



Information Commissioner's Office
Promoting public access to official information
and protecting your personal information

Press Release

30 April 2009

ICO issues stark reminder to NHS bodies on patient records

The Information Commissioner's Office (ICO) is reminding NHS bodies of the importance of data security having found four more NHS organisations in breach of the Data Protection Act.

Cambridge University Hospital NHS Foundation Trust, Central Lancashire Primary Care Trust, North West London Hospitals NHS Trust and Hull & East Yorkshire Hospitals NHS Trust have all signed formal [Undertakings](#) outlining that they will process personal information in line with the Data Protection Act. The organisations will implement a number of security measures to protect personal information more effectively. With immediate effect, all portable and mobile devices used to store and transmit personal data must be encrypted.

Cambridge University Hospital NHS Foundation Trust reported the loss of an unencrypted memory stick containing medical treatment details of 741 patients after a member of staff left it in an unattended vehicle. The memory stick, which was privately owned, was discovered by a car wash attendant who was able to access the contents to establish ownership. The information was downloaded without the knowledge of the Trust.

Central Lancashire Primary Care Trust reported the loss of an encrypted memory stick containing medical treatment details of 6,360 prison patients, some believed to be ex-inmates, of HMP Preston. The memory stick was thought to be lost by a member of staff returning it from the prison clinic to the administration offices. Despite being encrypted, the details could be easily accessed from a Post-It attached to the device listing the password necessary to read the information.

The North West London Hospitals NHS Trust reported the theft of two laptops and in a separate incident, the theft of a desktop computer, in total containing the details of test results and hospital numbers of 361 patients. The laptops were stolen from the audiology department of Central Middlesex Hospital whilst the desktop computer was taken from the Clinical Haematology offices at Northwick Park Hospital after the hospital security's swipe card system was disabled for maintenance. The laptops and desktop computer were password protected but not encrypted.

Hull & East Yorkshire Hospitals NHS Trust reported two incidents resulting in the loss and theft of a desktop computer and disused laptop in total containing unencrypted medical treatment details of 2,300 patients. The desktop computer, containing 300 patient details, was lost during the refurbishment of the Renal Peritoneal Dialysis Office whilst the laptop, containing the details of 2,000 urology cancer patients from before 2007, was stolen from a locked office.

All the NHS bodies will implement the appropriate security measures to ensure that personal details are properly protected by establishing physical safeguards, such as locking an office or ensuring a security swipe card system is working at all times. All mobile and portable devices held by all the organisations will be password protected and encrypted. Systems to restrict access to patient treatment details will be implemented to ensure that unauthorised access to personal information and unauthorised downloading do not occur. The four organisations will ensure every staff member is made aware of policies on data storage and the use of patient information, and, where necessary, training will be provided.

Mick Gorrill, Assistant Information Commissioner at the ICO, said: "These four cases serve as a stark reminder to all NHS organisations that sensitive patient information is not always being handled with adequate security. It is a matter of significant concern to us that in the last six months it has been necessary to take regulatory action against 14 NHS organisations for data breaches. In these latest cases staff members have accessed patient records without authorisation and on occasions, have failed to adhere to policies to protect such information in transit. There is little point in encrypting a portable media device and then attaching the password to it.

“Data protection must be a matter of good corporate governance and executive teams must ensure they have the right procedures in place to properly protect the personal information entrusted to them. Failure to do so could result in patient information, including sensitive medical records and treatment details falling into the wrong hands. Ultimately, the organisations risk losing the confidence of patients and their families.

“The Data Protection Act clearly states that organisations must take appropriate measures to ensure that personal information is kept secure. These four organisations recognise the seriousness of these data losses and have agreed to take immediate remedial action.”

Failure to meet the terms of the undertaking is likely to lead to enforcement action by the ICO. A copy of the undertakings can be downloaded from 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 Information Commissioner's Office has ordered a number of organisations to sign undertakings following breaches of the Data Protection Act. Organisations include the Department of Health, Foreign and Commonwealth Office and Orange Personal Communications Services Ltd.
2. The ICO promotes public access to official information and protects personal information. The ICO is an independent body with 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. For more information about the Information Commissioner's Office subscribe to our e-newsletter at www.ico.gov.uk
4. 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