Assertion	Input Type	OLD v3 20-21 Evidence ref	v4 21-22 Evidence ref	Change summary	Evidence Text - NHS Trusts and CSUs (Category 1)	Tool Tips - NHS Trusts (Category 1)	Required to meet standard (mandatory) - NHS Trusts and CSUs (Category 1)	Evidence Text - CCG and ALBs" (Category 2)	Tool Tips - CCG and ALBs (Category 2)	Required to meet standard (mandatory) - CCG and ALBs (category 2)	Evidence text - Others (Category 3)	Tool tips - Others (Category 3)	Required to meet standard (mandatory) - Others (Category 3)	Evidence text - GP (Category 4)	Tool tips - GP (Category 4)	Required to meet standard (mandatory) - GP (Category 4)
The organisation has a framework in place to support Lawfulness, Fairness and Transparency	Text	1.3.1	**1.1.1**	No changes	What is your organisation's Information Commissioner's Office (ICO) registration number?	You can get this number from the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search)	Yes	What is your organisation's Information Commissioner's Office (ICO) registration number?	You can get this number from the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search)	Yes	What is your organisation's Information Commissioner's Office (ICO) registration number?	Registration with the ICO is a legal requirement for every organisation that processes personal information, unless they are exempt as a small charity. If your organisation is not already registered, you should [register as a matter of urgency](https://ico.org.uk/for-organisations/data-protection-fee/). You can check whether you are registered and what your ICO registration number is on the [Information Commissioner's Office website](https://ico.org.uk/esdwebpages/search)	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)	Yes
	Document	1.4.1	**1.1.2**	Reword for cat 1 and 2	Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.	Please see [additional guidance.](https://www.dsptoolkit.nhs.uk/Help/88)	Yes	Your organisation has documented what personal data you hold, where it came from, who you share it with and what you do with it.	Please see [additional guidance.](https://www.dsptoolkit.nhs.uk/Help/88)	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent since 1st July 2021. Upload the document(s) or link to the document or specify where it is saved. Example IARs and ROPAs are available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/).	Yes	Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?	To be compliant with data protection legislation you must have a list or lists of the different ways in which your organisation holds personal and sensitive information (e.g. filing cabinet, care planning system, laptop). This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. It is fine to have either two separate documents or a single document that combines both lists. The list(s) should be reviewed and approved by the management team or equivalent since 1st April 2020. Upload the document(s) or link to the document or specify where it is saved. Example IARs and ROPAs are available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/).	Yes
	Document	New	**1.1.3**	New	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Please provide documentary evidence.	Yes	Your business has identified, documented and classified its hardware and software assets and assigned ownership of protection responsibilities.	Please provide documentary evidence.	Yes						
	Date	1.4.2	**1.1.4**	No changes	When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?	The list should be reviewed since 1st July 2021 to ensure it is still up to date and correct. It should be approved by the SIRO or equivalent.	Yes	When did your organisation last review both the list of all systems/information assets holding or sharing personal information and data flows?	The list should be reviewed since 1st July 2021 to ensure it is still up to date and correct. It should be approved by the SIRO or equivalent.	Yes						
	Text	1.1.2	**1.1.5**	No changes	List the names and job titles of your key staff with responsibility for data protection and/or security.	Details are required only for staff who have a specialised role.	Yes	List the names and job titles of your key staff with responsibility for data protection and/or security.	Details are required only for staff who have a specialised role.	Yes	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Whilst data security and protection is everybody's business, someone within your organisation must take overall senior responsibility for it. There must be at least one named person who leads on data security and protection. Their responsibility is to provide leadership and guidance from a senior level. In the text box, write the name(s) of the person or people within your organisation with overall responsibility for data security and protection. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job description, or be noted in the minutes of a management meeting, or be in an email from the appropriate director in your organisation. Your organisation may also have additional specialised roles, for example a Data Protection Officer (DPO). [Read more about data security and protection responsibilities and specialised roles](https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/)	Yes	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Whilst data security and protection is everybody's business, someone within your organisation must take overall senior responsibility for it. There must be at least one named person who leads on data security and protection. Their responsibility is to provide leadership and guidance from a senior level. In the text box, write the name(s) of the person or people within your organisation with overall responsibility for data security and protection. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job description, or be noted in the minutes of a management meeting, or be in an email from the appropriate director in your organisation. Your organisation may also have additional specialised roles, for example a Data Protection Officer (DPO). [Read more about data security and protection responsibilities and specialised roles.](https://www.digitalsocialcare.co.uk/resource/data-security-and-protection-responsibilities/)	Yes
	Yes/No	New	**1.1.6**	New	Your organisation has reviewed how you ask for and record consent.	Provide details in the comments. Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).		Your organisation has reviewed how you ask for and record consent. And has systems to record and manage ongoing consent.	Provide details in the comments. Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).		Your organisation has reviewed how you ask for and record consent. And has systems to record and manage ongoing consent.			Your organisation has reviewed how you ask for and record consent. And has systems to record and manage ongoing consent.	Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/).	
	Yes/No	1.7.2	**1.1.7**	Removed from Cat 3	Data quality metrics and reports are used to assess and improve data quality.	Published data quality metrics and reports such as the Data Quality Maturity Index (DQMI) are reviewed and actioned in a timely manner to continually improve data quality.	Yes	Was the scope of the last data quality audit in line with guidelines.	The data quality audit should be in the last twelve months and scoped to the [Service User Data Audit guidance.](https://www.dsptoolkit.nhs.uk/help/1	Yes						
	Text	New	**1.1.8**	New	A data quality forum monitors the effectiveness of data quality assurance processes.	Guidance on establishing internal data quality assurance processes and undertaking Clinical Coding Audits can be found in the [Data Security Standard 01 big picture guide](https://www.dsptoolkit.nhs.uk/Help/23).	Yes	A data quality forum monitors the effectiveness of data quality assurance processes.	Guidance on establishing internal data quality assurance processes and undertaking Clinical Coding Audits can be found in the [Data Security Standard 01 big picture guide](https://www.dsptoolkit.nhs.uk/Help/23).	Yes						
Individuals' rights are respected and supported	Document	1.3.2	**1.2.1**	No changes	How is transparency information (e.g. your Privacy Notice and Rights for individuals) published and available to the public?	This covers personal information you collect or manage for patients including children, and the public, include a list of rights and when/whether they apply to the processing undertaken, contact details and procedure for subject access, right to rectification and other rights requests. Provide a weblink if possible or other publicly available document.	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, include a list of rights and when/whether they apply to the processing undertaken, contact details and procedure for subject access and other rights requests. Provide a weblink if possible or other publicly available document.	Yes	Does your organisation have a privacy notice?	If you use and share personal data then you must tell people what you are doing with it. This includes why you need the data, what you'll do with it, who you're going to share it with and individual's rights under data protection legislation e.g. to access the information. This should be set out in writing in 'a privacy notice'. You should provide this information in a clear, open and honest way using easily understood language. Privacy notice should cover all data you process for example the data relating to the people you support and their relatives, staff, volunteers, members of the public. You may have more than one privacy notice e.g. one for staff and another one for the people you support. An example privacy notice is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/)	Yes	Does your organisation have a privacy notice?	Your organisation must set out in clear and easily understood language what it does with the personal data it processes regarding the people it supports, staff and volunteers, and members of the public, for example relatives or other professionals etc. This is called a privacy notice and there may be more than one privacy notice e.g. one notice for staff and one for the people you support. Your organisation's privacy notice(s) should be made available to these people and inform them about their rights under data protection legislation and how to exercise them. It is good practice to publish your privacy notice on your website if you have one. An example privacy notice is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/).	Yes
	Yes/No	New	**1.2.2**	New	Your organisation has a process to recognise and respond to individuals' requests to access their personal data.	Further guidance is available on the [NHSx website](https://www.nhsx.nhs.uk/information-governance/guidance/subject-access-requests/)	Yes	Your organisation has a process to recognise and respond to individuals' requests to access their personal data.	Further guidance is available on the [NHSx website](https://www.nhsx.nhs.uk/information-governance/guidance/subject-access-requests/)	Yes						
	Yes/No	New	**1.2.3**	New	Your organisation has procedures to handle an individual's objection to the processing of their personal data.	Further guidance is available on the [ICO website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/)	Yes									
	Yes/No	1.4.4	**1.2.4**	Newly mandatory cat 1 2, 3 and 4	Is your organisation compliant with the national data opt-out policy?	Please provide your published [compliance statement](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) e.g. within a privacy notice and/or Published Data Release Register in the comments box.	Yes	Is your organisation compliant with the national data opt-out policy?	Please provide your published [compliance statement](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) e.g. within a privacy notice and/or Published Data Release Register in the comments box.	Yes	Is your organisation compliant with the national data opt-out policy?	The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out. All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 30 September 2021. More detailed guidance that gives advice about compliance with the national data opt-out policy is available from [NHS Digital](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) and [Digital Social Care](https://www.digitalsocialcare.co.uk/national-data-opt-out/).	Yes	Is your organisation compliant with the national data opt-out policy?	The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. As a provider, you should help the people who use your services to understand that they can opt out of their data being used for other purposes. You should check that your policies, procedures, and privacy notice cover the opt out. All health and social care CQC-registered organisations in England must be compliant with the national data opt out by 30 September 2021. More detailed guidance that gives advice about compliance with the national data opt-out policy is available from [NHS Digital](https://digital.nhs.uk/services/national-data-opt-out-programme/compliance-with-the-national-data-opt-out) and [Digital Social Care](https://www.digitalsocialcare.co.uk/national-data-opt-out/).	Yes
Accountability and Governance in place for data protection and data security	Yes/No	1.2.1	**1.3.1**	No changes	Are there board-approved data security and protection policies in place that follow relevant guidance?	Confirm that you have policies, procedures and staff guidance in place that explain the organisation's plan or principles for data protection, DPIAs, Data protection by default, data sharing, data quality, records management, data security, registration authority, national data opt out, common law duties, professional codes, subject access requests, Freedom of Information and network security. Provide details of when each policy was updated.	Yes	Are there board-approved data security and protection policies in place that follow relevant guidance?	Confirm that you have policies, procedures and staff guidance in place that explain the organisation's plan or principles for data protection, data sharing, data quality, records management, data security, registration authority, national data opt out, common law duties, professional codes, subject access requests, Freedom of Information and network security. Provide details of when each policy was updated.	Yes	Does your organisation have up to date policies in place for data protection and for data and cyber security?	Confirm that your organisation has a policy or policies in place to cover: - data protection - data quality - record keeping - data security - where relevant, network security The policy or policies should be reviewed and approved by the management team or equivalent within the last 12 months. There is no set number of how many policies your organisation has to have on these topics as the different sizes and complexity of organisations means that some will have one all-encompassing policy, whilst others may have multiple policies. Policy templates are available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/)	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.	Yes

