DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Royal Cornwall Hospitals NHS Trust

Pendragon House
Royal Cornwall Hospital
Treliske
Truro
Cornwall
TR1 3LJ

I, Peter Colclough, Chief Executive of Royal Cornwall Hospitals 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. Royal Cornwall 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 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 inappropriate disclosure of third-party personal data in response to an individual's subject access request ("SAR").

3. On further investigation, it transpired that the Trust disclosed third-party personal data to the same requester on two occasions. Although the staff responsible for checking SAR responses had received information governance training, these errors demonstrate that supervision and checking procedures at the time were inadequate. The Trust asserts that the inexperience of recently recruited staff, combined with the volume of requests being handled contributed towards staff overlooking erroneous records prior to disclosure.

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) Procedures for dealing with such subject access requests are clearly defined and managed, and all staff involved in such work receive appropriate training and support in how to follow them;

(2) Appropriate checks and supervision are put in place to ensure that third party personal data is dealt with in accordance with the Act's requirements and the data controllers policies and procedures;

(3) Personal data and sensitive personal data is not disclosed to anyone except in accordance with the Act; and, in particular, staff tasked with checking and redacting material from subject access responses receive appropriate additional training and support;

(4) Procedures are introduced to monitor the accuracy of the data controller's patient records;

(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 ……
Peter Colclough
Chief Executive
Royal Cornwall Hospitals NHS Trust

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