ICO Ref: **ENF0466943**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: The Burnett Practice

Portadown Health Practice
Tavenagh Avenue
Portadown
County Armagh
BT62 3BE

I, Mrs J McCullough, Practice Manager of The Burnett Practice, for and on behalf of The Burnett Practice, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. The Burnett 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 The Burnett 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') was informed on 3 October 2012 that an email account used by the data controller had been subject to a third party attack, and that this had resulted in the email account being compromised. The data controller became aware of the incident after it was contacted by patients who had received emails purporting to be from a GP, but which had actually been generated by a third party who was unconnected to the data controller.

3. The Commissioner's investigation discovered that data stored in the email account, which had been placed at risk as a result of the attack, included a list of names and email addresses of patients. The account was primarily used for arranging and reporting on smear tests for female patients between the ages of 25 and 65. Appointment invitations and a notification to indicate normal test results were sent via the email account.

4. The data controller was unable to confirm the number of data subjects affected by the incident, as the account data required to determine this had been wiped as a consequence of the attack. However, it estimated that 175 patients were affected by the incident.

5. Further investigation by the Commissioner's staff determined that the email service provider used by the data controller was not

appropriate to communicate the outcome of the tests. The data controller was unable to ensure appropriate technical security measures were in place to provide an adequate level of protection. In the Commissioner's view, this demonstrates a lack of data protection awareness with regards to technical security measures. Further, the Commissioner's investigation revealed that the data controller did not have a sufficient data protection training programme in place, and that its information security policy and procedures in respect of the protection of personal data were lacking.

6. The Commissioner has considered the data controller's compliance with the provisions of the Act in 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 consisted of information relating to the health of the data subjects. Such information is considered 'sensitive personal data' as defined in section 2(e) of the Act.

7. 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) The data controller shall adopt a secure mode of communication to provide test results. Such measures shall provide a level of protection which is appropriate to the personal data being communicated;

(2) Clinical data shall not be sent via email unless the security of such transfers can be assured;

(3) The data controller shall put in place an adequate security policy to cover the secure transfer of patient data and all staff shall be made aware of that policy and trained in how to follow it;

(4) All those whose role involves the routine processing of personal data on behalf of the data controller shall undertake training in both the requirements of the Act and the data controller's policies relating to the use of personal data at induction and thereafter at regular intervals (not to exceed three years). Completion of such training shall be recorded and monitored to ensure compliance;

(5) Compliance with the data controller's policies on data protection and IT security issues shall be 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 ……
Mrs J McCullough, Practice Manager
The Burnett Practice

Signed ……..
Stephen Eckersley, Head of Enforcement
For and on behalf of the Information Commissioner