DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Southampton University Hospitals NHS Trust

Southampton General Hospital
Tremona Road
Southampton
Hampshire
SO16 6YD

I, Mark Hackett, Chief Executive of Southampton University Hospitals NHS Trust (SUHT), Southampton Hospital, Tremona Road, Southampton, Hampshire, SO19 6YD, for and on behalf of SUHT hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Southampton University Hospitals 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 out by SUHT, 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 an incident that took place on 19 October 2009 in which a laptop computer was stolen from a retinal screening vehicle.

3. Sensitive data was being held on a password protected but unencrypted laptop, which was stolen when the SUHT employee in charge of staffing the vehicle left it unlocked and unattended. The laptop was attached to the vehicle by a security cable which was cut during the theft. The information consisted of approximately 33,000 patient records including type of diabetes condition and in some cases, the results of patients' retinal screening tests.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in 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 stolen 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 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, particularly in relation to data held within mobile clinics;

(3) Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;

(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 process, accidental loss, destruction, and/or damage.

Dated..... 14 DECEMBER 2009

Signed.....
Mark Hacke
Chief Executive
Southampton University Hospitals NHS Trust

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