Data Protection Act 1998

Monetary Penalty Notice

Dated: 27 April 2012

Name: Central London Community Healthcare NHS Trust

Address: 6th Floor, 64 Victoria Street, London, SW1E 6QP

Statutory framework

---

1. Central London Community Healthcare 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 Central London Community Healthcare NHS Trust and is referred to in this notice 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 he is 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. Under sections 55A and 55B of the Act (introduced by the Criminal Justice and Immigration Act 2008 which came into force on 6 April 2010) the Commissioner may, in certain circumstances, where there has there been a serious contravention of section 4(4) of the Act, serve a monetary penalty notice on a data controller requiring the data controller to pay a monetary penalty of an amount determined by the Commissioner and specified in the notice but not exceeding £500,000. The Commissioner has issued Statutory Guidance under section 55C (1) of the Act about the issuing of monetary penalties which is published on the Commissioner's website. It should be read in conjunction with the Data Protection (Monetary Penalties and Notices)

Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010.

Power of Commissioner to impose a monetary penalty

(1) Under section 55A of the Act the Commissioner may serve a data controller with a monetary penalty notice if the Commissioner is satisfied that –

(a) there has been a serious contravention of section 4(4) of the Act by the data controller,

(b) the contravention was of a kind likely to cause substantial damage or substantial distress, and

(c) subsection (2) or (3) applies.

(2) This subsection applies if the contravention was deliberate.

(3) This subsection applies if the data controller –

(a) knew or ought to have known –

(i) that there was a risk that the contravention would occur, and

(ii) that such a contravention would be of a kind likely to cause substantial damage or substantial distress, but

(b) failed to take reasonable steps to prevent the contravention.

Background

4. On or about 28 March 2011, an administrator at the Pembridge Palliative Care Unit (the "Unit") received a verbal request from St John's Hospice (the "Hospice") to send their inpatient lists to an additional fax number to ensure that service provision was unaffected during the leave of absence of one of the out of hours doctors. The administrator then created a template/fax coversheet listing both numbers, and printed a number of copies for use when the inpatient

lists were faxed to the Hospice.

5. A fax protocol had been agreed between the Hospice and the Unit whereby the administrator would telephone the Hospice to confirm whether the inpatient lists had been received and the Unit would confirm receipt. However, the administrator did not update the fax protocol with the second number or obtain approval from his manager.

6. The administrator at the Unit then sent the inpatient lists to the second fax number in addition to the agreed fax number provided by the Hospice. After each transmission the administrator telephoned the Hospice as agreed and on each occasion the Hospice confirmed they had received the fax. However, unbeknown to the administrator the Hospice was only confirming receipt of the inpatient list sent to the fax number contained in the fax protocol and not the second fax number. As a result, the administrator continued to send the inpatient lists to the second fax number.

7. On 6 June 2011, a member of the public informed the administrator by telephone that he had been receiving the inpatient lists since 28 March 2011 but had shredded them. The data controller couldn't trace the unintended recipient following this telephone call. During this period the administrator had sent approximately 45 fax transmissions attaching inpatient lists of varying numbers which were intended for the Hospice but received by the member of the public. The inpatient lists contained confidential and sensitive personal data relating to 59 individuals in total many of whom were receiving palliative care including medical diagnoses, information about the patient's domestic situation and resuscitation instructions.

8. At the time of the security breach the administrator had not been specifically trained to obtain management approval and to vary the fax protocol in this situation. In addition, the data controller had not given any consideration to a possible alternative to the use of fax transmission such as secure email. It is clear that the fax protocol became ineffective as soon as the administrator failed to add the second fax number to the fax protocol or obtain management approval.

9. The data controller has now taken substantial remedial action which includes not sending inpatient lists by fax to the Hospice, carrying out a detailed internal investigation into the security breach and considering the use of more secure means available for sending confidential and sensitive personal data such as email.

