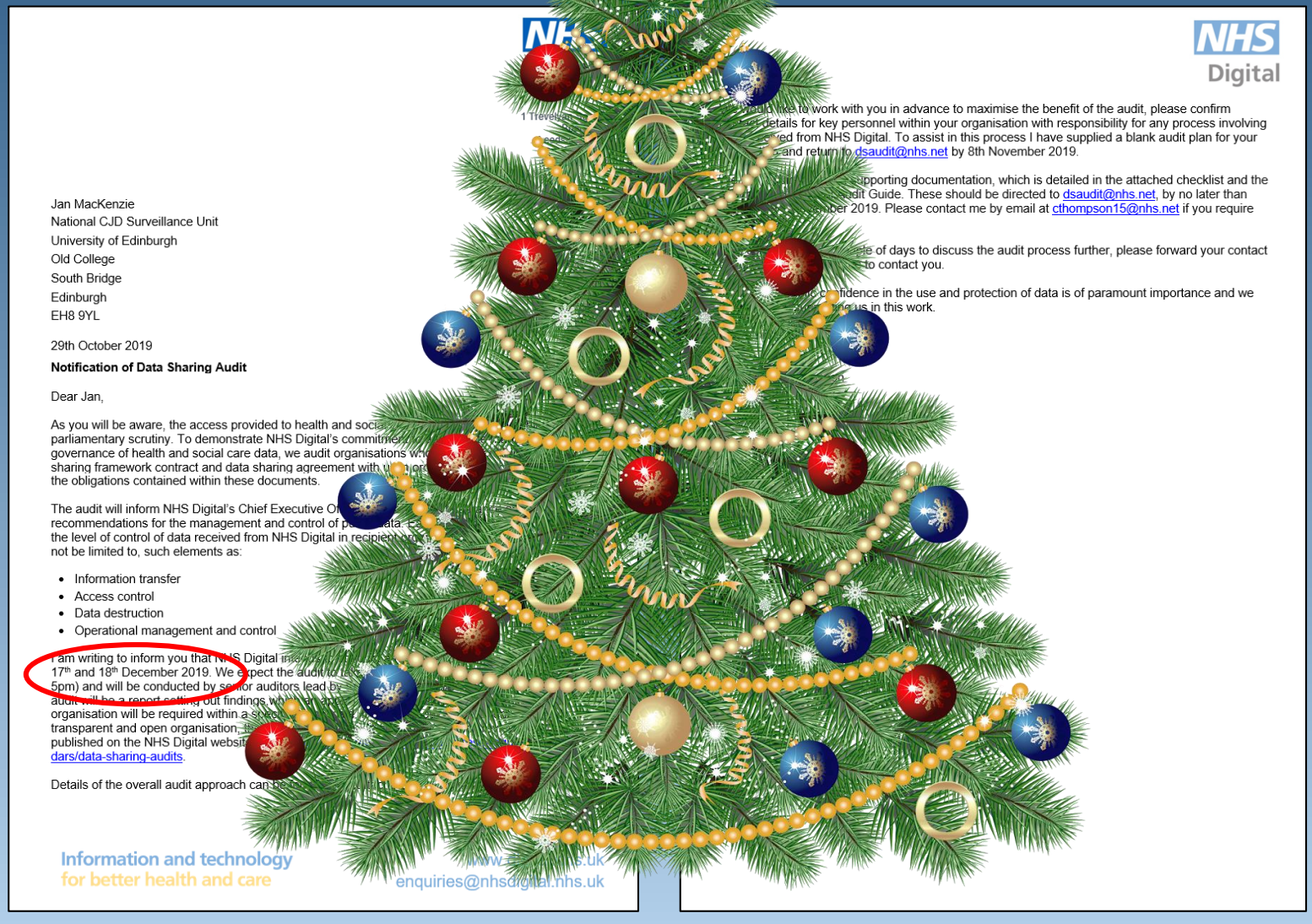
NHS Digital Audit: The Auditee's View

National CJD Research & Surveillance Unit (UK)

NHS Digital Audit – the Auditee's View

The Letter



NHS Digital

Jan MacKenzie
National CJD Surveillance Unit
University of Edinburgh
Old College
South Bridge
Edinburgh
EH8 9YL

29th October 2019

Notification of Data Sharing Audit

Dear Jan,

As you will be aware, the access provided to health and soci… parliamentary scrutiny. To demonstrate NHS Digital's commitme… governance of health and social care data, we audit organisations w… sharing framework contract and data sharing agreement with … the obligations contained within these documents.

