Data Protection Act 1998

Monetary Penalty Notice

Dated: 28 May 2012

Name: Brighton and Sussex University Hospitals NHS Foundation Trust

Address: Eastern Road, Brighton BN2 5BE

Statutory framework

---

1. Brighton and Sussex University Hospitals NHS Foundation 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 Brighton and Sussex University Hospitals NHS Foundation 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. The data controller's IT services (including disposal of IT equipment) were provided by Sussex Health Informatics Service ("HIS") who are accredited by the Department of Health. HIS is an NHS member organisation and they provide similar shared services to other NHS Trusts in Sussex. HIS sometimes sub-contracted certain work if they were unable to carry it out themselves, usually to Company A. The arrangement between the data controller and HIS was evidenced in a

service level agreement that had expired.

5. In March 2008, the data controller decommissioned a number of hard drives which were then kept in commercial storage in a locked room protected by CCTV. In April 2010, approximately 1000 of the old hard drives were moved to Brighton General Hospital (the "hospital") and stored in a room that could only be accessed using a key code, pending their destruction. As Company A could not destroy hard drives they suggested that the work be carried out by Company B who would destroy the hard drives without charge. The Commissioner understands that Company B was run by one individual (the "individual"). There was no contract in place between HIS and Company B to carry out this work (even though Company B offered to enter into a contract) and only very basic checks were made by HIS on the individual's credentials. Apparently, the data controller was not aware that HIS had engaged the individual to destroy the hard drives stored at the hospital.

6. From 28 to 30 September 2010 and 14 to 15 October 2010 the individual attended the hospital to carry out destruction of the 1000 drives. The Commissioner understands that the hard drives should have been destroyed in the former X-Ray department which again, could only be accessed using a key code. The individual was supervised and occasionally assisted by staff working for HIS but not constantly. On completion of the work a "certificate of destruction" should have been obtained from the individual containing serial numbers for each drive. Instead, only one generic document was provided for the whole batch.

7. In December 2010, a data recovery company bought four hard drives via an online auction site from a seller (the "seller") who had bought them from the individual. The data recovery company discovered that the drives held data belonging to the data controller and promptly returned them for further analysis. Amongst various types of personal data, the hard drives held information originating from a database in the HIV and Genito Urinary Medicine Department. The database contained personal data, some of which was highly sensitive, including names; dates of birth; occupations; sexual preferences; STD test results and diagnoses for 67,642 patients in readable format. A second database (which was a subset of the larger one) consisted of the names and dates of birth of 1527 HIV positive patients. With a basic knowledge of "Access" both databases could be matched up.

8. The Commissioner's office commenced an investigation and was given assurances by the data controller that only these four hard drives were affected and that all the other hard drives awaiting destruction had

been secured. However, in April 2011 the Commissioner's office was contacted by a university who explained that one of their students had purchased a number of hard drives via an Internet auction site in January 2011 as part of his computing studies. The student did not need any forensic software to access the contents of the hard drives which appeared to originate from the data controller. The Commissioner's office examined them and found that at least 15 out of the 20 hard drives contained information belonging to the data controller.

9. The Commissioner found that the hard drives contained personal data, some of which was highly sensitive, including names; dates of birth; patients' medical conditions and treatment; patient referral letters with full descriptions of medical conditions; named X-rays; comprehensive disability living allowance forms and children's reports. There were also several Excel spreadsheets containing thousands of staff details. One example included the full names, payroll ID, National Insurance numbers, telephone numbers, email addresses, home addresses, ward and hospital ID, dates of birth, sex, marital status and ethnic origin of 268 employees. There were also documents referring to staff criminal convictions and suspected offences.

10. As a result of a police investigation, the Commissioner understands that the individual sold at least 232 of the data controller's hard drives on an Internet auction site in two batches in October and November 2010 containing highly sensitive personal data of tens of thousands of patients and staff.

11. The data controller is unable to explain how the individual removed at least 252 of the 1000 hard drives he was supposed to be destroying from the hospital during his five days on the premises. The individual was not believed to have known the key code to the separate rooms where the hard drives were stored and destroyed respectively and was usually (but not constantly) supervised by staff working for HIS. However, the data controller acknowledges that the individual would have left the building for breaks and that the hospital is publicly accessible. The data controller is confident that the individual destroyed the majority of the hard drives on the premises even though there were no audit trails and inventory logs of the movement of and destruction of the hard drives to support this view. Active attempts have been made by the police and the data controller to recover the 232 hard drives known to have been sold to third parties. These have all now been accounted for although not all of them have been recovered.

12. The data controller has now taken remedial action which includes

providing a secure central store for hard drives and other media; reviewing the process for vetting potential IT suppliers; obtaining the services of a fully accredited ISO 27001 IT waste disposal company and making progress towards central network access.

