

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Royal Wolverhampton Hospitals NHS Trust

New Cross Hospital
Wednesfield Road
Wolverhampton
WV10 0QP

I, David Loughton, Chief Executive of Royal Wolverhampton 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. Royal Wolverhampton 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 alerted to a possible data security incident by a newspaper report dated 14 May 2010 and contacted the data controller to ascertain further details. The report concerned an unencrypted CD, with no password protection, which contained scans of patient charts from the Intensive Care Unit of the data controller's Heart and Lung Unit, and was allegedly found at a bus stop near the data controller's premises and passed to the newspaper anonymously. The patient charts related to some 112 patients and were several years old.
3. The data controller carried out a full investigation into the incident but was unable to discover exactly how the CD came to be made. Both the investigation and the Commissioner's enquiries revealed certain weaknesses in procedures, including that such charts are released to consultants if requested but are not chased for return for approximately one month.
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 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) All staff are aware of the data controller's policies for the storage and use of personal data and the management of patient records, and are appropriately trained how to follow those policies;**
- (2) Compliance with the data controller's policies on data protection and records management is appropriately and regularly monitored;**
- (3) Patient charts released to consultants are signed for on receipt and chased for return after one week and weekly thereafter;**
- (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
David Loughton
Chief Executive
Royal Wolverhampton Hospitals NHS Trust

Signed
Mick Gorrill
Head of Enforcement
For and on behalf of the Information Commissioner