Yes/No	1.5.2	**1.3.2**	Reword for cat 1 and 2	Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	Your organisation should carry out spot checks that staff are doing what it says in the data protection, records management and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward.	Yes	Your organisation monitors your own compliance with data protection policies and regularly reviews the effectiveness of data handling and security controls.	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.	Yes	Does your organisation carry out regular data protection spot checks?	Your organisation should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward, if applicable. There is an example audit checklist that you can download from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/).	Yes	Does your organisation carry out regular data protection spot checks?	Your organisation should carry out spot checks that staff are doing what it says in the data protection and/or staff confidentiality policy or guidance. These should be undertaken at least every year. They could be part of other audits that you carry out. It is good practice to keep evidence that spot checks have been carried out, including details of any actions, who has approved the actions and who is taking them forward, if applicable. There is an example audit checklist that you can download from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/)	Yes
Yes/No	1.1.1	**1.3.3**	No changes	Has SIRO responsibility for data security been assigned?	There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.	Yes	Has SIRO responsibility for data security been assigned?	There is a board-level individual who has overall accountability for the security of networks and information systems and drives regular discussion at board-level.	Yes								
Yes/No	1.1.3	**1.3.4**	Reword for cat 1 and 2	Are there clear lines of responsibility and accountability to named individuals for data security and data protection?	Please provide details in the comments field.	Yes	Are there clear lines of responsibility and accountability to named individuals for data security and data protection?	Please provide details in the comments field.	Yes								
Text	1.8.1	**1.3.5**	No changes	Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Further guidance is available from the [National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/risk-management-collection)	Yes	Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility?	Further guidance is available from the [National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/risk-management-collection)	Yes								
Text	1.8.3	**1.3.6**	No longer mandatory cat 3	What are your top three data security and protection risks?	Record at a heading level	Yes	What are your top three data security and protection risks?	Record at a heading level	Yes	What are the top three data and cyber security risks in your organisation and how does your organisation plan to reduce those risks?	All organisations have risks and should be able to identify what they are. Thinking about your responses to all of the questions in the toolkit, consider which three areas carry the most risk for your organisation. Provide a brief headline for each risk and say what your organisation plans to do to reduce that risk.		What are the top three data and cyber security risks in your organisation and how does it plan to reduce those risks?	All organisations have risks and should be able to identify what they are. Thinking about your responses to all of the questions in the toolkit, consider which three areas carry the most risk for your organisation. Provide a brief headline for each risk and say what your organisation plans to do to reduce that risk.	
Yes/No	1.6.1	**1.3.7**	Reword for cat 1 and 2. Removed from cat 4	Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	The procedures should be approved by the board or equivalent and aim to ensure that only the minimum necessary personal data are processed and that processing is transparent allowing individuals to monitor what is being done with their data.	Yes	Your organisation has implemented appropriate technical and organisational measures to integrate data protection into your processing activities.	The procedures should be approved by the board or equivalent and aim to ensure that only the minimum necessary personal data are processed and that processing is transparent allowing individuals to monitor what is being done with their data.	Yes	Does your organisation's data protection policy describe how you keep personal data safe and secure?	Your policy should describe how your organisation considers privacy and data protection issues right at the start when embarking on a new project or process. This is called Data protection by design. This might be a new data sharing initiative for example if becoming part of a shared care record or if you are using personal data for a new purpose such as research. Your policy should also describe how your organisation only collect, use and share the minimum amount of data you need, how you limit access to only those how need to know, keep the data for a short time as possible and how you let people know what you do with their data. This is called 'data protection by default'. There is guidance on data protection by design and by default on the [ICO's website](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/). The Data Protection Policy template that is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/) covers this subject.	Yes				
Yes/No	1.6.5	**1.3.8**	Newly mandatory cat 1 and 2. Reword for cat 1 and 2	Your organisation understands when you must conduct a Data Protection Impact Assessment and has processes in place, which links to your existing risk management and project management, to action this.	[Information commissioner's office guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) is available	Yes	Your organisation understands when you must conduct a Data Protection Impact Assessment and has processes in place, which links to your existing risk management and project management, to action this.	[Information commissioner's office guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/) is available	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?	Your policy should describe the process that your organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data. For example, when you introduce a new care recording system; if you install CCTV; if you use new remote care or monitoring technology; if you share data for research or marketing purposes. This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the [Information Commissioner's Office (ICO)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).	Yes	Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?	Your policy should describe the process that your organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data. For example, when you introduce a new care recording system; if you install CCTV; if you use new remote care or monitoring technology; if you share data for research or marketing purposes. This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the [Information Commissioner's Office (ICO)](https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/).	
Yes/No	1.1.4	**1.3.9**	No changes	Is data security direction set at board level and translated into effective organisational practices?		Yes	Is data security direction set at board level and translated into effective organisational practices?		Yes	Is data security direction set at management level and translated into effective organisational practices?							
Document	1.2.3	**1.3.10**	Reword cat 1 and 2	How are data security and protection policies and Data Protection Impact Assessments made available to the public?	Provide the web link, but if not available online then record where they are available. Making your policies and DPIAs available to the public will assist you to meet the transparency requirements of GDPR unless this causes a security risk to the organisation.		How are data security and protection policies and Data Protection Impact Assessments made available to the public?	Provide the web link, but if not available online then record where they are available. Making your policies and DPIAs available to the public will assist you to meet the transparency requirements of GDPR unless this causes a security risk to the organisation.		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.		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.	
Yes/No	1.6.6	**1.3.11**	Removed from cat 1 and 2							If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?	The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g. if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced. If nobody uses their own devices, then tick and write "Not applicable" in the comments box. A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/social-care-technology/mobile-devices)	Yes				
Text	1.6.2	**1.3.12**	Removed from cat 1 and 2							How does your organisation make sure that paper records are safe when taken out of the building?	Paper records may be taken out of your organisation's building(s), for example for hospital appointments or visits to people's homes. Leaving documents in cars, for instance, can be risky. How does your organisation make sure paper records are kept safe when 'on the move'? If you do not have any paper records or do not take them off site, write "Not applicable" in the text box.	Yes				
Text	1.6.3	**1.3.13**	Removed from cat 1 and 2							Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.	Physical controls that support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc. Provide details at high level and, if you have more than one building, summarise how compliance is assured across your	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.	Yes
Text	1.6.4	**1.3.14**	Removed from cat 1 and 2							What does your organisation have in place to minimise the risks if mobile phones are lost, stolen, hacked or used inappropriately?	Smartphones are especially vulnerable to being lost or stolen. What has been put in place by your organisation to protect them to prevent unauthorised access? E.g. is there a PIN or fingerprint or facial scan? Is there an app set up to track the location of a lost/ stolen smartphone, and 'wipe' its contents remotely? You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile phones, write "Not applicable" in the text box. Guidance is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/social-care-	Yes				
Records are maintained appropriately	Yes/No	1.7.4	**1.4.1**	Reword cat 1 and 2	The organisation has a records management policy including a records retention schedule	The policy which sets out records management responsibilities, covers the whole record lifecycle including secure storage, tracking, transfer and disposal. The retention schedule is based on business need with reference to statutory requirements and [other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes	The organisation has a records management policy including a records retention schedule	The policy which sets out records management responsibilities, covers the whole record lifecycle including secure storage, tracking, transfer and disposal. The retention schedule is based on business need with reference to statutory requirements and [other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes	Does your organisation have a timetable which sets out how long you retain records for?	Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records. The timetable, or schedule as it sometimes called, should be based on [statutory requirements or other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes	Has a records retention schedule been produced?	Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records. The timetable, or schedule as it sometimes called, should be based on [statutory requirements or other guidance](https://www.nhsx.nhs.uk/information-governance/guidance/records-management-code/).	Yes
Text	1.7.5	**1.4.2**	Removed cat 1 and 2, new for cat 3.							If your organisation uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed since 1st July 2021? This contract should meet the requirements set out in data protection regulations.	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If your organisation uses a contractor to destroy any records or equipment, such as a document shredding company or IT recycling organisation, then the contract(s) or other written confirmation with third parties must include the requirement to have appropriate security measures and the facility to allow audit by your organisation. Further information about the destruction of records is in chapter 5 of the Records Management Code of Practice. If you do not use third parties to destroy records or equipment, then tick and write "Not applicable" in the comments box. Advice on contracts for secure disposal of personal data is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latestguidance/contract-guidance/).	Yes				

	Text	1.7.3	**1.4.3**	Removed from Cat 1 and 2 (which becomes new question 1.1.8)							If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely. If you do not destroy records or equipment yourselves, or only use a third party to do so, write "Not applicable" in the text box. [Digital Social Care](https://www.digitalsocialcare.co.uk//latest-	Yes	If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?	It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks. If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely. If you do not destroy records or equipment yourselves, or only use a third party to do so, write "Not applicable" in the text box.	
Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards	Yes/No	2.2.1	**2.1.1**	No changes	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.	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.	Yes	Does your organisation have an induction process that covers data security and protection, and cyber security?	All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date. There is an 'Introduction to Information Sharing for Staff' available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/).	Yes	Does your organisation have an induction process that covers data security and protection, and cyber security?	All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date.	Yes
	Yes/No	2.2.2	**2.1.2**	No changes	Do all employment contracts contain data security requirements?	Please provide any explanatory text in the comments box	Yes	Do all employment contracts contain data security requirements?	Please provide any explanatory text in the comments box	Yes	Do all employment contracts, and volunteer agreements, contain data security requirements?	Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality. Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security. There is an example staff contract clause available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/).	Yes	Do all employment contracts, and volunteer agreements, contain data security requirements?	Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality. Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security.	Yes
	Text	2.2.3	**2.1.3**	No changes	The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.		The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.		The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.		The results of staff awareness surveys on staff understanding of data security are reviewed to improve data security.	Using the [staff awareness questions](https://www.dsptoolkit.nhs.uk/Help/21) either through the Data Security Awareness training or local materials.	
There has been an assessment of data security and protection training needs across the organisation	Yes/No	3.1.1	**3.1.1**	Wording change (date only)	Has an approved organisation-wide data security and protection training needs analysis been completed after 1 July 2021?	This is an assessment of data security and protection training (including records management and Subject access requests) and development needs for all your staff including Board Members. Approved by your SIRO or equivalent.	Yes	Has an approved organisation-wide data security and protection training needs analysis been completed after 1 July 2021?	This is an assessment of data security and protection training and development needs for all your staff including Board Members. Approved by your SIRO or equivalent.	Yes	Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st July 2021?	A training needs analysis is a process which helps identify the data security and protection, and cyber security, training and development needs across your organisation. Your organisation's training needs analysis should identify the level of training or awareness raising required by your staff, directors, trustees and volunteers if you have them. It should be reviewed and/or approved annually by the person(s) with overall responsibility for data security and protection within your organisation. An example training needs analysis is available to download from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/).	Yes			
Staff pass the data security and protection mandatory test	Yes/No	3.2.1	**3.2.1**	Wording change (date only)	Have at least 95% of all staff, completed their annual Data Security Awareness Training?	Please provide your highest percentage figure for the period 1st July 2021 - 30th June 2022 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.	Yes	Have at least 95% of all staff, completed their annual Data Security Awareness Training?	Please provide your highest percentage figure for the period 1st July 2021 - 30th June 2022 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.	Yes	Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st July 2021?	All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year. Your organisation's training needs analysis should identify the level of training or awareness raising that people need. There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it might not be possible for 100% of people to receive training every year. Therefore, the target is 95% of people with access to personal data. [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/train-staff-to-be-cyber-aware/) provides guidance on training, including sources of free online data and cyber security training.	Yes	Have at least 95% of staff, completed training on data security and protection, and cyber security, since 1st July 2021?	All people in your organisation with access to personal data must complete appropriate data security and protection, and cyber security, training every year. Your organisation's training needs analysis should identify the level of training or awareness raising that people need. There is an understanding that due to illness, maternity/paternity leave, attrition or other reasons it might not be possible for 100% of people to receive training every year. Therefore, the target is 95% of people with access to personal data.	Yes
Staff with specialist roles receive data security and protection training suitable to their role	Text	3.3.1	**3.3.1**	No changes	Provide details of any specialist data security and protection training undertaken.	Details of any additional training as identified by your Data Security Training Needs analysis. Such as staff with roles in Informatics (IT and Information areas), Records Management, Clinical Coding & Information Governance (including privacy / confidentiality & data protection).	Yes	Provide details of any specialist data security and protection training undertaken.	Details of any additional training as identified by your Data Security Training Needs analysis. Such as staff with roles in Informatics (IT and Information areas), Medical Records, Clinical Coding & Information Governance (including privacy / confidentiality & data protection).	Yes	Provide details of any specialist data security and protection training undertaken.	Details of any additional training as identified by your Data Security Training Needs analysis. Such as staff with roles as Caldicott Guardian, in Informatics (IT and Information areas), Medical Records, Clinical Coding & Information Governance (including privacy / confidentiality & data protection).				
	Yes/No	3.3.2	**3.3.2**	No changes	The organisation has appropriately-qualified technical cyber security specialist staff and/or service.	See guidance within [big picture guide 3.](https://www.dsptoolkit.nhs.uk/Help/23)	Yes	The organisation has appropriately-qualified technical cyber security specialist staff and/or service.	See guidance within [big picture guide 3.](https://www.dsptoolkit.nhs.uk/Help/23)	Yes						
	Yes/No	3.3.3	**3.3.3**	No changes	The organisation has a nominated member of the Cyber Associates Network.	Further details are available on the [NHS Digital website.](https://digital.nhs.uk/services/data-security-centre/cyber-associates-network)	Yes	The organisation has a nominated member of the Cyber Associates Network.	Further details are available on the [NHS Digital website.](https://digital.nhs.uk/services/data-security-centre/cyber-associates-network)	Yes						
Leaders and board members receive suitable data protection and security training	Yes/No	3.4.1	**3.4.1**	No changes	Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	As defined in your organisations data security and protection training needs analysis.	Yes	Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	As defined in your organisations data security and protection training needs analysis.	Yes	Have the people with responsibility for data security and protection received training suitable for their role?	It is likely that the person or people within your organisation who are responsible for data security and protection will need additional and more in depth training than the majority of your staff. Your organisation's training needs analysis should identify any additional training required by people with increased data security and protection responsibilities or specialist roles, for example a Data Protection Officer (DPO).	Yes			
	Yes/No	New	**3.4.2**	New	All board members have completed appropriate data security and protection training?	As defined in your organisation's data security and protection training needs analysis. All Board members are current permanent working board members (for example board members who are sick should not be included).	Yes	All board members have completed appropriate data security and protection training.	As defined in your organisations data security and protection training needs analysis. All Board members are current permanent working board members (for example board members who are sick should not be included).	Yes						
The organisation maintains a current record of staff and their roles	Yes/No	4.1.1	**4.1.1**	No changes	Your organisation maintains a record of staff and their roles.		Yes	Your organisation maintains a record of staff and their roles.		Yes	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.	Yes	Does your organisation have an up to date record of people and their roles?	Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers. This might be linked to your existing payroll or rostering system.	Yes
	Yes/No	4.1.2	**4.1.2**	No changes	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Each system may use its own user list(s) or use federated access. There may be systems where technically or operationally it is not possible to have individual logins but there are alternative methods of maintaining user lists. Where this occurs, it is understood and risk assessed by the organisation.	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?	Each system may use its own user list(s) or use federated access. There may be systems where technically or operationally it is not possible to have individual logins but there are alternative methods of maintaining user lists. Where this occurs, it is understood and risk assessed by the organisation.	Yes	Does your organisation know who has access to personal and confidential data through its IT system(s)?	Your organisation should know who has access to the personal and confidential data in its IT system(s). Each person needs to have their own account to access a system. If that is not currently possible, and users share a login, the organisation must risk assess the situation and agree a plan to end the use of shared logins. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box.	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.	Yes
	Yes/No	4.1.3	**4.1.3**	No changes	Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?			Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?								
The organisation assures good management and maintenance of identity and access control for it's networks and information systems	Date	4.2.1	**4.2.1**	No changes	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.	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.	Yes						
	Document	4.2.2	**4.2.2**	No changes	Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data were too high or too low. Do not name individuals.		Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data were too high or too low. Do not name individuals.		Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.	This can be an incident either where the staff member's rights to data were too high or too low. Do not name individuals.				
