DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

MONETARY PENALTY NOTICE

To: Bloomsbury Patient Network

Of: Mortimer Market, Off Tottenham Court Road, London, WC1E 6JB

1. The Information Commissioner ("Commissioner") has decided to issue Bloomsbury Patient Network ("BPN") with a monetary penalty under section 55A of the Data Protection Act 1998 ("DPA"). The penalty is being issued because of a serious contravention of the Seventh Data Protection Principle by BPN.

2. This notice explains the Commissioner's decision.

Legal framework

3. BPN is a data controller, as defined in section 1(1) of the DPA in respect of the processing of personal data. Section 4(4) of the DPA provides that, subject to section 27(1) of the DPA, 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.

4. The relevant provision of the DPA is the seventh data protection principle which provides, at Part I of Schedule 1 to the DPA, 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".

5. Paragraph 9 at Part II of Schedule 1 to the DPA 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".

6. Under section 55A (1) of the DPA 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 DPA 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.

7. The Commissioner has issued statutory guidance under section 55C (1) of the DPA about the issuing of monetary penalties that has been published on the ICO's website. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 prescribe that the amount of any penalty determined by the Commissioner must not exceed £500,000.

8. The DPA implements European legislation (Directive 95/46/EC) aimed at the protection of the individual's fundamental right to the protection of personal data. The Commissioner approaches the data protection principles so as to give effect to the Directive.

Background to the case

9. BPN is based in the Bloomsbury Clinic which is a specialist HIV treatment centre. BPN (an unincorporated association) was established in 2003 to provide a support network for patients who have been diagnosed as HIV positive.

10. BPN's website states that it offers "advice and support on all issues around living well with HIV, such as physical health and wellbeing, new diagnosis, counselling, dealing with the fears of stigma and discrimination, starting a family, legal referrals and finding GPs and dentists".

11. BPN is run by three Patient Representatives. They regularly send newsletters via e-mail to service users informing them of upcoming events, such as workshops or conferences.

12. On or about 17 February 2014, a Patient Representative sent an e-mail to between 60 and 200 service users on BPN's distribution list who all had HIV. The e-mail addresses were entered into the "to" field instead of the blind carbon copy ("bcc") field. The recipients of the e-mail could therefore see the e-mail addresses of all the other recipients.

13. The Patient Representative agreed to be more careful when sending future e-mails. However, there was no formal guidance or training to remind the Patient Representative to double check that the group e-mail addresses were entered into the correct field.

14. Further, BPN did not replace the e-mail account it was using with an account that could send a separate e-mail to each service user on the distribution list.

15. On 6 May 2014, the same Patient Representative sent an e-mail to 200 service users on BPN's distribution list. The group e-mail addresses were again entered into the "to" field in error.

16. The Commissioner understands that 56 out of the 200 group e-mail addresses contained the full or partial names of service users.

17. The Commissioner has made the above findings of fact on the balance of probabilities.

18. The Commissioner has considered whether those facts constitute a contravention of the DPA by BPN and, if so, whether the conditions of section 55A DPA are satisfied.

The contravention

19. The Commissioner finds that BPN contravened the following provisions of the DPA:

20. BPN failed to take appropriate technical and organisational measures against unauthorised processing of personal data in contravention of the Seventh Data Protection Principle at Part I of Schedule 1 to the DPA.

21. The Commissioner finds that the contravention was as follows:

- BPN failed to use an account that could send a separate e-mail to each service user.
- BPN failed to provide the Patient Representatives with any guidance or training on the importance of double checking that the group e-mail addresses were entered into the "bcc" field.

This was an ongoing contravention until BPN took remedial action following the second security breach on 6 May 2014.

