

DATA PROTECTION ACT 1998

13/9/10

UNDERTAKING

Data Controller: East & North Hertfordshire NHS Trust
Lister Hospital
Coreys Mill Lane
Stevenage
SG1 4AB

I, Nick Carver, Chief Executive of East & North Hertfordshire NHS Trust (the "Trust"), for and on behalf of the Trust, hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. East & North Hertfordshire NHS 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 the 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 provided with a report of the loss of an unencrypted USB stick containing sensitive personal data. The device, which was not issued by the data controller, was used by a junior doctor mainly to record brief details of patients' conditions and medication on each shift, so that the information could be passed to the next doctor on shift. The doctor concerned had forgotten to pass the data to the relevant colleague and took the USB stick home intending to forward the data electronically. The device was lost on the train journey home, with the doctor's wallet. Neither has since been recovered.
3. The doctor informed the data controller immediately on discovering the loss and a full investigation was conducted. The Commissioner's enquiries revealed that the doctor had not been aware of the data controller's policies and how to access these, and did not have access to email to receive data protection reminders. It was further discovered that the data controller's policy on use of personal USB sticks was not clear and no technical measures were in place to prevent such use.
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 or mental 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 Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

- (1) The data controller's policy for the use of portable media is clarified and all staff are made aware of its provisions;**
- (2) All staff with access to personal data are made aware of the data controller's policies for the storage and use of personal data and are appropriately trained how to follow those policies;**
- (3) Compliance with the data controller's policies on data protection and IT security issues is appropriately and regularly monitored;**
- (4) 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 13 September 2010

Signed
Nick Carver
Chief Executive
East & North Hertfordshire NHS Trust

Signed
Mick Gorrill
Head of Enforcement
For and on behalf of the Information Commissioner