OFFICE OF THE
Data Protection Supervisor
Oik Oaseir Coadey Fysseree Ellan Vannin

ico.
Information Commissioner's Office

Isle of Man DATA PROTECTION ACT 2002

and

UK DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Praxis Care Limited

25-31 Lisburn Road
Belfast
BT9 7AA

I, Nevin Ringland, Chief Executive of Praxis Care Ltd (the 'Company') for and on behalf of the Company, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Praxis Care Ltd is a data controller as defined in section 1(1) of the Isle of Man Data Protection Act 2002 (the 'IOM Act') and section 1(1) of the UK Data Protection Act 1998 (the 'UK Act') in respect of the processing of personal data carried out by the Company, and is referred to in this Undertaking as the 'data controller'. Section 2(4) of the IOM Act provides that, subject to section 23(1) of the IOM 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. Sections 4(4) and 27(1) of the UK Act make similar provision.

2. The Isle of Man Data Protection Supervisor (the 'Supervisor') and the UK Information Commissioner (the 'Commissioner') were both provided with reports about a single incident in August 2011, in which an unencrypted USB stick used as a backup and transfer device by one of the data controller's employees was lost on the Isle of Man. The device contained some sensitive personal data about 107 data subjects on the Isle of Man, but also contained similar data about 53 data subjects in N Ireland dating from two or more years previously when the employee had worked there.

3. The data controller acted swiftly to ascertain exactly what data was on the missing USB stick and appropriate support was provided to the affected data subjects. No reports of adverse consequences from the data loss have been received.

4. The Supervisor and the Commissioner have each considered the data controller's compliance with the provisions of the relevant Act in the light of this matter. The relevant provisions of both Acts are the Third, Fifth and Seventh Data Protection Principles. These Principles are set out in Part 1 of Schedule 1 to each Act. The Supervisor and the Commissioner have also considered the fact that some of the data involved in this incident consisted of information as to the mental health or condition of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under both section 1 of the IOM Act and section 2(e) of the UK Act.

5. Following consideration of the remedial action that has been taken and is proposed by the data controller it is agreed that, in consideration of the Supervisor not exercising his powers to serve an Enforcement Notice under section 36 of the IOM Act and the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the UK 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 IOM Act or the UK Act or other successor legislation, ensure that personal data are processed in accordance with the Third, Fifth and Seventh Data Protection Principles in Part 1 of Schedule 1 to each of the specified Acts, and in particular that:

(1) All 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) All staff are made aware of the data controller's policy for the storage, use, transmission and disposal of personal data and are appropriately trained how to follow that policy;

(3) Personal data shall not be retained when no longer relevant or required for its original purpose;

(4) Any personal data which is no longer needed shall be disposed of in a secure manner, the procedures for which shall be covered in the data controller's data protection policies and communicated to all relevant staff;

(5) Compliance with the data controller's policies on data protection and IT security issues, and with physical security requirements, is appropriately and regularly monitored;

(6) 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 (on publication):

Signed ……
Nevin Ringland
Chief Executive
Praxis Care Limited

Signed ……..
Iain McDonald
Isle of Man Data Protection Supervisor

Signed ……..
Christopher Graham
UK Information Commissioner