

DATA PROTECTION ACT 1998

SUPERVISORY POWERS OF THE INFORMATION COMMISSIONER

ENFORCEMENT NOTICE

DATED: 27 FEBRUARY 2015

To: North Tees and Hartlepool NHS Foundation Trust

of: University Hospital of Hartlepool, Holdforth Road, Hartlepool, TS24 9AH

1. North Tees and Hartlepool NHS Foundation 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 by North Tees and Hartlepool NHS Foundation Trust and is referred to in this notice as 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 The Act came into force on 1 March 2000 and repealed the Data Protection Act 1984 (the '1984 Act').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. In the course of 2014 and early 2015, the Commissioner was informed of a number of separate incidents involving the loss or unauthorised disclosure of personal data, mainly contained in paper documents. One incident involved the discovery of a folder containing highly sensitive personal data at a bus stop by a member of the public, while most of the other cases related to letters, notes and reports containing patient data being sent to the wrong recipients.
4. Investigations carried out by the Commissioner revealed that at least one internal department had been knowingly breaching the data controller's 'Data Protection and Caldicott Policy' on an ongoing basis as they found the rules around secure transportation of documents impractical for the daily tasks they were required to carry out. This indicates that the data controller's policy may not have been fit for purpose for all Trust departments. In addition, the transportation solutions required by the policy may not have been sufficient to

prevent the loss or unauthorised disclosure of personal data, even if followed. The Commissioner's enquiries also highlighted the fact that several of the document addressing errors occurred due to the overtyping of previous patient letters.

5. The Commissioner has previously issued the controller with recommendations around the removal of paper documents from the office, and accuracy of correspondence addresses. Addressing issues and the rules around overtyping of letters were two of the points included in an action plan subsequently produced by the controller in light of earlier breaches. However, the current incidents would indicate that to date, some of the implemented actions have been ineffective. In cases where the controller has ultimately located lost or misdirected documents, the security and appropriateness of retrieval solutions has also raised concerns.
6. The Commissioner has considered the data controller's compliance with the provisions of the Act in light of these matters.
7. 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 with respect to which he is the data controller. The relevant provision of the Act is the Seventh Data Protection Principle.
8. The Seventh Data Protection Principle 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 of 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."*

9. Having considered the information provided by the data controller in response to his investigations, the Commissioner is satisfied that the data controller has contravened the Seventh Data Protection Principle in that it failed to take appropriate measures to ensure the security of personal data.
10. The Commissioner considered, as he is required to do under section 40(2) of the Act when deciding whether to serve an Enforcement Notice, whether any contravention has caused or is likely to cause any person damage or distress. The Commissioner took the view that the likelihood of distress is self-evident. The individuals whose personal data was put at risk of unauthorised access and further dissemination would be likely to have suffered worry and anxiety on account of the risk that their data would come into the possession of unauthorised individuals. While there is no evidence that damage has been caused there was a significant risk that it could have been.
11. The Commissioner has further taken account of the effect of the incorporation in English law of the European Convention on Human Rights ('ECHR'), by virtue of the Human Rights Act 1998, in deciding whether or not to serve an Enforcement Notice. In particular, the Commissioner is mindful of the provisions of Article 8 of the ECHR in that both the individuals whose personal data was in the documents found by members of the public and hospital staff have the right to respect for private and family life, home and correspondence.

In view of the matters referred to above the Commissioner hereby gives notice that, in exercise of his powers under section 40 of the Act, he requires that North Tees and Hartlepool NHS Foundation Trust shall within 3 months of the date of this Notice:

- (1) Review its 'Data Protection and Caldicott Policy' to reflect the specific needs and practicalities associated with each internal department. The review should involve a requirement to redact or minimise the personal data contained in correspondence removed from the office wherever possible, and to use secure electronic solutions for document storage and transmission when available;
- (2) Put an action plan in place and carry out comprehensive quality assurance and spot checks to ensure all departments are complying with policies relating to the protection of personal data on an ongoing basis including the 'Data Protection and Caldicott Policy', the 'Clinical Administration Standard Operating Procedure', the

'Information Security Policy' and the 'Information Governance and Caldicott Policy'.

- (3) As part of this action plan, implement additional technical or organisational measures to ensure that the 'Clinical Administration Standard Operating Procedure' is being strictly adhered to by all staff dealing with patient correspondence, particularly with regard to the checking of addresses and non-overtyping of letters; and
 - (4) Establish a data breach management policy to deal specifically with containment and recovery solutions, including requirements around the secure retrieval of recovered information.
12. There is a right of appeal against this Notice to the First-tier Tribunal (Information Rights), part of the General Regulatory Chamber. Information about appeals is set out in the attached Annex 1.

Dated the 27th day of February 2014

Signed:
David Smith
Deputy Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

ANNEX 1

RIGHTS OF APPEAL AGAINST DECISIONS OF THE COMMISSIONER

1. Section 48 of the Data Protection Act 1998 gives any person upon whom an enforcement 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
Leicester
LE1 8DJ

Tel: 0300 1234504
Fax: 0870 739 5836
Email: GRC@hmcts.gsi.gov.uk
Website: www.justice.gov.uk/tribunals/general-regulatory-chamber

The notice of appeal should be served on the Tribunal within 28 days of the date on which the enforcement notice was sent.

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))

