

# DATA PROTECTION ACT 1998

## UNDERTAKING

Data Controller: **Epsom & St Helier University Hospitals NHS Trust.**  
**St Helier Hospital, Wrythe Lane, Carshalton, Sutton. SM5 1AA.**

I, Peter Coles, Interim Chief Executive of the Epsom & St Helier University Hospitals NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following undertaking:

1. Epsom & St Helier University 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 from Mr Paul Kenny acting on behalf of the data controller, regarding the discovery, by a press reporter, of the insecure storage of hospital records relating to a large number of the hospitals patients. The information contained data relating to medical tests and treatment ("sensitive personal data" as defined by the Act). It is understood that in March 2007 the data was in the process of being transferred by an outside contractor from an existing store to a new secure storage area at Sutton hospital. On discovering that the data had been inappropriately boxed for storage it was temporarily placed in a less secure area at Sutton hospital pending refilling. Delays in the refilling of the data resulted in it remaining in the insecure storage area until its discovery in February 2009. During this period further sensitive personal data, relating to eye casualties, was placed within this temporary store.
3. The data controller did not ensure sufficient security measures were in place to prevent the possibility of unauthorised access to the data in question. In particular the Trust failed to ensure that minimal security measures were applied, with the door to the store being regularly left unlocked for the convenience of staff accessing records. The Commissioner has taken into account the facts that, over a near two year period, staff failed to recognise, and address, the security risk in relation to the records, disclosure of which could have resulted in significant distress being caused to the individuals concerned. The resultant concern which may have been caused by the press article is also noted.
4. The Commissioner has concerns that, in its root cause analysis into this incident, the Trust appears to have failed to recognise the staff training issues, equipment and resources factors, individual knowledge and skills areas, organisation and strategic issues and the question of culpability in respect of this breach.

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 1 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 or from other data controllers in similar circumstances, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Schedule 1 Part 1 of the Act, and in particular that:**

- (1) The data controller shall take all reasonable measures to ensure the physical security of personal data, particularly paper records, being processed in furtherance of the duties of the Trust;**
- (2) The data controller shall implement such other security measures it deems appropriate to ensure that personal data is protected against unauthorised and unlawful process, accidental loss, destruction, and/or damage;**
- (3) Physical security measures are adequate to prevent unauthorised access to personal data;**
- (4) Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained on how to recognise personal data, and to follow the Trusts data protection policy accordingly.**

Dated.....

Signed.....

Peter Coles  
Interim Chief Executive  
The Epsom & St Helier University Hospitals NHS Trust

Signed.....

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