The audit will inform NHS Digital's Chief Executive O… recommendations for the management and control of p… the level of control of data received from NHS Digital in recipient … not be limited to, such elements as:

- Information transfer
- Access control
- Data destruction
- Operational management and control

I am writing to inform you that NHS Digital … 17th and 18th December 2019. We expect the audit to … 5pm) and will be conducted by senior auditors lead by … audit will be a report setting out findings, w… organisation will be required within a … transparent and open organisation, … published on the NHS Digital websit… dars/data-sharing-audits.

Details of the overall audit approach can be …

Information and technology for better health and care

www.…uk
enquiries@nhsdigital.nhs.uk

…like to work with you in advance to maximise the benefit of the audit, please confirm …details for key personnel within your organisation with responsibility for any process involving …ed from NHS Digital. To assist in this process I have supplied a blank audit plan for your … and return to dsaudit@nhs.net by 8th November 2019.

…upporting documentation, which is detailed in the attached checklist and the …dit Guide. These should be directed to dsaudit@nhs.net, by no later than …ber 2019. Please contact me by email at cthompson15@nhs.net if you require …

…e of days to discuss the audit process further, please forward your contact … to contact you.

…confidence in the use and protection of data is of paramount importance and we …g us in this work.

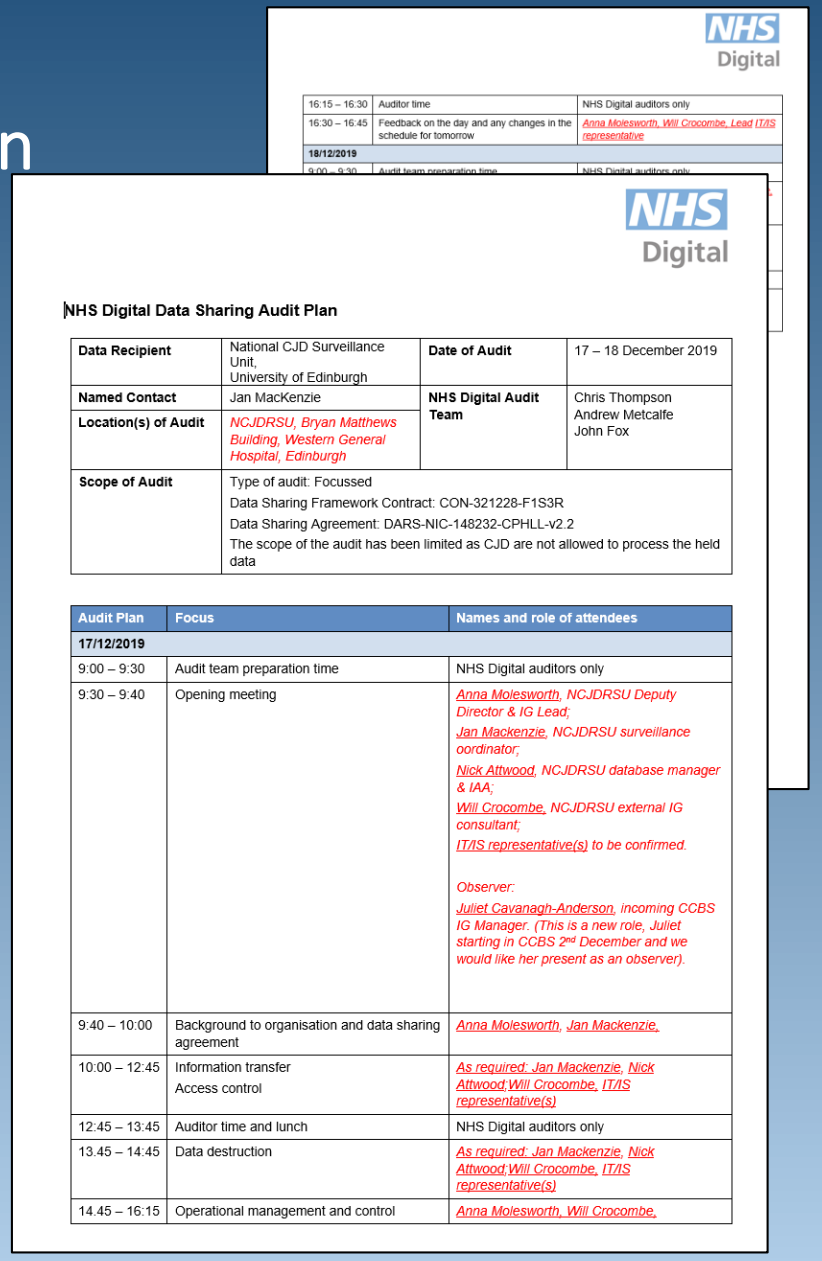
NHS Digital Audit: The Auditee's View

Preparing for The Visit: The Plan

- Teleconference
- 1 week to complete the audit plan

- **Good points….**
- Auditors were clear as to what was needed (focus on evidence)
- Immediate engagement by CJD Unit staff / Legal services

- **More difficult….**
- Identifying representation from Info Sec and IT Infrastructure



NHS Digital

16:15 – 16:30	Auditor time	NHS Digital auditors only
16:30 – 16:45	Feedback on the day and any changes in the schedule for tomorrow	*Anna Molesworth, Will Crocombe, Lead IT/IS representative*
18/12/2019		

