Data Protection Act 1998

Monetary Penalty Notice

Dated: 2 July 2012

Name: St George's Healthcare NHS Trust

Address: Blackshaw Road, Tooting, London, SW17 0QT

Statutory framework

---

1. St George's 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 St George's 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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

4. [redacted] two letters [redacted] were mistakenly sent by post to the address [redacted] Both letters contained confidential and highly sensitive personal data including a summary of [redacted] allegations; details of the data subject's medical history, details of the physical examination undertaken and its findings; a medical opinion on the findings together with the data subject's microbiology results.

5. [redacted] the data subject's [redacted] had not resided at the [redacted] address for nearly five years. The Commissioner understands that it is common for [redacted] individuals to change address [redacted] The [redacted] current address was provided when the data subject was first referred to the data controller for a medical examination on [redacted]. It was also logged onto the national NHS SPINE ("SPINE") [redacted] which holds the most recent patient demographic information for all patients with a valid NHS number.

6. The security breach occurred because iClip (the local patient administration programme) had not been aligned with SPINE. The medical secretaries [redacted] should have received an electronic prompt to carry out a patient demographic search ("PDS") to verify the data subject's address at various stages of the process including registration of the data subject's referral [redacted] booking the data subject's appointment; collecting and creating hospital notes; checking-in the data subject at hospital [redacted]

7. Both of the medical secretaries who were directly involved with compiling the incorrectly addressed letters had received iClip training which included advice on conducting a PDS and were also aware that the patient address information on iClip did not always match the information on SPINE. The Commissioner understands that a third medical secretary (who was absent at the time of the security breach) normally booked any medical appointments on iClip, this being a key opportunity to conduct a PDS. However, there is no record of any medical appointment ever being made on iClip for the data subject.

8. Further, the staff who were directly involved in compiling the letters did not verbally check the address with the data subject's [redacted] or check that the address on iClip matched the address on the original referral form. In addition, the data subject's medical records were incorrectly made up by the medical secretaries so that they did not have the usual patient demographic front sheet or [redacted] which might have alerted staff to the discrepancy.

9. At the time of the security breach it was possible for staff to bypass or disable the PDS prompt generated by iClip. The data controller was also aware that many staff found the iClip system difficult to use and that conducting a PDS against the SPINE was cumbersome. This was identified as a failing by the data controller and placed on its risk register in October 2010. A request for change was submitted to the data controller's software supplier on 17 December 2010 and a solution

to the problem was implemented on 30 September 2011.

10. Following the security breach the data controller commissioned a report and some remedial action has now been taken which includes booking all such medical appointments on iClip; reminding staff through team meetings and appraisals about the importance of conducting a PDS; reminding staff to check that information received about patients on social service referrals matches the information on iClip and SPINE and finally, implementing the technical solution that will prevent staff from bypassing or disabling the PDS function on iClip in future.

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".

- The Commissioner is satisfied that there has been a serious contravention of section 4(4) of the Act.

  In particular, the data controller had failed to take appropriate technical and organisational measures against unauthorised processing of personal data, such as ensuring that the PDS function could not be bypassed or disabled and that staff [redacted] are provided with appropriate training that covers the importance of checking that personal data such as names and addresses are accurate

and alerts them to the opportunities to verify the accuracy of the information that are likely to arise. 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 the nature of the data to be protected.

- The Commissioner is satisfied that the contravention is of a kind likely to cause substantial distress. It is likely that confidential and highly sensitive personal data was disclosed to an unauthorised third party due to the inappropriate technical and organisational measures taken by the data controller. The failure to take appropriate technical and organisational measures has the potential to cause substantial distress to the data subject whose confidential and highly sensitive personal data may have been disclosed to a third party [redacted]

  In this particular case, the data subject would suffer from substantial distress knowing that [redacted] confidential and highly sensitive personal data may have been disclosed to a third party and that [redacted] 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 individual was [redacted] considered to be vulnerable.

- 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 the staff who worked in the [redacted] team were used to dealing with such cases and the data controller would have been aware of the confidential and highly sensitive nature of the personal data they were dealing with. The data controller was also aware from at least October 2010 that many staff found the iClip system difficult to use and that conducting a PDS against the SPINE was cumbersome resulting in the PDS being bypassed or disabled.

  In the circumstances, the data controller knew or 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 ensuring that the PDS function could not be bypassed or disabled and that staff working in the [redacted] team were provided with appropriate training that covers the importance of checking that

personal data such as names and addresses are accurate and alerts them to the opportunities to verify the accuracy of the information that are likely to arise. Further, it should have been obvious to the data controller whose staff worked in the [redacted] team that such a contravention would be of a kind likely to cause substantial distress to the data subject 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

- Two similar security breaches occurred within seven days of each other
- It is likely that unauthorised confidential and highly sensitive personal data [redacted] was disclosed to an unauthorised third party [redacted]
- Contravention involved confidential and highly sensitive personal data

Effect of the contravention

- Unauthorised disclosure may prejudice any criminal prosecution
- The contravention was of a kind likely to cause substantial distress to the data subject

Behavioural issues

- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate technical and organisational measures against the unauthorised processing of personal data

Impact on the data controller

- Data controller is a public authority so liability to pay a monetary penalty does not fall on an individual
- 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

- There has been no similar security breach as far as the Commissioner is aware
- Data controller identified the information security risk posed by bypassing or disabling the PDS function

Effect of the contravention

- Data subject's [redacted] was informed about the security breach
- Both letters may have been disclosed to unintended recipient during any court proceedings

Behavioural issues

- Voluntarily reported to Commissioner's office
- Detailed investigation report compiled
- Remedial action 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 Fourth Data Protection Principle at Part I of Schedule 1 to the Act was also contravened by the data controller in that inaccurate personal data was held on its database
- The Commissioner's underlying objective in imposing a monetary penalty notice is to promote compliance with the Act. This is an opportunity to reinforce the need for data controllers to review the handling of confidential and sensitive personal data and to ensure that appropriate and effective security measures are applied

Notice of Intent

A notice of intent was served on the data controller dated 15 March 2012. The Commissioner received written representations from the data controller in a letter dated 20 April 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 serious and that the imposition of a monetary penalty is appropriate. Further that a monetary penalty in the sum of £60,000 (Sixty 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 2 August 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 1 August 2012 the Commissioner will reduce the monetary penalty

by 20% to £48,000 (Forty eight 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 1 August 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 2nd day of July 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 1 August 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)).