

# DATA PROTECTION ACT 1998

## UNDERTAKING

Data Controller:                   NHS Stoke on Trent

Trust Headquarters  
Herbert Minton Building, 79 London Road  
Stoke-on-Trent  
ST4 7PZ

I, Graham Urwin, CEO, of NHS Stoke on Trent, for and on behalf of NHS Stoke on Trent hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. NHS Stoke on Trent 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 NHS Stoke on Trent 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 informed of security breach by NHS Stoke on Trent.
3. Following a request for information about a patient's medical records it was discovered that the physical paper records were not within the records storage system. Further enquiries revealed that a total of some 2,000 physiotherapy records had not been filed within the archive system, as was required by Trust policy. It is believed that the records may have been accidentally destroyed or misfiled within the Trust.
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 'lost' 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. Physical security measures in respect of paper medical records are sufficiently adequate to prevent unauthorised access to, accidental loss or destruction of, or damage to personal data, particularly when records are in transit;
2. Staff are aware of the data controller's policy for the retention, archiving, storage and use of personal data and are appropriately trained how to follow that policy;
3. 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.....

Graham Urwin  
Chief Executive Officer  
NHS Stoke on Trent.

Signed.....

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