DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Croydon Health Services NHS Trust

530 London Road
Croydon
CR7 7YE

I, John Goulston, Chief Executive of Croydon Health Services NHS Trust, for and on behalf of Croydon Health Services NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Croydon Health Services 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 Croydon Health Services NHS 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 informed by the data controller that a mailing giving the outcome of a complaint made by a patient had been sent to the wrong address. The mailing contained the complaint response letter and copies of notes from two meetings held as part of the complaint investigation process. These documents contained sensitive personal data, comprising clinical information, relating to the patient.

3. The complaint response letter was initially correctly addressed but when amendments were made to the letter a digit was accidentally deleted. Although the content of the letter was checked prior to it being sent the address was not checked. This incident followed several others of a similar nature previously reported to the Commissioner involving the misdirection of clinical correspondence.

4. On investigating these matters further, the Commissioner discovered that: the error had been made by a temporary bank staff employee who had not received all the appropriate training and guidance in relation to the role they were

expected to fulfil; there was a lack of a formal checking procedure to ensure the accuracy of correspondence as to both address and content before dispatch; key recommendations from previous breach investigation reports in relation to similar incidents had not been implemented and were identified as being a major contributory factor in relation to this breach; there was a lack of senior managerial oversight due to managerial absence.

5. During the course of this investigation the data controller has also advised the Commissioner of a further breach. The data controller reported that a Birth Register covering dates from April 2009 to May 2010 could not be located, although it was subsequently recovered. Issues in relation to records management had contributed to this incident.

6. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of these matters. 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 compromised in these incidents 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.

7. 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. **The achievement of IG training targets and staff awareness of IG issues is given a key priority subject to regular ongoing review, testing and oversight by the Information Governance Committee (IGC).**

2. **All staff in the Complaints team complete data protection training on an annual basis, which is in**

addition to the mandatory information governance training. This training should cover Consent, Confidentiality, Security and Records Management.

3. **The data controller should ensure that attendance at data protection training sessions is monitored and that appropriate follow up procedures are in place to ensure completion.**

4. **A thorough review of data flows and an information risk assessment of information assets within the Trust are completed together with a detailed and updated Information Asset Register (IAR) to ensure there is oversight of the variety of sites and records management practices operating within the Trust. The final report in relation to this to be submitted to the Commissioner by 31 March 2016.**

5. **The approved option for legacy record disposal should be implemented as soon as is practicable; with progress to be regularly monitored and outcomes to be reported at each Information Governance Committee.**

6. **Correspondence checking procedures throughout the organisation are captured in a clearly written procedural document which is brought to the attention of all relevant staff who are required to sign to the effect that they are aware of this procedure and understand its requirements.**

7. **The implementation of recommendations from data protection incident investigation reports is closely monitored and evidence of completion made available to the relevant committees with oversight for data protection and information governance matters.**

8. **The data controller shall provide evidence of the implementation of the above measures by 31 March 2016.**

9. **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: ……

John Goulston
Chief Executive
Croydon Health Services NHS Trust

Dated: …….

Signed: ……

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

Dated: …….