DATA PROTECTION ACT 1998 9/4/10

UNDERTAKING

Data Controller: Birmingham and Solihull Mental Health NHS Foundation Trust.

Unit 1 B1
50 Summer Hill Road
BIRMINGHAM
B1 3RB

I, Sue Turner, CEO of Birmingham and Solihull Mental Health NHS Foundation Trust, for and on behalf of Birmingham and Solihull Mental Health NHS Foundation Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Birmingham and Solihull Mental Health 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 Birmingham and Solihull Mental Health 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. On 22 December 2009 the Information Commissioner (the "Commissioner") was informed of a security breach by the data controller's Director of ICT.

3. On 20 November 2009 a laptop computer, storing a number of details relating to patients who had received mental health care within the Trust, together with a number of staff records, was discovered to be missing from the Reaside Clinic. The computer had been last seen on 12 November and had been stored in an unlocked filing cabinet in a secure, but not alarmed, office.

4. At this time the majority of data stored on the computer were out of date and there was no business case for the retention

of the data.

5. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Fifth and Seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that a quantity of the data stolen 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.

6. 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 Fifth and Seventh Data Protection Principles 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, or theft of, personal data;

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

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..... 9/4/2010 .....

Signed.....
Sue Turner
Chief Executive Officer.
Birmingham and Solihull Mental Health NHS Foundation Trust.

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