

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Hull & East Yorkshire Hospitals NHS Trust
Castle Hill Hospital
Castle Road
Cottingham
North Humberside
HU16 5JQ

I, Stephen Greep, Chief Executive, on behalf of Hull & East Yorkshire Hospitals NHS Trust hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Hull & East Yorkshire Hospitals 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 on 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") received a report from the data controller's Information Governance Manager about two separate incidents involving the loss of personal data relating to around 2300 patients in total. Some of the lost personal data was "sensitive personal data", as defined by section 2 of the Act.
3. In the first incident, a desktop PC, containing personal data relating to around 300 patients, was lost during refurbishment of the renal peritoneal dialysis office; and in the second, a disused laptop, containing personal data relating to around 2000 urology cancer patients from prior to January 2007, was stolen from a locked office. Both devices were unencrypted and access to the data would not have required great technical knowledge. The data controller had in place policies and procedures relating to data security and the storage and transfer of equipment and data, which were not followed in either instance.
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 Fifth and Seventh Data Protection Principles. These are set out at Part I of Schedule 1 to the Act.
5. In view of the circumstances of this incident and the remedial steps taken by the data controller as a result, it has been 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 is processed in accordance with the Fifth and Seventh Data Protection Principles in Part I of Schedule 1 to the Act, and in particular that:

- The data controller shall ensure that any personal data held on a laptop computer or other removable media either by the data controller, or by a data processor processing personal data on behalf of the data controller, is suitably encrypted according to Department of Health guidance so as to provide effective protection against unauthorised access;**
- The data controller shall ensure that personal data is not held on any media for longer than is required for the purpose(s) for which it was originally stored on that media, and that when it is no longer needed (and in any event, prior to disposal of the storage media), personal data is securely erased;**
- The data controller shall ensure that all staff, including any contract or temporary staff, are made fully aware of its internal policies and procedures relating to data and IT security and the requirements of the Data Protection Act 1998, normally at induction training, and that such training is refreshed on a regular basis;**
- The data controller shall ensure that adequate security measures are in place to control access to buildings and offices, including the secure storage of keys and implementation of swipe-card or similar access controls where possible;**
- The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised or unlawful processing, accidental loss, destruction and/or damage.**

Dated.....

Signed.....
For Hull & East Yorkshire Hospitals NHS Trust

Signed.....
Mick Gorrill (Assistant Commissioner, Regulatory Action Division)
For the Information Commissioner