records, and are appropriately trained how to follow those policies;
  - Compliance with the data controller's policies on data protection and records management is appropriately and regularly monitored;
  - Patient charts released to consultants are signed for on receipt and chased for return after one week and weekly thereafter;
  - 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.
2. The Information Commissioner's Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
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. For more information about the Information Commissioner's Office subscribe to our e-newsletter at [www.ico.gov.uk](http://www.ico.gov.uk). Alternatively, you can find us on Twitter at [www.twitter.com/ICOnews](http://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
6. The Data Protection Act (1998) does not cover the acts of interception of communications or 'hacking' of personal information. The interception of communications falls under the Regulation of Investigatory Powers Act (2000) which is regulated by the Interception of Communications Commissioner.
7. The ICO has legal powers to ensure that organisations comply with the requirements of the Data Protection Act. In using its regulatory powers, the ICO considers the nature and severity of the breach which has occurred. Dependent on circumstances, the powers the ICO has at its disposal include:
  - conducting assessments to check organisations are complying with the Act;
  - serving information notices requiring organisations to provide the ICO with specified information within a certain time period;
  - serving enforcement notices requiring organisations to take specified steps in order to ensure they comply with the law;
  - issuing monetary penalties of up to £500,000 for serious breaches of the Data Protection Act;
  - conducting audits to assess whether organisations are processing personal data in accordance with good practice;
  - reporting to Parliament on data protection issues of concern;
  - prosecuting those who commit criminal offences under the Act. The ICO prosecutes individuals and organisations for specific breaches of the Act such as the illegal trading of personal data and non-notification.