



Information Commissioner's Office

Press Release

For immediate release

22 January 2010

Privacy watchdog takes action after thousands of health records are stolen

Mark Hackett, the Chief Executive of Southampton University Hospitals NHS Trust (SUHT), has made a formal commitment to improve data security after the Information Commissioner's Office (ICO) found SUHT in breach of the Data Protection Act.

On 19 October 2009 a member of SUHT staff left an unencrypted laptop containing sensitive personal information in a retinal screening vehicle. The vehicle was unlocked and unattended. The laptop contained around 33,000 password protected patient records including details about patients' type of diabetes and results of retinal screening tests. The laptop was attached to the van by a security cable which was cut during the theft.

Sally-anne Poole, Head of Investigations at the ICO, said: "Storing large volumes of personal information on portable devices is unnecessarily risky. Why were so many records downloaded on to an unencrypted laptop in the first place? It is vital that NHS organisations ensure their staff handle personal information securely, especially where so much sensitive personal information is concerned. I am pleased that SUHT has taken action to guard against security breaches of this nature in future."

A copy of the Undertaking can be downloaded from

[http://www.ico.gov.uk/what we cover/data protection/enforcement.aspx](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 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 relation to data held within mobile clinics;
 - (3) Staff are aware of the data controller's policy for the storage 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 process, 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. 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. 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
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
6. "Sensitive personal data" means personal data consisting of information as to—
 - the racial or ethnic origin of the data subject,
 - his political opinions,

- his religious beliefs or other beliefs of a similar nature,
- whether he is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992),
- his physical or mental health or condition,
- his sexual life,
- the commission or alleged commission by him of any offence, or
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.