Type	Change	v1 ref	v2 ref	Req	Evidence text - GP	Tool tips - GP	Notes	Resource
Text	Reword	1.1.4	1.1.2	Yes	Who are your staff with responsibility for data protection and / or security.	Record names and job titles only for staff who have a specialised role.	Needs to be decided at practice level, normally Caldicott Guardian or IG/IT lead, partners and PM	
Y/N	Reword	1.2.1	1.2.1	Yes	Are there approved data security and protection policies in place that follow relevant guidance?	Confirm that you have policies in place that explain the organisation's plan or principles for data protection, data quality, records management, data security, registration authority, Subject access requests, Freedom of Information and network security.	The policies supplied last year are included again this year- these have been reviewed but not amended, however new FOI and SAR policies are included as this is a new requirement this year.	
Text	Reword - and now "text" item	1.2.2	1.2.2	Yes	When were each of the data security and protection policies last updated?	Policies should be reviewed and updated regularly.	These policies (with the exception of the FOI and SAR) were supplied last year. They have been reviewed by the CCG and are still compliant, but some slight amendments have been made.	
Doc	Reword	1.2.4	1.2.3		How are data security and protection policies available to the public?	Provide the web link, but if not available online then record where they are available. Publishing your policies will assist you to meet the transparency requirements of GDPR unless this causes a security risk to the organisation.	This is not a mandatory requirement, but if you wish you can add these to your practice website (or state they are available upon request)	
Text	Reword	1.3.1	1.3.1	Yes	What is your ICO Registration Number?	You can get this number from the Information Commissioner's Office website https://ico.org.uk/esdwebpages/search	If you do not know your ICO registration number you can find it from https://ico.org.uk/esdwebpages/search	
Doc	Reword	1.3.2	1.3.2	Yes	How is transparency information (e.g. your Privacy Notice) published and available to the public?	This covers personal information you collect or manage for patients and the public. Provide a weblink if possible or other publicly available document.	Privacy notices should contain this and be published on the website, waiting room etc.- a CCG template is available- this is an amended version of the one released last year- changes to it have been made using Tracked Changes within MW Word	

Doc	Retained	1.3.3	1.3.3	Yes	How have Individuals been informed about their rights and how to exercise them?	This could be a website, leaflet, letter or other method. Would include a list of rights and when/whether they apply to the processing undertaken by the organisation, contact details and procedure for subject access, and other rights requests.	This information is included with the Privacy Notice and SAR procedure and policy document.	
Doc	Reword	1.4.1	1.4.1	Yes	Provide details of the record or register that details each use or sharing of personal information.	The record should include for each entry: Purpose of processing, Legal basis relied on from GDPR Article 6 and Article 9, Categories of data subject/personal data, Categories of recipients, whether information is transferred overseas, whether data is retained and disposed of in line with policies, or if not, why not. Whether a written data-sharing agreement or contract is in place and when it ends.	Much of this should be included within the privacy notice, however this also incorporated in the data flow map template (part of the "article 30 register") we have drafted. You will need to delete those that do not apply, and if necessary add ones that may be applicable to your practice.	
Dat e	Reword	1.4.3	1.4.2	Yes	When was the record or register of information flows approved by the Management team or equivalent?	This date should be within the last twelve months.	The date the Article 30 register was approved as correct and complete by the practice. This was not originally included in last year's submission.	
Doc	Retained	1.4.4	1.4.3	Yes	Provide a list of all systems/information assets holding or sharing personal information.	This may be your information asset register including details of the: type, location, software, owner, support and maintenance arrangements, quantity of data and how critical they are to the organisation.	As above , this is included in your article 20 register.	
Doc	New	N/A	1.4.4	Yes	Is your organisation compliant with the national data opt-out policy?	Please provide your published compliance statement e.g. within a privacy notice and/or Published Data Release Register (https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out)	This is a new requirement- we are awaiting guidance from NHS Digital about how GPs will be supported with this.	

