Data Protection Act 1998

Monetary Penalty Notice

Dated: 13 June 2012

Name: Belfast Health & Social Care Trust

Address: Trust Headquarters, A Floor, Belfast City Hospital, Lisburn Road, Belfast, BT9 7AB

Statutory framework

1. Belfast Health & Social 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 carried out by Belfast Health & Social 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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. In April 2007, six acute and community Trusts amalgamated into the Belfast Health & Social Care Trust which meant that the data controller took over responsibility for more than 50 disused sites. Confidential and sensitive personal data consisting of patient and staff records (some dating from the 1950s) were stored in one of the disused sites, namely Belvoir Park Hospital (the "site"). The site consisted of approximately 40 separate buildings which over the years had treated fever and then cancer patients before closing on 17 March 2006. The data controller did not carry out an inspection when it took over responsibility for the site.

5. However, the data controller did arrange for the 26 acre site to be

patrolled by two permanent security guards together with five daily mobile patrols. The CCTV systems covering the clinical areas were isolated although the electricity supply to some of the buildings was maintained for the operation of CCTV equipment, fire and intruder alarms and security lighting. But by the end of 2007 the CCTV system monitoring the main entrance was not recording and the fire and intruder alarms had been isolated after developing faults.

6. The Commissioner understands that trespassers gained access to the site on several occasions to photograph the records which were then posted on the internet. The most recent photographs are thought to have been taken in or around May 2010, although it is accepted that very few of the data subjects were identifiable from these photographs. Apparently, the data controller was not aware that the security of the data on the site was being compromised until 2 March 2010 when they received a report from a third party that images of the records were accessible on-line.

7. On 22 March and 23 April 2010, the data controller arranged for an inspection of seven of the buildings on the site (most recently used to treat cancer patients). A large quantity of patient and staff records were discovered but some parts of the site were either locked or inaccessible due to concerns about asbestos contamination and many of the records were damaged by damp and mould. The data controller was also informed by letter dated 30 December 2010 that an Order had been made by PRONI (which applied to public authorities in Northern Ireland) to suspend the destruction of records until March 2011. Between April and July 2010, further improvements were made to the security of the site which involved repairing damaged doors and windows; installing a pedestrian gate in a fence; improving foot patrol efficiency and clearing overgrown vegetation.

8. Due to these factors, the records remained on site until the media reported that security of the data on the site had again been compromised in April 2011. The number of security guards was then increased from two to four. In early May 2011, the data controller also carried out an inspection of the whole site which revealed the full scale of the problem and the discovery of further records many of which were being retained in breach of the data controller's "Records Retention and Disposal" policy.

9. It was found that records on the site were stored either in boxes, in cabinets, on shelves or on the floor. The patient records included, among other things, approximately 100,000 paper medical records; x-rays; microfiche records; hard copies of medical scans; hard copies of scan reports; lab results; paper ward records and various letters. In addition, 15,000 staff records were held in a building that had been vacated in 1992 including unopened wage slips. However, it is accepted that

approximately 20% of the patient records were likely to relate to deceased individuals and would not be covered by the Act.

10. The data controller has now taken remedial action which involved removing the records from the site; examining them and either retaining or securely disposing of the records. In addition, a Decommissioning Policy to prevent a recurrence was implemented on 6 June 2011.

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 technical and organisational measures against accidental loss of personal data such as carrying out a full inspection of the site and making an inventory of the records at the outset; maintaining the integrity of the buildings that held any records; having the appropriate CCTV systems; intruder alarms; security lighting and a sufficient number of security guards to secure a 26 acre site pending its decommissioning. 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 accidental loss 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 subject to unauthorised access and put at risk of loss due to the inappropriate technical and organisational measures taken by the data controller. The failure to take appropriate technical and organisational measures is likely to cause substantial distress to data subjects whose confidential and sensitive personal data has been accessed by individuals who had no right to see that information.

  In this particular case the data subjects would suffer from substantial distress knowing that their confidential and sensitive personal data has also been posted on the internet. Further, they would be justifiably concerned that their data may be further disseminated even if those concerns do not actually materialise.

- 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 large 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 records on site 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 carrying out a full inspection of the site and making an inventory of the records at the outset; maintaining the integrity of the buildings that held any records; having the appropriate CCTV systems; intruder alarms; security lighting and a sufficient number of security guards to secure a 26 acre site pending its decommissioning.

  Further, taking over responsibility for more than 50 disused sites holding large amounts of confidential and sensitive personal data was a huge undertaking and in the restructure 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

- Contravention was serious because of the confidential and sensitive nature of some of the personal data
- It took nearly four years to fully decommission the site

Effect of the contravention

- Large amount of confidential and sensitive personal data was held on the site relating to hundreds of thousands of patients and staff
- The contravention was of a kind likely to cause substantial distress to the data subjects
- Complaints were made by some of the affected individuals

Behavioural issues

- Security breaches were not reported to the ICO
- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the accidental loss 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

- The site was extensive; there were concerns about asbestos contamination and a suspension order was in force for approximately three months

Effect of the contravention

- No evidence that records have been further disseminated as far as the Commissioner is aware

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 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
- 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 2 April 2012. The Commissioner received written representations from the data controller's Chief Executive in a letter dated 4 May 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 very serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £225,000 (Two 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 17 July 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 16 July 2012 the Commissioner will reduce the monetary penalty by 20% to £180,000 (One hundred and eighty 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 16 July 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 13th day of June 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 16 July 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)).