	Yes/No	4.2.3	**4.2.3**	Wording change cat 1 and 2.	Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Organisations should consider the ability to trace an incident end to end e.g. network address translation. Please refer to [National Cyber Security Centre guidance.](https://www.ncsc.gov.uk/files/NCSC_SOC_Feeds.pdf)	Yes	Logs are retained for a sufficient period, managed securely, reviewed regularly and can be searched to identify malicious activity.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. Organisations should consider the ability to trace an incident end to end e.g. network address translation. Please refer to [National Cyber Security Centre guidance.](https://www.ncsc.gov.uk/files/NCSC							
	Yes/No	4.2.5	**4.2.4**	No changes	Are unnecessary user accounts removed or disabled?	Former employees', guest and other unnecessary accounts are routinely and promptly removed or disabled from internal workstations, Active Directory domains and other user directories. Privileged user access is also removed when no longer required or appropriate.	Yes	Are unnecessary user accounts removed or disabled?	Former employees', guest and other unnecessary accounts are routinely and promptly removed or disabled from internal workstations, Active Directory domains and other user directories. Privileged user access is also removed when no longer required or appropriate.	Yes	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box	Yes	Does your organisation have a reliable way of removing or amending people's access to IT systems when they leave or change roles?	When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people's access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses.	Yes
All staff understand that their activities on IT systems will be monitored and recorded for security purposes	Yes/No	4.3.1	**4.3.1**	No longer mandatory cat 3	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 a agreement affirming the highest standard of use.	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 a agreement affirming the highest standard of use.	Yes	Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?	The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others. This requirement applies to IT system administrators working in external companies who support your organisation's IT systems. This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.		Have all the administrators of your organisation's IT system(s) signed an agreement to hold them accountable to higher standards?	The people within your organisation who are IT system administrators may have access to more information than other staff. Therefore, they need to be held accountable in a formal way to higher standards of confidentiality than others. This requirement applies to IT system administrators working in external companies who support your organisation's IT systems This formal agreement could be part of a job description or a contract with your IT support company and/or systems supplier/s. If your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.	Yes

	Text	4.3.2	**4.3.2**	No changes	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Please provide details. For critical systems you should consider if device authentication is required.	Yes	Are users, systems and (where appropriate) devices always identified and authenticated prior to being permitted access to information or systems?	Please provide details. For critical systems you should consider if device authentication is required.	Yes								
	Yes/No	4.3.5	**4.3.3**	No changes	Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.		Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.		Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.		Have all staff been notified that their system use could be monitored?	Staff are informed and understand that their system use can be monitored and recorded. The notification method is periodic.	Yes		
You closely manage privileged user access to networks and information systems supporting the essential service	Yes/No	New	**4.4.1**	New	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. [Guidance from NCSC](https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide) on maintaining security of logs is available. Note: you are not expected to purchase a CSOC.	Yes	The organisation ensures that logs, including privileged account use, are kept securely and only accessible to appropriate personnel. They are stored in a read only format, tamper proof and managed according to the organisation information life cycle policy with disposal as appropriate.	Organisational policy should set out the rules defining log retention. The average time to detect a cyber attack is over three months and it is not uncommon for incidents to take significantly longer to detect. The most important logs for identifying malicious activity should be held for six months as a minimum. [Guidance from NCSC](https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide) on maintaining security of logs is available. Note: you are not expected to purchase a CSOC.		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 your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.		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 your organisation does not use any IT systems, then 'tick' and write "Not applicable" in the comments box.		
	Yes/No	4.4.3	**4.4.2**	Non-material wording change cat 1 and 2	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 email and web browsing.	Provide details in the comments section	Yes	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 email and web browsing.	Provide details in the comments section	Yes								
	Yes/No	4.4.4	**4.4.3**	Non-material wording change cat 1 and 2	The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	Explain any exceptions or risk management applied.		The organisation only allows privileged access to be initiated from devices owned and managed or assured by your organisation	Explain any exceptions or risk management applied.									
You ensure your passwords are suitable for the information you are protecting	Yes/No	4.5.1	**4.5.1**	Newly mandatory cat 2	Do you have a password policy giving staff advice on managing their passwords?	The password policy must cover: (a) How to avoid choosing obvious passwords (such as those based on easily-discoverable information). (b) Not to choose common passwords (use of technical means, such as using a password blacklist, is recommended). (c) No password reuse. (d) Where and how they may record passwords to store and retrieve them securely. (e) If password management software is allowed, and if so, which. (f) Which passwords they really must memorise and not record anywhere. (g) Assessing risks to ensure systems use appropriate authentication measures e.g. high-strength passwords enforced technically for all users of internet-facing authentication services.	Yes	Do you have a password policy giving staff advice on managing their passwords?	The password policy must cover: (a) How to avoid choosing obvious passwords (such as those based on easily-discoverable information). (b) Not to choose common passwords (use of technical means, such as using a password blacklist, is recommended). (c) No password reuse. (d) Where and how they may record passwords to store and retrieve them securely. (e) If password management software is allowed, and if so, which. (f) Which passwords they really must memorise and not record anywhere. (g) Assessing risks to ensure systems use appropriate authentication measures e.g. high-strength passwords enforced technically for all users of internet-facing authentication services.	Yes								
	Yes/No	4.5.2	**4.5.2**	Newly mandatory cat 2	Technical controls enforce password policy and mitigate against password-guessing attacks.	Examples of technical controls are [provided by the National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/passwords)	Yes	Technical controls enforce password policy and mitigate against password-guessing attacks.	Examples of technical controls are [provided by the National Cyber Security Centre.](https://www.ncsc.gov.uk/collection/passwords)	Yes								
	Yes/No	4.5.3	**4.5.3**	No changes	Multifactor authentication is used [wherever technically feasible].	Multifactor authentication can include hardware-based certificates. This applies to end user devices. [Where it is not possible to apply multifactor authentication, this should be considered in your response to 9.5.9]	Yes	Multifactor authentication is used [wherever technically feasible].	Multifactor authentication can include hardware-based certificates. This applies to end user devices.									
	Text	4.5.4	**4.5.4**	No changes	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.		Yes	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength.		Yes	How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?	If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be 'strong' i.e. hard to guess. This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password. If your organisation does not use any IT systems, computers or other devices, write "Not applicable" in the text box. Information about good password practice is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/).	Yes						
	Yes/No	4.5.5	**4.5.5**	Reword cat 1 and 2	Does your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is it planning to do so?			Does your organisation, or your supply chain with access to your systems, grant limited privileged access and third party access only for a limited time period, or is it planning to do so?			Do you ensure that passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and should have high strength?							
Process reviews are held at least once per year where data security is put at risk and following data security incidents	Yes/No	5.1.1	**5.1.1**	Non-material wording change cat 1 and 2	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security or protection incident, with findings acted upon.	Explain, in the comments, how any incident response and management tests/process review findings tests have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again.	Yes	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security or protection incident, with findings acted upon.	Explain, in the comments, how any incident response and management tests/process review findings tests have informed the immediate future technical protection and remediated any systemic vulnerabilities of the system or service, to ensure identified issues cannot arise in the same way again.	Yes	If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?	Confirm that your organisation has reviewed any processes that have caused a breach or a near miss, or which force people to use unauthorised workarounds that could compromise your organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. It is good practice to review processes annually even if a breach or near miss has not taken place. If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.	Yes	If your organisation has had a data breach or a near miss in the last year, has the organisation reviewed the process that may have allowed the breach to occur?	Confirm that your organisation has reviewed any processes that have caused a breach or a near miss, or which force people to use unauthorised workarounds that could compromise your organisation's data and cyber security. Workarounds could be things such as using unauthorised devices such as home computers or personal memory sticks or forwarding emails to personal email addresses. It is good practice to review processes annually even if a breach or near miss has not taken place. If no breaches or near misses in the last 12 months then please tick and write "Not applicable" in the comments box.	Yes
	Document	5.1.3	**5.1.3**	No changes	List of actions arising from each process review, with names of actionees.	For each process review a list of actions should be produced with each action having an owner. If no actions mark none in other text.		List of actions arising from each process review, with names of actionees.	For each process review a list of actions should be produced with each action having an owner. If no actions mark none in other text.		List of actions arising from each process review, with names of actionees.	For each process review a list of actions should be produced with each action having an owner. If no actions mark none in other text.						
Participation in reviews is comprehensive, and clinicians are actively involved	Document	5.2.1	**5.2.1**	No changes	Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.	An example of a scanned registration sheet, photo or minutes. The attendees should be from a multi-disciplinary team with active clinical involvement for care related processes and systems.		Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.	An example of a scanned registration sheet, photo or minutes. The attendees should be from a multi-disciplinary team with active clinical involvement for care related processes and systems.		Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.	An example of a scanned registration sheet, photo or minutes. The attendees should be from a multi-disciplinary team with active clinical involvement for care related processes and systems.						
