

News release

20 April 2011

Lax IT security measures led to NHS data breach in Birmingham

NHS Birmingham East and North breached the Data Protection Act by failing to restrict access to files on their IT network, the Information Commissioner's Office (ICO) announced today. The breach led to some NHS staff at their own Trust and two other NHS Trusts nearby potentially being able to access restricted information.

NHS Birmingham East and North reported the breach to the ICO in September last year after discovering that electronic files, stored on a shared network, were potentially accessible to their own employees and the employees of two other local Trusts. The files contained information relating to thousands of individuals, including members of staff. Although health records were not compromised as part of the breach, the files also contained some high level information relating to patients.

The ICO's investigation has found that, while most of the files were not easily accessible and some security restrictions were in place, file security in general was inadequate.

Acting Head of Enforcement, Sally-Anne Poole said:

"It's vitally important that IT networks storing personal information have robust security measures in place. Whilst nobody outside of the Trust environment was able to access the files, problems with the security of the network still led to a situation where sensitive information was

potentially available to NHS staff that did not need it to carry out their daily role.

“We are pleased that NHS Birmingham East and North has agreed to improve the security of its network as well as reviewing the processes it follows when handling personal data.”

Denise McLellan, Chief Executive of NHS Birmingham East and North, has signed an undertaking to ensure that adequate technical security measures are in place to prevent unauthorised access to personal data. The Trust will also make sure that comprehensive policies are established regarding the storage and usage of personal data and that staff receive the necessary training on how to follow them.

A full copy of the undertaking can be viewed here:

http://www.ico.gov.uk/what_we_cover/promoting_data_privacy/taking_action.aspx#undertakings

ENDS

If you need more information, please contact the ICO press office on 0303 123 9070 or visit the website at: www.ico.gov.uk.

Notes to Editors

1. The Information Commissioner’s Office upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.
2. The ICO has specific responsibilities set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.
3. The ICO is on [Twitter](#), [Facebook](#) and [LinkedIn](#), and produces a monthly [e-newsletter](#). Our [For the media](#) page provides more information for journalists.
4. Anyone who processes personal information must comply with eight principles of the

Data Protection Act, which make sure that personal information is:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate and up to date
- Not kept for longer than is necessary
- Processed in line with your rights
- Secure
- Not transferred to other countries without adequate protection