Y/N	Reword	1.5.1	1.5.1	Yes	Is there approved staff guidance on confidentiality and data protection issues?	In line with the organisation's data protection policy, there is guidance for staff on using and sharing personal information in accordance with data protection legislation, common law duties, and professional codes and national data opt-out operational policy guidance document, e.g. staff code of conduct, national data opt out model operational policy guidance document and Data Protection Impact Assessment guidance etc.	Should be available as part of the staff handbook but is also supplied as a specific policy template as part of this package	
Doc	New in lieu of 1.5.3	N/A	1.5.2	Yes	What actions have been taken following Confidentiality and Data Protection monitoring/spot checks during the last year?	The spot checks should check that staff are doing what it says in your staff Confidentiality and Data Protection guidance and the response should include details of any actions, who has approved the actions and who is taking them forward.	Last year's toolkit specified that spot checks were carried out (a template for this was supplied) and a report was made regarding findings- a template for this report is attached.	
Y/N	Reword	1.6.1	1.6.1	Yes	There is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements.	The procedures should be approved by the board or equivalent and aim to ensure that only the minimum necessary personal data is processed, that pseudonymisation is used where possible, that processing is transparent allowing individuals to monitor what is being done with their data.	Any new processing activity should be accompanied by a DPIA- two DPIA templates have been provided- one for changes the practice initiates, and one for changes imposed upon the practice.	
Text	Retained	1.6.3	1.6.2	Yes	There are technical controls that prevent information from being inappropriately copied or	Technical controls that can support data protection include access control, encryption, computer port control, pseudonymisation techniques etc. Provide details at high level.	Clinical system should only be accessed using smartcards or specific log ins. The downloading of software is restricted to administrator passwords. As part of the Windows10 rollout, all machines will be encrypted with bitlocker	

					downloaded.			
Text	Reword	1.6.4	1.6.3	Yes	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Physical controls that can support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas, records libraries, etc. Provide details at high level.	Records containing personal data are either stored securely within computer systems or in locked cabinets etc.	
Y/N	Reword	1.6.7	1.6.5		There is a staff procedure, agreed by the person with responsibility for data security, on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.	ICO guidance available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/	A DPIA is required for any large scale processing of personal data- as above, we have provided resources to support this.	
Y/N	Reword	1.6.11	1.6.6	Yes	Is a Data Protection Impact Assessment carried out before high risk processing commences?	'High risk processing' encompasses • Automated processing. • Large scale processing of special categories data - which includes health and genetic data. • Systematic monitoring of a public area. If not relevant for your organisation tick to confirm.	There will be relatively few occasions when you will need to carry out a DPIA, for instance if you change any of their clinical or administrative systems or providers. All services provided by the CCG will have a DPIA carried out.	
Text	New in lieu of 1.6.10 and 1.6.12	N/A	1.6.7	Yes	Have any unmitigated risks been identified through the Data Protection	Identification of unmitigated risks should form part of the Data Protection Impact Assessments procedure.	The DPIA document is written in such a way as to help you identify any risks as you proceed through it. any issues raised from DPIA should be addressed- in the unlikely event of	

