

Press Release

For immediate release

Date: 14 July 2010

Birmingham Children's Hospital found in breach of privacy rules

The Information Commissioner's Office (ICO) has found Birmingham Children's Hospital NHS Foundation Trust to be in breach of the Data Protection Act (DPA).

The Information Commissioner was initially informed of a data security breach by the Trust after two unencrypted laptops containing personal information relating to 17 patients were stolen from the Medical Day Centre.

The laptops contained sensitive personal data such as patient diagnoses, video recordings and information on the health of the individual patients. The laptops belonged to the Respiratory Medicine department and were used as part of the diagnostic and on-going assessment of patients with breathing problems linked to sleep.

The Trust has agreed to sign a formal [Undertaking](#) outlining that it will now process personal information in line with the Data Protection Act. The Trust will implement a number of security measures to protect personal information more effectively. These include ensuring that the removal of encryption software against the Trust's security policies is prevented, all portable devices such as laptops and memory sticks used to store and transmit personal data are encrypted and that physical security measures are in place to prevent unauthorised access to personal information.

Mick Gorrill, Head of Enforcement at the ICO, said: "It is unacceptable to leave portable devices containing personal information unencrypted. The fact that these laptops contained sensitive personal data highlights the gravity of the case. I am pleased that the Trust has agreed to take these remedial steps to ensure such an incident does not happen again."

A full copy of the Undertaking can be found here:

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

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 1 of schedule 1 to the Act, and in particular that:
 - Adequate measures are put in place to ensure that data security policies are adhered to consistently across all data controller departments. Such measures would seek to ensure that the unauthorised removal of encryption software against the data controller's security policies is prevented, thereby removing any potential for unauthorised access to that personal data.
 - Portable and mobile electronic devices, including laptops, which are 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. Where such encryption software is genuinely incompatible with a programme performing a necessary data controller function, then the data controller must ensure other adequate means of ensuring data is held securely are implemented. This might include the use of a secure network system for the storage of such personal data.
 - Physical security measures are adequate to prevent unauthorised access to personal data. This includes adequate security management of areas that are not operational out of hours, adequate monitoring of swipe card door access and the effective use of security patrols.
 - 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. Alternatively, you can find us on Twitter at 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