Action is taken to address problem processes as a result of feedback at meetings or in year	Yes/No	5.3.1	**5.3.1**	No changes	Are the actions to address problem processes, 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, such as through reports and briefing notes, during the last twelve months.		Are the actions to address problem processes, 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, such as through reports and briefing notes, during the last twelve months.		Are the actions to address problem processes, being monitored and assurance given to the senior team?	Explain the governance around escalation of any issues and findings to the board, or equivalent, such as through reports and briefing notes, during the last twelve months.		Are the actions to address problem processes, being monitored and assurance given to the senior team?	Explain the governance around escalation of any issues to management through reports and briefing notes during the last twelve months.		
A confidential system for reporting data security and protection breaches and near misses is in place and actively used	Yes/No	6.1.1	**6.1.1**	No changes	A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.	Confirmation that a functioning data security and protection breach reporting and management mechanism is in place including use of the DSP Toolkit incident reporting tool	Yes	A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.	Confirmation that a functioning data security and protection breach reporting and management mechanism is in place including use of the DSP Toolkit incident reporting tool	Yes	Does your organisation have a system in place to report data breaches?	All staff, and volunteers if you have them, are responsible for noticing and reporting data breaches and it is vital that you have a robust reporting system in your organisation. There is an incident reporting tool within this toolkit which should be used to report health and care incidents to Information Commissioner's Office ICO. If you are not sure whether or not to inform the Information Commissioner's Office of a breach, the toolkit's incident reporting tool and guide can help you to decide.	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.	Yes	
	Yes/No	6.1.4	**6.1.3**	No changes	Is the board or equivalent notified of the action plan for all data security and protection breaches?	Outline in the comments, the processes of notifying the board.	Yes	Is the board or equivalent notified of the action plan for all data security and protection breaches?	Outline in the comments, the processes of notifying the board.	Yes	If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?	In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. If no breaches in the last 12 months then please tick and write "Not applicable" in the comments box.	Yes	If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?	In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt. If no breaches have occurred in the last 12 months then please tick and write "Not applicable" in the comments box.		
	Yes/No	6.1.5	**6.1.4**	No changes	Individuals affected by a breach are appropriately informed.	Data subjects are appropriately informed of data breaches in [accordance with guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/). If no breaches then please tick and state "No breaches".	Yes	Individuals affected by a breach are appropriately informed.	Data subjects are appropriately informed of data breaches in [accordance with guidance](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/). If no breaches then please tick and state "No breaches".	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible. If your organisation has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box. More information is available from the [Information Commissioner's Office](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/).	Yes	If your organisation has had a data breach, were all individuals who were affected informed?	If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible. If your organisation has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box. More information is available from the [Information Commissioner's Office](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/).	Yes
All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway	Yes/No	6.2.3	**6.2.1**	No changes	Has antivirus/anti-malware 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, tablets and mobile devices running windows desktop operating systems. Please include the name of your anti-virus product in the comments.	Yes	Has antivirus/anti-malware 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, tablets and mobile devices running windows desktop operating systems. Please include the name of your anti-virus product in the comments.	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?	This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box. Further information is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/).	Yes	Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?	This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box. Further information is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/).	Yes

	Yes/No	6.2.4	**6.2.3**	Newly mandatory cat 2	Antivirus/anti-malware is kept continually up to date.	Provide an explanation of how this is achieved. This could be through automatic update, central deployment, ATP etc.	Yes	Antivirus/anti-malware is kept continually up to date.	Provide an explanation of how this is achieved. This could be through automatic update, central deployment, ATP etc.	Yes						
	Yes/No	6.2.5	**6.2.4**	No changes	Antivirus/anti-malware software scans files automatically upon access.	This includes when files are downloaded and opened, and when they are accessed from a network folder.	Yes	Antivirus/anti-malware software scans files automatically upon access.	This includes when files are downloaded and opened, and when they are accessed from a network folder.							
	Yes/No	6.2.6	**6.2.5**	No changes	Connections to malicious websites on the Internet are prevented.	This applies to all corporate devices. It may be achieved by one or more of the following using a web proxy, antivirus/anti-malware, browser tools, Protective DNS services, blacklisting or other mechanisms.	Yes	Connections to malicious websites on the Internet are prevented.	This applies to all corporate devices. It may be achieved by one or more of the following using a web proxy, antivirus/anti-malware, browser tools, Protective DNS services, blacklisting or other mechanisms.							
	Text	6.2.9	**6.2.6**	No changes	Number of phishing emails reported by staff per month.	From your service desk system or service the number of reported phishing mails.		Number of phishing emails reported by staff per month.	From your service desk system or service the number of reported phishing mails.		Number of phishing emails reported by staff per month.	From your service desk system or service the number of reported phishing mails.				
	Yes/No	6.2.10	**6.2.7**	No changes	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?	This applies to: email, Servers, desktop computers, laptop computers; tablets and mobile phones. Provide details of how this is enforced.	Yes									
	Yes/No	6.2.11	**6.2.8**	No changes	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.	This applies to email systems	Yes	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.	This applies to email systems	Yes						
	Yes/No	6.2.12	**6.2.9**	No changes	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	This applies to email systems and should include the name of the filtering product.	Yes	You have implemented spam and malware filtering, and enforce DMARC on inbound email.	This applies to email systems and should include the name of the filtering product.	Yes						
Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses	Text	6.3.1	**6.3.1**	No changes	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). Known vulnerabilities are those listed on the [Cyber alerts portal](https://digital.nhs.uk/cyber-alerts). If no incidents have occurred, state: "None".	Yes	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). Known vulnerabilities are those listed on the [Cyber alerts portal](https://digital.nhs.uk/cyber-alerts). If no incidents have occurred, state: "None".	Yes	If you have had a data security incident, was it caused by a known vulnerability?	Provide details of incidents over the reporting period (a year). If no incidents have occurred state "None".				
	Yes/No	6.3.2	**6.3.2**	Reword cat 1 and 2	The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Your response should cover 'high severity' cyber alerts issued over the last 12 months.	Yes	The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.	Your response should cover 'high severity' cyber alerts issued over the last 12 months.	Yes	Have staff, directors, trustees and volunteers been advised that use of public Wi-Fi for work purposes is unsafe?	Use of public Wi-Fi (e.g. Wi-Fi freely available at cafes and train stations etc) or unsecured Wi-Fi (Wi-Fi where no password is required to access it) could be unsafe and lead to unauthorised access of personal data. Staff, directors, trustees and volunteers if you have them, should be advised of this. If nobody uses mobile devices for work purposes out of your building/offices, then tick and write “Not applicable” in the comments box.	Yes			
	Text	6.3.3	**6.3.3**	No changes	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Since 1st July 2021, all systems monitoring requirements have been assessed.	Yes	The organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Since 1st July 2021, all systems monitoring requirements have been assessed.	Yes						
	Yes/No	6.3.5	**6.3.4**	No changes	Are all new digital services that are attractive to cyber criminals (such as for fraud) implementing transactional monitoring techniques from the outset?	Includes an assessment of which services are susceptible to fraud. If none, please 'tick' and explain in the comments section.	Yes	Are all new digital services that are attractive to cyber criminals (such as for fraud) implementing transactional monitoring techniques from the outset?	Includes an assessment of which services are susceptible to fraud. If none, please 'tick' and explain in the comments section.	Yes						
	Text	6.3.6	**6.3.5**	No changes	Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.		Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.		Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.		Have you had any repeat data security incidents within the organisation during the past twelve months?	A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within three calendar months of a previous occurrence. Provide details.	
Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services	Document	7.1.1	**7.1.1**	No changes	Your organisation understands the health and care services it provides.	This should cover: i. What their key operational services are, ii. What technologies and services their operational services rely on to remain available and secure, iii. What other dependencies the operational services have (power, cooling, data, people etc.), iv. The impact of loss of availability of the service	Yes	Your organisation understands the health and care services it provides.	This should cover: i. What their key operational services are, ii. What technologies and services their operational services rely on to remain available and secure, iii. What other dependencies the operational services have (power, cooling, data, people etc.), iv. The impact of loss of availability of the service	Yes	Organisations understand the health and care services they provide.	This should cover: i. What their key operational services are, ii. What technologies and services their operational services rely on to remain available and secure, iii. What other dependencies the operational services have (power, cooling, data, people etc.), iv. The impact of loss of availability of the service				
	Yes/No	7.1.2	**7.1.2**	No changes	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.	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.	Yes	Does your organisation have a business continuity plan that covers data and cyber security?	Your organisation’s business continuity plan should cover data and cyber security – for example what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g. through fire). An example business continuity plan is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/).	Yes	Does your organisation have a business continuity plan that covers data and cyber security?	Your organisation’s business continuity plan should cover data and cyber security – for example what would you do to ensure continuity of service if: you had a power cut; the phone line/internet went down; you were hacked; a computer broke down; the office became unavailable (e.g. through fire).	Yes
	Yes/No	7.1.3	**7.1.3**	No changes	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.			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.			You understand the resources and information that will be needed if there is a data security incident and arrangements are in place to make these resources available.					
	Text	7.1.4	**7.1.4**	No changes	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.			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.								