					Impact Assessment process and notified to the ICO?		unmitigated high risks in any project you undertake the ICO should be informed- if you have any quires about these kind of risk please contact Leedsccg.dataprotectionoffice@nhs.net	
Doc	Retained	1.6.13	1.6.8		Data Protection Impact Assessments are published and available as part of the organisation's transparency materials.	Usually a link to where they are held on your website, or available through other means. This should be in redacted form if the publication of a full document causes a security risk to the organisation.	This will not generally be required by practices, as very few changes implemented at practice level will pass the threshold for a full DPIA	
Y/N	Reword	1.7.1	1.7.1	Yes	There is a policy and staff guidance on data quality.	In line with the organisation's data quality policy, there is guidance and training available to staff that details how to assure the quality of data information and how to report and resolve errors.	staff handbook and/or specific policy may cover this, however a data quality policy document has also been created as part of this package.	
Y/N	Reword	1.8.2	1.7.4	Yes	Has a records retention schedule been produced?	The organisation has produced a retention schedule based on business need with reference to statutory requirements and other guidance (https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016).	the IGA produces a thorough guide to records management with retention schedules- if you have data that is not covered within these guidelines please contact Leedsccg.dataprotectionoffice@nhs.net for advice	
Text	Retained	1.8.3	1.7.5		Provide details of when personal data disposal contracts were last reviewed/updated.	The contract should include the requirement to have appropriate security measures in compliance with data protection law and the facility to allow audit by the organisation. If no contract explain how personal data is disposed.	If you have a shredding policy, include it here. There are a number of companies that provide this service and you will need to check they are GDPR compliant NB as one for the market leaders we have received assurances from "Shred It" that they are compliant.	
Text	Retained	9.4.2	1.8.3		What are your top three data security and protection risks?	Record at a heading level	Employees Network security Data Loss Non-compliance with legislation	

Date	Reword	2.1.1	2.1.2	Yes	When did your organisation last review the list of all systems/information assets holding or sharing personal information?	The list should be reviewed annually to ensure it is still up to date and correct. It should be approved by the SIRO or equivalent.		
Y/N	Reword	2.3.1	2.2.1	Yes	Is there a data protection and security induction in place for all new entrants to the organisation?	The induction can be delivered face to face or digitally. Records are maintained and the induction is reviewed on a regular basis to ensure its effectiveness.	This should covered in the induction process, the staff hand book and is also part of the mandatory online training	
Y/N	Reword	2.3.2	2.2.2	Yes	Do all employment contracts contain data security requirements?	Please provide any explanatory text in the comments box	All contracts should contain standard clauses re IG/data security/confidentiality	
Text	New in lieu of various	N/A	2.2.3		The results of Staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the staff awareness questions in https://www.dsptoolkit.nhs.uk/Help/21 either through the Data Security Awareness training or local materials.	The staff awareness survey (provided) which was part of last years toolkit are reviewed.	
Y/N	New in lieu of 3.3.1	N/A	3.2.1	Yes	Have at least 95% of all staff, completed their annual Data Security awareness training in the period 1 April to 31 March?	Please also provide the percentage figure for the financial year 2019-20 in the space below with an explanation of how you have calculated the figure. This can be calculated from local materials/E Learning system and/or the national Data Security Awareness E-Learning system.	This can be addressed by staff completing mandatory training on an annual basis	

Text	Reword	3.3.2	3.2.2		What is the average mark of staff completing the Data Security Awareness Training?	This can be calculated from all training methods used.	This can be addressed by staff completing mandatory training on an annual basis	
Y/N	Reword	4.1.1	4.1.1	Yes	Your organisation maintains a record of staff and their roles.	Confirmation by the person with responsibility for staff management that the organisation maintains a record of staff and their roles.	Practice should have a list of all current staff, with their job roles	
Doc	Reword	4.1.2	4.1.2	Yes	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	A list of all systems, showing your staff roles and numbers split by the system access level they have.	This has been incorporated into the Article 30 register on the Information Asset Register page	
Dat e	Reword	4.2.1	4.2.1	Yes	When was the last audit of user accounts held?	An audit of staff accounts from your organisation, to make sure there aren't any inappropriate access permissions. Record the date when the last user audit was held. This should be completed annually as a minimum	The guidance regarding this is that this is an audit of all user accounts- a template is provided for this.	
Y/N	Retained	4.3.1	4.3.1	Yes	All system administrators have signed an agreement which holds them accountable to the highest standards of use.	With great power comes great responsibility and all administrators should attest to that responsibility by being signatory to agreement affirming the highest standard of use. If no systems select Yes.	This should be part of the standard contract conditions.	

