DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Basildon and Thurrock University Hospitals NHS Foundation Trust

Nethermayne
Basildon
Essex
SS16 5NL

I, Alan Whittle, Chief Executive of Basildon and Thurrock University Hospitals NHS Foundation Trust ('BTUH'), for and on behalf of BTUH, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Basildon and Thurrock 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 BTUH 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 the data controller about a fax sent to a member of the public in error. The recipient contacted the data controller in November 2010 to advise that they had received the fax in July of that year, along with several others over a period of approximately two years, both from this organisation and a number of other healthcare providers. The data controller's subsequent investigations confirmed that since March 2009, it had sent at least ten faxes to this individual in error, which had originated from several different internal departments. Although the data controller is unable to ascertain the actual content of these faxes, it is possible that they also contained personal data.

3. The most recent fax, and that which is at the centre of the Commissioner's investigations, consisted of a cancer meeting outcome form containing sensitive personal data relating to a patient. The data controller had intended to send the fax to the patient's GP but the number had been typed incorrectly on the document and was subsequently input manually into the fax machine. The data controller is required to send a high number of these forms to GPs on a daily basis (for information only), and at the time of the breach, faxing was considered the most efficient way to transmit them. This procedure had been in place for several

years although was in direct contravention of the data controller's written policies.

4. In deciding what action to take, the Commissioner has considered that, whilst the fax contained sensitive personal data, the volume of data was limited and related to one individual. Further, the information compromised was unlikely to cause substantial damage or distress to the affected data subject, especially as the patient was already aware of the document's contents at the time the fax was sent. Whilst a 'ring-ahead' procedure was not in use within the Cancer Services Team, cover sheets were attached to every fax sent from the department, and only safe haven machines were used.

5. 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 disclosed in this incident consisted of information relating to the physical or mental health or condition of the data subject. 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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

(1) MDT cancer meeting outcome forms are no longer faxed to GP surgeries, and a permanent secure alternative means of transmission is implemented;

(2) The data controller's fax machines are pre-programmed with the most frequently used numbers, and a ring-ahead procedure is always used;

(3) Staff are aware of the data controller's policies for the storage, use and disposal of personal data, and are appropriately trained how to follow those policies;

(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…….

Signed……

Alan Whittle
Chief Executive
Basildon and Thurrock University Hospitals NHS Foundation Trust

Signed……
Sally-anne Poole
Head of Enforcement
For and on behalf of the Information Commissioner