There is an effective test of the continuity plan and disaster recovery plan for data security incidents	Text	7.2.1	**7.2.1**	No changes	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.	This should be since 1st July 2021 with active board and business representation. Exercise scenarios should be based on incidents experienced by your and other organisations, or are composed using threat intelligence.	Yes	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.	This should be since 1st July 2021 with active board and business representation. Exercise scenarios should be based on incidents experienced by your and other organisations, or are composed using threat intelligence.	Yes	How does your organisation test the data and cyber security aspects of its business continuity plan?	Describe how your organisation tests these aspects of its plan and what the outcome of the exercise was the last time you did this. This should be since 1st July 2021. Guidance for testing your business continuity plan for the data and cyber security aspects is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/).	Yes			
	Document	7.2.4	**7.2.2**	No changes	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Each action should have an owner and timescale.	Yes	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Each action should have an owner and timescale.	Yes	From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item.	Each action should have an owner and timescale.				
You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions	Text	7.3.1	**7.3.1**	No changes	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Advice is available from NHS Digital or a cyber incident response company.	Yes	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Advice is available from NHS Digital or a cyber incident response company.	Yes	How does your organisation make sure that there are working backups of all important data and information?	It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation’s back up systems work and how you have tested them. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, write “Not applicable” in the text box. For advice about backups, see [Digital Social	Yes			
	Yes/No	7.3.2	**7.3.2**	No changes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Contacts include phone number as well as email.	Yes
	Yes/No	7.3.3	**7.3.3**	No changes	Are draft press materials for data security incidents ready?	The press materials you have such as skeleton press statements in the eventuality of an incident.		Are draft press materials for data security incidents ready?	The press materials you have such as skeleton press statements in the eventuality of an							
	Yes/No	7.3.4	**7.3.4**	No changes	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 backup, testing and review process is effective.	Yes	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 backup, testing and review process is effective.	Yes	Are backups routinely tested to make sure that data and information can be restored?	It is important that your organisation’s backups are tested at least annually to make sure data and information can be restored (in the event of equipment breakdown for example). You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, then tick and write “Not applicable” in the	Yes	How does your organisation make sure that there are working backups of all important data and information?	It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation’s back up systems work and how you have tested them. You may need to ask your IT supplier to assist with answering this question.	Yes
	Text	7.3.5	**7.3.5**	Reword for cat 1 and 2	Do you test your backups regularly to ensure you can restore the service from a backup?	Backups should be tested frequently. The example provided may relate to a live or test environment.	Yes	Do you test your backups regularly to ensure you can restore the service from a backup?	Backups should be tested frequently. The example provided may relate to a live or test environment.	Yes						
	Yes/No	7.3.6	**7.3.6**	Reword for cat 1, 2 and 3	Are your backups kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose?	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)	Yes	Are your backups kept securely and separate from your network ('offline'), or in a cloud service designed for this purpose?	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)	Yes	Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose?	Cloud synching services, such as OneDrive, SharePoint or Google Drive, should not be used as your only backup and stored backup should not be permanently connected to your network. Further guidance is available from the [National Cyber Security Centre](https://www.ncsc.gov.uk/blog-post/offline-backups-in-an-online-world)				
All software and hardware has been surveyed to understand if it is supported and up to date	Document	8.1.1	**8.1.1**	No changes	Provide evidence of how the organisation tracks and records all software assets and their configuration.	This is a list of all the software that is used in the organisation including version numbers and whether the software is supported i.e. it still receives security updates.	Yes	Provide evidence of how the organisation tracks and records all software assets and their configuration.	This is a list of all the software that is used in the organisation including version numbers and whether the software is supported i.e. it still receives security updates.	Yes						
	Yes/No	8.1.2	**8.1.2**	No changes	Does the organisation track and record all end user devices and removable media assets?	e.g. You hold an up to date list of all your end user devices and removable media.	Yes	Does the organisation track and record all end user devices and removable media assets?	e.g. You hold an up to date list of all your end user devices and removable media.	Yes	Does the organisation track and record all end user devices and removable media assets?	e.g. You hold an up to date list of all your end user devices and removable media.				
	Yes/No	8.1.3	**8.1.3**	Newly mandatory cat 2	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.	Provide summary details in the comments box. Documentation should be held locally for protections for these devices . This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes	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.	Provide summary details in the comments box. Documentation should be held locally for protections for these devices . This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers; desktop computers; laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes						

	Yes/No	8.1.4	**8.1.4**	No changes	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.	Covers software running on computers that are connected to the internet.					Are all the IT systems and the software used in your organisation still supported by the manufacturer or the risks are understood and managed?	Systems and software that are no longer supported by the manufacturer can be unsafe as they are no longer being updated to protect against viruses for example. You may need to ask your IT supplier to assist with answering this question. Examples of unsupported software include: Windows XP, Windows Vista, Windows 7, Java or Windows Server 2008. Windows 8.1 is supported until January 2023. Windows 10 is supported and is the most up to date version of Windows. This question also applies to software systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems or software, then tick and write "Not applicable" in the comments box. For guidance (including information on how to check which software versions you have), see [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-	Yes			
Unsupported software and hardware is categorised and documented, and data security risks are identified and managed	Document	8.2.1	**8.2.1**	No changes	List any unsupported software prioritised according to business risk, with remediation plan against each item.	Unsupported software is software which is no longer receiving security updates e.g. Windows XP, Java or Windows Server 2008. Unsupported software is less secure and so poses a larger risk to your organisation. The unsupported software list will comprise of the results of the software survey where the software is not supported/updated.	Yes	List any unsupported software prioritised according to business risk, with remediation plan against each item.	Unsupported software is software which is no longer receiving security updates e.g. Windows XP, Java or Windows Server 2008. Unsupported software is less secure and so poses a larger risk to your organisation. The unsupported software list will comprise of the results of the software survey where the software is not supported/updated.	Yes	If your answer to 8.1.4 (on IT systems and software being supported by the manufacturer) was that software risks are being managed, please provide a document that summarises the risk of continuing to use each unsupported item, the reasons for doing so and a summary of the action your organisation is taking to minimise the risk.	This is a conscious decision to accept and manage the associated risks of unsupported systems. This document should indicate that your board or management team have formally considered the risks of continuing to use unsupported items and have concluded that the risks are acceptable. If your answer to the previous question was yes, write "Not	Yes			
	Yes/No	8.2.2	**8.2.2**	Reword cat 1 and 2	The SIRO confirms that the risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.	The SIRO has been briefed on the unsupported systems and has made a conscious decision to accept and manage the associated risks. A report has been provided to the board in the last 12 months. If no unsupported systems please tick and state "No unsupported systems" as a comment.	Yes	The SIRO confirms that the risks of using unsupported systems are being managed and the scale of unsupported software is reported to your board along with the plans to address.	The SIRO has been briefed on the unsupported systems and has made a conscious decision to accept and manage the associated risks. A report has been provided to the board in the last 12 months. If no unsupported systems please tick and state "No unsupported systems" as a comment.	Yes						
Supported systems are kept up-to-date with the latest security patches	Document	8.3.1	**8.3.1**	No changes	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.	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.	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.	Yes
	Text	8.3.2	**8.3.2**	No changes	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Remote endpoints being those devices or computers that are not on the core network (such as home or mobile workers). Provide the usual number of days between one wave of remote patching and the next.	Yes	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Remote endpoints being those devices or computers that are not on the core network (such as home or mobile workers). Provide the usual number of days between one wave of remote patching and the next.	Yes	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Remote endpoints being those devices or computers that are not on the core network (such as home or mobile workers). Provide the usual number of days between one wave of remote patching and the next.				
	Yes/No	8.3.3	**8.3.3**	No changes	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Provide details in the comments box. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.	Yes	There is a documented approach to applying security updates (patches) agreed by the SIRO.	Provide details in the comments box. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud	Yes						
	Yes/No	8.3.4	**8.3.4**	No changes	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.	Provide summary details in the comments box. Documentation should be held locally for all security patches. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are unable to be patched should be captured under 8.1.3. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes	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.	Provide summary details in the comments box. Documentation should be held locally for all security patches. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services. Devices that are unable to be patched should be captured under 8.1.3. Devices that are standalone or air-gapped should be captured under 9.5.9.	Yes						
	Text	New	**8.3.5**	New	Where a security patch has been classed as critical or high-risk vulnerability has not been applied, explain the technical remediation and risk management that has been undertaken.	Provide details for each patch not applied. This applies to any device (managed internally or by a third party) that has the ability to connect to the Internet including application servers, desktop computers, laptop computers, tablets and mobile devices running windows desktop operating systems. Example routes to the Internet include (but are not limited to) HSCN, N3/Transition network, VPNs, or cloud computing services.	**Yes**				How does your organisation make sure that the latest software updates are downloaded and installed?	It is important that your organisation's IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any IT systems, devices or software, write "Not applicable" in the text box. Further information is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/).	Yes			
	Yes/No	8.3.5	**8.3.6**	Changed to yes/no	Is your organisation actively using and managing Advanced Threat Protection (ATP) or equivalent?	e.g. using NHS Digital Endpoint Detection and Response. Please provide details of the product used in the comments.		Is your organisation actively using and managing Advanced Threat Protection (ATP) or equivalent?	e.g. using NHS Digital Endpoint Detection and Response. Please provide details of the product used in the comments.							
