DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Billing Pharmacy Limited

5 Kings Chase Shopping Centre
Regent Street
Bristol
BS15 8LP

I, John Billing, proprietor of Billing Pharmacy Limited, for and on behalf of Billing Pharmacy Limited, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Billing Pharmacy Limited 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 Billing Pharmacy Limited 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 South Gloucestershire Primary Care Trust of the theft of a computer from one of the data controller's branches over the weekend of 26-27 April 2009. The computer was used to record prescriptions and produce medicine labels. It was unencrypted, although each member of pharmacy staff had an individual password to access the database. The computer contained the personal data of around 1,000 patients, including details of their past and present medications and allergies.

3. It was not possible to notify the patients affected by the theft as the data on the computer was not separately backed up. Further enquiries also revealed that the data controller did not have in place appropriate policies and procedures with regard to data protection matters.

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. 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) Any portable computers, devices or 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) The data controller shall draft a formal data protection policy, providing appropriately detailed guidance for staff on procedures to be followed in relation to the collection, storage, use and disposal of personal data;

(4) Staff are made aware of the above-mentioned data protection policy and procedures, and adequately trained how to follow these;

(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..... 8/9/09

Signed...
John Billing
Proprietor
Billing Pharmacy Limited

Signed.
~~Mick Gorrill~~ CHRISTOPHER GRAHAM
~~Assistant Commissioner, Regulatory Action Division~~
~~For and on behalf of the~~ Information Commissioner