Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

**Data Protection Act 1998**
**Undertaking follow-up**

**Northern HSC Trust**
**ICO Reference: COM0587506**

In March 2017 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Northern HSC Trust in relation to the undertaking it signed in July 2016.

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 Northern HSC Trust supplied to demonstrate the action it had taken in respect of the undertaking requirements. As part of the documentation provided by Northern HSC Trust, an Undertaking Follow up schedule was submitted which outlined changes that had taken place within the business.

In response to the review, Northern HSC Trust also sent through documents and evidence including:

- Induction Checklist
- Training material
- Compliance reports/emails
- KPI reports
- Staff IG Screensavers
- Incident reporting that appears on Staffnet
- Emails sent to staff in regards to Incident reporting
- IG Improvement plans
- Data protection contract clauses

Northern HSC Trust has taken some steps to meet the requirements of the undertaking; however there are still some areas of concern which need addressing to mitigate the highlighted risks.

In summary, they confirmed that they have taken the following steps:

**(1) The data controller must ensure that all staff, including locum doctors, 3rd Party contractors, temporary (agency /bank staff) and volunteers, whose role involves the routine processing of personal and sensitive personal data undertakes mandatory data protection and data handling induction training and regular refresher training on the requirements of the Act.**

From the evidence provided all staff at the Trust are required to do IG awareness training during their induction. This training will then be refreshed every 3 years. The most recent compliance report that has been provided, states that 84% of staff have completed the IG Training and 84% of managers have completed the POPI training in December 2016. Although this is an improvement, the Trust still needs to ensure that all staff are completing the IG training within the given time. It has been reported that the IG Training booklet and package for locum doctors and agency staff is still under review. Due to the fact that this has yet to be implemented, there is still a risk that IG incidents will occur due to the lack of training. However the Trust has provided evidence showing that the contractual terms with external domiciliary care providers have been revised. This will reassure the trust the relevant IG training will be given to these contractual staff.

**(2) Provision of such training shall be recorded and monitored with oversight provided at a senior level against agreed Key Performance Indicators to ensure completion. In addition, the data controller shall implement follow-up procedures to ensure that staff who have not attended/completed training do so as soon as is practicable.**

Evidence has been provided by the Trust showing that IG Training KPI and monitoring reports are being produced. These reports should be produced every quarter; we have received evidence of the September report but nothing from this year. It has been reported that these reports are provided to all the directorates, the Trust Board and the Corporate Governance Steering Group. However no evidence has been provided to show that this information is being reported to the Trusts Board. The said reports are also used by management to monitor staff members that have not completed the training in given timeframe. Again there is no evidence showing this. There are also no processes in place to show what the

consequences are if staff members repeatedly fail to complete the IG training.

**(3) The data controller shall ensure that staff, including Locum doctors, 3rd party contractors, temporary (agency/bank staff) and volunteers are aware of the content and location of its policies and procedures relating to the processing of personal data, specifically the procedure for reporting and recording IG breaches. If not already in place, a mechanism to ensure that staff are updated of any changes to these policies and procedures should also be implemented.**

Evidence has been provided showing that policies are kept on the Trusts staffnet website. During the staffs departmental induction they are informed of where the Policies are and which ones are specifically relevant to them. If there are any changes to policies or there are new policies implemented, staff are made aware of this via email and the staff newsletter. Managers will also mention any updates in team meetings, to inform staff who have not got access to email. However we have not been provided any evidence of this.

It has been reported that the Trust fully implemented Datix web in November 2016. Evidence has been provided showing the training and information has been given to all staff about this system and incident reporting in general. However it has been reported that the Incident management policy has yet to be updated with the new process for reporting incidents. The updating of this policy should be completed as soon as possible to ensure staff have guidance on what to do if an IG incident occurs.

**(4) The data controller shall implement such other security measures as are appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and or damage.**

The Trust created an IG improvement plan after the undertaking was issued. This plan has identified key risks that the Trust needs to look into; one of which was risk management. It was reported that an element of this risk has been addressed by ensuring risk assessments are completed and reviewed for all of the Trusts information assets. However the Trust has not provided evidence to confirm this new procedure. The Trust has also stated that they are now ISO27001 compliant, which should help with the implementation of measures to ensure the security of the personal data they process. However there has been no ISO27001 certificate or other evidence provided showing this. There are also regular

reviews of IG incidents at the Trusts IG Forum. If any trends occur from incidents lessons learnt can be discussed in this arena.

Date Issued: 3rd April 2017.

*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 rest with the management of Northern HSC 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.*