

Press Release

For immediate release

03 June 2010

8,000 people's details lost in transit in Lampeter

The Information Commissioner's Office (ICO) has found Lampeter Medical Practice to be in breach of the Data Protection Act, after an unencrypted memory stick containing the personal details of 8,000 patients was reported lost to the privacy watchdog.

In March 2010, a member of staff downloaded a database containing patient details in contravention of practice policy. The staff member downloaded the information on to an unencrypted and non password protected computer memory stick which was then posted by recorded delivery to the Health Boards Business Service Centre. The memory stick did not arrive at its intended destination and is now accepted to be lost.

Dr Rowena Mathew, Head of Practice of Lampeter Medical Practice, has [agreed to take remedial action](#) by ensuring that sufficient steps are taken to ensure a security breach doesn't occur again. This includes ensuring all mobile devices including laptops and memory sticks are encrypted, ensuring physical security measures are sufficient and making staff fully aware of the organisations' data security policy.

Sally-anne Poole, Enforcement Group Manager, said: "It is unnecessarily risky to download 8,000 personal details on to a memory stick. It is imperative that staff are made fully aware of an organisation's policy for

securing personal data and any portable device containing personal information should always be encrypted to prevent it being accessed in the event of loss or theft. I am pleased Lampeter Medical Practice has agreed to take action to prevent a similar security breach happening again.”

ENDS

A copy of the undertaking can be viewed here:

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

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

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:

1. 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;
2. Physical security measures are adequate to prevent unauthorised access to personal data, particularly in respect of the unauthorised use of computer memory sticks;
3. 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;
4. 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. 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

5. 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

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