

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
1.1.1	Has SIRO responsibility for data security been assigned?	Yes	Jenny Pope	Yes		29/01/2021 Caldicott Guardian Register was last updated 22/01/2021. Ray Smith is registered as our Caldicott Guardian. Cindy is still showing as SIRO on the SIRO Register. 03.02.2021 SIRO form prepared by JM. SIRO form sent to NHS Digital from Mel's email. Check to see whether SIRO Register has been updated. 17.02.2021 checked SIRO Register. Not updated yet. Last update was 5 February 2021 and form was sent 4 February 2021 so presumably missed that update? Check again in a couple of weeks. 24.02.2021 SIRO Register was updated 19 February 2021. Paul Rice is registered as our SIRO.	Y	Y	Yes
1.1.2	List the names and job titles of your key staff with responsibility for data protection and/or security.	Yes	Jenny Pope	Yes			Y	Y	Yes
1.1.3	Are there clear lines of responsibility and accountability to named individuals for data security?	Yes	Jenny Pope	Yes			Y	Y	Yes
1.1.4	Is data security direction set at board level and translated into effective organisational practices?	Yes	Jenny Pope	Yes			Y	Y	Yes
1.2.1	Are there board-approved data security and protection policies in place that follow relevant guidance?	Yes	Ian Scott	Yes	26.03.2021 Toolkit updated. Have asked Ian to re-confirm 12/05/2021 IG reviewed. to complete and confirm or re-confirm.	04.03.2021- Complete but Links need checking, are they current? 25.03.2021 unable to change as confirmed. Links need to be changed to https://intranet.bradfordhospitals.nhs.uk/policies/ . Have asked Ian to unconfirm.	Y	Y	Yes
1.2.3	How are data security and protection policies made available to the public?		Ian Scott	Yes	26.03.2021 Toolkit updated. Have asked Ian to re-confirm 12/05/2021 IG reviewed. to complete and confirm or re-confirm. Done 26/5	04.03.2021- Complete but Links need checking, are they current? 25.03.2021 unable to change as confirmed. Have asked Ian to unconfirm.	Y	Y	Yes
1.3.1	What is your ICO registration number?	Yes	Jenny Pope	Yes			y	y	Yes
1.3.2	How is transparency information (e.g. your privacy notice) published and available to the public?	Yes	Jenny Pope	Yes			y	y	Yes
1.3.3	How have individuals been informed about their rights and how to exercise	Yes	Jenny Pope	Yes			y	y	Yes
1.3.5	Have there been any ICO actions taken against the organisation in the last 12 months, such as fines, enforcement notices or decision notices?		Jenny Pope	Yes			y	y	Yes
1.4.1	Provide details of the record or register that details each use or sharing of personal information.	Yes	Jenny Pope	Yes		04.03.2021- Updated re IAR (ROPA checklist added). 24.03.2021 note added to Toolkit as per GH email. 27.04.2021 Dataflows diagram saved in evidence folder and Toolkit noted.	y	y	Yes
1.4.2	When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?	Yes	Jenny Pope	Yes	12.05.2021 IAR validation to be looked at.		Y	Y	Yes, some outstanding actions are still underway or yet to happen
1.4.4	Is your organisation compliant with the national data opt-out policy?	No	Jenny Pope	Yes		25.03.2021 to be non-mandatory this year (not yet published, news due out April)	y	y	Yes
1.5.2	What actions have been taken following confidentiality and data protection monitoring/spot checks during the last year?	Yes	Jenny Pope	Yes	12.05.2021 do a couple of virtual spot checks? Jenny has seen a template so will send to Graeme.	2020 Covid-19 has meant physical spot checks on hold. Schedule for 2021 tbc 23.03.2021 note added to Toolkit as per GH email. 25.03.2021 Spot checks do not have to be face-to-face, can be digital or remote/virtual (auditors informed)	y	y	Yes, some outstanding actions are still underway or yet to happen

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
1.6.1	There is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.	Yes	Jenny Pope	Yes		04.3.2021-Checked Pseudo Policy is current (Review scheduled Feb 22) and updated on DSPT. 24.03.2021 note added to Toolkit as per GH email.	Y	Y	Yes
1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.	Yes	Jenny Pope	Yes			y	y	Yes
