

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

**Barking, Havering & Redbridge University Hospitals NHS
Trust**

ICO Reference: ENF0495248

On 7 January 2015 the Information Commissioner's Office (ICO) conducted a follow-up assessment of the actions taken by Barking, Havering & Redbridge University Hospitals NHS Trust (the Trust) in relation to the undertaking it signed in March 2014.

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. The undertaking requirements were:

- (1) The data controller ensures that attendance for its mandatory Information Governance training is properly enforced, through whatever means it deems appropriate;**
- (2) The data controller ensures that it maintains a full and accurate record of who has received the training, and that;**
- (3) 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 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.

The Trust provided the following response in relation to each point of the undertaking:

1. The Trust is committed to ensuring that all staff who handle personal identifiable information (whether staff or patient records) undertake mandatory information governance training annually.

Training is mandatory for the Trust's entire workforce. Training is delivered using a blend of in depth face to face training sessions (which is mandatory for all starters) and an e-learning module which includes an assessment.

As of 14th November (2014) 85% of permanent members of staff had undertaken IG training a rise of 18% since April (equating to approximately 1100 staff). 100% of individual's volunteering at the Trust have completed their IG training. Overall this constitutes a significant improvement when compared to our training compliance at the time of the incidents in January 2013 where only 50% of staff had completed their Information Governance training. The Trust is committed to ensuring 100% of its workforce refresh and maintains compliance with information governance training.

Compliance with Information Governance training is monitored by the Trust's Information Governance Steering Group and Trust Executive Committee. Monthly reminders are sent out by the Information Governance team to Directorates with lists of non-compliant staff.

In order to gain access a clinical information system and in particular the Trust's Patient Administration System staff are now required to complete information governance training. Upon confirmation that information governance training is complete staff user login details are released. Any members of staff who persistently fails to complete their Information Governance training may have their network account restricted and access to systems and records containing personal identifiable data removed pending completion of the training.

2. Information Governance training is now monitored using the WIRED (Workforce Information Reporting Engine Database) web based software tool. The WIRED tool provides full visibility of staff training records which can be accessed via the Trust's Intranet. The Tool introduced following the incident in January 2013 enables the Information Governance Team and managers to monitor compliance with training. WIRED enables managers to export data and to quickly create a wide range of high quality and accurate training compliance reports. Reports generated can be organisation wide,

or segmented by individual, department or division and staff groups. Using WIRED managers are now able to take responsibility for ensuring compliance, which makes improved compliance in respect of information governance training easier to achieve. The HR Directorate and Information Governance Team are jointly responsible for updating staff training records.

3. In order to prevent a similar incident occurring in the future the Trust has introduced a suite of new staff guidance to help ensure personal data is adequately protected at the Trust. The guidance consists of the following documents:

- Transmission of Confidential Information Policy (provided for review)
- Staff Guide – Consent and Disclosure (provided for review)
- Information Governance Staff Handbook (provided for review)

All information governance and data protection policies and guidance are published on the Trust's intranet pages. The Information Governance Pages on the intranet are currently being updated and will include additional guidance to staff on handling and transmitting personal data securely. The revised intranet page will centralise all Information Governance policies and guidance to ensure they are easily accessible for all staff.

It is worth noting that Trust Guidance actively encourages staff to use secure methods of transmitting personal data (i.e. NHS Mail) discouraging the use of fax which should only be used as a last resort. The use of secure email over fax is enshrined in the Transmission of Confidential Information Policy.

The Trust has also recently included an article in the weekly staff bulletin around the need to send personal identifiable information securely (copy provided for ICO review).

Paper-Lite Environment

Recognising the continued risks involved in handling and transmitting paper records and documents containing personal data the organisation is committed to becoming a paper-lite organisation. Initiatives include the introduction of the e-Handover solution. The electronic handover solution provides a paperless handover record available to all clinical staff thereby eliminating the risk of paper handover sheets being accidentally lost.

The imminent introduction of WiFi across both hospitals will also enable the Trust to introduce tablets and laptops to clinical wards which will further reduce the need for paper based records containing personal data.

Furthermore as part of the managed print business case we are planning to give employees the facility to scan documents electronically to their home drive. This feature alone which will be introduced in 2015 will help eliminate the need for staff to fax sensitive documents containing personal data.

In line with the National Information Board Framework Document published in November 2014 titled 'Personalised Health and Care 2020' the Trust is further committed to ensuring that all patient records will be digital, real-time and interoperable by 2020. By 2018 clinicians in emergency care will be operating without needing to use paper records.

We are currently taking steps to achieve this target. This includes the electronic recording of VTE and Dementia assessments which was previously paper based. We also have plans underway to begin recording electronically MRSA and MUST (a nutritional scoring tool).

Fax Rationalisation Programme

Alongside this the Trust is proposing to embark on a fax rationalisation programme in the New Year which will be aimed at reducing the number of machines capable of faxing from circulation. The first phase will be to conduct a Trust wide fax usage survey to enable the Trust to better understand under what circumstances documents containing personal information are faxed both in and out of the organisation. The second phase will be to remove all standalone desktop fax machines, leaving only a limited number of multi-functional devices which are capable of faxing. The third phase will be to contact all partner organisations to whom we receive and send faxes containing personal information to requesting that they provide a secure email address as an alternative means of transmitting documents. The proposal is on the agenda for discussion at the next Information Governance Steering Group meeting.

These measures described above along with our commitment to ensure staff complete mandatory information governance training are designed to ensure that the organisation can ensure that personal data is protected against unlawful processing, accidental loss or destruction.

ICO Response

While the ICO is encouraged by the above response, the Trust should take further action with regards to the following:

(1) It is encouraging to see that the Trust is withholding access to clinical systems where people haven't completed IG training. We note that the Trust has plans for removing access rights from those

members of staff who currently have access to clinical systems but fail to complete the mandatory training, this would be good practice however, the Trust has not provided the ICO of any indication in relation to when this tactic might be implemented. Without a formal framework for enforcing training via the addition or removal of access rights, there is a risk that the plan may never be fully enforced.

Upon reviewing the training completion figures which have been provided by the Trust (and indicate a 95% target for training completion), it is encouraging to see the increase of training completion since the undertaking was signed. However, it is of concern that as of September 2014 only 42.31% of the executive team had completed mandatory training. This could indicate a lack of buy in from senior staff – who should be leading by example in relation to the Information Governance agenda and should also have an adequate understanding of the importance of good Information Governance to ensure them to fulfil their IG responsibilities.

In addition to the above, the low level of bank staff and contractors who have completed mandatory training is a concern which will need to be addressed. It is however noted that there is a plan in place to roll out training to contractors from January 2015

Date Issued: 7 January 2015

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 Barking, Havering & Redbridge University Hospitals NHS 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.

