

# DATA PROTECTION ACT 1998

## UNDERTAKING

Data Controller: Ipswich Hospital NHS Trust  
Heath Road  
Ipswich  
IP4 5PD

I, Andrew Reed, Chief Executive of Ipswich Hospital 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. Ipswich Hospital 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 that a ward handover / summary sheet had been found outside the data controller's premises. This was the second time inside a year that such an incident had been reported to the Commissioner.
3. The document contained personal data (names, ages, and some clinical information) relating to 25 patients on a particular ward. In the previous incident, in 2008, a similar document containing such data relating to 15 patients on another ward had been found among the papers of a discharged patient, who had raised a complaint with the data controller about security of personal data as a result of this. The report of the investigation into the 2008 incident had made recommendations intended to minimise the risk of these documents going astray, including instructions to dispose of these in confidential waste and never to remove them from Trust premises, but it was clear that these had not been adhered to by staff.
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 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.

5. Following consideration of the remedial action proposed and 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) Physical security measures are adequate to prevent unauthorised access to personal data;**
- (2) The policy covering the storage and use of personal data, and in particular the instructions with regard to ward round lists and handover summaries, is followed by staff;**
- (3) Staff are aware of the data controller's policy for the storage, use and disposal 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 28/8/09.....

Signed.....  
Andrew Reed  
Chief Executive  
Ipswich Hospital NHS Trust

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