ICO Refs: ENF0410948, ENF0412072 & ENF0418458

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: South London Healthcare NHS Trust

Frognal Avenue
Sidcup
Kent
DA14 6LT

I, Dr Chris Streather, Chief Executive, of, South London Healthcare NHS Trust for and on behalf of South London Healthcare NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. South London Healthcare 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 South London Healthcare 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 of the loss of two unencrypted memory sticks, the leaving of a clipboard with ward lists attached in a grocery store and a failure to adequately secure some patient paper files when not in use. Each of these incidents involved sensitive personal data relating to patients.

3. In the first incident the device contained data relating to approximately 600 maternity patients. A data controller employee downloaded the data on to a personal memory stick in order to do some work at home. Due to not having received up to date information governance training the employee was unaware that an encrypted device issued by the data controller should have been used.

   In the second incident the device contained the names and dates of birth of 30 children and full audiology reports for a further 3 children.

In these incidents the data was put at unnecessary risk by it not being encrypted but both devices were later found and it is unlikely that they were readily accessible during the time they could not be located.

In the third incident a junior doctor took ward lists out of a hospital in breach of data controller policy. These lists contained the name, date of birth, diagnosis, treatment plan and test results for 122 patients.

In the fourth incident the data controller reported that some Genito-Urinary Clinic outpatient files were not being locked away when not in use although they were being stored in areas with secure access controls.

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 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.

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;

2. Physical security measures are adequate to prevent unauthorised access to personal data;

3. The policy covering the storage and use of personal data is followed by staff;

4. Staff are made aware of the data controller's policy for the retention, storage and use of personal data and are appropriately trained to follow that policy;

5. 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……

Dr Chris Streather
Chief Executive
South London Healthcare NHS Trust

Signed……

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