	Document	New	**8.3.7**	New	Are 95% of your server estate and 98% of your desktop estate on supported versions of operating systems?	Please upload a screenshot/s from Advanced Threat Protection (ATP) demonstrating the percentage of servers and desktops on supported versions of operating systems. If not met, please provide details in the comments on the plan to achieve 95% of your server estate and 98% of your desktop estate on supported versions of operating systems.		Are 95% of your server estate and 98% of your desktop estate on supported versions of operating systems?	Please upload a screenshot/s from Advanced Threat Protection (ATP) demonstrating the percentage of servers and desktops on supported versions of operating systems. If not met, please provide details in the comments on the plan to achieve 95% of your server estate and 98% of your desktop estate on supported versions of operating systems.							
You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service	Text	8.4.1	**8.4.1**	No changes	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).	Yes	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).	Yes	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Explain at a summary level. Where it is not possible to apply these measures, explain any mitigations (such as logical separation).				
	Yes/No	8.4.2	**8.4.2**	No changes	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Covers software running on computers that are connected to or capable of connecting to the Internet. Unsupported software should be covered under 8.3.4.	Yes	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Covers software running on computers that are connected to or capable of connecting to the Internet. Unsupported software should be covered under 8.3.4.	Yes	All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support.	Covers software running on computers that are connected to or capable of connecting to the Internet.				
	Yes/No	8.4.3	**8.4.3**	No changes	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	This may include NHS Digital's VMS and / or Bitsight service.		You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.	This may include NHS Digital's VMS and / or Bitsight service.		You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.					
All networking components have had their default passwords changed	Yes/No	9.1.1	**9.1.1**	No changes	The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	This covers all network components under the organisation's control.	Yes	The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed to a high strength password.	This covers all network components under the organisation's control.	Yes	Does your organisation make sure that the passwords of all networking components, such as a Wi-Fi router, have been changed from their original passwords?	Networking components include routers, switches, hubs and firewalls at all of your organisation's locations. Your organisation may just have a Wi-Fi router. This does not apply to Wi-Fi routers for people working from home. You may need to ask your IT supplier to assist with answering this question. If your organisation does not have a network or internet access, then tick and write "Not applicable" in the comments	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.	Yes
	Yes/No	9.1.2	**9.1.2**	Newly mandatory cat 2	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	This covers the organisation's servers, desktop computers, laptop computers, tablets and mobile phones.	Yes	The Head of IT, or equivalent role, confirms all organisational devices have had their default passwords changed.	This covers the organisation's servers, desktop computers, laptop computers, tablets and mobile phones.	Yes						
A penetration test has been scoped and undertaken	Yes/No	9.2.1	**9.2.1**	No changes	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.	Please include the scope and redact any elements of the results that are sensitive.	Yes	Annual IT penetration testing is scoped through negotiation between the SIRO, business and testing team, and includes a vulnerability scan and a check that all networking components have had their default passwords changed.	Please include the scope and redact any elements of the results that are sensitive.	Yes	Annual IT penetration testing is scoped through negotiation between the person responsible for IT, management and testing team, and includes a vulnerability scan and a check that all networking components have had their default passwords changed.	This should be since 1st July 2021. Please include the scope and redact any elements of the results that are sensitive.		Annual IT penetration testing is scoped through negotiation between the SIRO, business and testing team, and includes a vulnerability scan and a check that all networking components have had their default passwords changed.	This should be since 1st July 2021. Please include the scope and redact any elements of the results that are sensitive.	
	Date	9.2.2	**9.2.2**	No changes	The date the penetration test and vulnerability scan was undertaken.	This should be since 1st July 2021.	Yes	The date the penetration test was undertaken.	This should be since 1st July 2021.	Yes	The date the penetration test was undertaken.	This should be since 1st July 2021.				
Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities	Yes/No	9.3.1	**9.3.1**	No changes	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.	If no web applications, 'tick' yes and explain in the comments.	Yes	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.	If no web applications, 'tick' yes and explain in the comments.	Yes	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.	If no web applications, 'tick' yes and explain in the comments.				
	Document	9.3.2	**9.3.2**	No changes	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.	Provide the action plan with confirmation of SIRO review.	Yes	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with an action plan for its findings.	Provide the action plan with confirmation of SIRO review.		The person responsible for IT has reviewed the results of latest penetration testing, with an action plan for its findings.	Provide the action plan with confirmation of SIRO review.				
	Yes/No	9.3.3	**9.3.3**	No changes	The organisation uses the UK Public Sector DNS service, or equivalent protective DNS service, to resolve Internet DNS queries.		Yes	The organisation uses the UK Public Sector DNS service, or equivalent protective DNS service, to resolve Internet DNS queries.		Yes						
	Yes/No	9.3.4	**9.3.4**	No changes	The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.		Yes	The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.		Yes	The organisation ensures that changes to its authoritative DNS entries can only be made by strongly authenticated and authorised administrators.					
	Yes/No	9.3.5	**9.3.5**	No changes	The organisation understands and records all IP ranges in use across the organisation.		Yes	The organisation understands and records all IP ranges in use across the organisation.		Yes	The organisation understands and records all IP ranges in use across the organisation.					
	Yes/No	9.3.6	**9.3.6**	No changes	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.		Yes	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.		Yes	The organisation is protecting it's data in transit (including email) using well-configured TLS v1.2 or better.					
	Yes/No	9.3.7	**9.3.7**	No changes	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	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						
	Document	New	**9.3.8**	New	The organisation maintains a register of medical devices connected to its network.	The register should be uploaded and include Vendor, maintenance arrangements, any network segmentation is in place and whether network access is given to supplier/maintainer.	Yes	The organisation maintains a register of medical devices connected to its network.	The register should include Vendor, maintenance arrangements and whether network access is given to supplier/maintainer.		The organisation maintains a register of medical devices connected to its network.	The register should include Vendor, maintenance arrangements and whether network access is given to supplier/maintainer.		The organisation maintains a register of medical devices connected to its network.	The register should include Vendor, maintenance arrangements and whether network access is given to supplier/maintainer.	
	Document	New	**9.3.9**	New	What is the organisation's data security assurance process for medical devices connected to the network.	This should be a policy / process document or full explanation covering how the organisation assures data security during the full life cycle of the medical device.										

You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services	Text	9.4.1	**9.4.1**	Removed from Cat 3	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.	Please provide an explanation.		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.	Please provide an explanation.								
	Yes/No	9.4.2	**9.4.2**	Removed from Cat 3	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.	The review period for assurance methods should be in the last twelve months.		You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.	The review period for assurance methods should be in the last twelve months.								
	Text	9.4.3	**9.4.3**	No changes	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.	Using an on-site technical assessment from [NHS Digital's Cyber Security Support Model](https://digital.nhs.uk/services/data-security-centre/data-security-onsite-assessment) or equivalent. Organisations receiving IT provision from an NHS organisation may provide evidence from the supplying organisations assessment, subject to appropriate scope.		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.	Using an on-site technical assessment from [NHS Digital's Cyber Security Support Model](https://digital.nhs.uk/services/data-security-centre/data-security-onsite-assessment) or equivalent. Organisations receiving IT provision from an NHS organisation may provide evidence from the supplying organisations assessment, subject to appropriate scope.		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.	Organisations that have outsourced their entire IT function may be covered by their supplier's assessment.				
	Text	9.4.4	**9.4.4**	No changes	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.		Yes	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.		Yes	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.						
	Document	9.4.6	**9.4.5**	Removed from Cat 3	What level of assurance (overall risk rating & confidence level rating) did the independent audit of your Data Security and Protection Toolkit provide to your organisation?	Upload a copy of your full DSPT audit/independent assessment report, which should cover the mandatory audit-scope set out in the ['Strengthening Assurance Independent Assessment Guide'](https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides)	Yes	What level of assurance did the independent audit of your Data Security and Protection Toolkit provide to your organisation?	Upload a copy of your full DSPT audit/independent assessment report, which should cover the mandatory audit-scope set out in the ['Strengthening Assurance Independent Assessment Guide'](https://www.dsptoolkit.nhs.uk/Help/Independent-Assessment-Guides)	Yes							
You securely configure the network and information systems that support the delivery of essential services	Yes/No	9.6.1	**9.5.1**	No changes	All devices in your organisation have technical controls that manage the installation of software on the device.	Describe how this is managed across your devices with detail of any exceptions.	Yes	All devices in your organisation have technical controls that manage the installation of software on the device.	Describe how this is managed across your devices with detail of any exceptions.	Yes	All devices in your organisation have technical controls that manage the installation of software on the device	Describe how this is managed across your devices with detail of any exceptions.					