NHS Digital

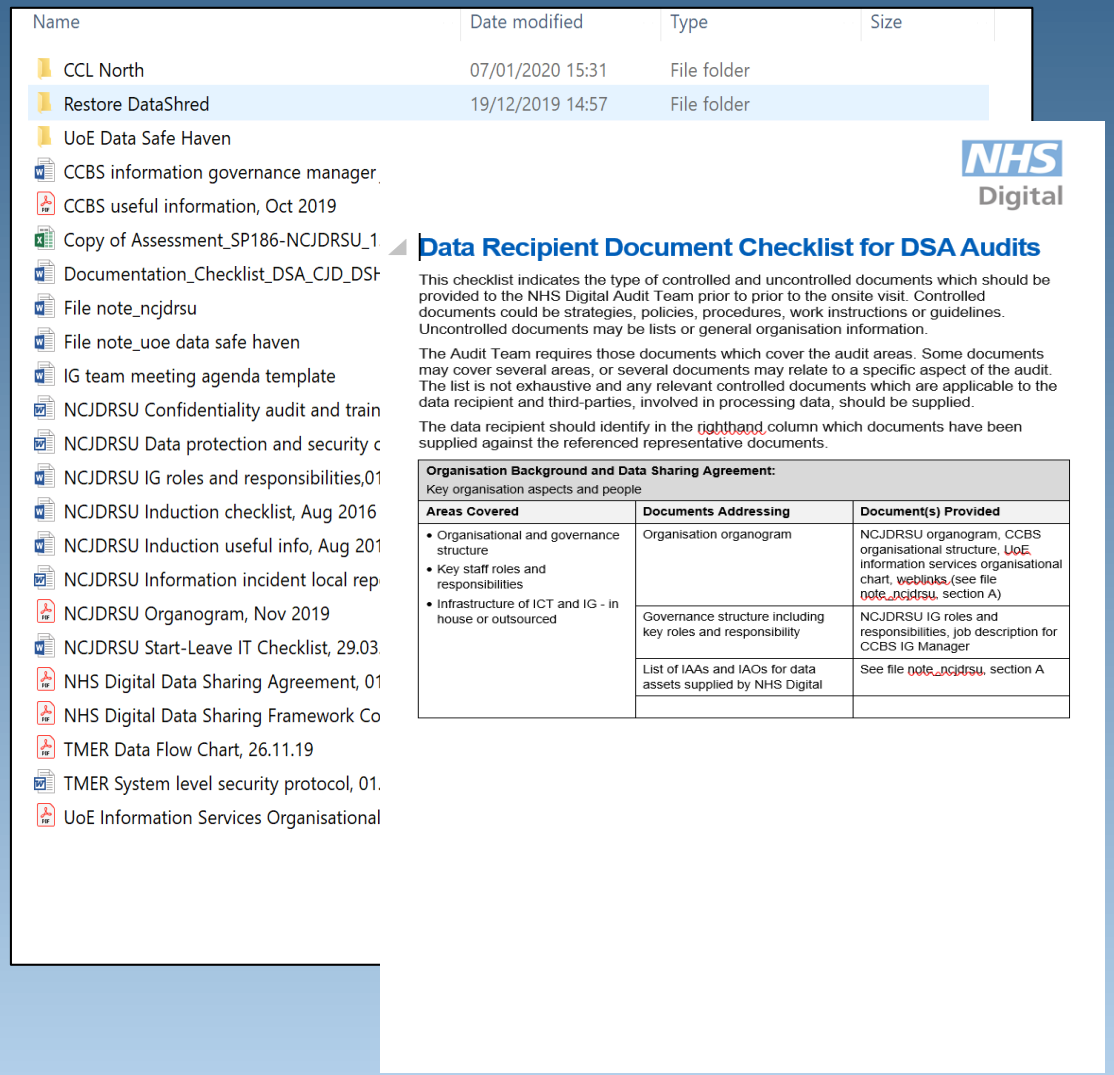
NHS Digital Data Sharing Audit Plan

Data Recipient	National CJD Surveillance Unit, University of Edinburgh	**Date of Audit**	17 – 18 December 2019
Named Contact	Jan MacKenzie	**NHS Digital Audit Team**	Chris Thompson Andrew Metcalfe John Fox
Location(s) of Audit	*NCJDRSU, Bryan Matthews Building, Western General Hospital, Edinburgh*		
Scope of Audit	Type of audit: Focussed Data Sharing Framework Contract: CON-321228-F1S3R Data Sharing Agreement: DARS-NIC-148232-CPHLL-v2.2 The scope of the audit has been limited as CJD are not allowed to process the held data		

Audit Plan	Focus	Names and role of attendees
17/12/2019		
9:00 – 9:30	Audit team preparation time	NHS Digital auditors only
9:30 – 9:40	Opening meeting	*Anna Molesworth, NCJDRSU Deputy Director & IG Lead;* *Jan Mackenzie, NCJDRSU surveillance oordinator;* *Nick Attwood, NCJDRSU database manager & IAA;* *Will Crocombe, NCJDRSU external IG consultant;* *IT/IS representative(s) to be confirmed.* *Observer:* *Juliet Cavanagh-Anderson, incoming CCBS IG Manager. (This is a new role, Juliet starting in CCBS 2nd December and we would like her present as an observer).*
9:40 – 10:00	Background to organisation and data sharing agreement	*Anna Molesworth, Jan Mackenzie,*
10:00 – 12:45	Information transfer Access control	*As required: Jan Mackenzie, Nick Attwood;Will Crocombe, IT/IS representative(s)*
12:45 – 13:45	Auditor time and lunch	NHS Digital auditors only
13.45 – 14:45	Data destruction	*As required: Jan Mackenzie, Nick Attwood;Will Crocombe, IT/IS representative(s)*
14.45 – 16:15	Operational management and control	*Anna Molesworth, Will Crocombe,*

NHS Digital Audit: The Auditee's View

Preparing for The Visit: The Key Documents



Name	Date modified	Type	Size