1.6.3	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Yes	Jenny Pope	Yes	CT has confirmed Med Recs Library Security -3 doors into the medical records library. The main door has an external key lock with and internal digi lock. The door down from this is padlocked with estates control. The end door is purely a digi lock. This building is accessed based on clinical necessity of notes so once a day max.	Check Link http://bhts-intraweb/bhts-policies/docs/pmcp/CP40%202018%20(1)%20(D)%20Trust%20Security%20Policy.pdf 25.03.2021 link does not work. Policies are at https://intranet.bradfordhospitals.nhs.uk/policies/ . Have updated links.	y	y	Yes, some outstanding actions are still underway or yet to happen
1.6.4	Provide the overall findings of the last data protection by design audit.	Yes	Jenny Pope	Yes		04.03.2021- To check with NB re Pseudo Audit. 25.03.2021 have sent an email to Nadine asking for an update re progress of Pseudo Audit. Have not added the note to the Toolkit as don't think it needs adding? 27.04.2021 Copy of Pseudo Audit saved in evidence folder	y	y	Yes
1.6.5	There is a staff procedure, agreed by the SIRO, on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.		Jenny Pope	Yes	E block is a fob entry there are 4 members of staff who work in here, the one desk is behind a digi locked door.		y	y	Yes
1.6.6	Is a Data Protection Impact Assessment carried out before high risk processing commences?	Yes	Jenny Pope	Yes			y	y	Yes
1.6.7	Have any unmitigated risks been identified through the Data Protection Impact Assessment process been notified to the ICO?		Jenny Pope	Yes	C3 block is also fob entry with restricted access		y	y	Yes
1.6.8	Data Protection Impact Assessments are published and available as part of the organisation's transparency materials.		Jenny Pope	Yes	Action for 2021/22 consider publication of redacted list - not required for submission	04.03.2021- DPIAs available on request , IG considering publication of DPIA list in 2021 23.03.2021 note added to Toolkit as per GH email.	y	y	Yes
1.7.2	Data quality metrics and reports are used to assess and improve data quality.	Yes	Nadine Boczkowski	Yes		30.03.2021 JM reviewed and suggested new wording. To go to Nadine for approval once 1.7.5 updated. 07.04.2021 confidential waste information added at 1.7.5. Have asked Nadine to review/amend/confirm when she has time. 27.04.2021 Nadine's wording added to the Toolkit. Have asked Nadine to confirm when she has time. Nadine has confirmed this assertion.	Y	Y	Yes
1.7.3	A data quality forum monitors the effectiveness of data quality assurance processes.		Nadine Boczkowski	Yes		30.03.2021 JM reviewed and suggested new wording. To go to Nadine for approval once 1.7.5 updated. 07.04.2021 confidential waste information added at 1.7.5. Have asked Nadine to review/amend/confirm when she has time. 27.04.2021 Nadine's wording added to the Toolkit. Have asked Nadine to confirm when she has time. Nadine has confirmed this assertion. 18/05/2021 Email from Nick Dodds with Clinical Coding scores is in the DSPT folder of the IG inbox.	Y	Y	Yes
1.7.4	Has a records retention schedule been produced?	Yes	Nadine Boczkowski	Yes		27.04.2021 Have asked Nadine to confirm when she has time. Nadine has confirmed this assertion.	Y	Y	Yes
1.7.5	Provide details of when personal data disposal contract/s were last reviewed/updated.	Yes	Nadine Boczkowski	Yes		30.03.2021 JM reviewed and suggested new wording. To go to Nadine for approval once 1.7.5 updated. Have asked Kristy for the confidential waste contract information 07.04.2021 confidential waste information added. 27.04.2021 Have asked Nadine to confirm when she has time. Nadine has confirmed this assertion.	Y	Y	Yes

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
1.8.1	Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework	Yes	Ian Scott	Yes			Y	Y	Yes
1.8.3	What are your top three data security and protection risks?	Yes	Ian Scott	Yes			Y	Y	Yes
2.2.1	Is there a data protection and security induction in place for all new entrants to the organisation?	Yes	Jenny Pope	Yes		25.03.2021 evidence saved in folder and link added to Toolkit as per GH email. 29.03.2021 evidence saved in folder and link added to Toolkit as per GH email.	y	y	Yes
2.2.2	Do all employment contracts contain data security requirements?	Yes	Jenny Pope	Yes	Audit recommendation to discuss changes to IG clauses in contracts of employment with HR agreed.	25.03.2021 evidence saved in folder and link added to Toolkit as per GH email	Y	Y	Yes, some outstanding actions are still underway or yet to happen