22. The Commissioner is satisfied that BPN was responsible for this contravention.

23. The Commissioner has gone on to consider whether the conditions under section 55A DPA were met.

Seriousness of the contravention

24. The Commissioner is satisfied that the contravention identified above was serious. 56 of the 200 e-mail addresses contained the full or partial names of service users with HIV. The recipients of the e-mails could infer the HIV status of many of the other recipients. This is confidential and sensitive personal data.

25. In the circumstances, the Commissioner considers that the contravention was serious having regard to the number of affected individuals and the nature of the confidential and sensitive personal data involved.

26. The Commissioner is therefore satisfied that condition (a) from section 55A (1) DPA is met.

Contraventions of a kind likely to cause substantial damage or substantial distress

27. The relevant features of the kind of contravention are:

28. A Patient Representative sent an e-mail to between 60 and 200 service users on two separate occasions. The recipients of the e-mails could infer the HIV status of many of the other recipients. BPN serves a small geographical area, increasing the possibility that the affected individuals knew one another. E-mail addresses can also be searched via social networks and search engines.

29. The Commissioner considers that the contravention identified above had the following potential consequences:

30. The contravention would cause distress to the service users who know that their names have been disclosed to unauthorised recipients who could infer their HIV status. BPN serves a small geographical area, increasing the possibility that the affected individuals knew one another. E-mail addresses can also be searched via social networks and search engines. It would therefore be possible for the unauthorised recipients to identify the affected individuals.

31. Further, the service users would be distressed by justifiable concerns that their data has been further disseminated even if those concerns do not actually materialise. In the circumstances, the distress suffered by the service users is considered to extend beyond mere irritation.

32. In this context it is important to bear in mind that the service users were suffering from a potentially life threatening condition that can still carry a stigma.

33. If this information has been misused by those who had access to it, or if it was in fact disclosed to untrustworthy third parties, then the contravention would cause further distress to the service users.

34. The Commissioner considers that the distress described above was likely to arise as a consequence of the kind of contravention. In other words, the Commissioner's view is that there was a significant and weighty chance that a contravention of the kind described would have such consequences.

35. The Commissioner also considers that such distress was likely to be substantial, having regard to the number of affected individuals and the confidential and sensitive nature of the personal data involved. In the circumstances, the likely distress was certainly more than trivial.

36. The Commissioner has also given weight to the number of affected individuals. The Commissioner considers that even if the distress likely to have been suffered by each affected individual was less than substantial, the cumulative impact would clearly pass the threshold of "substantial". In addition, given the number of affected individuals, it was inherently likely that at least a small proportion of those individuals would have been likely to suffer substantial distress on account of their particular circumstances. For example, a service user is extremely worried that he will suffer from discrimination at work.

37. The Commissioner is therefore satisfied that condition (b) from section 55A (1) DPA is met.

Deliberate or negligent contraventions

38. The Commissioner has considered whether the contravention identified above was deliberate. In the Commissioner's view, this means that BPN's actions which constituted the contravention were deliberate actions (even if BPN did not actually intend thereby to contravene the DPA).

39. The Commissioner considers that in this case the BPN did not deliberately contravene the DPA in that sense.

40. The Commissioner has gone on to consider whether the contraventions identified above were negligent. First, he has considered whether BPN knew or ought reasonably to have known that there was a risk that this contravention would occur. He is satisfied that this condition is met, given that the Patient Representatives sent regular emails to the 200 service users on BPN's e-mail distribution list. Therefore, BPN must have been aware that there was a risk that a Patient Representative could enter the group e-mail addresses into the wrong field, particularly after the first security breach.

41. In the circumstances, BPN ought reasonably to have known that the group e-mail addresses would be vulnerable to a security breach in the absence of appropriate technical and organisational measures.

42. Second, the Commissioner has considered whether BPN knew or ought reasonably to have known that those contraventions would be of a kind likely to cause substantial distress. He is satisfied that this condition is met, given that BPN was aware that 56 of the 200 group e-mail addresses contained the full or partial names of service users who had HIV. The recipients of the e-mails could therefore infer the HIV status of many of the other recipients. This is confidential and sensitive personal data. Therefore, it should have been obvious to BPN (a network that offers advice and support to service users with HIV) that such a contravention would be of a kind likely to cause substantial distress to the affected individuals.

