DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: NHS Grampian

Summerfield House
2 Eday Road
Aberdeen
AB15 6RE

I, Richard Carey, Chief Executive of NHS Grampian, for and on behalf of NHS Grampian, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. NHS Grampian 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 NHS Grampian 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 provided with reports of three separate incidents involving data security. The first involved the inappropriate distribution of an email containing sensitive personal data relating to an individual; the second concerned documents which had been taken from a confidential waste bag and contained personal data of around 200 patients and staff; and the third related to the theft of an unencrypted laptop containing the personal data of over 1500 patients.

3. In the first incident, a senior nursing manager distributed an email received from another senior manager, which contained sensitive personal data relating to a patient, to over 50 other staff without first consulting either the sender or the data controller's Information Governance Manager.

4. The second incident occurred when someone removed documents from a confidential waste bag held at the nursing station on the labour ward, and sent these to the data controller's Chief Executive claiming that they had been found in a skip. The documents were traced to the relevant ward and it was found that, due to the lack of secure storage, access to confidential waste could have been gained by staff, patients and even visitors. Enquiries also revealed that many staff were unaware of the correct procedures for disposing of confidential waste.

5. In the third incident, a laptop containing details of patients in the gastroenterology clinic was stolen from a locked office. The laptop was unencrypted and contained the entire database of patients suffering from a particular disease. The laptop had not been successfully backed up to the data controller's network server in the month prior to the theft, with the result that a small amount of the data was only stored on the laptop.

6. The Commissioner's enquiries into these three incidents also led to the finding that certain staff were using home computers for work-related tasks involving personal data and then transferring that work via unencrypted USB sticks, in contravention of the data controller's policies and procedures.

7. 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 concerned the physical or mental health of the data subjects. Personal data containing such information is defined as "sensitive personal data" under section 2 of the Act.

8. In light 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) Any personal data stored on portable devices or media is backed up to the data controller's network server on a daily basis, or at least at the end of every day on which changes have been made to the personal data. Confirmation of the success of each backup attempt is to be obtained from the IT department and any failure corrected without delay, or the device securely stored pending completion of a successful backup;

(3) Physical security measures are adequate to prevent unauthorised access to personal data;

(4) Staff are aware of the data controller's policies for the storage, use and disposal of personal data and are appropriately trained how to follow those policies;

(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.....3/9/09.....

Signed...[redacted]
Richard Carey
Chief Executive
NHS Grampian

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