

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: The Royal Free Hampstead NHS Trust
Royal Free Hospital
Pond St
London
NW3 2QG

I, Charles Bruce, Interim Chief Executive of The Royal Free Hampstead NHS Trust, Pond St, London, ('The Trust') 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 Royal Free Hampstead 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 on 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 regarding a missing disk containing patient information from the hospital's Cardiology Department.
3. The disk was password protected but not encrypted and was initially believed to contain echocardiography test data from the period 2000 to 2006 relating to approximately 20,000 patients. The member of staff responsible for downloading the data was believed to have known of the data loss for approximately five months before reporting it. Further investigation by the Trust revealed the staff member involved can no longer remember any details of the download. The Trust states that it is not possible to identify what information was copied to the disk. The whereabouts of the disk and the precise circumstances regarding its loss are unknown.
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 at Part I of Schedule 1 to the Act. The Commissioner has also considered the fact that the data involved in this incident 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.

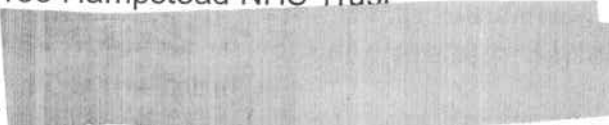
5. In view of the circumstances of this incident and the remedial steps taken by the data controller as a result, it has been agreed that, in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

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 is processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to 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) 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;**
- (4) The policy covering the storage and use of personal data is followed by staff;**
- (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..... 8th June 2009

Signed. 
Charles Bruce
Interim Chief Executive
Royal Free Hampstead NHS Trust

Signed. 
Mick Go (Assistant Commissioner, Regulatory Action Division)
For the Information Commissioner