

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: The North West London Hospitals NHS Trust

 Northwick Park Hospital
 Watford Road
 Harrow
 Middlesex
 HA1 3UJ

I, Ms Fiona Wise, Chief Executive of The North West London Hospitals NHS Trust (the Trust), Northwick Park Hospital, Watford Road, Harrow, Middlesex, HA1 3UJ, for and on behalf of the Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. The North West London Hospitals 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 two reports from Mr Rick Juniper acting on behalf of the data controller, regarding the theft of two laptop computers and, in a separate incident, the theft of a desktop computer. Both the laptop computers and the desktop computers held the personal data of patients of the data controller.
3. In the first of these incidents, two laptop computers were stolen from the Audiology department of Central Middlesex Hospital. The laptops held information relating to 181 babies including their name, date of birth, NHS or hospital number and hearing test results. There were no signs of forced entry to the offices involved. The data in question was password protected but was not encrypted.
4. In the second of these incidents, a desktop computer was stolen from the data controller's Clinical Haematology offices at Northwick Park Hospital. The computer held information relating to 180 patients of the data controller including their name, hospital number, date of birth and some clinical follow up information. At the time of the theft, the swipe card security system that controlled entry to the building had been disabled for maintenance. The database containing the personal data in question was password protected, but was not encrypted.
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. The Commissioner has also considered the fact that some of the data stolen in these incidents consisted of information as to the physical or mental health or condition of the data subjects. Personal data containing such information is defined as "sensitive personal data" under Section 2(e) 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) 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 and procedures are adequate to prevent the theft of desktop computers that contain personal data, or ensure that such desktop computers are encrypted using encryption software which meets the current standard or equivalent;**
- (3) A clear policy covering the storage and use of personal data is implemented;**
- (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;**
- (5) 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.**

Dated..... 19th MARCH 2009

Signed.....
Fiona Wise
Chief Executive
The North West London Hospitals NHS Trust

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