43. Third, the Commissioner has considered whether BPN failed to take reasonable steps to prevent the contravention. Again, he is satisfied

that this condition is met. Reasonable steps in these circumstances would have included using an e-mail account that could send a separate e-mail to each service user or providing the Patient Representatives with guidance or training on the importance of double checking that the group e-mail addresses were entered into the "bcc" field. BPN failed to take any of those steps.

44. The Commissioner is therefore satisfied that condition (c) from section 55A (1) DPA is met.

The Commissioner's decision to issue a monetary penalty

45. For the reasons explained above, the Commissioner is satisfied that the conditions from section 55A(1) DPA have been met in this case. He is also satisfied that section 55A(3A) and the procedural rights under section 55B have been complied with.

46. The latter has included the issuing of a Notice of Intent dated 3 November 2015, in which the Commissioner set out his preliminary thinking. BPN has not made any written representations in response to that Notice.

47. The Commissioner is accordingly entitled to issue a monetary penalty in this case.

48. The Commissioner has considered whether, in the circumstances, he should exercise his discretion so as to issue a monetary penalty. He has taken into account BPN's representations made in other correspondence on this matter.

49. The Commissioner has also considered whether the contravention identified above could be characterised as one-off events or attributable to mere human error. He does not consider that the contravention could be characterised in those ways.

50. The Commissioner has decided that it is appropriate to issue a monetary penalty in this case, in light of the nature and seriousness of the contravention, BPN's shortcomings in terms of its DPA duties and the risks posed to a number of individuals. He has also considered the importance of monetary penalties in dissuading future contraventions of the DPA and encouraging compliance, in accordance with his policy.

51. For these reasons, the Commissioner has decided to issue a monetary penalty in this case.

The amount of the penalty

52. The Commissioner has taken into account the following **mitigating features** of this case:

- BPN has been fully co-operative with the ICO.
- BPN apologised to the affected individuals.
- BPN has now taken substantial remedial action.
- There will be a significant impact on BPN's reputation as a result of this security breach.

53. The Commissioner has also taken into account the following **aggravating features** of this case:

- BPN received 5 complaints from the affected individuals.
- BPN did not ask the unauthorised recipients to delete the e-mails.

54. The Commissioner has considered the likely impact of a monetary penalty on BPN. He has decided that BPN has access to sufficient financial resources to pay the proposed monetary penalty without causing undue financial hardship.

55. Taking into account all of the above, the Commissioner has decided that the appropriate amount of the penalty is **£250 (Two hundred and fifty pounds).**

Conclusion

56. The monetary penalty must be paid to the Commissioner's office by BACS transfer or cheque by **13 January 2016** 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.

57. If the Commissioner receives full payment of the monetary penalty by **12 January 2016** the Commissioner will reduce the monetary penalty by 20% to **£200 (Two hundred pounds).** However, you should be aware that the early payment discount is not available if you decide to exercise your right of appeal.

58. There is a right of appeal to the First-tier Tribunal (Information Rights) against:

a) the imposition of the monetary penalty and/or;

b) the amount of the penalty specified in the monetary penalty notice.

59. Any notice of appeal should be received by the Tribunal within 28 days of the date of this monetary penalty notice.

60. Information about appeals is set out in Annex 1.

61. The Commissioner will not take action to enforce a monetary penalty unless:

- the period specified within 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 appealing against the monetary penalty and any variation of it has expired.

62. 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 of any sheriffdom in Scotland.

Dated the 11th day of December 2015

Signed ……..

Stephen Eckersley
Head of Enforcement
Information Commissioner's Office
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 sent so it is received by the Tribunal within 28 days of the date of the notice.

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)).