| | | | |
|---|---|---|---|
| Directorate / Programme | **Care Services** | Project | **Data Sharing Audits** |
| | | Status | **Approved** |
| Director | **Catherine O'Keeffe** | Version | **1.0** |
| Owner | **Rob Shaw** | Version issue date | **04/01/2018** |

# NHS Digital Audit of Data Sharing Activities: London Borough of Enfield Council – Public Health

# 1 Audit Summary

## 1.1 Purpose

This document records the key findings of a data sharing audit at London Borough of Enfield Council – Public Health (LBE) on the 28 and 28 November 2017. It provides an evaluation of how LBE conforms to the requirements of the data sharing framework contract (DSFC) CON-387613-L8G0N and the data sharing agreement (DSA) DARS-NIC-35531-X3Y7Q with respect to continuous user access of the Hospital Episode Statistics (HES) Data Interrogation System (HDIS) for:

| Data Assets | Classification of data | Dataset period |
|---|---|---|
| Admitted Patient Care | Pseudonymised / anonymised<br>Non-sensitive | 2006/07 to 2017/18 |
| Outpatients | Pseudonymised / anonymised<br>Non-sensitive | 2006/07 to 2017/18 |
| Accident and Emergency | Pseudonymised / anonymised<br>Non-sensitive | 2006/07 to 2017/18 |

The report also considers whether LBE conforms to its own policies and procedures.

This is an exception report based on the criteria expressed in the NHS Digital Audit Guide.

## 1.2 Scope and Assurance Statement

The audit considered the fitness for purpose of the main processes with respect to data handling at LBE along with its associated documentation against the scope areas shown in Table 1.

The NHS Digital Audit Team has assigned the following assurance ratings to these areas based upon the findings of the audit.

No rating has been assigned to “Information Transfer” and “Data Use and Benefits” as the source data has not been accessed and the current HDIS agreement does not allow records to be downloaded. The proposed use of the data as discussed during the audit nevertheless concurred with the objectives presented in the DSA.

| | |
|---|---|
| Access Control | Moderate assurance |
| Risk Management | Moderate assurance |
| Operational Management and Control | Limited assurance |
| Data Destruction | Unsatisfactory assurance |

**Table 1: Scope and Assurance rating**

Detailed findings related to the areas of scope are detailed in Table 2.

## 1.3 Overall Risk Statement

It is the Audit Team's opinion that based on evidence presented during the audit and the type of data being shared, there is a high risk of a breach of information security, duties of care, confidentiality or integrity (including inappropriate access to or loss of data) provided by NHS Digital to LBE under the terms and conditions of the data sharing agreements signed by both parties.

## 1.4 Response

LBE has reviewed this report and confirmed that it is accurate.

LBE will establish a corrective action plan to address each finding shown in Table 2. NHS Digital will validate this plan and the resultant actions at a post audit review with LBE to confirm the findings have been satisfactorily addressed.

# 2 Findings

Table 2 identifies the one major nonconformity, six minor nonconformities and six observations raised as part of the audit.

In addressing a finding the data recipient must take account of any referenced supplementary notes.

| Ref | Comments | Link to Area | Clause | Designation | Notes |
|---|---|---|---|---|---|
| 1. | Papers that contained personal identifiable information and one with personal sensitive information were found by the Audit Team in unlocked waste disposal containers located within the goods-in area of the Council building. There was no evidence of this information being lost or used inappropriately but storage protocols were not being followed. It was noted by LBE that some of the material may have emanated from another company located in the building.<br>LBE immediately raised a security incident and is expected to investigate and report accordingly. | Data Destruction | LBE - Corporate Records Management Policy, Section 11 (Appendix 4)<br>DSFC, Schedule 2, Section A, clause 4.9 | Major | |
| 2. | Reviews of user folder permissions and domain administrator accounts are not being undertaken on a regular basis to ensure that they remain valid. | Access Control | DSFC, Schedule 2, Section A, clause 1.2 and 4.1 | Minor | |
| 3. | Whilst a refresh of the Council's policies and procedures is currently being undertaken as part of its General Data Protection Regulations (GDPR) readiness, along with preparations for roll out to staff, existing documents have not been reviewed for some years. As a result, some of the practices witnessed onsite did not conform to existing documents. | Operational Management | DSFC, Schedule 2, Section A, clause 3 | Minor | |
| 4. | The retention of faulty or end of life hardware prior to destruction by the third-party destruction company does not meet the requirements of the NHS Digital's guidance. | Data Destruction | DSFC, Schedule 2, Section A, clause 4.10 | Minor | 1 |
| 5. | LBE does not currently have a Public Service Network (PSN) connection compliance certificate due to the number of recorded internal vulnerabilities. The Council does, however, have an active resolution process and is keeping PSN informed of progress. | Access Control | DSFC, Schedule 2, Section A, clause 1.1 | Minor | |
| 6. | No Privacy Impact Assessments (PIA) for NHS Digital supplied data has been undertaken, though PIAs should have been completed from 2016. PIAs will be undertaken under the new GDPR requirements. | Risk Management | LBE, Privacy Impact Assessment (template) | Minor | |

