DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: University College London Hospitals NHS Foundation Trust

250 Euston Road
London
NW1 2PG

I, Robert Naylor, Chief Executive of University College London Hospitals NHS Foundation Trust (UCLH), 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. University College London Hospitals 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 by Brighton and Sussex University Hospitals NHS Trust (BSUH) concerning the discovery of an unencrypted memory stick which had been left plugged into a computer in a training room at a BSUH Hospital in October 2010. The memory stick subsequently proved to be the personal property of a doctor employed at BSUH who was conducting research at UCLH. The device contained urology images, patient diagnosis and a spreadsheet indexing patients.

3. The memory stick in question contained sensitive personal data relating to 750 UCLH patients, the doctor had been given access to UCLH clinical systems by a UCLH employee supervising their MSc course. While access to patient information was provided to facilitate academic studies, sensitive personal data should not have been removed from UCLH systems on an unencrypted and unapproved portable device.

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 I to the Act. The Commissioner has also considered the fact that some of 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. 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) Portable and mobile devices including memory sticks 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 standards or equivalent;

(2) Staff acting as educational supervisors are made aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;

(3) Access to personal data for non-clinical purposes such as research and education is appropriately and regularly monitored for compliance with the data controller's policies on data protection and IT security;

(4) 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

Signed ……
Sir Robert Naylor
Chief Executive
University College London Hospitals NHS Foundation Trust

Signed ……
Sally Anne Poole
Head of Enforcement
For and on behalf of the Information Commissioner