Grounds on which the Commissioner proposes to serve a monetary penalty notice

The relevant provision of the Act is the Seventh Data Protection Principle which provides, at Part I 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 at Part II of Schedule 1 to 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".

- The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act in that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle in relation to all personal data with respect to which he is the data controller.

  In particular, the data controller has failed to take appropriate technical and organisational measures against unauthorised processing of personal data such as providing its employees with appropriate training, management sign-off of any numbers to be added to the fax protocol and considering the use of a more secure means of transmission such as sending inpatient lists containing confidential and sensitive personal data via secure email. The Commissioner considers that the contravention is serious because the measures did not ensure a level of security appropriate to the harm that might result from such unauthorised processing and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial distress. Confidential and sensitive personal data was disclosed to an unauthorised third party due to the inappropriate technical and organisational measures taken by the data controller.

The failure to take appropriate technical and organisational measures has the potential to cause substantial distress to data subjects whose confidential and sensitive personal data has been disclosed to a third party who had no reason to see it.

In this particular case, the data subjects would suffer from substantial distress knowing that their confidential and sensitive personal data has been disclosed to a third party and that their data may have been further disseminated and possibly misused, even if those concerns do not actually materialise. In this context it is important to bear in mind that many of the affected individuals were patients receiving palliative care at the time of the security breach.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller ought to have known that there was a risk that the contravention would occur, and that such a contravention would be of a kind likely to cause substantial distress, but failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken this view because staff working in the Unit were used to handling inpatient lists and the data controller was aware of the confidential and sensitive nature of the personal data they were sending by fax to the Hospice on a regular basis hence the fax protocol.

  In the circumstances, the data controller ought to have known that there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention, such as providing its employees with appropriate training, management sign-off of any numbers to be added to the fax protocol and considering the use of a more secure means of transmission such as sending inpatient lists containing confidential and sensitive personal data via secure email. The risks of using simple fax facilities are self evident and, in the Commissioner's view, widely known.

  Further it should have been obvious to the data controller whose staff were routinely involved in handling such confidential and sensitive personal data that such a contravention would be of a kind likely to cause substantial distress to the data subjects due to the nature of the data involved.

Aggravating features the Commissioner has taken into account in determining the amount of a monetary penalty

Nature of the contravention

- Confidential and sensitive personal data relating to 59 individuals in total many of whom were patients receiving palliative care at the time of the security breach was disclosed to an unauthorised third party
- Contravention continued for over two months
- Contravention was serious because of the confidential and sensitive nature of the personal data

Effect of the contravention

- Unintended recipient couldn't be traced to confirm that he had destroyed the inpatient lists
- The contravention was of a kind likely to cause substantial distress to the data subjects

Behavioural issues

- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the unauthorised processing of personal data

Impact on the data controller

- Sufficient financial resources to pay a monetary penalty up to the maximum without causing undue financial hardship

Mitigating features the Commissioner has taken into account in determining the amount of the monetary penalty

Nature of the contravention

- No previous similar security breach that the Commissioner is aware of
- To the Commissioner's knowledge the personal data involved in the security breach has not been further disseminated

Effect of the contravention

- Unintended recipient informed the data controller when he telephoned the administrator that he had destroyed the inpatient lists
- No complaints received from the affected data subjects

Behavioural issues

- Voluntarily reported to Commissioner's office
- Data subjects or their representatives were notified
- Detailed investigation report was compiled
- Substantial remedial has now been taken
- Fully cooperative with Commissioner's office

Impact on the data controller

- Liability to pay monetary penalty will fall on the public purse although the penalty will be paid into the Consolidated Fund
- Significant impact on reputation of data controller as a result of these security breaches

Other considerations

- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act. This is an opportunity to reinforce the need for data controllers to review the sending of confidential and sensitive personal data by fax and to ensure either that alternative more secure means are used or that, at a minimum, appropriate and effective security measures are applied to the use of fax

