

DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Barking, Havering & Redbridge University
Hospitals NHS Trust

Queen's Hospital
Rom Valley Way
Romford
Essex
RM7 0AG

I, Averil Dongworth, Chief Executive of Barking, Havering & Redbridge University Hospitals NHS Trust (BHRUT), for and on behalf of BHRUT hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. BHRUT 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 BHRUT 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 on 24 January 2013 that BHRUT had sent a fax containing personal data to an incorrect fax number belonging to a member of the public. In the course of investigating this potential breach, the ICO was informed that BHRUT had sent another fax to the same number.
3. On further investigation of the matters, it came to light that the Trust had taken some steps to prevent a breach of this nature, and that a Confidentiality and Disclosure Policy and Fax Policy were in place at the time of the incidents. However, neither employee involved had received Information Governance training, despite the fact that the training was supposedly mandatory. The investigation further revealed that the overall attendance rate for the training across BHRUT was between 35 and 40%.
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 disclosed in this incident consisted of information as to the physical or mental health of the data subjects. Personal data containing such information is defined as 'sensitive personal data' under section 2(d) 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 ensures that attendance for its mandatory Information Governance training is properly enforced, through whatever means it deems appropriate;**
- (2) the data controller ensures that it maintains a full and accurate record of who has received the training, and that ;**
- (3) the data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

Signed:

Averil Dongworth
Chief Executive
Barking, Havering & Redbridge University Hospitals NHS Trust

Dated:

Signed:

Stephen Eckersley
Head of Enforcement
For and on behalf of the Information Commissioner

Dated: