DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Basingstoke and North Hampshire NHS Foundation Trust

Aldermaston Road
Basingstoke
Hampshire
RG24 9NA

I, Mary Edwards, Chief Executive Officer, of Basingstoke and North Hampshire NHS Foundation Trust, for and on behalf of Basingstoke and North Hampshire NHS Foundation Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Basingstoke and North Hampshire NHS Foundation 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 Basingstoke and North Hampshire NHS Foundation 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 the Foundation Trust that an excessive amount of data, given the intended purpose, was emailed to another Trust partner via a non-secure email account.

3. An excel spreadsheet detailing pathology results concerning some 917 of the Trust's patients was emailed via a non-secure email account to a partnership sexual health team. The spreadsheet was not password protected and the ~~accounts~~ department had no 'business need' to have access to the clinical data.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provisions of the Act are the Third and

Seventh Data Protection Principles. These Principles are set out in Schedule 1 Part I to the Act. The Commissioner has also considered the fact that some of the data transferred in this incident consisted of information as to the physical 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. 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 Third and Seventh Data Protection Principles 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. Only the minimum data necessary for the intended purpose is extracted and/or transferred for any processing requirement;

3. Physical security measures are adequate to prevent unauthorised access to personal data, in particular data must be subject to password and/or encryption protection where appropriate;

4. 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;

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..... 9 June 2010 .....

Signed... [redacted]

Mary Edwards
Chief Executive Officer
Basingstoke and North Hampshire NHS Foundation Trust
Aldermaston Road
Basingstoke
Hampshire
RG24 9NA

Signed..... [redacted] 14/6/10

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