DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Salford Royal NHS Foundation Trust

Stott Lane
Salford
M6 8HD

I, David Dalton, Chief Executive, on behalf of Salford Royal NHS Foundation Trust, Stott Lane, Salford M6 8HD (the Trust), hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Salford Royal 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 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 was provided with a report from the data controller's Information Governance Manager, regarding the theft of a desktop computer containing personal data relating to around 3500 patients from a locked office in the neurosciences department. Some of the data lost was "sensitive personal data" as defined in section 2 of the Act.

3. The computer had a Windows password in place, but was not encrypted, and the personal data was contained in Word and Excel documents with no further password protection. The computer was not secured to the desk. Some of the data had been copied from another computer, due for decommissioning, but the data was also retained on that old machine. Initially, the incident was treated only as a theft of equipment, resulting in a delay of over one month in reporting and investigating the loss of personal data.

4. The Information Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Fifth and Seventh Data Protection Principles. These are set out at Part I of Schedule 1 to 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 Information 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 Fifth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

- ***The data controller shall ensure that appropriate security measures are in place to restrict access to areas where personal data is stored;***

- ***The data controller shall ensure that personal data is held on secure network servers so that none is stored on the hard drives of desktop computers, and that all desktop computers and laptops located on the wards are secured to desks to prevent easy removal;***

- ***The data controller shall ensure that any personal data required to be held on a laptop computer or other removable media either by the data controller, or by a data processor processing data on the data controller's behalf, is suitably encrypted so as to provide effective protection against unauthorised access;***

- ***The data controller shall ensure that no personal data is retained on any laptop computer or other removable media for longer than is required for the purpose(s) for which it was initially stored on those media and that, as soon as it is no longer needed (and in any event before disposal of the storage media), personal data is securely erased;***

- ***The data controller shall enforce the use of strong passwords on all computer equipment;***

- ***The data controller shall implement mandatory induction training in data protection and IT security for all staff, including temporary staff, recording each individual's level of understanding to identify training needs, and shall refresh such training on a regular mandatory basis;***

- ***The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised or unlawful processing, accidental loss, destruction and/or damage.***

Dated....22/5/09.....

Signed..
David Da... (Chief Executive)
For Salford Royal NHS Foundation Trust

Signe...
Mick Gorrill (Assistant Commissioner, Regulatory Action Division)
For the Information Commissioner