

Data Protection Act 1998 Undertaking follow-up

Pennine Care NHS Foundation Trust ICO Reference: COM0579293 & COM0641364

In the week beginning 15 January 2018 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Pennine Care NHS Foundation Trust (the Trust) in relation to the Undertaking it signed on 1 February 2017.

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:

- An Internal Audit report of the actions taken by the Trust in respect of the Undertaking.
- The Incident Reporting Management and Investigation Policy.
- The Information Governance Serious Incident Requiring Investigation Process and Procedure document.
- An updated Action Plan from the consensual audit undertaken by the ICO at Trust premises in February 2017.
- Screenshots from the new NHS Data Security and Awareness training.
- Recent induction training materials.

The review demonstrated that the Trust has taken appropriate steps and put plans in place to address the requirements of the Undertaking.

In particular the Trust confirmed that it has taken the following steps in relation to the various requirements in the Undertaking:

1. Procedures are put in place to ensure any reported breach of security relating to personal data is acted upon promptly and any containment and remedial measures are swiftly enforced. The Incident Reporting Policy should include provisions to train staff around reporting to timescales and to provide the most pertinent information to assist an investigation, internal categorisation and prompt remedial measures.

- The internal auditors have seen a revised Incident Reporting Policy which includes management, staff training and investigation. We understand that the Trust is currently in the process of a major revision of its incident investigation process.
- Incident reporting training has been undertaken.
- Information regarding risks and incidents has been communicated to staff.

2. The data controller shall ensure all processes within the CAMHS service are standardised across all teams and staff duties between administration staff and clinicians are clearly defined.

- Standardisation of processes and differentiation between administrative and clinical staff has been undertaken within the CAMHS service. This was evidenced by a documentation flow chart seen by the internal auditors.
- The internal auditors have also seen evidence of training being provided and training compliance being enforced.

3. To review and clarify relevant checking procedures when sending patient correspondence. This is to include procedures around patient record keeping to ensure they are kept up to date. Any related guidance should be disseminated to all staff.

- The Trust's Information Governance have produced range of guidance covering posting, faxing and other communications to patients.
- Key messages have been sent out within a payroll letter.
- The Trust is in the process of developing a programme across some services to ensure that processes are appropriate and are being appropriately implemented.

4. The completion of mandatory induction data protection training, in relation to both the requirements of the Act and the data controller's policies concerning the use of personal data, is appropriately enforced. Completion of such training including that of regular refresher training shall be recorded and monitored to ensure compliance.

- The internal auditors have seen evidence that the Trust has reviewed training compliance and monitoring, with monthly emails received by managers to detail the training compliance within their teams.
- The Trust provided evidence of the new NHS Data Security and Awareness training and confirmed that it is now live and available on the Trust's e-learning system. The updated Action Plan says that the training has been available since December.
- Before the new NHS training was available staff were required to complete their mandatory training by means of an interim IG training tool or through delivered sessions. Figures provided by the Trust show that an average of 93% of staff across all departments completed the mandatory training between December 2016 and December 2017.
- The Trust also provided details of the mandatory induction training which has been provided to new starters.

A copy of this report will be passed to the Enforcement Department.

Date Issued: 30 January 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 rests with the management of Pennine Care NHS Foundation 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.