Y/N	Reword	4.3.3	4.3.3		Is an acceptable IT usage banner displayed to all staff when logging in, including a personal accountability reminder?	This can take the form of an operating system banner (such as Windows login banner) or if appropriate one per system. A combination of banners is also valid.	This was rolled out as part of last year's DSP requirements	
Doc	Reword	4.3.4	4.3.4		Provide a list of all systems to which users and administrators have an account, plus the means of monitoring access.	For each system holding personal data that support users and administrative accounts, how user access is monitored should be recorded. If it is not monitored then this should be recorded.	This can be incorporated into your IG spot check regime	
Y/N	Reword	4.3.5	4.3.5	yes	Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system can be monitored and recorded. The notification method is periodic.	Staff should be made aware that their use of systems within the practice can be monitored	
Y/N	Reword	4.3.2	4.4.1		The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel.	IT Support staff typically have high level access to systems. The activities of these users should be logged and only available to appropriate personnel. If no systems then please tick and state "No systems" as a comment.	The refers to access to systems containing personal data.	
Text	New	N/A	5.1.2	Yes	Provide a summary of process reviews held after security breaches to identify and	Processes which have caused breaches or near misses, are reviewed to identify and improve processes which force staff to use workarounds which compromise data security.	Review of IG related DATIX and/or internal SE reviews to identify any issues	

					manage problem processes.			
Text	Retained	5.3.1	5.3.1		Explain how the actions to address problem processes are being monitored and assurance given to the Board or equivalent senior team?	Explain the governance around escalation of any issues and findings to the board, or equivalent, through reports and briefing notes during the last twelve months.	This should be part of your procedure review process	
Y/N	Retained	6.1.1	6.1.1	Yes	A data security and protection breach reporting system is in place.	Confirmation that a functioning data security and protection breach reporting mechanism is in place including use of the DSP Toolkit Incident reporting tool	The Datix should be available to all users within the practice for incident reporting. https://leedswestccg.datix.thirdparty.nhs.uk/Live/index.php	
Text	New in lieu of 6.1.2	N/A	6.1.2		How can staff report data security and protection breaches and near misses?	Explain the options that staff have to be able to raise near misses and incidents. This may be in-person, through incident report forms, a phone number, email address etc.	The Datix should be available to all users within the practice for incident reporting. https://leedswestccg.datix.thirdparty.nhs.uk/Live/index.php	
Text	New in lieu of 6.1.3	N/A	6.1.3	Yes	List of all notifiable data security breach reports in the last twelve months.	Notifiable to the ICO and/or DHSC	A list of breaches, if any, that have reached the threshold to be reported to the ICO or the ICO and the Department for Health and Social Care	
Text	New in lieu of 6.1.4	N/A	6.1.4		The person with overall responsibility for data security is notified of the action plan for all data security breaches.	If no breaches then please state "No breaches".	This is likely to be your DPO/Caldicott Guardian	

Y/N	Retained	6.1.5	6.1.5	Yes	Individuals affected by a breach are appropriately informed.	If a data security breach occurs under GDPR which requires notification (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) individuals are appropriately informed? If no breaches then please tick and state "No breaches".	As part of these resources we have included the NHS Digital Data Breach guide (also available on the DSP toolkit website)	
Text	Retained	6.3.1	6.2.1	Yes	Name of anti-virus product.	The software supplier, product name and version of each type of product used with an indication of its use / scope. This information will not be shared publicly.	Symantec AV	
Text	Retained - but now a "text" item	6.3.2	6.2.2	Yes	Number of alerts recorded by the AV tool in the last three months.	Your antivirus software should record alerts of any potential threats to your system. Provide the number which have been recorded over the last three months. You may need to speak to your IT Supplier to learn how to view this information.	There is no centralised function for this- individual practices will have to approach their helpdesk (LCC or Egton) and request this information	
Y/N	New	N/A	6.2.3		Has anti-virus or malware protection software been installed on all computers that are connected to or capable of connecting to the Internet?	This applies to: application servers; desktop computers; laptop computers and tablets.	All device supplied by the CCG for connecting are configured with AV protection	
Text	Retained	6.3.3	6.2.7		Name of spam email filtering product. (Exempt for NHS Mail)	The software supplier, product name and version of each type of product used with an indication of it use / scope. You may need to speak to your IT Supplier to learn how to view this information. This will not be shared publicly.	Exempt for NHS Mail	
Text	Retained - but now a "text"	6.3.4	6.2.8	Yes	Number of spam emails blocked per month. (Exempt for NHS	Your email services product should record the number of emails blocked as spam from the previous calendar month at the time of completion. You may need to speak to your IT	Exempt for NHS Mail	

