

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Chelsea & Westminster Hospital
NHS Foundation Trust
369 Fulham Road
London
SW10 9NH

I, Heather Lawrence, Chief Executive of Chelsea & Westminster Hospital NHS Foundation Trust (the Trust), 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:

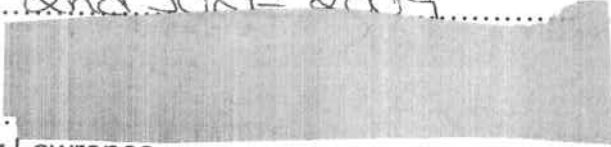
1. Chelsea & Westminster Hospital NHS Foundation Trust is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the "Act"), in respect of the processing of personal data carried out by the Trust and is referred to in this Undertaking as the "data controller". Section 4(4) of 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 data controller, regarding the theft of an unencrypted USB memory stick that held the personal data of patients of the data controller.
3. The memory stick was stolen from an unattended and unlocked office being used for a walk in clinic. The memory stick belonged to the employee holding the clinic and held sensitive information relating to 143 patients which was not even password protected. The Trust employee was not aware that secure network drive and encryption facilities were available and used their own memory stick because Trust equipment was not available. It was also discovered that the Trust employee had used the memory stick and their own computer for home working.
4. 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.


5. 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 are adequate to prevent unauthorised access to personal data;**
- (3) The policy covering the storage and use of personal data is followed by staff;**
- (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... 2nd June 2009

Signed.. 
Heather Lawrence
Chief Executive
Chelsea & Westminster Hospital NHS Foundation Trust

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