CCL North	07/01/2020 15:31	File folder	
Restore DataShred	19/12/2019 14:57	File folder	
UoE Data Safe Haven			
CCBS information governance manager			
CCBS useful information, Oct 2019			
Copy of Assessment_SP186-NCJDRSU_1			
Documentation_Checklist_DSA_CJD_DSH			
File note_ncjdrsu			
File note_uoe data safe haven			
IG team meeting agenda template			
NCJDRSU Confidentiality audit and train			
NCJDRSU Data protection and security c			
NCJDRSU IG roles and responsibilities,01			
NCJDRSU Induction checklist, Aug 2016			
NCJDRSU Induction useful info, Aug 201			
NCJDRSU Information incident local rep			
NCJDRSU Organogram, Nov 2019			
NCJDRSU Start-Leave IT Checklist, 29.03			
NHS Digital Data Sharing Agreement, 01			
NHS Digital Data Sharing Framework Co			
TMER Data Flow Chart, 26.11.19			
TMER System level security protocol, 01.			
UoE Information Services Organisational			

NHS Digital

Data Recipient Document Checklist for DSA Audits

This checklist indicates the type of controlled and uncontrolled documents which should be provided to the NHS Digital Audit Team prior to prior to the onsite visit. Controlled documents could be strategies, policies, procedures, work instructions or guidelines. Uncontrolled documents may be lists or general organisation information.

The Audit Team requires those documents which cover the audit areas. Some documents may cover several areas, or several documents may relate to a specific aspect of the audit. The list is not exhaustive and any relevant controlled documents which are applicable to the data recipient and third-parties, involved in processing data, should be supplied.

The data recipient should identify in the righthand column which documents have been supplied against the referenced representative documents.

