

15/10/09

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Gloucestershire Primary Care Trust

Sanger House
5220 Valiant Court
Gloucester Business Park
Brockworth
Gloucestershire GL3 4FE

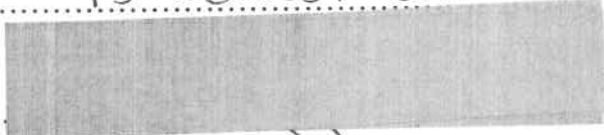
I, Jan Stubbings, Chief Executive, of Gloucestershire Primary Care Trust, for and on behalf of the Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:


1. Gloucestershire 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 Gloucestershire Primary Care 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 informed by Gloucestershire Primary Care Trust about the theft of 6 desktop computers holding personal data relating to patients.
3. The password protected desktop computers containing personal data relating to 2270 patients were stolen from a locked office. The computers were used by medical secretaries for preparing letters and notes relating to diagnosis and referral of patients. This patient data should have been held on a local server rather than on the hard drives of the stolen computers.
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 stolen in this incident consisted of information defined as "sensitive personal data" under section 2 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) 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 are adequate to prevent unauthorised access to personal data;
- (3) Staff are aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;
- (4) The policy covering the storage and use of personal data is followed by staff;
- (5) 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..... 15 October 09

Signed. 
Jan Stubbings
Chief Executive
Gloucestershire Primary Care Trust

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