DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Nightingale Practice
City & Hackney Teaching Primary Care Trust
St. Leonard's
Nuttall Street
London N1 5LZ

I, Dr Sarah Williams, of Nightingale Practice, within City & Hackney Teaching Primary Care Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. The Nightingale Practice within the City & Hackney Teaching Primary Care 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 Trusts Information Governance Manager acting on behalf of the data controller, regarding the theft of 10 back up tapes and a USB portable hard drive which contained the personal data of some 7,700 patients of the data controller. The portable USB hard drive and 5 of the back up tapes were not encryption protected.

3. The portable USB hard drive contained data relating to medical records ("sensitive personal data" as defined by the Act). It is understood that the device and the back up tapes were kept in a locked firesafe in locked and alarmed premises.

4. The data controller did not ensure sufficient security measures were in place to prevent the theft of the data in question. In particular the Practice failed to ensure that the data was protected by the mandatory minimum standard of encryption. The Commissioner has taken into account the fact that the personal data in question related to medical treatment and could therefore potentially result in significant distress being caused to the individuals concerned. It is understood that the practice relies on the IT department of the PCT to provide encryption, and that at the time of the theft this service had not been made available by the PCT.

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.

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) The data controller shall take all reasonable measures to ensure the physical security of personal data being processed in furtherance of the duties of the Practice;

(2) Portable and mobile devices, including USB hard drives, 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 as soon as practicable, and in any event by no later than 26 February 2010;

(3) 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;

(4) Physical security measures, including on site storage and the quantity of back up tapes retained, are adequate, but not excessive, to prevent unauthorised access to personal data;

(5) 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.

Dated....10/7/09.....

Signed [redacted]

Dr. Sarah Williams
Nightingale Practice
City & Hackney Teaching Primary Care Trust

Signed... [redacted]

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