| Ref | Comments | Link to Area | Clause | Designation | Notes |
|---|---|---|---|---|---|
| 7. | The Public Health team is recording risk in a manner that is not compliant with the corporate definition. The team is, however, expecting to move its risks to the corporate risk management tool which will ensure future consistency. Risk management is currently being improved within the Council as a whole and a new Risk Manager has been appointed. | Risk Management | LBE, Risk Management Strategy | Minor | |
| 8. | LBE should review whether access to sensitive folders should be approved by the requestor's manager (which is the current approach) or by the Information Asset Owner (IAO) who may be more aware of any contractual restrictions. | Access Control | | Observation | |
| 9. | Whilst equipment being sent for destruction is recorded and the third-party provides a certificate of destruction, LBE does not reconcile the two lists to ensure they are consistent. | Data Destruction | | Observation | |
| 10. | The Audit Team recommends that a representative of the Council visits the third-party destruction company to ensure that equipment is being destroyed in an acceptable manner. | Data Destruction | | Observation | |
| 11. | There is no central Information Asset Register (IAR) at the moment, though LBE reported it is working towards one as part of its GDPR preparations. | Operational Management | | Observation | |
| 12. | No specialist training is currently being provided for Information Asset Owners, though plans are underway for such training as part of the GDPR rollout. | Operational Management | | Observation | |
| 13. | LBE should ensure that any new system that will hold NHS Digital data conforms to the full requirements of the existing and new contracts/agreements and relevant guidelines to maximise return. | Operational Management | | Observation | |

**Table 2: Nonconformities and Observations**

## 2.1 Supplementary Notes

The following notes refer back to Table 2 and provide additional commentary on the linked finding.

Note 1. Currently, all equipment marked for destruction is held in a locked steel container in in an unsecured area. The Council does not currently hold any NHS Digital data and the Public Health team use laptops which are encrypted using BitLocker. It was suggested by the Audit Team that hard discs are removed from devices awaiting destruction and held separately in a secure environment.

## 2.2 Data Location

LBE confirmed that processing and storage, including disaster recovery and backups, of the data will be limited to the location shown in Table 3. This location conforms with the locality defined in clause 2c of the DSA.

| | |
|---|---|
| Data Location | England |

**Table 3: Data Location**

## 2.3 Backup Retention

The duration for which data may be retained on backup media is shown in Table 4.

| | |
|---|---|
| Backup retention | No data has been downloaded at present |

**Table 4: Data Retention Period**

## 2.4 Good Practice

In addition to the findings presented in Table 2 the Audit Team noted the following areas of good practice:

- LBE are making good progress in terms of re-structuring and updating their ICT infrastructure following the transfer of ICT services from the service provider to bringing the service in-house.

## 2.5 Disclaimer

NHS Digital has prepared this audit report for its own purposes. As a result, NHS Digital does not assume any liability to any person or organisation for any loss or damage suffered or costs incurred by it arising out of, or in connection with, this report, however such loss or damage is caused. NHS Digital does not assume liability for any loss occasioned to any person or organisation acting or refraining from acting as a result of any information contained in this report.