

News release

1 July 2011

Health service must get it right on data security, says ICO

The health service needs to do more to keep patients' personal information secure, the Information Commissioner said today. The warning comes as the ICO finds a further five health organisations in breach of the Data Protection Act.

Information Commissioner, Christopher Graham, said:

"The health service holds some of the most sensitive personal information of any sector in the UK. Millions of records are constantly being accessed and we appreciate that there will be occasions where human error occurs. But recent incidents such as the loss of laptops at NHS North Central London - which we are currently investigating - suggest that the security of data remains a systemic problem.

"The policies and procedures may already be in place but the fact is that they are not being followed on the ground. Health workers wouldn't dream of discussing patient information openly with friends and yet they continue to put information on unencrypted memory sticks or fax it to the wrong number. The sector needs to bring about a culture change so that staff give more consideration to how they store and disclose data. Complying with the law needn't be a day-to-day burden if effective measures are built in and then become second nature.

“My office is working with Connecting for Health to identify how we can support the health service to tackle these issues.”

The five undertakings the ICO has issued to health bodies all relate to incidents where they failed to take appropriate steps to ensure that sensitive personal information was kept secure.

For example:

- In February 2011, Ipswich Hospital NHS Trust misplaced 29 patient records after a member of staff took them home to update a training log and then lost the records. The information, which included sensitive personal data relating to operations carried out on patients, was subsequently recovered. The Trust introduced mandatory data protection training for all relevant staff to be completed by 30 June 2011.
- Also in February 2011, Dunelm Medical Practice in Durham sent discharge letters about two patient's routine operations to the wrong recipient. A member of staff had failed to spot that they had entered the recipients' fax number incorrectly. The faxes were received by a third party organisation which immediately alerted County Durham and Darlington NHS Foundation Trust before destroying both documents. The Practice has now agreed to send Electronic Discharge Letters by secure email and only fax them in exceptional circumstances. The Practice will also programme the fax machine with the numbers for the regional branches to better protect the information in future.

Further undertakings have been signed by East Midlands Ambulance Service NHS Trust, Lancashire Teaching Hospitals NHS Foundation Trust and Basildon and Thurrock NHS Trust.

A full copy of all of the undertakings can be viewed here:

http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/taking_action.aspx#undertakings

The ICO has produced guidance for health organisations explaining their obligations to keep the personal information they handle secure, as well as giving advice on the security measures that must be in place. The guidance can be found here:

http://www.ico.gov.uk/for_organisations/sector_guides/health.aspx

The ICO has also carried out a number of audits with health organisations to help them identify ways in which they can improve their handling of personal information. Details of the audits carried out by the ICO can be found at:

http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/conducting_audits.aspx

ENDS

If you need more information, please contact the ICO press office on 0303 123 9070 or visit the website at: www.ico.gov.uk.

Notes to Editors

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. The ICO is on [Twitter](#), [Facebook](#) and [LinkedIn](#), and produces a monthly [e-newsletter](#). Our [For the media](#) page provides more information for journalists.
4. Anyone who processes personal information must comply with eight principles of the Data Protection Act, 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