

## **Press Release**

30 September 2010

### **Forth Valley NHS Board puts sensitive patient details at risk**

The Information Commissioner's Office (ICO) has found the Forth Valley NHS Board in breach of the Data Protection Act (DPA) after the loss of sensitive personal data relating to Board staff and patients.

The ICO was informed that an unencrypted memory stick with no password protection and containing personal information held by the Forth Valley NHS Board had been handed in to the press. Enquiries established that the information had been uploaded by a member of staff onto a personally owned memory stick that was then lost or stolen.

Ken Macdonald, Assistant Commissioner for Scotland at the ICO said:

"This case highlights the importance of health bodies complying with the Data Protection Act when storing and transferring patients' sensitive personal information. All staff members should be fully aware of the policies and procedures in place to safeguard personal information to stop it falling into the wrong hands. I am pleased the organisation is taking remedial steps to ensure such an incident does not happen again."

Fiona Mackenzie, Chief Executive Officer of the Forth Valley NHS Board, has signed [a formal undertaking](#) outlining that the organisation will only use portable and mobile devices issued by the Board to process personal data. All staff members will be fully aware of the policies and procedures in place to safeguard personal information and will be appropriately

trained to follow those policies. The Board will also implement a number of security measures to protect personal information more effectively, including physical security measures to prevent the upload of Board data onto any unauthorised mobile device.

A full copy of the undertaking can be found here:

[http://www.ico.gov.uk/Home/what we cover/promoting data privacy/taking action.aspx#undertakings](http://www.ico.gov.uk/Home/what_we_cover/promoting_data_privacy/taking_action.aspx#undertakings)

## **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:
  - As from 31st December 2010, any new Board issued portable and mobile devices including memory sticks and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, will be encrypted using encryption software which meets the current standard or equivalent;
  - Physical security measures are adequate to prevent unauthorised access to personal data, and in particular the uploading of Board data onto any unauthorised mobile device;
  - Encryption software will be rolled out to assist in securing physical access from desktops to mobile media to the majority of the core sites. Essentially this will cover core Hospital and NHS FV COIN connected sites. Remote community and GP sites will be investigated and covered in the medium to longer term;
  - 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.
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:
  - 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.