	item				Mail)	Supplier to learn how to view this information.		
Text	Reword - and now "text" item	6.4.2	6.3.6		Have you had any repeat data security incidents of the same issue within the organisation?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within 3 calendar months of the original or subsequent occurrences. Provide details.	There is no centralised mechanism for ascertaining this.	
Y/N	New in lieu of 7.1.1	N/A	7.1.2	Yes	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?	This may include the preservation of manual processes for essential services.	this should be included in the practice BCP	
Y/N	Retained	7.2.4	7.3.2	Yes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as e-mail.	this should be included in the practice BCP	
Text	New	N/A	7.3.4		Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Provide evidence that your back up, testing and review process is effective.	Clinical data is backed up on hosted servers, and practice server data is backed up via tape. It is the practice responsibility to ensure that these backups are successful. It will be the practice responsibility to ensure any data processed by other providers (e.g. dictation, document management etc.) is backed up. Please note that PC drives are not routinely	

							backed up as part of the CCG service and important data should not be stored on PC drives	
Doc	Reword	8.3.1	8.3.1	Yes	How do your systems receive updates and how often?	This is your Strategy for System updates. You may need your IT Supplier/s to assist with this.	Copy of patch schedules included for practices managed by LCC and Egton	
Y/N	New	N/A	9.1.1	Yes	The Head of IT, or equivalent role confirms all networking components have had their default passwords changed.	If you don't have network or internet access please contact the helpdesk to request an exemption.	Both Egton and Embed have confirmed that they change the default passwords of all networking equipment. All networking equipment supplied by the CCG has had the default password changed	
Text	New in lieu of 9.3.1 and various	N/A	9.2.1		The annual IT penetration testing is scoped in negotiation between management, business and testing team including checking that all networking components have had their default passwords changed.	Please only include the scope and redact any elements of the results that are sensitive.	This is not mandatory and there are no plans at present to carry this out at CCG level	
Y/N	New	N/A	9.6.2	Yes	Confirm all health and care data is encrypted at rest on all mobile devices and		All mobile devices issued by the CCG are encrypted	

					removable media.			
Doc	Reword	10.1.1	10.1.1	Yes	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.	A list containing suppliers that handle personal information, systems/services and contract start and end dates. If no suppliers mark N/A as "other text"	list of suppliers required- your article 30 register can assist with this.	
Y/N	Reword	10.1.2	10.1.2		Contracts with all third parties that handle personal information are compliant with ICO guidance.	A review of all contracts has been undertaken to ensure that they comply with the requirements set out in Article 28 of the GDPR. If you hold no contracts please contact the helpdesk and request an exemption.	confirmation that each supplier is compliant with current Data Protection law- the CCG has approached the major suppliers and received assurances.	
text	New	N/A	10.2.1	Yes	Organisations ensure that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification	Suppliers may include other health and care organisations. As per the 2017-18 DSR letter. https://improvement.nhs.uk/documents/2643/17-18_DSPR_Statement_of_Requirements_-_QUESTIONS_11April.pdf		