2.2.3	The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.		Jenny Pope	Yes	07/05/2021 Check to see if survey included in Global Email for 13/05/2021. Need to run results about a fortnight after the last notification to ensure capture all results. 13/05/2021 responses received today so don't close yet!	07.04.2021 survey sent to Comms for inclusion in next week's Global Email. 21/04/2021 and 28/04/2021 and 06/05/2021 survey was included in Global Email.	y	y	Yes
3.1.1	Has an approved organisation-wide data security and protection training needs analysis been completed in the last twelve months?	Yes	Jenny Pope	Yes			y	y	Yes, some outstanding actions are still underway or yet to happen
3.2.1	Have at least 95% of all staff, completed their annual Data Security Awareness Training?	Yes	Graeme Holmes	Yes		25.03.2021 Training - % compliance anytime between 1/4/20 and 30/06/21	y	y	Yes
3.2.2	What is the average mark of staff completing the Data Security Awareness training?		Graeme Holmes	Yes			y	y	Yes
3.3.1	Provide details of any specialist data security and protection training undertaken.	Yes	Jenny Pope	Yes		12.05.2021 JM to check that certificate are up-to-date. Also to ask if anyone in Informatics has done any subject specific training in the last year i.e. Clinical Coding? 18.05.2021 Email sent to Nick. Copy of up-to-date trainer's certificate saved in evidence folder. Nick has confirmed by email that four of the Clinical Coders have passed the clinical coding course 2020-2021. Email in DSPT folder in IG inbox.	Y	Y	Yes, some outstanding actions are still underway or yet to happen
3.3.2	The organisation has appropriately-qualified technical cyber security specialist staff and/or service.	Yes	Jenny Pope	Yes	Confirmed yes but checking for recent training to add 12.05.2021 JM to ask whether or not anyone has done update training. Not known whether the cyber training which has been done is annual training or once only? 18.0.2021 Email sent to Steve. Steve responded to say that the course was a one-off. No-one else in Steve's team has undertaken qualification(s) this past year. Checking with Ian also in case he is aware of anyone.		Y	Y	Yes, some outstanding actions are still underway or yet to happen
3.3.3	The organisation has a nominated member of the Cyber Associates Network.	Yes	Jenny Pope	Yes			Y	Y	Yes, some outstanding actions are still underway or yet to happen

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
3.4.1	Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	Yes	Jenny Pope		External SIRO Training scheduled 29/6/21	04.03.21 check with SIRO and CG for evidence of training 23.03.2021 note added to Toolkit as per GH email. Also, emailed SIRO and CG for evidence of training 24.03.2021 Dr Smith has provided evidence. Saved in folder. DSPT noted. April/May 2021: has SIRO evidence (if any) been received? 07/05/2021 reminder sent to Paul 12/05/2021 Tracy thinks that Paul has not done specific SIRO training yet (only on-line induction) but she will ask him. Await response. 18/05/2021 Tracy is to book Paul onto a SIRO course. Couple of suggestions sent. Possible that the course will be post-June 2021. 21/05/2021 Tracy has booked Paul onto a course on 29 June 2021. Evidence saved in folder		Y	Yes
3.4.2	What percentage of board members have completed appropriate data security and protection training?	Yes	Jenny Pope	Yes			Y	Y	Yes
4.1.1	Your organisation maintains a record of staff and their roles.	Yes	Ian Scott	Yes			Y	Y	Yes
4.1.2	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Yes	Ian Scott	Yes			Y	Y	Yes
4.1.3	Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?		Ian Scott	Yes			Y	Y	Yes
4.2.1	When was the last audit of user accounts held?	Yes	James Townend		User access Audit o/s Audit completed 15/6/2021	30.03.2021 JT advised John Greenaway/Kay Pagan will carry out in year audit. Evidence from John saved to folder as per GH email 12/05/2021 IG reviewed. to complete and confirm or re-confirm.		Y	Yes
4.2.2	Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.		James Townend	Yes			Y	Y	Yes
4.2.3	Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.	Yes	James Townend	Yes			Y	Y	Yes
