



Data Protection Act 1998: Civil Monetary Penalties and NHS bodies

A briefing from our Information Governance team - July 2012

Data Protection Act 1998

Civil Monetary Penalties and NHS bodies

The power to impose Civil Monetary Penalties (CMPs) for serious data protection breaches was first introduced in April 2010. Until April 2012 the primary recipients of CMPs were local authorities and no NHS body had been served with a penalty notice. Since April 2012 however four NHS bodies have been served with penalty notices imposing fines totalling £710,000.

The high level of fines imposed on NHS bodies reflects the very high degree of sensitivity of records held by the NHS and the correspondingly high expectations of patients in relation to the secure handling of these records. Details of the circumstances giving rise to the imposition of these CMPs highlight the importance for NHS bodies of keeping their data security and data handling arrangements under continuing review in order to minimise the likelihood of serious data protection breaches and significant financial penalties.

Aneurin Bevan Health Board

Aneurin Bevan Health Board was fined £70,000 in April 2012 after a letter intended for one patient was sent in error to a patient with an almost identical surname. The secretary responsible for issuing the letter had been sent a draft letter from the patient's clinician by email. The email contained two different spellings of the patient's name and no unique patient identifier. Significantly, there was an absence of robust systems within the Health Board to verify patient identity and the secretary was used to working in this way. She used the patient's name to obtain an address for correspondence from the Health Board's patient record system but selected the incorrect patient details because of the variable spelling of the patient's name and the absence of any unique identifier. The consequence was that confidential and highly sensitive personal data relating to a patient was disclosed to an unauthorised third party; the sensitive nature of this

information was such that the Health Board ought to have significantly more robust arrangements in place for verifying patient identity for the purpose of correspondence.

The Monetary Penalty Notice published by the ICO following this breach noted that this incident afforded an opportunity for the Commissioner "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"

Central London Community Healthcare NHS Trust

Also in April 2012, the Central London Community Healthcare NHS Trust received a CMP for £90,000 following administrative errors which resulted in inpatient lists being faxed to an unintended recipient. A total of 45 fax transmissions, intended for a local Hospice were misdirected to a fax machine belonging to a member of the public. These lists contained confidential sensitive personal data relating to 59 individuals many of whom were receiving palliative care. Although a fax protocol was in use by the Trust in relation to its communications with the Hospice, the protocol became ineffective when a second fax number came into use in the absence of any update to the protocol. In imposing the CMP the ICO paid particular regard to the sensitivity of the information concerned and the lack of staff training in relation to the use of the fax protocol.

Brighton and Sussex University Hospitals NHS Foundation Trust

In May 2012, Brighton and Sussex University Hospitals NHS Foundation Trust was served with a CMP for £325,000, the highest financial penalty imposed by the ICO to date, as a result of failings relating to the disposal of computer hard drives containing information originating from a database in the HIV and Genito Urinary Medicine Department. As a result of failure properly to supervise arrangements made on behalf of the Trust for the decommissioning of these computer

hard drives, some 250 hard drives containing highly sensitive personal data of tens of thousands of patients and staff were sold on an internet auction site. The data included names, dates of birth, patient medical conditions and treatment, patient referral letters, X-rays, disability living allowance forms and children's reports. Insofar as staff data was concerned, the data included staff national insurance and payroll numbers, home addresses and CRB records.

Arrangements for disposal of some 1000 hard drives were made on behalf of the Trust by Sussex Health Informatics Services (HIS) although the service level agreement between the Trust and HIS had expired. HIS engaged a contractor to carry out the decommissioning work but carried out only very basic checks in relation to the contractor's credentials. In addition, HIS did not enter into a written contract with the contractor and did not inform the Trust that the contractor had been engaged. A subsequent police investigation established that the contractor had personally auctioned a percentage of the Trust's hard drives on an online site.

The absence of a written contract between the Trust and HIS was a key factor in the ICO's decision to impose a financial penalty on the Trust. The Commissioner noted, in particular, the obligation imposed on all data controllers by the seventh data protection principle when engaging contractors to process personal data, to enter into a written contract requiring the contractor to act only on the instructions of the data controllers and requiring the contractor to have in place appropriate technical and organisation measures in relation to data security. The Commissioner took the view that such a contract ought to have included specific provisions in relation to the appointment of subcontractors by HIS and that the failure in this case to have in place effective contractual controls resulted in the failure to ensure a level of security that was appropriate to the harm that would inevitably result from the loss of the hard drives.

Belfast Health and Social Care Trust

The Trust was served with a CMP for £225,000 in June 2012 after trespassers gained access to a 26 acre disused hospital site where patient records were stored in one of 50 disused buildings. On several occasions the trespassers took photographs of the records and then posted them on the internet. The Trust had become responsible for the site following amalgamation of six acute and community Trusts but had not carried out any site inspection when it took over responsibility for the site. Although the site was patrolled by security guards and although CCTV cameras were in use, the ICO found that the failure to carry out site inspection and conduct an inventory of records stored at the site, and failure to ensure an appropriate level of security was in place pending decommissioning of the site amounted to a serious contravention of the Trust's

obligations under the Data Protection Act of a kind likely to cause substantial distress.

More information

To discuss your individual requirements, please contact:



Heledd Lloyd-Jones, Senior Associate
T: 029 2038 5914
E: heledd.lloyd-jones@morgan-cole.com

This publication is © Morgan Cole and may not be reproduced without our express permission. Recipients may forward this publication and view, print and download the contents for personal use only. The contents must not be used for any commercial purposes and the material in this publication or any part of it is not to be incorporated or distributed in any work or in any publication in any form without the prior written consent of Morgan Cole.

Professional advice should always be sought where you require assistance in specific areas of the law. No responsibility can be accepted for any action based on these articles.