Nottinghamshire County Council

NCC Improvement Plan in response to NHS Digital Audit of Data Sharing Agreement 2017

VERSION CONTROL

Author	Creation Date	Version	Status/ changes
Kay Massingham	14.08.2017	1.0	Draft
Changed by	**Revision Date**		
David Gilding	22.08.2017	2.0	Due dates and status added
Kay Massingham	9.10.2017	2.1	Updates to status and items completed added.
Kay Massingham	05.12.2017	2.2	Updates to status and items completed added.
David Gilding	18.12.2017	2.3	Updates to status and items completed added.
Kay Massingham	20.12.2017	2.4	Updates to status and items completed added.
Kay Massingham	22.1.2018	2.5	Updates to status and items completed added.

Ref	Comments	Type	Designation	Planned actions / updates	Action By	Due Date	Status
1.	NHS Digital data is being processed and stored at locations that are not declared on the DSA, namely the NCC DR site and the NHIS (Nottinghamshire Health Informatics Service) data centre. Although the NCC DR site is not council owned, the equipment is and is maintained by council staff.	Information Transfer	Minor non conformity	1. Collate list of addresses. Complete. 2. Amend DSA to show full list of addresses. **Remaining Action: DSAs in process of being updated as part of renewal.**	NHIS / NCC ICT DG	28/02/2018	Open

Ref	Comments	Type	Designation	Planned actions / updates	Action By	Due Date	Status
2.	Training for certain NCC PH staff has not been renewed in the last year as the corporate policy states every two years.	Operational Management	Minor non conformity	1. PHIT staff have undertaken all necessary training, July 2017. 2. Mandatory training list for PH division updated to specify annual data protection training requirement for relevant staff, July 2017.	DG KM	31/07/2017	Closed
3.	No Privacy Impact Assessment has been undertaken by NCC for the NHS Digital data. It is NCC practice to complete at least the Part 1 to assess if a full PIA is required.	Operational Management	Minor non conformity	1. Complete PIAs for HES, ONS births and deaths following NCC process. PIA for HES complete. **PIA for births and deaths completed and sent to DPH for final approval, 22 January 2018.** 2. Develop procedure for consideration of PIAs within PH. Complete: Procedure in place, Oct 2017.	DG / WS / NCC Legal KM	31/01/2018	Open
4.	Whilst NCC and NHIS were very open during the on-site visit and provided a range of evidence, NCC refused to give the Audit Team sight of the vulnerability (NESSUS) / penetration testing and associated remediation plan(s) citing that it had provided the current Public Services Network (PSN) certificate.	Operational Management	Minor non conformity	Discussed at August 2017 IMG meeting. Agreed to refer report to Governance and Ethics Committee. **Action: Report referred to Governance and Ethics committee for consideration at meeting 1 Feb 2018.**	BB / JFW	01/02/2018	Open
5.	NCC should ensure that the appropriate teams have seen the DFSC and DSA to ensure the organisation is fully compliant. This is particularly the case	Operational Management	Observation	Email sent to relevant teams 18.10.2017: Legal Services, Information Manager; ICT; all members of PH Information Team.	KM	18/10/2017	Closed

Ref	Comments	Type	Designation	Planned actions / updates	Action By	Due Date	Status
	of those DSA covering the provisions of ONS (Office of National Statistics) data.			Copies were attached of • Data Sharing Agreement Hospital Episode Statistics • Data Sharing Agreement Access to Primary Care Mortality Database • Data Sharing Framework Contract			
6.	NCC should produce a document which sets out the obligations of NHIS as the Data Processor, including any pertinent requirements in NCC's DSFC/DSA.	Operational Management	Observation	NCC Legal to produce suitable third party agreement. Discussed with Legal at meeting, 30.10.2017, Draft supplied by Legal, 22.1.2018. **Remaining action is to discuss with Legal and finalise document.**	Simon Gill	28/02/2018	Open
7.	Incident reporting is under review. As part of this review NCC should ensure that the need to inform NHS Digital of any data/contract breach is reflected.	Operational Management	Observation	Review of reporting personal data breaches is complete and the system approved by the IMG in August 2017. Any potential personal data breaches can currently be reported through the intranet form. The process for reporting personal data breaches has not changed and all staff should be aware how to make a report. Other information security incidents involving the systems/transfer of data, equipment theft/loss etc, should be reported through the ICT security incident process, as per standard	WS / KM	28/02/2018	Open