4.2.5	Are unnecessary user accounts removed or disabled?	Yes	James Townend	Yes		18/03/21-When a member of staff leaves, the manager is required to send an IT Termination Form to the ITSD (attached is the template) which then means the account is stripped of it's access and disabled there and then. If a manager fails to do this, the user account would be picked up as part of the 90 days. EUC disable all inactive accounts after 90 days, every month. This list is then provided to various members of staff who managed downstream systems. I have attached an example of this email and report from this month's run. The log off this is stored on our server and also we mark this as a task in the EUC monthly tasks,see screenshot in evidence folder. 23.03.2021 note added to Toolkit as per GH email. Link to evidence added as per GH email.	Y	Y	Yes

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
4.3.1	All system administrators have signed an agreement which holds them accountable to the highest standards of use.	Yes	James Townend	Yes			Y	Y	Yes
4.3.2	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Yes	James Townend	Yes			Y	Y	Yes
4.3.5	Have all staff been notified that their system use could be monitored?		James Townend	Yes			Y	Y	Yes
4.4.1	Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged and those logs are only accessible to appropriate personnel?	Yes	Ian Scott	Yes			Y	Y	Yes
4.4.3	The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.	Yes	Ian Scott	Yes			Y	Y	Yes
4.4.4	The organisation only allows privileged access to be initiated from devices owned and managed by your		Ian Scott	Yes			Y	Y	Yes
4.4.5	You record and store all privileged user sessions for offline analysis and investigation.		Ian Scott	Yes			Y	Y	Yes
4.5.1	Do you have a password policy giving staff advice on managing their passwords?	Yes	James Townend	Yes			Y	Y	Yes
4.5.2	Technical controls enforce password policy and mitigate against password-guessing attacks.	Yes	James Townend	Yes			Y	Y	Yes
4.5.3	Multifactor authentication is used [wherever technically feasible].	Yes	James Townend	Yes			Y	Y	Yes
4.5.4	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.	Yes	James Townend	Yes			Y	Y	Yes
4.5.5	Does your organisation grant limited privileged access and third party access only for a limited time period, or is it planning to do so?		James Townend	Yes			Y	Y	Y
4.5.6	Do you have high-strength passwords defined in policy and enforced technically for all users of internet-facing authentication services?		James Townend	Yes			Y	Y	Yes
5.1.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident, with findings acted upon.	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian 12/05/2021 IG reviewed. to complete and confirm or re-confirm.	No incidents in year, last incident 10/2/20, minutes of review provided 21/05/21	Y	Y	Y
5.1.2	Provide summary details of process reviews held to identify and manage problem processes that cause security breaches.	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian 12/05/2021 IG reviewed. to complete and confirm or re-confirm.	No incidents in year, last incident 10/2/20, minutes of review provided 21/05/21	Y	Y	Y

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
5.1.3	List of actions arising from each process review, with names of actionees.		Ian Scott	Yes	04.03.2021- IS to provide evidence 07/05/2021 email sent to Ian 12/05/2021 IG reviewed. to complete and confirm or re-confirm.		Y	Y	Y
5.2.1	Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.		Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian 12/05/2021 IG reviewed. to complete and confirm or re-confirm. IG reviewed with IS w/c 24/5				Pending Review of Pathology DT exercise
5.3.1	Are the actions to address problem processes, being monitored and assurance given to the board or equivalent senior team?		Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian 12/05/2021 IG reviewed. to complete and confirm or re-confirm.		Y	Y	Y
6.1.1	A data security and protection breach reporting system is in place.	Yes	Jenny Pope	Yes			Y	Y	Y
6.1.2	How can staff report data security and protection breaches and near misses?		Jenny Pope	Yes			Y	Y	Y
6.1.4	How is the board or equivalent notified of the action plan for all data security and protection breaches?	Yes	Jenny Pope	Yes			Y	Y	Y
6.1.5	Individuals affected by a breach are appropriately informed.	Yes	Jenny Pope	Yes			Y	Y	Y
