

Data Protection Act 1998 Undertaking follow-up

Northern Health and Social Care Trust

ICO Reference: ENF0460222

In December 2013 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Northern Health and Social Care Trust (the Trust) in relation to the undertaking it signed on 7 August 2013.

The objective of the follow-up is to provide the ICO with a level of assurance that the agreed undertaking requirements have been appropriately implemented. We believe that appropriate implementation of the undertaking requirements will mitigate the identified risks and support compliance with the Data Protection Act 1998.

The follow-up assessment consisted of a desk based review of the documentary evidence the Trust supplied to demonstrate the action it had taken in respect of the undertaking requirements. This included

- A completed Undertaking Follow-up Schedule, detailing the steps taken to meet the requirements of the undertaking
- Security policy
- Information Governance Training – Monitoring Update Report as at 30/11/2013
- Incident Management Policy and Procedure (including Procedure for Serious Adverse Incidents)

The review demonstrated that the Trust has taken appropriate steps and put plans in place to address some of the requirements of the undertaking, however further work needs to be completed by the Trust to fully address the agreed actions.

In particular the Trust confirmed that it has taken the following steps:

Sixteen additional training sessions on the Trust's Processing of Personal Information (POPI) Policy and Procedures have been organised. These have been targeted at level 5 and 6 Trust managers on the basis that they deliver instruction and best practice within their business areas. Eleven sessions have already been delivered and the remaining 5 are fully booked.

The need to deliver mandatory Information Governance (IG) Awareness to all staff has been met via 20 IG Awareness sessions delivering face to face training. This is in addition to the e-learning programme which all staff with access to a PC can avail of.

Evidence was provided that all laptop and portable computers are encrypted using encryption tools that meet or exceed current standards. The Trust explained that it is currently using two encryption tools, MS Bitlocker and Wave. However it was proposing to move to one unified tool, Sophos Safeguard.

End point security has also been implemented on all PCs and laptops which prevents unencrypted USB media from being used on these devices.

Trust Information Asset Owners (IAOs) have agreed a supplementary procedure for the reporting of IG incidents. This has been incorporated into the Trust's Risk Management Incident Reporting Procedures (Incident Management Policy and Procedure - NHSCT/09/127) and has been formally issued via the Trust's Policy Framework.

However the Trust should take further steps to address the agreed actions:

- Ensure that IAO's provide assurance to the SIRO that local departmental procedures for the storage and use of personal data are in place where required.
- Review and update corporate induction materials in relation to IG.
- Review physical security measures where sensitive and/or personal information is stored. The SIRO will be seeking assurance from Directorates on this issue in January 2014.
- Finalise POPI Policy in terms of strengthening guidance regarding physical security of information and obtain input regarding this from the Trust IG Forum.

Date Issued: 8 January 2014

The matters arising in this report are only those that came to our attention during the course of the follow up and are not necessarily a comprehensive statement of all the areas requiring improvement.

The responsibility for ensuring that there are adequate risk management, governance and internal control arrangements in place rests with the management of Northern Health and Social Care Trust.

We take all reasonable care to ensure that our Undertaking follow up report is fair and accurate but cannot accept any liability to any person or organisation, including any third party, for any loss or damage suffered or costs incurred by it arising out of, or in connection with, the use of this report, however such loss or damage is caused. We cannot accept liability for loss occasioned to any person or organisation, including any third party, acting or refraining from acting as a result of any information contained in this report.