

DATA PROTECTION ACT 1998

6/10/10

UNDERTAKING

Data Controller: Healthcare Locums Plc

10 Old Bailey
London
EC4M 7NG

I, Mo Dedat, Chief Operating Officer of Healthcare Locums Plc, for and on behalf of Healthcare Locums Plc hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Healthcare Locums Plc 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 Healthcare Locums Plc 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 of a security breach involving the loss and recovery of a network storage device containing personal data relating to doctors employed by the data controller. Neither the network storage device, nor the personal data contained within it, was encrypted.
3. In February 2010, the network storage device was due to be transferred from the data controller's Skipton branch to its Loughton branch with a number of other pieces of equipment for secure storage prior to decommissioning. At the time, no inventory of the equipment being transferred was taken, and it was assumed that all pieces of equipment had reached the Loughton branch safely. However, on 21 June 2010, the data controller was contacted by an individual who stated that he had been sold the network storage device via the website eBay. The device was eventually returned to the data controller and the personal data stored on it was wiped. The data controller was not aware of the number of individuals affected by this incident. The information held on the device

consisted of personal data relating to doctors employed by the data controller. The doctors' files consisted of documentation relating to their security clearance, public registrations, visa documentation and proof of identity.

4. Following further questioning by the Commissioner, it became apparent that the network storage device had most likely been lost or stolen in transit, as the devices being transferred were stored securely at both the data controller's Skipton and Loughton branches. However, no investigation was carried out by the data controller into the actions of the company contracted to transport the equipment (the "data processor"), nor was there a contract in place between the data controller and the data processor as required by Schedule 1 Part II Paragraph 12 of the Act.
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 I to the Act. It should be noted that compliance with Schedule 1 Part II Paragraph 12 of the Act is required in order to comply with the Seventh Data Protection principle when a data processor is used by a data controller.
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, 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) **Contracts are put in place between the data controller and any contractors it uses to process personal data on its behalf, which comply with the requirements laid out in Schedule 1 Part II Paragraph 12 of the Act;**
- (2) **Adequate checks are carried out on contractors and their staff before such contracts are entered into, and compliance with such contracts will be monitored by the data controller;**

- (3) **Physical security measures put in place by both the data controller and any contractors are adequate to prevent unauthorised access to personal data;**
- (4) **Inventories of equipment used to process personal data will be kept to ensure that similar incidents are detected quickly;**
- (5) **A record of the personal data held on any device used to process personal data will be kept to ensure that this can be identified in the event that a device is lost or stolen;**
- (6) **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.**

Dated..... 6/10/10

Signed.....
Mo Dedat
Chief Operating Officer
Healthcare Locums Limited

Signed.....
Mick Gorrill
Head of Enforcement
For and on behalf of the Information Commissioner