6.2.10	Does the organisation maintain a list of approved applications, and are users prevented from installing any application that is unsigned or has an invalid signature?	Yes	James Townend	Yes		18/03/21 from JT re audior questions:The Palo Alto firewalls (our Internet proxy) have specific rule-sets on them that prevent users from downloading software such as .exe or .msi or .zip files with the exception of IT staff. Furthermore, the Palo Alto firewalls use reputation rules so don't allow users to visit websites known for hosting malicious software etc. Users do not have the administrative rights to install software – only permitted IT Staff have administrative rights on PC. In addition, the trust uses Microsoft's ATP service on all computers in the trust, and this flags up any software that is known by Microsoft's AI to be malicious and we are notified almost immediately via email of any instances of incidents/alerts. -With users not having administrative rights, how is this enforced and exceptions approved? Would you have three cases where that could be demonstrated if an exception is applied. The administrative rights on computers is enforced via Group Policy which is controlled and managed by the End User Computing Team. In addition, any time a member of staff (typically IT staff) are added or removed from the group that permits them these rights, the End User Computer team get an instant email about the change. This highlights any un-authorised changes. We do have instances where users outside of IT have administrative rights, for justified reasons, such as the PACS Manager who manages a large fleet of PACS Workstations that aren't typically managed by EUC or ZENworks, and the Head of Clinical Engineering who has a large range of software that needs to be installed any various computers in order to calibrate and test medical / clinical equipment etc. -Does the FT have application whitelisting in place as a control?	Y	Y	

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
6.2.11	You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.	Yes	James Townend	Yes			Y	Y	
6.2.12	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	Yes	James Townend				Y	Y	
6.2.2	Number of alerts recorded by the antivirus/anti-malware tool in the last three months.	Yes	James Townend		<p>AV/Malware alerts come in two fashions:</p> <p>1. ATP</p> <p>2. McAfee EPO</p> <p>ATP – When ATP detects something suspicious, it flags this on the NHS wide ATP instance hosted by NHS Digital, and sends an email alert immediately to EUC and IT Management. We then login to the ATP dashboard and have to acknowledge the alert/incident. The incident details give us a very powerful timeline of events and details about what happened. We then remediate the issue and mark this alert/incident as resolved or ongoing, and whether it was a true or false alert. ATP has the ability to automatically isolate a Windows 10 device from the network to stop further spread of malware should it deem the risk high enough. EPO – Alerts are flagged up in the Incident Manager for us to acknowledge. Typically both ATP and McAfee EPO will show the same sort of information. In any case, once we have acknowledged the alert and determined the risk, we typically have the device re-imaged (wiped clean) as a standard procedure and disable this from accessing the domain and VPN as a fail-safe until the device is wiped. Screenshots of a typical ATP and EPO alerts along with the incident/alert page and time line etc in evidence folder</p>		Y	Y	Y
6.2.3	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?	Yes	James Townend	Yes			Y	Y	Y
6.2.4	Antivirus/anti-malware is kept continually up to date.	Yes	James Townend	Yes		15/03/21-We have a Product Update Client task within ePo and the latest DATs and product updates are deployed as part of this, screenshot in evidence folder.. This client task is assigned globally to all endpoints which is deployed on a daily schedule – the clients pick this task up as soon as it next checks in. (Screenshots in evidence folder). 22/03/21- All machines are covered by the automatic update either via our EPO server (automatically accessible either on-site or at home via VPN) or via the internet. We have a script that ensures the machines get the latest DAT which we update monthly as one of our team's monthly task, but this is only ever called by a machine if it's on the original DAT on the image. 15/04/2021 have not added this note to the Toolkit as don't think it required to be added. Information for auditor only.	Y	Y	Y
