Data Protection Act 1998

Monetary Penalty Notice

Dated: 24 April 2012

Name: Aneurin Bevan Health Board

Address: Block C, top floor, Mamhilad House, Mamhilad Park Estate, Pontypool, NP4 OYP

Statutory framework

---

1. Aneurin Bevan Health Board 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 Aneurin Bevan Health Board 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the "1984 Act").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

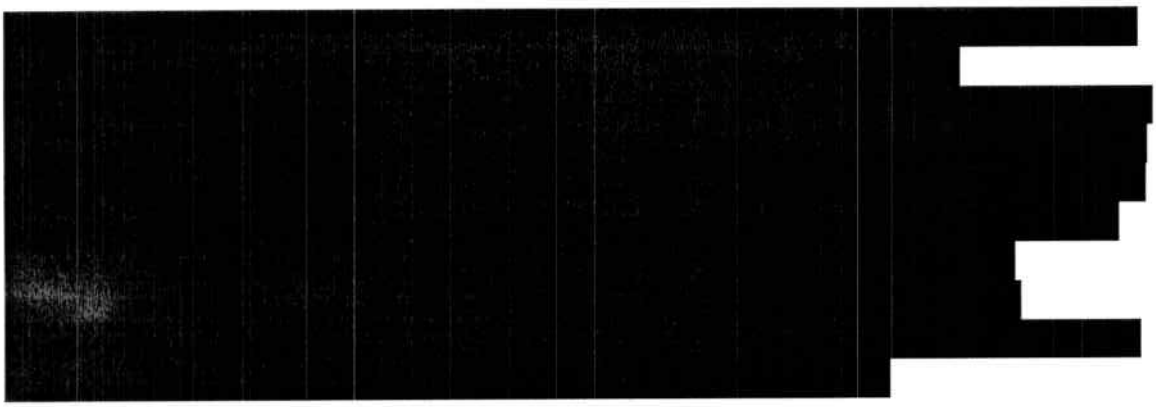
(b) failed to take reasonable steps to prevent the contravention.

Background

4. On 24 March 2011, a secretary in the [redacted] Team (the "Team") sent a letter intended for one patient, to a former patient who had an almost identical surname. Normally, the consultant [redacted] in the Team would draft [redacted] own letters and email them to the secretary for formatting, printing and posting. On this occasion, [redacted] emailed a letter to the secretary containing two different spellings of the patient's surname. Further, it did not identify the patient by way of [redacted] address or a unique identifier such as the patient's hospital number or NHS number. The

consultant [redacted] later emailed an amendment to the letter but again without any proper identifiers.

5. The secretary was used to working in this way and simply relied on the electronic patient record system (the "system") to provide [redacted] details of the patient. [redacted] line manager permitted this method of work so that an effective secretarial service could be provided across multiple sites. But given the lack of further identifiers in the letter the secretary chose the wrong patient in the system. The letter contained confidential and highly sensitive personal data including a report (the "report") from the consultant [redacted] detailing [redacted] contacts with the patient over a period of approximately 5 to 6 months.

6. 

7. An investigation into the security breach revealed an absence of robust systems to ensure the identity of service users and recommended changes to the Team and the whole Division's processes, such as not despatching correspondence unless the patient name is accompanied by at least one unique identifier (hospital number or NHS number), introducing procedures to implement this change and reminding clinical staff (including consultants) that they are responsible for ensuring that the patient's identity is clearly communicated to secretaries dealing with such correspondence. The Commissioner understands that in the interim an email has been sent to the professional heads in the Division reminding them to check that patient details such as their date of birth and address are correct before sending out such correspondence.

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 that there has been a breach of the data controller's duty to comply with the Seventh Data Protection Principle in relation to all personal data with respect to which it is the data controller.

  In particular, the data controller had failed to take appropriate organisational measures against unauthorised processing of personal data such as having appropriate policies, procedures and training for staff working in the Team to ensure that letters containing confidential and sensitive personal data are not despatched unless the patient's name has been carefully checked against at least one unique identifier (hospital number or NHS number). 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. Confidential and sensitive personal data was disclosed to an unauthorised third party 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 a data subject 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 subject would suffer substantial distress knowing that their confidential and sensitive personal data has been disclosed to a third party and that their data may have been

further disseminated and possibly misused, 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 the data controller would have been aware of the confidential and sensitive nature of the personal data that staff in the Team dealt with on a daily basis.

  In addition, the secretary involved in this security breach was used to working in this way and simply relying on the electronic patient record system to provide her with details of the patient. Her line manager permitted this system of work so that a secretarial service could be provided across multiple sites.

  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 having appropriate policies, procedures and training for staff working in the Team so that letters containing confidential and sensitive personal data are not despatched unless the patient's name has been carefully checked against at least one unique identifier (hospital number or NHS number).

  Further, it should have been obvious to the data controller 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

- Confidential and highly sensitive personal data was disclosed to an unauthorised third party
- Contravention was serious because of the confidential and highly sensitive nature of the personal data

Effect of the contravention

- The contravention was of a kind likely to cause substantial distress to the data subject
- Unintended recipient admitted she had read the letter

Behavioural issues

- Failed to provide the Commissioner's office with timely responses to its enquiries
- Contravention was due to the negligent behaviour of the data controller in failing to take appropriate 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

- This was a "one off" incident as far as the Commissioner is aware

Effect of the contravention

- Data subject was informed and offered appropriate support

Behavioural issues

- Voluntarily reported to Commissioner's office
- Detailed investigation report compiled
- Generally co-operative with the Commissioner's office
- Remedial action has now been taken

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. This is an opportunity to reinforce the need for data controllers in the NHS to review the handling of confidential and sensitive personal data by Consultants and clinical staff 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 31 January 2012. The Commissioner received representations from the data controller in a letter from the Chief Executive dated 28 February 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 £70,000 (Seventy 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 24 May 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 23 May 2012 the Commissioner will reduce the monetary penalty by 20% to £56,000 (fifty six 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 23 May 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 24th day of April 2012

Signed: .....

David Smith
Deputy Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5A

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 23 May 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)).