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.

- 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 providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and take reasonable steps to ensure compliance with those measures.

  Further, the processing was not carried out under a contract between the Trust and HIS (whether made or evidenced in writing) under which the data processor was to act only on instructions from the data controller, and which required HIS to comply with obligations equivalent to those imposed on a data controller by the Seventh Data Protection Principle.

  The Commissioner is of the view that such a contract should also have given some consideration to the possibility that HIS might appoint sub-contractors to process the personal data, such as either prohibiting their use altogether or requiring the prior consent of the data controller.

  The data controller could then have carried out a risk assessment and taken steps to ensure the reliability of the individual who would have access to the personal data. They could also have checked that the terms of the contract were equivalent to the main contract and that the individual had provided sufficient guarantees in respect of the technical and organisational security measures governing the destruction of the hard drives.

  Such security measures might have included the effective supervision of the individual by HIS when he attended the hospital, maintaining audit trails and inventory logs of hard drives destroyed by the

individual and obtaining a "certificate of destruction" containing serial numbers, for each drive. The data controller could also have put in place regular monitoring to ensure compliance with these and other measures and, in view of the nature of the information involved might even have chosen to directly supervise the individual itself.

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

Consequently, the data controller was not aware that HIS had engaged the individual to destroy the hard drives stored at the hospital and therefore failed to ensure a level of security appropriate to the harm that resulted from the accidental loss of the hard drives and the nature of the data to be protected.

- The Commissioner is satisfied that the contravention was of a kind likely to cause substantial distress to data subjects whose highly sensitive personal data was taken by an individual who had no right to see that information. The data subjects would also suffer from substantial distress knowing that their personal data (some of which was highly sensitive) has been disclosed to at least eight 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 disclosed to untrustworthy third parties then it is likely that the contravention would cause further distress and also substantial damage to the data subjects such as exposing them to identity fraud or even blackmail.

- 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 damage or substantial distress, but failed to take reasonable steps to prevent the contravention.

  The Commissioner has taken the view that the data controller knew or ought to have known that there was a risk that the contravention would occur because a huge amount of personal data (much of which was highly sensitive) 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 as such had its own Information Governance Team. They had therefore taken some steps to safeguard the information on the hard drives before the security

breach occurred by paying for the hard drives to be stored in a locked room with CCTV with the intention of securely destroying them.

Further, this was a huge project involving the destruction of 1000 hard drives containing a large amount of personal data (much of which was highly sensitive) and 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 damage or substantial distress to the data subjects due to the nature of the data involved.

In the circumstances, the data controller failed to take reasonable steps to prevent the contravention such as complying with the "data processor" requirements of the Seventh Data Protection Principle which if properly complied with should have alerted the data controller to the fact that HIS had engaged the individual to destroy the hard drives. The data controller could then have carried out a risk assessment and taken steps to ensure that the individual was reliable and that he was effectively supervised by HIS, or even by itself, when he attended the hospital. They could have ensured that audit trails and inventory logs of hard drives destroyed by the individual were maintained and obtained a "certificate of destruction" containing serial numbers, for each drive. The data controller could also have put in place regular monitoring to ensure compliance with these and other measures.

Finally, when the security breach involving four hard drives was first discovered, the data controller could not identify the risk to the remaining hard drives even though the individual had been given the responsibility of destroying approximately 1000 of the data controller's hard drives. In the Commissioner's view the data controller should have been able to identify the wider risks to the remaining hard drives at an earlier stage which may have gone some way to mitigating the risk of damage and distress being caused to individuals.

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

---

Nature of the contravention

- Contravention was serious because of the highly sensitive nature of some of the personal data

Effect of the contravention

- Huge amount of personal data some of which was highly sensitive held on 1000 hard drives relating to tens of thousands of patients and staff

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 security breach has been relatively contained
- The contravention was exacerbated by circumstances outside the direct control of the data controller

Effect of the contravention

- The 232 hard drives known to have been sold on the Internet have all been accounted for although not all of the drives have been recovered

Behavioural issues

- Data controller selected HIS to act as its processor which had been accredited by the Department of Health, and might reasonably have been expected to be familiar with the nature of the personal data in question and the need for appropriate security
- Active attempts made by the data controller to recover the sold hard drives and assist the police in their investigation
- Initial loss of four of the hard drives voluntarily reported to ICO
- Detailed investigation report compiled
- Remedial action has now been taken
- Data controller may consider an audit
- 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 12 December 2011. The Commissioner received written and oral representations from the data controller. The Commissioner has considered the written and oral 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 most serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £325,000 (Three hundred and twenty five 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 26 June 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 25 June 2012 the Commissioner will reduce the monetary penalty by 20% to £260,000 (Two 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 Monday 25 June 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 28th day of May 2012

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 Monday 25 June 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)).