6.2.5	Antivirus/anti-malware software scans files automatically upon access.	Yes	James Townend	Yes			Y	Y	Y

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
6.2.6	Connections to malicious websites on the Internet are prevented.	Yes	James Townend	Yes			Y	Y	Y
6.2.9	Number of phishing emails reported by staff per month.		James Townend	Yes		07/04/2021 have asked James and John for the number of phishing emails reported per month. Information input.	Y	Y	Y
6.3.1	If you have had a data security incident, was it caused by a known vulnerability?	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian		Y	Y	Y
6.3.2	The organisation has responded to high severity CareCERT alerts within 48 hours over the last twelve months.	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian		Y	Y	Y
6.3.3	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian	IS to provide in year evidence. 26/5 updated	Y	Y	Y
6.3.5	Are all new digital services that are attractive to cyber criminals (such as for fraud) implementing transactional monitoring techniques from the outset?	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian		Y	Y	Y
6.3.6	Have you had any repeat data security incidents within the organisation during the past twelve months?		Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian		Y	Y	Y
7.1.1	Your organisation understands the health and care services it provides.	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian	26/5 IS Updated	Y		
7.1.2	Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian	26/5 IS Updated	Y		
7.1.3	You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.		Ian Scott	Yes		26/5 IS Updated	Y		
7.1.4	You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.		Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian	We have not had a security incident. In evidence folder: Example minutes of the security meeting Cyber process from the intranet Open risks, updated monthly.	Y		
7.2.1	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.	Yes	Carl Hanson		CH 21/05/21-The go dark / EPR downtime exercise was last done on 6/3/2020, so not in this window (since 1/4/20) I'm aware Steve Amos is looking to schedule this in again soon. 27/05/21- Scheduled for Q1 2021/22		Y	Y	
7.2.4	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Yes	Carl Hanson				Y	Y	
7.3.1	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian	IS to provide in year evidence	Y	Y	Y

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Yes	Ian Scott	Yes			Y	Y	Y
7.3.3	Are draft press materials for data security incidents ready?		Ian Scott	Yes			Y	Y	Y
7.3.4	Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Yes	Ian Scott	Yes			Y	Y	Y
7.3.5	When did you last successfully restore from backup?	Yes	Ian Scott	Yes			Y	Y	Y
7.3.6	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose	Yes	Ian Scott	Yes		51/03/21-two safe locations. First is next to Clinical Engineering in the main BRI building. It contains 3 fire proof safes. Second is in the new build concourse in a service corridor and consists of 2 fire proof safes Backup Procedure doc in evidenc folder	Y	Y	Y
8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration.	Yes	Ian Scott	Yes		IS to provide in year evidence or statement that evidenc still current. Add latest iteration of IAR U:\IG\Information Assets\Information Asset Register\2020	Y	Y	y
8.1.2	Does the organisation track and record all end user devices and removable media assets?	Yes	Ian Scott	Yes		IS to confirm if 'Trial Leavers Process'now fixed ? 27/05/21-confirmed in place	Y	Y	y
8.1.3	Devices that are running out-of-date unsupported software and no longer receive security updates (patches) are removed from the network, or the software in question is uninstalled. Where this is not possible, the device should be isolated and have limited connectivity to the network, and the risk assessed, documented, accepted and signed off by the SIRO.	Yes	Ian Scott	Yes			Y	Y	y
8.1.4	The organisation ensures that software that is no longer within support or receiving security updates is uninstalled. Where this is impractical, the endpoint should be isolated and have limited connectivity to the network.		Ian Scott	Yes			Y	Y	y
