

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Lampeter Medical Practice

 Taliesin Court
 Lampeter
 Ceredigion
 SA48 7AA

I, Dr. Rowena Mathew, Head of Practice, of Lampeter Medical Practice, for and on behalf of Lampeter Medical Practice hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Lampeter Medical Practice 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 Lampeter Medical Practice 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") received a report that a number of data sets had been lost in the post by the data controller.
3. The data controller reported that in March 2010 a member of staff had, in contravention of practice policy, downloaded a practice database onto an unencrypted and non password protected computer memory stick. The memory stick was then placed in an envelope and posted by recorded delivery to the Health Boards Business Service Centre. The memory stick failed to arrive at its intended destination and is accepted to be lost.
4. The data contained within the memory stick consisted solely of patient identifying details in relation to some 8,000 patients. No clinical information was stored on the memory stick.

5. 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.
6. 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, particularly in respect of the unauthorised use of computer memory sticks;
3. Staff are aware of the data controller's policy for the retention, storage, transfer and use of personal data and are appropriately trained how to follow that policy;
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.....26.5.2010.....

Signed....

Dr. R. Mathew
Head of Practice
Lampeter Medical Practice
Taliesin Court
Lampeter
Ceredigion
SA48 7AA

Signed...

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