DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: **Cambridge University Hospitals NHS Foundation Trust**
Addenbrookes Hospital, Hills Road
Cambridge, CB2 0QQ

I, Dr Gareth Goodier, Chief Executive of the Cambridge University Hospitals NHS Foundation Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Cambridge University 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 from Mrs Susan Wood acting on behalf of the data controller, regarding the loss of an unencrypted computer memory stick which contained the personal data of some 741 patients of the data controller. The memory stick, which was privately owned and unencrypted, contained data relating to medical treatment ("sensitive personal data" as defined by the Act). It is understood that the memory stick was left in an unattended vehicle by a Trust employee. The memory stick was discovered by a car wash attendant who was able to access the device and establish it's ownership. The data had been downloaded on to the memory stick without the knowledge of the Trust.

3. The data controller did not ensure sufficient security measures were in place to prevent the unauthorised transfer of the data in question on to a non-Trust owned, unencrypted, memory stick. In particular the Trust failed to ensure that the data was protected by the Government 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.

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 1 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 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 Trust;

(2) 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;

(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 are adequate 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...03/04/09.....

Signed [redacted]

PP Dr Gareth Goodier
Chief Executive
The Cambridge University Hospitals NHS Foundation Trust

Signed... [redacted]

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