8.2.1	List any unsupported software prioritised according to business risk, with remediation plan against each item.	Yes	Ian Scott	Yes	04.03.2021- IS to provide evidence/update notes 07/05/2021 email sent to Ian	IS to provide updated Unsupported software list of confirm old one still current-27/05/21-Confirmed	Y	Y	y
8.2.2	The SIRO confirms that the risks of using unsupported systems are being managed.	Yes	Ian Scott	Yes			Y	Y	y
8.3.1	How do your systems receive updates and how often?	Yes	Ian Scott	Yes	CH is AO	15/03/21 IS -Normal patch cycle, tracked at weekly security meeting	Y	Y	
8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Yes	Carl Hanson	Yes		CH to update ref ;Example of Informatics Performance Report is at Informatics Performance Report 30 September 2019 Draft v2.0.'	Y	Y	
8.3.3	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Yes	Carl Hanson	Yes			Y	Y	

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
8.3.4	Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied.	Yes	Carl Hanson	Yes			Y	Y	
8.3.5	Is your organisation actively using and managing Advanced Threat Protection (ATP)?		Carl Hanson	Yes			Y	Y	
8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Yes	Ian Scott	Yes		15/03/21 IS- Normal patch cycle, tracked at weekly security meeting 07/05/2021 note added to Toolkit	Y	Y	Y
8.4.2	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Yes	Ian Scott	Yes		15/03/21 Copy of Digital Performance Report Feb 21 in evidence folder. Also, we can patch legacy servers using the Trend product we have bought. Although the action plan will be developed to migrate to the new Data Centre SANs we have just procured. 07/05/2021 note added to Toolkit.	Y	Y	Y
8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.		Ian Scott	Yes			Y	Y	Y
9.1.1	The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	Yes	Steve Pearson	Yes			Y		
9.1.2	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	Yes	Steve Pearson	Yes			Y		
9.2.1	The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan and checking that all networking components have had their default passwords changed to a high strength password.	Yes	Steve Pearson	Yes		25.02.2021 Penetration test has been scheduled to start Monday 1st March. Steve will update the Toolkit in due course. 07.04.2021 Steve has updated the Toolkit and confirmed.	yes	yes	Y
9.2.2	The date the penetration test and vulnerability scan was undertaken.	Yes	Steve Pearson	Yes			yes	yes	Y
9.3.1	All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.	Yes	Ian Scott	Yes			Y	Y	y
9.3.2	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.	Yes	Ian Scott	Yes		IS commetns states evidenced elsewhere but not wht evidence is or where?-27/05/21-Confirmed ref to Pen Test	Y	Y	y
9.3.3	The organisation uses the UK Public Sector DNS service, or equivalent protective DNS service, to resolve Internet DNS queries.	Yes	Ian Scott	Yes			Y	Y	y
9.3.4	The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.	Yes	Ian Scott	Yes			Y	Y	y

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
9.3.5	The organisation understands and records all IP ranges in use across the organisation.	Yes	Ian Scott	Yes			Y	Y	y
9.3.6	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.	Yes	Ian Scott	Yes			Y	Y	y
9.3.7	The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service, or equivalent web check service, for its publicly-visible applications.	Yes	Ian Scott	Yes	IS to udate commetn, is this still the case re NCSC (i.e not able to register)	IG reviewed all with IS w/c 24/5	Y	Y	y
9.4.1	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.		Ian Scott	Yes		26/5 IS Updated	Y	Y	
9.4.2	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.		Ian Scott	Yes			Y	Y	
9.4.3	Your confidence in your security as it relates to your technology, people, and processes has been demonstrated to, and verified by, a third party onsite assessment.	Yes	Ian Scott	Yes		01/12/2020 message from NHS Digital: for NHS Trusts, evidence item 9.4.3 is currently exempted pending final confirmation. Evidence item 9.4.3 covers the requirement for a Cyber Essentials on-site assessment. We will write to you again as soon as we have confirmation. IS 15/03/21-ISO27001 accreditation cert in evidence folder.	Y	Y	
9.4.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.	Yes	Ian Scott	Yes	IS to update comments/evidence		Y	Y	
