Data Protection Act 1998

Monetary Penalty Notice

Dated: 18 June 2013

Name: NHS Surrey c/o Department of Health Regional Legacy Management Team

Statutory framework

1. NHS Surrey 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 NHS Surrey 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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 12 January 2010, the Head of the data controller's IT team was contacted by the Director of a company (the "company") who was looking for new business. Subsequently, the company's Director came to visit the IT team to discuss their requirements for the disposal of redundant equipment such as old PCs. The IT team explained that the hard drives would have to be physically destroyed because they may store confidential medical information. The company's Director provided an assurance to the IT team that the hard drives would be crushed by an industrial guillotine.

5. The company's Director explained that they could provide this service free of charge because the recycled materials could be re-sold by the company. The company's Director informed the IT team that his

clients included well-known companies and handed them a sales brochure describing the company's services. The company also had (among other things) a 'waste management and approved authorised treatment facility' licence issued by the Environment Agency which provided the data controller with reassurance that the company was reliable.

6. The IT team decided to give the company a trial and arranged for two collections to take place on 8 March 2010. The IT team supervised both collections and the company subsequently provided destruction certificates. However, the disposal process for redundant equipment did not require the IT team to carry out an assessment of the risks of using a data processor to dispose of the hard drives and they did not observe the destruction process.

7. The IT team then decided to engage the company for hard drive destruction (among other things) even though the data controller had an existing arrangement in place with an approved contractor. The Commissioner understands that the accountable officer for Information Governance was not involved in this decision. Further, there was no written agreement with the company although the data controller did receive written assurances that the hard drives would be destroyed.

8. Further collections then took place between 8 March 2010 and 28 May 2012 under the supervision of the IT team. Between 10 February 2011 and 28 May 2012 approximately 1570 PCs with individual hard drives were collected by the company. Some of the 'Data Devices Destroyed' certificates issued before January 2011 stated that the hard drives had been 'wiped/destroyed/recycled' so it was unclear exactly what had happened to them.

9. On 29 May 2012, a member of the public informed the data controller that he had purchased a PC with a hard drive storing confidential medical information from a third party company (the "third party company") via an online auction site. The data controller reclaimed the PC and on booting up the hard drive using data recovery software it was found to hold 1,428 files. Many of the files contained confidential sensitive personal data and HR records including patient records relating to approximately 900 adults and 2000 children.

10. The hard drive's serial number was checked against the destruction certificate and was identified as one of 235 hard drives collected by the company on 14 February 2012. On further investigation the data controller discovered that the third party company had purchased 28 PCs from the company's trading arm via an online auction site.

11. The data controller reclaimed the PCs and then cross referenced the serial numbers for the hard drives against the destruction certificates. Seven matches were found and file recovery software revealed that three of these hard drives again contained confidential sensitive personal data.

12. On 2 July 2012, the third party company informed the data controller that they had bought another 12 PCs from the company's trading arm. Again, the data controller reclaimed the PCs and found that three of the serial numbers for the hard drives matched destruction certificates, although no recoverable data was found on that occasion.

13. The data controller has been unable to trace the destinations of the remaining PCs collected by the company between 10 February 2011 and 28 May 2012.

14. The data controller has now taken remedial action which includes developing a new policy framework to address the internal re-use of information and appliances and the disposal process for redundant equipment.

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".

Paragraph 11 at Part II of Schedule 1 to the Act provides that:

"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle-

(a) choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and

(b) take reasonable steps to ensure compliance with those measures.

Paragraph 12 at Part II of Schedule 1 to the Act further provides that:

"Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless-

(a) the processing is carried out under a contract-

(i) which is made or evidenced in writing, and

(ii) under which the data processor is to act only on instructions from the data controller, and

(b) the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.

In deciding to issue this monetary penalty notice, the Commissioner has considered the facts of the case and the deliberations of those within his office who have recommended this course of action. In particular, he has considered whether the criteria for the imposition of a monetary penalty have been met; whether, given the particular circumstances of this case and the underlying objective in imposing a monetary penalty, the imposition of such a penalty is justified and whether the amount of the proposed penalty is proportionate.