Organisation Background and Data Sharing Agreement: Key organisation aspects and people		
Areas Covered	**Documents Addressing**	**Document(s) Provided**
• Organisational and governance structure • Key staff roles and responsibilities • Infrastructure of ICT and IG - in house or outsourced	Organisation organogram	NCJDRSU organogram, CCBS organisational structure, UoE information services organisational chart, weblinks (see file note_ncjdrsu, section A)
	Governance structure including key roles and responsibility	NCJDRSU IG roles and responsibilities, job description for CCBS IG Manager
	List of IAAs and IAOs for data assets supplied by NHS Digital	See file note_ncjdrsu, section A

- Teleconference
- 1 week: to complete the audit plan
- + 3 weeks: to provide documents

- **Good points….**
- Generally easy to identify what would be needed
- Support from DPO, Procurement, HR, IS
- Uploading documentation

- **More difficult….**
- Chasing documents across multiple departments with no prior contact
- Access to the documents once found
- Countering push-back in some areas

NHS Digital Audit: The Auditee's View

Preparing for The Visit: Final Preparations

- Teleconference
- 1 week: to complete the audit plan
- + 3 weeks: to provide documents
- + 2 weeks: to do final preparations (checking & collating evidence, logistics)
- **Good points….**
- Possible questions had been provided by audit team
- CJD Unit had an existing IG infrastructure with an evidence base
- Included areas outwith remit of audit (risk assessment and benefits)
- Logistics and admin relatively straightforward
- Computer provided and locked down

- **More difficult….**
- Migration to Data Safe Haven just before audit – was this sensible?
- ISO27001 compliance clouded some issues
- Substantial impact on other work areas

NHS Digital Audit: The Auditee's View

The Visit

Auditor 1

Auditor 2

Auditor 3

CCBS IG Obs.

CJD IAA

IG/ Systems Consult.

CJD IG Lead

CJD Study Coord.

UoE Head of Research IT

Head of Science Comp

UoE Waste Disposal

UoE Legal

UoE DPO

UoE HR

- Evidence
- Site Visit – to the server room/backup storage
- Further questions
- Feedback

NHS Digital Audit: The Auditee's View

Focus

- **Information transfer:**
- eg. data flow, data classification, asset register, backup procedures, data deletion

- **Access Control:**
- eg. starters/leavers/movers processes, training, patching, security, privilege controls, access logs, risk logs

- **Data destruction:**
- eg. responsibilities, processes, contracts, certificates, paper, digital, re-use vs destruction

- **Operational management:**
- eg. IG training, local vs UoE policies, DPIA, internal audit, risk register, incident management; asset management; privacy statement

