

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: University Hospitals Coventry &
Warwickshire NHS Trust

Walgrave Hospital
Clifford Bridge Road
Coventry
CV2 2DX

I, Andrew Hardy, Chief Executive Officer, of University Hospitals Coventry & Warwickshire NHS Trust, for and on behalf of University Hospitals Coventry & Warwickshire NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. University Hospitals Coventry & Warwickshire 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 University Hospitals Coventry & Warwickshire NHS 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 notified of two separate incidents involving the loss of personal data.
3. One incident concerned a patient's medical record. The record had allegedly been found in a waste bin outside Coventry's University Hospital by a member of the public. The medical record included details relating to sensitive medical procedures and test results. The Commissioner's enquires revealed the Trust's policies and procedures were not sufficiently robust. In particular the location of the clinic's delivery and collection points for patient notes was identified as a matter of concern.
4. A previous incident had also been reported to the

Commissioner after patient information was found in a public waste bin in a residential apartment block. The information related to 18 patients and included "sensitive personal data" as defined by the Act. Enquiries revealed that the breach occurred because a Trust staff member took the data home and unintentionally disposed of it in a communal waste bin. Had the Trust's policy been followed the paperwork would have been returned to the hospital to be destroyed securely.

5. Although each separate incident did not involve a large quantity of personal data, they occurred within a two month period suggesting that the data controller did not take sufficient measures to safeguard the personal data it held. The Commissioner has taken into account the fact that a proportion of the personal data in question related to medical conditions and could potentially result in distress being caused to the individuals concerned. It has been noted that the Trust has introduced remedial measures as a result of these incidents.
6. 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 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.
7. 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. The data controller shall ensure that its policies in respect of the security of personal information, particularly the storage and use of "sensitive personal information" are adequate, clear and that staff are adequately trained on how to fulfil their obligations**

under such policies;

- 2. Compliance with the new procedures put in place by the Trust for the delivery, pick up and tracking of clinical data is appropriately and regularly monitored;**
- 3. A formal policy be written and implemented for appropriate staff on the handling and disposal of patient based information taken off Trust premises;**
- 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.....

Andrew Hardy
Chief Executive Officer
University Hospitals Coventry & Warwickshire NHS Trust

Signed.....

Sally Anne Poole
Head of Enforcement
For and on behalf of the Information Commissioner