- 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 choose a data processor which provided sufficient guarantees in respect of the organisational security measures governing the processing to be carried out, and to take reasonable steps to ensure compliance

with those measures.

Further, the data controller did not have a written contract with the company under which the data processor was to act only on instructions from the data controller, and which required the company to comply with obligations equivalent to those imposed on a data controller by the Seventh Data Protection Principle.

In particular, the Commissioner would expect the data controller to have carried out a proper risk assessment and chosen a data processor providing sufficient guarantees in a written agreement that the hard drives would be physically destroyed and that destruction certificates containing serial numbers for each individual drive would be provided.

The data controller should then have taken reasonable steps to ensure compliance with those measures such as effectively monitoring the destruction process and maintaining audit trails and inventory logs of hard drives destroyed by the company based on the serial numbers in the destruction certificates for each individual drive.

The Commissioner considers that the contravention is serious because the data controller failed to comply with any of the requirements set out in paragraphs 11 and 12 in Part II of Schedule 1 to the Act.

Consequently, the company did not physically destroy the hard drives resulting in approximately 1570 hard drives containing confidential and sensitive personal data relating to an unknown number of patients and staff being offered for sale via the internet.

The data controller therefore failed to ensure a level of security appropriate to the harm that resulted from the unauthorised processing and accidental loss of the hard drives 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.

  The failure to take appropriate organisational measures is likely to cause substantial distress to data subjects whose sensitive personal data has been retrieved by a member of the public who had no right to see that information.

The data subjects would also suffer from substantial distress knowing that their sensitive personal data might have been offered for sale to unauthorised third parties via the internet.

Further, they would be justifiably concerned that their data may be further disseminated even if those concerns do not actually materialise. If the data is in fact disclosed to untrustworthy third parties then it is likely that the contravention would cause further distress to 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 a large amount of confidential and sensitive personal data relating to the data controller's patients and staff was held on the hard drives. The data controller was used to dealing with such information on a daily basis and had therefore taken some steps to safeguard the information on the hard drives by engaging the company (and a previous contractor) to dispose of them.

  Further, some of the 'Data Devices Destroyed' certificates issued before January 2011 stated that the hard drives had been 'wiped/destroyed/recycled' and this should have alerted the data controller to the fact that some of the hard drives may not have been physically destroyed. Instead, the data controller accepted the company's word on 28 February 2011 that the certificates they were receiving were in fact destruction certificates.

  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 carrying out a proper risk assessment; choosing a data processor providing sufficient guarantees in a written agreement that the hard drives would be physically destroyed; that destruction certificates containing serial numbers for each individual drive would be provided and then effectively monitoring compliance with those measures.

  Further, this was a huge project involving the destruction of approximately 1570 hard drives containing a large amount of sensitive personal data over a two year period which should have

been afforded 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

---

Effect of the contravention

- Approximately 1570 hard drives holding confidential sensitive personal data relating to an unknown number of patients and staff
- The majority of the hard drives sold on the internet have not been recovered

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 is a large organisation with a budget of £1.7 billion per annum
- 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

- No previous similar security breach that the Commissioner is aware of

Effect of the contravention

- The data can only be retrieved from the hard drives using data recovery software

Behavioural issues

- Data controller received written assurances from the company that the hard drives would be physically destroyed

- Voluntarily reported to ICO
- 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 notice 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 held on hard drives

Notice of Intent

A notice of intent was served on the data controller dated 28 March 2013. The data controller was dissolved on 31 March 2013. The Commissioner received written representations from the Solicitor acting for the Department of Health Regional Legacy Management Team who have taken over responsibility for any outstanding issues arising from the dissolution of NHS Surrey. 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 very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £200,000 (Two 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 as well as the facts and aggravating and mitigating factors referred to above. Of particular relevance is that the security breach resulted in a large number of hard drives containing confidential and sensitive personal data being offered for sale via the internet.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by 22 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 19 July 2013 the Commissioner will reduce the monetary penalty by 20% to £160,000 (One hundred and sixty 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 19 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 18th day of June 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 19 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;

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

h) 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)).