ICO Ref: **ENF0382612**

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: HCA International Limited

242 Marylebone Road
London
NW1 6JL

I, Michael Neeb, Chief Executive of HCA International Ltd (HCA), for and on behalf of HCA, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. HCA International Ltd 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 HCA 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 a report of the theft, in March 2011, of two unencrypted laptops containing sensitive personal data relating to patients of the Harley Street Clinic, one of the data controller's hospitals. The laptops were kept in a locked room in the administrative and laboratory area at the hospital, but the key to this room was kept on a hook on the inside of the door to the next office, which was not normally locked as it contained a fire escape. In addition, at the time of the theft, the door to the corridor used to access these rooms was kept 'on the latch' during the day, potentially allowing unauthorised access to the area.

3. The Commissioner's enquiries revealed that the devices, which were used for specific cancer treatments, contained custom software and neither would be covered under the supplier's warranty if encryption or other software were added. Subsequently, the data controller has encrypted the replacement laptops and made further improvements to physical security at the premises.

4. 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 involved 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. However, despite this the risk of

substantial damage or distress to the data subjects in this instance is remote.

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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, 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 aware of the data controller's policy for the storage and use of personal data and are appropriately trained how to follow that policy;

(3) Physical security controls are improved to prevent further unauthorised access to sensitive personal data, to include the use of key safes and all doors leading to limited access areas being kept properly secured;

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

(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

Signed ……
Michael Neeb
Chief Executive
HCA International Ltd

Signed ……
Sally-anne Poole
Acting Head of Enforcement
For and on behalf of the
Information Commissioner