20/10/09

# DATA PROTECTION ACT 1998

## UNDERTAKING

Data Controller: Ashford & St Peter's Hospitals NHS Trust

Guildford Road
Chertsey
Surrey
KT16 0PZ

I, Andrew Liles, Chief Executive of Ashford & St Peter's Hospitals NHS Trust (the "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. Ashford & St Peter's Hospitals 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 the 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 detailing the loss or theft of three unencrypted USB memory sticks from Cancer Services over a period of several weeks between 28 May and 26 June 2009. Each of the devices contained sensitive personal data, including full treatment and diagnosis history, relating to a number of cancer patients. As the data was in Word format, it could have been easily accessed by anyone with use of a computer.

3. The USB sticks were used to transfer up-to-date patient data for display at weekly multi-disciplinary clinical team meetings, held to discuss and plan treatment and care for cancer patients. The loss of the USB sticks was not formally reported to the data controller's management until after the third incident in late June 2009.

4. The investigation into these incidents revealed a lack of understanding and awareness among staff of the requirements of data protection legislation and of internal policies and procedures. It further revealed a lack of provision for staff training, with some staff never having received any formal data protection training.

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 involved in this

incident consisted of information as to the physical 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 is processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:**

**(1) All portable and mobile devices, including laptops, USB sticks 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) All staff are aware of the data controller's policy for the 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..... 20 October 2009

Signed..
Andrew Liles
Chief Executive
Ashford & St Peter's Hospitals NHS Trust

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