ICO Ref: **ENF0455232**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Hillingdon Hospitals NHS Foundation Trust

Pield Health Road
Uxbridge
Middlesex
UB8 3NN

I, Shane DeGaris, Chief Executive, of Hillingdon Hospitals NHS Foundation 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. Hillingdon 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 Hillingdon Hospitals NHS Foundation 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 on the 05 July 2012, which stated that the data controller had been informed that a local newspaper was in possession of 4 two week wait cancer referral forms containing sensitive clinical data relating to four data subjects.

3. Following investigation, it was established that the documents had been prepared for transfer between The Hillingdon Hospital and Mount Vernon Hospital via the internal mail system but failed to arrive at their intended destination. The documents were subsequently found to be in the possession of the local newspaper. It is unclear at which point the documents were lost or taken off-site and how they came in to the newspaper's possession. It was identified that whilst staff were aware that the documents had not arrived the incident was not escalated. It was also identified that there was a gap in the data controller's reporting mechanism for data protection incidents and near misses.

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 lost 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) Appropriate breach reporting mechanisms shall be implemented, with staff made fully aware of the reporting procedures and requirements.

(2) The data controller shall effectively manage an escalation process in the event that sensitive personal data does not arrive at its intended destination.

(3) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.

Signed: ……

Shane DeGaris
Chief Executive
For and on behalf of The Hillingdon Hospitals NHS Foundation Trust

Dated: …….

Signed: ……

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: …….