9.4.6	What level of assurance did the independent audit of your Data Security and Protection Toolkit provide to your organisation?	Yes	Ian Scott	Yes		GH to update DSPT audit outcome	Y	Y	
9.6.1	All devices in your organisation have technical controls that manage the installation of software on the device.	Yes	Ian Scott	Yes			Y	Y	Y
9.6.10	You have a plan for protecting devices that are natively unable to connect to the Internet, and the risk has been assessed, documented, accepted and signed off by the SIRO.	Yes	Ian Scott	Yes			Y	Y	Y
9.6.11	Does your organisation meet the secure email standard?		Ian Scott	Yes			Y	Y	Y
9.6.2	Confirm all data are encrypted at rest on all mobile devices and removable media and you have the ability to remotely wipe and/or revoke access from an end user device.	Yes	Ian Scott	Yes			Y	Y	Y
9.6.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.		Ian Scott	Yes			Y	Y	Y
9.6.4	Only approved software can be installed and run and unnecessary software is removed.	Yes	Ian Scott	Yes			Y	Y	Y

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
9.6.5	End user devices are built from a consistent and approved base image.	Yes	Ian Scott	Yes			Y	Y	Y
9.6.6	End user device security settings are managed and deployed centrally.	Yes	Ian Scott	Yes			Y	Y	Y
9.6.7	AutoRun is disabled.	Yes	Ian Scott	Yes			Y	Y	Y
9.6.9	All remote access is authenticated.	Yes	Ian Scott	Yes			Y	Y	Y
9.7.1	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	Yes	Steve Pearson	Yes			Y		
9.7.2	Has the administrative interface used to manage the boundary firewall been configured such that; it is not accessible from the Internet, it requires second factor authentication or is access limited to a specific address?	Yes	Steve Pearson	Yes			Y		
9.7.3	The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	Yes	Steve Pearson	Yes			Y		
9.7.4	All inbound firewall rules (other than default deny) are documented with business justification and approval by an authorised individual.	Yes	Steve Pearson	Yes			Y		
9.7.5	Have firewall rules that are no longer required been removed or disabled?	Yes	Steve Pearson	Yes			Y		
9.7.6	Do all of your desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by	Yes	Steve Pearson	Yes			Y		
10.1.1	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.	Yes	Julie Thrippleton	Yes	02.02.2021 Julie has submitted version 1 spreadsheet. Ian to comment. Copy saved in evidence folder. 04.03.21 V1 Spreadsheet uploaded to DSPT, IS to comment. 07.05.2021 email sent to		Y	Y	
10.1.2	Contracts with all third parties that handle personal information are compliant with ICO guidance.		Julie Thrippleton	Yes	02.02.2021 Julie has submitted version 1 spreadsheet. Ian to comment. Copy saved in evidence folder. 07.05.2021 email sent to Ian	JT TO CONFIRM	Y	Y	Y
10.2.1	Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	Yes	Ian Scott	Yes	IS TO CONFIRM COVERS ITSUPPLIERS		Y	Y	
10.2.2	Your organisation determines, as part of its risk assessment, whether the supplier certification is sufficient assurance.	Yes	Ian Scott	Yes			Y	Y	
10.2.3	Percentage of suppliers with data security contract clauses in place.		Ian Scott	Yes	IS % CURRENT		Y	Y	
10.2.4	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.	Yes	Ian Scott	Yes	IS TO CONFIRM THIS		Y	Y	

Item ref	Evidence Text - NHS Trusts (Category 1)	Mandatory?	Assertion Owner	Complete?	Notes - working on	Notes - completed (no further action required)	MET	Confirmed by AO	Signed off by IG
10.2.5	All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	No	Ian Scott	Yes			Y	Y	
10.3.1	List of data security incidents – past or present – with current suppliers who handle personal information.	No	Julie Thrippleton	Yes	02.02.2021 Julie has submitted version 1 spreadsheet. Ian to comment. Copy saved in evidence folder. 07.05.2021 email sent to Ian		Y	Y	
10.4.1	List of instances of suppliers who handle health and care data not complying with National Data Guardian standards, with date discussed at board or equivalent level.	No	Julie Thrippleton	Yes	02.02.2021 Julie has submitted version 1 spreadsheet. Ian to comment. Copy saved in evidence folder. 07.05.2021 email sent to Ian		Y	Y	
10.5.2	Where appropriate, you offer support to suppliers to resolve incidents.	No	Julie Thrippleton	Yes	02.02.2021 Julie has submitted version 1 spreadsheet. Ian to comment. Copy saved in evidence folder. 07.05.2021 email sent to Ian		Y	Y	