Data Protection Act 1998

Monetary Penalty Notice

Dated: 30 May 2013

Name: Stockport Primary Care Trust c/o NHS Commissioning Board

Address: Quarry House, Quarry Hill, Leeds LS2 7UE

Statutory framework

1. Stockport Primary Care Trust was 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 Stockport Primary Care 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. During 2011, a purchaser bought a site that was previously owned by the data controller. The site had been closed during 2010, although it was alarmed and patrolled during that time. The purchaser had visited the site twice as part of the viewing process and had noticed boxes of waste in one of the rooms but assumed they would be removed. The purchaser was among five other prospective purchasers who had viewed the premises with third party agents and staff from the data controller's Estates department.

5. On completion, the purchaser discovered that the boxes of waste had been left behind by the data controller. The purchaser looked into some of the boxes and discovered there was information relating to patients

including names they recognised together with some HR records.

6. The purchaser contacted Stockport MBC who notified the data controller. The data controller then arranged to collect the information from the purchaser. On further examination by the data controller the boxes were found to contain approximately 1,000 documents containing patient identifiable data including work diaries, letters, referral forms and patient records. These included confidential and highly sensitive personal data relating to over 200 data subjects including details about miscarriages, incontinence problems, child protection issues and a document from the police about the death of a child.

7. At the time of the security breach, the data controller was in the process of decommissioning the site and several Services were being moved to different locations around the area within a short period of time. Each Service within the site had been asked to ensure that confidential waste was ready for collection so that it could be disposed of securely but there was no specific guidance about who was responsible for ensuring its collection.

8. The Commissioner understands that the Estates department was responsible for the buildings, fixtures, fittings and furniture and each of the Services was responsible for its records, property and any other contents. Therefore, the Estates department didn't conduct a thorough search before they locked the building because they assumed that it had already been cleared by the relevant Services.

9. The subsequent investigation revealed two earlier security incidents where confidential and highly sensitive personal data had been left behind in secure buildings owned by the data controller. Again, the data controller was fortunate that the information was discovered by responsible third parties who notified the data controller.

10. The Commissioner understands that remedial action has now been taken by the data controller which includes implementing a new policy for the decommissioning of services and buildings to ensure that, in future, patient records will be disposed of promptly and securely.

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 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 particular, the data controller failed to take appropriate organisational measures against unauthorised processing and accidental loss of confidential and sensitive personal data relating to approximately 1,000 documents such as having a decommissioning policy.

  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 accidental loss given 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 at risk of unauthorised processing and accidental loss due to the inappropriate organisational measures taken by the data controller.

  The failure to take appropriate organisational measures might well cause substantial distress to data subjects by simply knowing that their confidential and sensitive personal data has been accessed by the purchaser who had no right to see that information.

  Further, the data subjects would be justifiably concerned that their data may be further disseminated even if those concerns do not actually materialise. The position is further exacerbated because the purchaser knew some of the data subjects.

- The Commissioner is satisfied that section 55A (3) of the Act applies in that the data controller knew or 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 of the amount of confidential and sensitive personal data relating to patients and staff held on the site. The data controller was used to dealing with such information and had taken some steps to safeguard the patient records even though the steps taken were inadequate.

  In the circumstances, the data controller knew or ought to have known there was a risk that the contravention would occur unless reasonable steps were taken to prevent the contravention such as having a decommissioning policy.

  Further, the decommissioning of two sites holding large amounts of confidential and sensitive personal data within a short time period was a huge undertaking and the data controller should have provided for the highest level of security.

  In the Commissioner's view it should have been obvious to the data controller (as part of the NHS) 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

- The site was not fully decommissioned for over 12 months

Effect of the contravention

- Some of the data subjects were known to the purchaser who accessed the information
- Five prospective purchasers had access to the site in total

Behavioural issues

- There were two similar security incidents prior to this security breach that had not been escalated to the senior management team

Impact on the data controller

- Sufficient financial resources to pay a monetary penalty up to the maximum without causing undue financial hardship. The data controller was a large NHS Trust with assets of around £36 million in the financial year ending 2011
- The data controller is a public authority, so liability to pay any monetary penalty will not fall on any individual

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

---

Nature of the contravention

- The site was maintained in a secure state

Effect of the contravention

- No evidence that records have been further disseminated as far as the Commissioner is aware
- No complaints received from the affected data subjects

Behavioural issues

- Remedial action has now been taken
- Fully cooperative with ICO

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 this security breach

Other considerations

- The Commissioner's underlying objective in imposing a monetary penalty is to promote compliance with the Act and this is an opportunity to reinforce the need for data controllers to ensure that appropriate and effective security measures are applied to personal data
- The Fifth Data Protection Principle at Part I of Schedule 1 to the Act was also contravened by the data controller in that data was kept for longer than was necessary for its purposes

Notice of Intent

A notice of intent was served on the data controller dated 12 March 2013. The data controller was dissolved on 31 March 2013. The Commissioner received written representations dated 8 April 2013 from the NHS Commissioning Board who have taken over responsibility for this security breach from the data controller. 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 £100,000 (One hundred thousand pounds) is reasonable and proportionate given the particular facts of the case and the underlying objective in imposing the penalty.

In reaching this decision, the Commissioner considered another case of a similar nature in which a monetary penalty had been imposed, the facts and aggravating and mitigating features referred to above. Of particular relevance is firstly, that this security breach could have resulted in patient records being dumped on the local tip and secondly, the purchaser who accessed the information knew some of the data subjects.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 3 July 2013 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 2 July 2013 the Commissioner will reduce the monetary penalty by 20% to £80,000 (Eighty thousand pounds) but the NHS Commissioning Board on behalf of the data controller would then forfeit any right of appeal.

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 2 July 2013 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 30th day of May 2013

Signed: …….....

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

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 2 July 2013 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)).