

## DATA PROTECTION ACT 1998

### SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

#### ENFORCEMENT NOTICE DATED 25 FEBRUARY 2009

To: Camden Primary Care Trust

of: 4<sup>th</sup> Floor East Wing  
St Pancras Hospital  
4 St Pancras Way  
London  
NW1 0PE

1. Camden Primary Care 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 by Camden Primary Care Trust and is referred to in this notice as the "data controller".
2. The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act"). By virtue of section 6(1) of the Act, the office of the Data Protection Registrar originally established by section 3(1)(a) of the 1984 Act became known as the Data Protection Commissioner. From 30 January 2001, by virtue of section 18(1) of the Freedom of Information Act 2000 the Data Protection Commissioner became known instead as the Information Commissioner (the "Commissioner").
3. The Commissioner was informed of an incident involving the loss of redundant personal computers holding the sensitive personal data (including names, addresses and medical diagnoses) of over 2,500 individuals. The personal computers had been left by a skip inside the grounds of St. Pancras Hospital for a period of 13 days before the data controller discovered that they had been removed without its authority.
4. In response, the incident was investigated as a Serious Untoward Incident ("SUI") resulting in a report from the SUI Panel, which made a series of recommendations as follows:
  - (a) To implement a communication campaign to all staff informing them of the Disposal of Redundant IT Equipment & Storage Media policy and procedure;
  - (b) To bring forward the encryption of all USB sticks, laptops and desktops;
  - (c) To implement a robust asset register for all IT equipment;
  - (d) To implement a robust decommissioning register;

- (e) To establish a Data Security Action Group to oversee the urgent implementation of these recommendations.
5. The Commissioner has considered the report and recommendations referred to in paragraph 4 above and further considered the data controller's compliance with the provisions of the Act in light of these matters.
  6. 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 with respect to which he is the data controller. The relevant provision of the Act is the Seventh Data Protection Principle.
  7. The Seventh Data Protection Principle provides at Part 1 of Schedule 1 to the Act that:

*“Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data”.*

Paragraph 9 of Part II of Schedule 1 of the Act further provides that:

*“Having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to -*

*(a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and*

*(b) the nature of the data to be protected”.*

8. Having considered the report and recommendations referred to in paragraph 4 above, the Commissioner is satisfied that the data controller has contravened the Seventh Data Protection Principle in that it failed to take appropriate measures to ensure the security of its data.
9. The Commissioner considered, as he is required to do under Section 40(2) of the Act when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner took the view that the likelihood of distress is self-evident. The 2,500 or so individuals whose sensitive personal data has been lost are likely to have suffered worry and anxiety on account of the risk that their data will come into the possession of unauthorised individuals. Whilst there is no evidence that damage has been caused there was a significant risk that it could have been.
10. The Commissioner has further taken account of the effect of the incorporation in English law of the European Convention on Human Rights (“ECHR”), by virtue of the Human Rights Act 1998, in deciding whether or not to serve an Enforcement Notice. In particular, the Commissioner is mindful of the

provisions of Article 8 of the ECHR in that the individuals whose sensitive personal data were held on the missing personal computers all have the right to respect for private and family life, home and correspondence.

**In view of the matters referred to above the Commissioner hereby gives notice that, in exercise of his powers under section 40 of the Act, he requires that the data controller shall within 35 days of the date of this Notice take the following steps:**

- (1) Ensure that any personal data is expunged from computer equipment as soon as it has been decommissioned, for example, by removal and destruction of the hard drives.**
- (2) Give effect to the recommendations of the SUI Panel still to be implemented by 31 December 2009 at the latest.**
- (3) Provide the Commissioner with a progress report through its Data Security Action Group programme documenting in detail how the recommendations of the SUI Panel have been, or are being, implemented by 31 March 2009 at the latest.**

#### Right of Appeal

There is a right of appeal against this Notice to the Information Tribunal. Information about appeals is set out in the attached Annex 1.

Any Notice of Appeal should be served on the Tribunal within 28 days of the date on which this Notice is served. If the notice of appeal is served late the Tribunal will not accept it unless it is of the opinion that it is just and right to do so by reason of special circumstances.

Dated the 25<sup>th</sup> day of February 2009

Signed: .....

David Smith  
Deputy Information Commissioner  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

## **ANNEX 1**

### **THE DATA PROTECTION ACT 1998 (PART V, SECTION 40)**

#### **RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER**

1. Section 48 of the Data Protection Act 1998 gives any person upon whom an enforcement notice or an information notice has been served a right of appeal to the Information Tribunal (the "Tribunal") against the notice.
2. If you decide to appeal and if the Tribunal considers:-
  - a) that the notice against which the appeal is brought is not in accordance with the law; or
  - b) to the extent that the notice involved an exercise of discretion by the Commissioner, that he ought to have exercised his discretion differently,

the Tribunal will allow the appeal or substitute such other decision as could have been made by the Commissioner. In any other case the Tribunal will dismiss the appeal.
3. You may bring an appeal by serving a notice of appeal on the Secretary to the Information Tribunal, Arnhem House Support Centre, PO Box 6987, Leicester, Leicestershire, LE1 6ZX.
  - a) The notice of appeal should be served on the Tribunal within 28 days of the date on which notice of the Commissioner's decision was served on or given to you.
  - b) If your notice of appeal is late the Tribunal will not accept it unless it is of the opinion that it is just and right to do so by reason of special circumstances.
  - c) If you send your notice of appeal by post to the Tribunal, either in a registered letter or by the recorded delivery service, it will be treated as having been served on the Tribunal on the date on which it is received for dispatch by the Post Office.
4. The notice of appeal should state:-
  - a) your name and address;

- b) the decision which you are disputing and the date on which the notice relating to such decision was served on or given to you;
- c) the grounds of your appeal;
- d) whether you consider that you are likely to wish a hearing to be held by the Tribunal or not;
- e) if you have exceeded the 28 day time limit mentioned above the special circumstances which you consider justify the acceptance of your notice of appeal by the Tribunal; and
- f) an address for service of notices and other documents on you.

In addition, a notice of appeal may include a request for an early hearing of the appeal and the reasons for that request.

5. By virtue of section 40(7), an enforcement notice may not require any of the provisions of the notice to be complied with before the end of the period in which an appeal can be brought and, if such an appeal is brought, the notice need not be complied with pending the determination or withdrawal of the appeal.

However, section 40(7) does not apply where the notice contains a statement that the Commissioner considers that the notice should be complied with as a matter of urgency.

Section 48(3) provides that where an enforcement notice contains a statement that the notice should be complied with as a matter of urgency then, whether or not you intend to appeal against the notice, you may appeal against –

- (a) the Commissioner's decision to include the statement in the notice, or
- (b) the effect of the inclusion of the statement as respects any part of the notice.

6. Before deciding whether or not to appeal you may wish to consult your solicitor or another adviser. At the hearing of an appeal a party may conduct his case himself or may be represented by any person whom he may appoint for that purpose.
7. The statutory provisions concerning appeals to the Information Tribunal are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and the Information Tribunal (Enforcement Appeals) Rules 2005 (Statutory Instrument 2005, No. 14).