Ref	Comments	Type	Designation	Planned actions / updates	Action By	Due Date	Status
				reporting procedure. Public Health intelligence specialist is the primary point of contact for NHS Digital and will need to be informed of any incidents identified by NCC personnel or NHIS data processors. He will then need to report incidents to NHS Digital. Relevant NCC staff were informed of the NHS Digital incident reporting process by email on 18.10.2017. NHIS staff were also informed of the NHS Digital incident reporting process by forwarding this email. **Remaining action is to write this into the data processing agreement with NHIS at item 6 above.**			
8.	NCC needs to review its data deletion policy to ensure that any NHS Digital supplied data is permanently destroyed when no longer needed. As PH staff use Outlook and Outlook Web Access (OWA) as a mechanism to transfer data between NHIS and NCC networks, NCC needs to recognise that NHS Digital data has a footprint on its	Data Destruction	Observation	1. Deletion of data: The draft Information Security Policy references the draft Data Destruction Standard. There is an ICT asset disposal process that can be accessed here: http://home.nottscc.gov.uk/working/ict/arrange-collection. All ICT equipment, either collected as part of this process, or disposed of due to its age or	ICT	28/02/2018	Open

Ref	Comments	Type	Designation	Planned actions / updates	Action By	Due Date	Status
	Exchange server. *The Audit Team provided a copy of NHS Digital's latest guidance.*			due to being faulty has its data securely deleted before being disposed of as part of a contract with SCC. NCC also verifies that all new externally hosted systems also comply with our Information Retention and Data Destruction Standards. Compliance with the Data Destruction Standard is monitored both via a system provided by SCC, and via the issuing of Certificates of Destruction. 2. Discuss transfer of data using OWA / outlook and identify either how to address data deletion given the footprint on Exchange server, or identify appropriate alternatives for data transfer between NCC and NHIS. Response sought from ICT 9.10.2017. – **Action: To be followed up with ICT.**	ICT		
9.	Guidance should be developed by NCC around the handling and processing of NHS Digital data to provide consistency, including recognition of the various touch points.	Operational Management	Observation	Develop guidance for within PH on the handling of NHS digital data. Complete. Procedures agreed with PH Intelligence Team, October 2017	DG	27/10/2017	Closed
10.	Site visits should be undertaken by NCC to ensure that contracted third parties	Operational Management	Observation	Undertake site visits to test discharge of activities.	TBC	31/08/2017	Closed

Ref	Comments	Type	Designation	Planned actions / updates	Action By	Due Date	Status
	are discharging their activities appropriately.			Was noted by the Information Management Group in August 2017 that site visits should be undertaken to third parties.			
11.	The Audit Team is to review further evidence associated with the destruction lifecycle of hardware, namely PCs and laptops.	Data Destruction	Follow-up	ICT confirmed with the third party supplier that data on devices sent for destruction was permanently destroyed, and supplied information from the SCC lifecycle portal in support. Certificates of data destruction are placed on the Portal on completion. Screenshots were provided as examples and are available on request.	ICT	08/11/2017	Closed

Ref	Comments	Link to Area	Designation	Planned actions	Action By	Due Date	Status
12.	NHIS (Notts Health Informatics Service) needs to review its media deletion practices to ensure that any NHS Digital supplied data is permanently destroyed from its systems when no longer needed. This will include both the raw HES files and the database tables.	Data Destruction	Observation	DG to meet Mat Cooke / Debbie Pallant and agree actions. **Actions: Data Destruction is to be covered in the agreement referenced in items 6 and 7 above.**	DG / NHIS	28/02/2018	Open
13.	NHIS should review its access control policy to consider whether the annual review for ensuring correct access is too infrequent.	Access Control	Observation	DG to meet Mat Cooke / Debbie Pallant and agree actions. Complete: procedure amended to 6 month checks	DG / NHIS	27/10/2017	Closed

Ref	Comments	Link to Area	Designation	Planned actions	Action By	Due Date	Status
14.	NHIS should review its external approval process to ensure that it only processes requests for data access from known NCC managers.	Access Control	Observation	DG to meet Mat Cooke / Debbie Pallant and agree actions. Complete: approval process amended.	DG / NHIS	27/10/2017	Closed