NHS Digital Audit: The Auditee's View

Feedback

NHS Digital Audit: The Auditee's View

Impressions

Overall

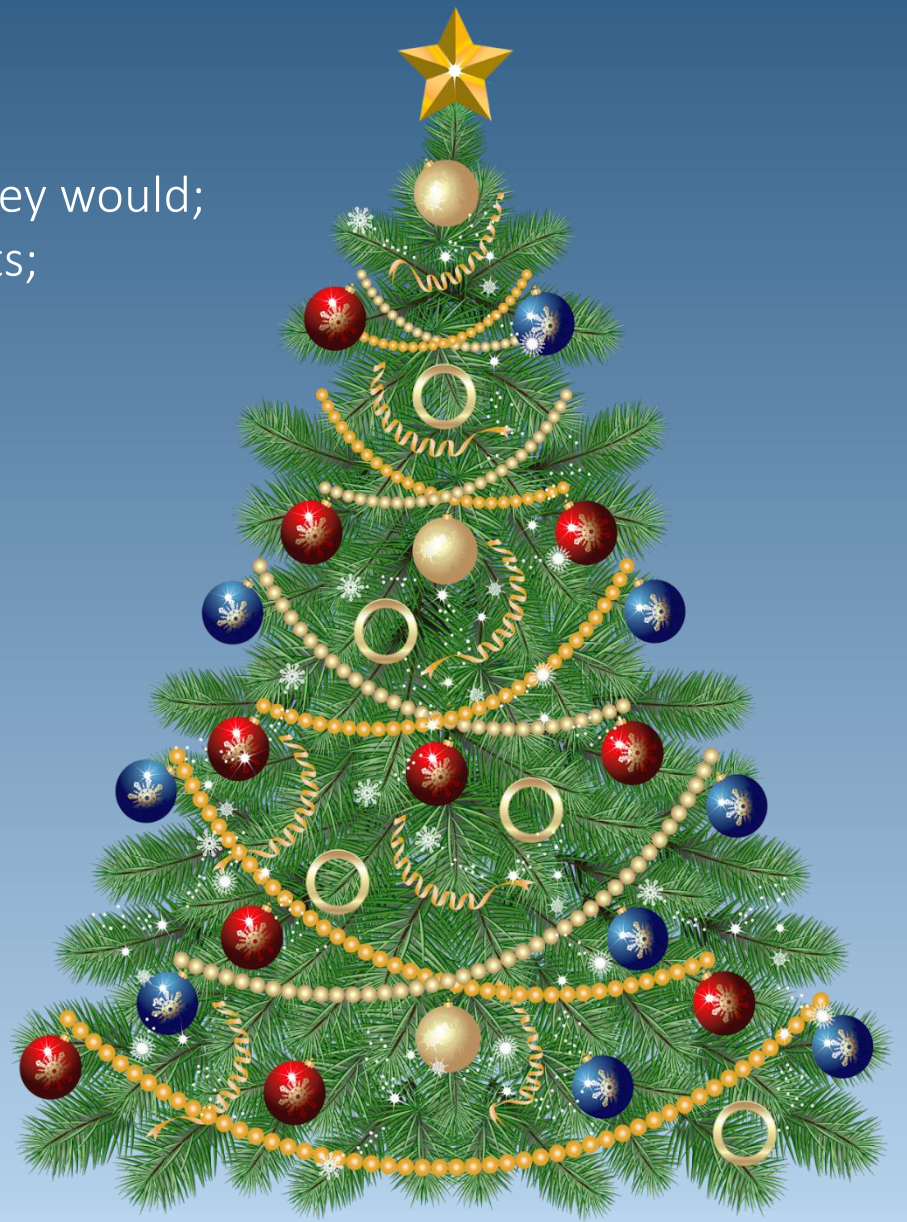
- The auditors were pleasant, professional and did what they said they would;
- The audit was **useful** in informing processes/highlighting blind spots;
- Did it help enlist engagement at higher level?

As auditees, what worked for us:

- We identified and engaged with relevant departments early on;
- We had a coordinator with autonomy to make decisions;
- We didn't rely on ISO27001 accreditation (although it will help);

NHS Digital need to provide:

- More discussion time for findings (good and bad)
- Clarity on how the final risk category is derived
- Greater granularity in the relationship between findings and risk



NHS Digital Audit: Another Auditee's View (University of Sheffield)

Good

- A clear plan was given up front; good guidance regarding what evidence was required before the audit (we provided all documentation in one document – 148 pages, plus numerous links to public facing policies and processes). The auditors were available and responsive.
- The auditors identified up front what study they were auditing.
- Whole heartedly agree that the auditors were pleasant, professional and did what they said they would.
- The auditors had clearly read all the provided documentation, reviewed all our web pages and stuck to the structure of the agenda.
- The auditors also stuck to all agreed post audit timeframes and provided the final report on time, communication was very good.
- Being audited demonstrates how seriously IG is taken by data providers and is useful for getting 'buy in' from staff at all levels.

NHS Digital Audit: Another Auditee's View (University of Sheffield)

As auditees, what worked for us:

- We have a departmental level DSPT (ScHARR) and a departmental IG committee which works closely with our central IT security team and the local study team. Representatives from all areas attended the audit meeting.
- We gave a short presentation at the start of the audit covering the structure of our organisation and how the study being audited fits within the overall governance structure.
- We are clear about the scope of our DSPT.

Unexpected

- The auditors had clicked through and read a lot of information on the University website and were very keen to know about formal structures of disseminating policies, procedures, guidance and information throughout the University (both from top down and back again).
- We have a member of the central information security team on our ScHARR IG Committee and on the UEB Information Management and Security Group (IMSG), which reports to the UEB. However, it was difficult to evidence a formal structure.

NHS Digital Audit: Another Auditee's View (University of Sheffield)

For NHS digital

- We believe there could be more specific requirements; it feels that that the auditors assessed us on unstated, subjective and moving target of "best practice".
- This makes it difficult to move forward with a 'concrete roadmap' and has in the past caused confusion around requirements, taking a lot of time to resolve.
- A clear requirements document would be very helpful.