Notice of Intent

A Notice of Intent was served on the data controller dated 8 February 2012. The Commissioner received representations from the data controller in a letter from the Chief Executive dated 8 March 2012. The Commissioner has considered the written representations made in relation to the notice of intent when deciding whether to serve a monetary penalty notice. In particular, the Commissioner has taken the following steps:

- reconsidered the amount of the monetary penalty generally, and whether it is a reasonable and proportionate means of achieving the objective which the Commissioner seeks to achieve by this imposition;
- ensured that the monetary penalty is within the prescribed limit of £500,000; and
- ensured that the Commissioner is not, by imposing a monetary penalty, acting inconsistently with any of his statutory or public law duties and that a monetary penalty notice will not impose undue financial hardship on an otherwise responsible data controller.

Amount of the monetary penalty

The Commissioner considers that the contravention of section 4(4) of the Act is serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £90,000 (Ninety thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by Tuesday 29 May 2012 at the latest. The monetary penalty is not kept by the Commissioner but will be paid into the Consolidated Fund which is the Government's general bank account at the Bank of England.

Early payment discount

If the Commissioner receives full payment of the monetary penalty by Monday 28 May 2012 the Commissioner will reduce the monetary penalty by 20% to £72,000 (Seventy two thousand pounds).

Right of Appeal

There is a right of appeal to the (First-tier Tribunal) General Regulatory Chamber against:

a. the imposition of the monetary penalty

and/or;

b. the amount of the penalty specified in the monetary penalty notice.

Any Notice of Appeal should be served on the Tribunal by 5pm on Monday 28 May 2012 at the latest. If the notice of appeal is served late the Tribunal will not accept it unless the Tribunal has extended the time for complying with this rule.

Information about appeals is set out in the attached Annex 1.

Enforcement

The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified in the notice within which a monetary penalty must be paid has expired and all or any of the monetary penalty has not been paid;
- all relevant appeals against the monetary penalty notice and any variation of it have either been decided or withdrawn; and
- the period for the data controller to appeal against the monetary penalty and any variation of it has expired.

In England, Wales and Northern Ireland, the monetary penalty is recoverable by Order of the County Court or the High Court. In Scotland, the monetary penalty can be enforced in the same manner as an extract registered decree arbitral bearing a warrant for execution issued by the sheriff court or any sheriffdom in Scotland.

Dated the 27th day of April 2012

Signed: ……..

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

ANNEX 1

SECTION 55 A-E OF THE DATA PROTECTION ACT 1998

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom a monetary penalty notice or variation notice has been served a right of appeal to the (First-tier Tribunal) General Regulatory Chamber (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 Tribunal at the following address:

   GRC & GRP Tribunals
   PO Box 9300
   Arnhem House
   31 Waterloo Way
   Leicester
   LE1 8DJ

   a) The notice of appeal should be served on the Tribunal by 5pm on Monday 28 May 2012 at the latest.

   b) If your notice of appeal is late the Tribunal will not admit it unless the Tribunal has extended the time for complying with this rule.

4. The notice of appeal should state:-

a) your name and address/name and address of your representative (if any);

b) an address where documents may be sent or delivered to you;

c) the name and address of the Information Commissioner;

d) details of the decision to which the proceedings relate;

e) the result that you are seeking;

f) the grounds on which you rely;

d) you must provide with the notice of appeal a copy of the monetary penalty notice or variation notice;

e) if you have exceeded the time limit mentioned above the notice of appeal must include a request for an extension of time and the reason why the notice of appeal was not provided in time.

5. 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.

6. The statutory provisions concerning appeals to the First-tier Tribunal (General Regulatory Chamber) are contained in sections 48 and 49 of, and Schedule 6 to, the Data Protection Act 1998, and Tribunal Procedure (First-tier Tribunal) (General Regulatory Chamber) Rules 2009 (Statutory Instrument 2009 No. 1976 (L.20)).