

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Imperial College Healthcare NHS Trust
St Mary's Hospital
The Bays Building
South Wharf Road
London

I, Professor Stephen Smith, Chief Executive of Imperial College Healthcare NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Imperial College Healthcare NHS Trust is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried out by the Trust and is referred to in this Undertaking as the "data controller". Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.
2. The Information Commissioner (the "Commissioner") was provided with a report from the Trust's Interim Information Governance Manager, acting on behalf of the data controller, regarding the theft of 6 laptop computers (In two separate incidents of theft) and the loss of a small number of paper records which contained, in total, personal data relating to some 6,000 of the Trust's patients.
3. One laptop computer, which was not Trust owned, was password protected but was unencrypted. It contained data relating to medical treatment ("sensitive personal data" as defined by the Act). The laptop computers were stolen by means of burglary from a secure area within the hospital. The paper records were contained within a cycle pannier which was lost in transit.
4. The data controller did not ensure sufficient security measures were in place to prevent the unauthorised or unlawful processing of the data in question. In particular the computer held data was not protected by the Government minimum standard of encryption. The Commissioner has taken into account the fact that the personal data in question related to medical treatment and could therefore potentially result in significant distress being caused to the individuals concerned.
5. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the Seventh Data Protection Principle. This Principle is set out in Schedule 1 Part 1 of the Act.
6. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:-

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 or from other data controllers in similar circumstances, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part 1 of the Act, and in particular that:

- (1) The data controller shall take all reasonable measures to ensure the physical security of personal data being processed in furtherance of the duties of the Trust;
- (2) 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;
- (3) The data controller shall implement such other security measures it deems appropriate to ensure that personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage;
- (4) Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained on how to follow that policy. In particular staff should be made aware of Trust agreed retention periods and should ensure that data is not retained for longer than is necessary.

Dated..... 29/7/09

Signed.....

Professor Stephen Smith,
Chief Executive
Imperial College Healthcare NHS Trust
St Mary's Hospital
The Bays Building
South Wharf Road
London

Signed...

Mick Gorrill
Assistant Commissioner Regulatory Action Division
For and on behalf of the Information Commissioner.