

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Doncaster Primary Care Trust
White Rose House
Ten Pound Walk
Doncaster, DN4 5DJ

I, Sheenagh Powell, Acting Chief Executive of Doncaster Primary Care 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. Doncaster Primary Care 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 by the data controller, regarding the unauthorised removal of an obsolete out of hours GP service voice recording server that held the personal data of patients of the data controller.
3. The obsolete server was removed from the Trust's Devonshire House site by the external contractor's engineer who installed the new server. The obsolete server was not missed until the new server failed. Although the obsolete server was returned it was out of the Trust's control for almost three weeks during which time it was briefly booted up twice. The server held 220000 clinical voice records although it seems unlikely that these were accessed.
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 1 of 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 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) Portable and mobile devices including laptops and other portable media used to store and transmit personal data, the loss of which could cause damage or distress to individuals, are encrypted using encryption software which meets the current standard or equivalent;**
- (2) Physical security measures and procedures are adequate to prevent the unauthorised removal or theft of computer server equipment that contains personal data, or ensure that such equipment is encrypted using encryption software which meets the current standard or equivalent;**
- (3) The data controller shall implement such other security measures it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

Dated... 27.4.09

Signed [Redacted]
Sheenagh Powell
Acting Chief Executive
Doncaster Primary Care Trust

Signed [Redacted]
Mick Gorrill
Assistant Commissioner Regulatory Action Division
For and on behalf of the Information Commissioner