DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Warrington and Halton Hospitals NHS Foundation Trust

Warrington Hospital
Lovely Lane
Warrington
Cheshire
WA5 1QG

I, Melany Pickup, Chief Executive of Warrington and Halton Hospitals NHS Foundation Trust (the "Trust"), 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. Warrington and Halton 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 by the data controller with a report of the theft of an unencrypted laptop storing personal data. The laptop was used by the Audiology department to carry out medical diagnostics. The laptop stored 110 patients' names, addresses, telephone numbers and medical charts. It was noted that it was unlikely that the medical charts would be intelligible to anyone other than an audiology professional.

3. It is the data controller's policy to encrypt all portable media. The laptop had no alternative security features and was not password protected. This laptop was not encrypted because it was issued by the Medical Engineering department as a diagnostic device. A failure in internal communication meant that the laptop was not identified as a security risk by the data controller's IT department. The data controller has proposed appropriate remedial action following this incident.

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 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. Where encryption software is incompatible with equipment performing a necessary data controller function, the data controller must ensure other adequate means of ensuring personal data is held securely, for example; the use of networked systems or Kensington locks.

(2) Adequate measures are put in place to ensure that data security policies are adhered to consistently across all data controller departments;

(3) Physical security measures are adequate to prevent unauthorised access to personal data. This includes adequate security management of areas that may need to be accessed out of hours;

(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 ……
Melany Pickup
Chief Executive
Warrington and Halton Hospitals NHS Foundation Trust

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