Data Protection Act 1998

Monetary Penalty Notice

Dated: 11 June 2013

Name: North Staffordshire Combined Healthcare NHS Trust

Address: Harplands Hospital, Hilton Road, Stoke-on-Trent ST4 6TH

Statutory framework

---

1. North Staffordshire Combined 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 North Staffordshire Combined 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 it 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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

1. In August and September 2011, the data controller's Single Point of Access Team (the "Team") sent three faxes from a fax machine designated as a safe haven (in that only staff authorised to see the information had access through a secure entry point). The faxes were intended for the Wellbeing Centre (the "Centre") whose aim is to improve access to psychological therapies, but instead they were received by a member of the public. The faxes contained confidential and highly sensitive personal data relating to three individuals, including patient information consisting of (among other things) their full name, date of birth, address, ethnic origin, religion, medical history, details of mental and physical health problems and their causes, any special needs/mental health services provided and whether

the individual was at risk of self-harm, serious self-neglect or exploitation by others.

2. The Commissioner understands that the Centre's new fax number had not been pre-programmed into the Team's fax machine even though staff in the Team regularly sent faxes to the Centre. As a result, the Centre's fax number was input manually each time by staff in the Team, and the fax number of the unintended recipient differed from the Centre's number by just one digit. Further, staff in the Team did not operate a "call ahead" system which would have at least alerted the data controller to the fact that the faxes had not been received by the Centre.

3. At the time of the security breaches the data controller had a safe haven policy and best practice guidelines (available on its intranet), which included the requirement for staff to pre-program the most frequently-used numbers into safe haven fax machines and to operate a "call ahead" system. However, the Team were not aware of the safe haven policy and best practice guidelines and hadn't received any specific training relating to fax use. These shortcomings were exacerbated by a lack of effective management control.

4. Remedial action has now been taken and the members of this Team are now fully aware of the data controller's policies and guidelines relating to fax use, which is closely monitored, although the Commissioner understands that a further incident has recently occurred in which a member of a different team sent a blank referral form to the same member of the public's fax number in error. Fortunately, this did not contain any personal data.

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".

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 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 has failed to take appropriate organisational measures against unauthorised processing of personal data, such as providing its staff with appropriate training and having in place effective management controls.

  The Commissioner considers that the contravention is serious because the measures in place did not ensure a level of security appropriate to the harm that might result from such unauthorised processing, 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 disclosed to an unauthorised third party on several occasions due to the inappropriate organisational measures taken by the data controller.

  The failure to take appropriate 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 might well have suffered substantial distress by simply knowing that their confidential and sensitive personal data has been disclosed to a third party.

  Further, the data subjects would be justifiably concerned 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 the affected individuals were vulnerable adults.

- 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 the members of the Team were used to handling patient information and the data controller was aware of the confidential and sensitive nature of the personal data they were sending by fax to the Centre on a regular basis, hence it had introduced the safe haven policy and best practice guidelines.

  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 staff with appropriate training and having effective management controls in place. 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 employees 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

- It is noted that a further incident has since occurred where the same unintended recipient received another fax from a different team, although fortunately this did not contain any personal data

Effect of the contravention

- Data controller was unable to obtain confirmation from the unintended recipient that he had destroyed the patient information

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 NHS Trust with turnover of £74 million per year at the present time
- The data controller is a public authority, so liability to pay any 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

- To the Commissioner's knowledge the personal data involved in the security breach has not been further disseminated

Effect of the contravention

- No complaints received from the affected data subjects

Behavioural issues

- No previous similar security breach as far as the Commissioner is aware
- Voluntarily reported to Commissioner's office
- Data subjects were notified
- Detailed audit report was compiled
- Substantial remedial has now been taken
- Fully co-operative 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 is to promote compliance with the Act. This is an

opportunity to reinforce the need for data controllers to ensure that 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 12 March 2013. The Commissioner received written representations from the data controller's Chief Executive dated 12 April 2013. 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 £55,000 (Fifty five 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 other cases of a similar nature in which a monetary penalty had been imposed, and the facts and aggravating and mitigating factors noted above. In particular, the Commissioner has noted the remedial actions taken by the data controller, although he also notes that a further incident involving a different team but the same unintended recipient has occurred during his office's investigation into this matter.

Payment

The monetary penalty must be paid to the Commissioner's office by BACS

transfer or cheque by 15 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 12 July 2013 the Commissioner will reduce the monetary penalty by 20% to £44,000 (Forty four thousand pounds) but 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 12 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 11th 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 12 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)).