



Information Commissioner's Office

Press Release

22 October 2009

Local NHS Trust pledges to improve data security

Antony Sumara, the Chief Executive of Mid Staffordshire NHS Foundation Trust, has agreed to take action to comply with the Data Protection Act following a significant security breach. The breach occurred after a member of the Trust's human resources team transferred personal information to a home computer. The information, known as a 'Statement of Case', contained sensitive personal details about an employee and two further documents. Some of the information related to the employee's previous criminal conviction.

Investigators at the Information Commissioner's Office (ICO) considered this security breach very carefully. The ICO found that the information in question was not password or encryption protected and that the Trust had breached the Data Protection Act by failing to comply with security requirements. Antony Sumara has signed an [Undertaking](#) with the ICO pledging to adopt a wide range of security improvements, including the introduction of new rules for staff concerning personal information when working at home. The Undertaking notes that, after discovering the breach had occurred, the Trust initially 'failed to demonstrate appropriate urgency' to secure the data concerned. Should data security breaches be suspected in the future, the Trust has pledged to take appropriate remedial action as soon as is practicable to recover, or prevent access to, any data rendered insecure.

Mick Gorrill, Assistant Information Commissioner, said: "I strongly advise organisations to avoid instances where employees can download and transfer personal information to home computers. This incident should never have occurred and could easily have been averted. If personal details fall into the wrong hands, individuals can experience considerable distress. It is vital that personal information

is handled securely, especially where sensitive personal information, such as conviction data is concerned. I am pleased that the Trust is taking remedial action to guard against security breaches of this nature.”

A copy of the Undertaking can be downloaded from

http://www.ico.gov.uk/what_we_cover/data_protection/enforcement.aspx and the ICO's guidance on managing breaches is [here](#).

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 is processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular:
 - Physical security measures are adequate to prevent unauthorised access to, and or transfer of, personal data;
 - The policy covering the storage and use of personal data is followed by staff, particularly in respect of staff working from home;
 - 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. Consideration should be given to the provision of periodic refresher training and the 'dip sampling' of staff understanding of the policy;
 - The data controller shall implement a formal 'Working from home' policy which will ensure the security of Trust data accessed from any such remote site. The policy to be introduced within 3 months from the date of the signing of this undertaking;
 - Trust policies are amended as appropriate to include explicit reference to staff data in terms of protecting personal information;
 - 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.
 - 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;
 - Where a data security breach is suspected, the data controller will take appropriate remedial action as soon as practicable to ensure the recovery of, or prevent access to, any data rendered insecure;

- The Trust IT Security policy to be amended to require that where a data security breach is suspected the Director of Nursing and Governance is informed as soon as practicable.
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
 6. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
 - a) Fairly and lawfully processed
 - b) Processed for limited purposes
 - c) Adequate, relevant and not excessive
 - d) Accurate and up to date
 - e) Not kept for longer than is necessary
 - f) Processed in line with your rights
 - g) Secure
 - h) Not transferred to other countries without adequate protection