	Yes/No	9.6.2	**9.5.2**	No changes	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	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	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box. For advice on encrypting mobile devices and equivalent security arrangements, see [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/protect-mobile-devices-and-tablets/).	Yes	Are all laptops and tablets or removable devices that hold or allow access to personal data, encrypted?	Mobile computers like laptops and tablets and removable devices like memory sticks/cards/CDs are vulnerable as they can be lost or stolen. To make these devices especially difficult to get into, they can be encrypted (this protects information by converting it into unreadable code that cannot be deciphered easily by unauthorised people). Devices can be further protected, for example, by preventing the use of removable devices like memory sticks. This is called computer port control. You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any mobile devices, or equivalent security arrangements are in place, then tick and write "Not applicable" in the comments box.	Yes
	Text	9.6.3	**9.5.3**	No changes	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.			You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.			You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.						
	Yes/No	9.6.4	**9.5.4**	No changes	Only approved software can be installed and run and unnecessary software is removed.	This is for all devices in your organisation including servers, desktop computers; laptop computers, tablets, mobile phones. This could be a whitelisting solution.	Yes	Only approved software can be installed and run and unnecessary software is removed.	This is for all devices in your organisation including servers, desktop computers; laptop computers, tablets, mobile phones. This could be a whitelisting solution.								
	Yes/No	9.6.5	**9.5.5**	No changes	End user devices are built from a consistent and approved base image.	Applies to the organisation's desktop computers, laptop computers and tablets.	Yes	End user devices are built from a consistent and approved base image.	Applies to the organisation's desktop computers, laptop computers and tablets.								
	Yes/No	9.6.6	**9.5.6**	No changes	End user device security settings are managed and deployed centrally.	Applies to the organisation's desktop computers, laptop computers and tablets. This could be achieved using Group policy, mobile device management or similar mechanisms.	Yes	End user device security settings are managed and deployed centrally.	Applies to the organisation's desktop computers, laptop computers and tablets. This could be achieved using Group policy, mobile device management or similar mechanisms.								
	Yes/No	9.6.7	**9.5.7**	No changes	AutoRun is disabled.	This applies to servers, desktop and laptop computers. AutoRun relates to automatic execution of files without user interaction, and should not be confused with AutoPlay (which requires user interaction).	Yes	AutoRun is disabled.	This applies to servers, desktop and laptop computers. AutoRun relates to automatic execution of files without user interaction, and should not be confused with AutoPlay (which requires user interaction).								
	Yes/No	9.6.9	**9.5.8**	No changes	All remote access is authenticated.	Strong (ideally multifactor) authentication is required to remotely access personal, confidential information. This includes both web applications and remote access to corporate networks.	Yes	All remote access is authenticated.	Strong (ideally multifactor) authentication is required to remotely access personal, confidential information. This includes both web applications and remote access to corporate networks.								
	Yes/No	9.6.10	**9.5.9**	No changes	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.	This applies to any device (managed internally or by a third party) that does not have a route to/from the Internet, such as air-gapped networks or stand-alone devices. Such as an MRI Scanner.	Yes	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.	This applies to any device (managed internally or by a third party) that does not have a route to/from the Internet, such as air-gapped networks or stand-alone devices. Such as an MRI Scanner.	Yes							
	Yes/No	9.6.11	**9.5.10**	No changes	Does your organisation meet the secure email standard?	[Further detail on the standard](https://digital.nhs.uk/services/nhsmail/the-secure-email-standard) is available on the NHS Digital website.		Does your organisation meet the secure email standard?	[Further detail on the standard](https://digital.nhs.uk/services/nhsmail/the-secure-email-standard) is available on the NHS Digital website.								
The organisation is protected by a well managed firewall	Yes/No	9.7.1	**9.6.1**	No changes	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	This may include NHS Digital's Secure Boundary cloud-based firewall. IT Healthcheck would provide suitable evidence.	Yes	Have one or more firewalls (or similar network device) been installed on all the boundaries of the organisation's internal network(s)?	This may include NHS Digital's Secure Boundary cloud-based firewall. IT Healthcheck would provide suitable evidence.	Yes							
	Yes/No	9.7.2	**9.6.2**	No changes	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	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/No	9.7.3	**9.6.3**	No changes	The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	All protocols (such as HTTP/S, SMB, NetBIOS, Telnet, TFTP, RPC, rlogin, rsh, rexec etc.) are blocked by default.	Yes	The organisation has checked and verified that firewall rules ensure that all unauthenticated inbound connections are blocked by default.	All protocols (such as HTTP/S, SMB, NetBIOS, Telnet, TFTP, RPC, rlogin, rsh, rexec etc.) are blocked by default								
	Yes/No	9.7.4	**9.6.4**	No changes	All inbound firewall rules (other than default deny) are documented with business justification and approval by an authorised individual.	Confirm documentation of approval is available. This must be accurate and up to date.	Yes	All inbound firewall rules (other than default deny) are documented with business justification and approval by an authorised individual.	Confirm documentation of approval is available. This must be accurate and up to date.								
	Yes/No	9.7.5	**9.6.5**	No changes	Have firewall rules that are no longer required been removed or disabled?	Explain the process of removal and be ready to demonstrate to an onsite assessment.	Yes	Have firewall rules that are no longer required been removed or disabled?	Explain the process of removal and be ready to demonstrate to an onsite assessment.								
	Yes/No	9.7.6	**9.6.6**	No changes	Do all of your desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default?	Provide details of how you have implemented this and describe the confirmation process.	Yes	Do all of your desktop and laptop computers have personal firewalls (or equivalent) enabled and configured to block unapproved connections by default?	Provide details of how you have implemented this and describe the confirmation process.								
The organisation can name its suppliers, the products and services they deliver and the contract durations	Document	10.1.1	**10.1.1**	No changes	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.	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.	Yes							
	Yes/No	10.1.2	**10.1.2**	No changes	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 have no such suppliers, then 'tick' and write "Not applicable" in the comments box.		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 have no such suppliers, then 'tick' and write "Not applicable" in the comments box.		Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box. A template example is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/).	Yes	Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?	Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided. If you have no such suppliers, then 'tick' and write "Not applicable" in the comments box. A template example is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/).	Yes
Basic due diligence has been undertaken against each supplier that handles personal information	Yes/No	10.2.1	**10.2.1**	No changes	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.	For more information see the [2017/18 Data Security Protection Requirements guidance](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf).	Yes	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.	For more information see the [2017/18 Data Security Protection Requirements guidance](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/675420/17-18_statement_of_requirements_Branded_template_final_22_11_18-1.pdf).	Yes	Do your organisation's IT system suppliers have cyber security certification?	Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace, or by completing this Toolkit. An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box. Guidance is available from [Digital Social Care](https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/).	Yes	Do your organisation's IT system suppliers have cyber security certification?	Your organisation should ensure that any supplier of IT systems has cyber security certification. For example, external certification such as Cyber Essentials, or ISO27001, or by being listed on Digital marketplace, or by completing this Toolkit. An IT systems supplier would include suppliers of systems such as rostering, care planning or electronic medicine administration record (MAR) charts for example. If your organisation does not use any IT systems, then tick and write "Not applicable" in the comments box.	Yes
	Yes/No	10.2.2	**10.2.2**	Removed from cat 1 and 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 have no such suppliers, then 'tick' and write "Not applicable" in the comments box.		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 have no such suppliers, then 'tick' and write "Not applicable" in the comments box.		
	text	10.2.3	**10.2.3**	No changes	Percentage of suppliers with data security contract clauses in place.	The percentage snapshot of current suppliers handling personal data that currently have security clauses.		Percentage of suppliers with data security contract clauses in place.	The percentage snapshot of current suppliers handling personal data that currently have security clauses.								
	Yes/No	10.2.4	**10.2.4**	No changes	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	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							
	Yes/No	10.2.5	**10.2.5**	No changes	All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	Provide confirmation that all suppliers have successfully completed a Data Security and Protection Toolkit or the organisation has assured itself separately that they reach a similar or higher data security standard.		All suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	Provide confirmation that all suppliers have successfully completed a Data Security and Protection Toolkit or the organisation has assured itself separately that they reach a similar or higher data security standard.		All Suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.	All suppliers have successfully completed a Data Security and Protection Toolkit or the organisation has assured itself separately that they reach a similar or higher data security standard.					

All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented	Document	10.3.1	**10.3.1**	No changes	List of data security incidents – past or present – with current suppliers who handle personal information.	All current ongoing incidents are listed and all historical incidents (up to 2 calendar rolling years). Redact any sensitive information.		List of data security incidents – past or present – with current suppliers who handle personal information.	All current ongoing incidents are listed and all historical incidents (up to 2 calendar rolling years). Redact any sensitive information.		List of data security incidents – past or present – with current suppliers who handle personal information.	All current ongoing incidents are listed and all historical incidents (up to 2 calendar rolling years). Redact any sensitive information.				
All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and discussed at board	Text	10.4.1	**10.4.1**	No changes	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.	Where an organisation finds itself unable to comply with National Data Guardian standards and this is purely due to supplier related issues, these issues should be raised at the board.		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.	Where an organisation finds itself unable to comply with National Data Guardian standards and this is purely due to supplier related issues, these issues should be raised at the board.		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.	Where an organisation finds themselves unable to comply with National Data Guardian standards and this is purely due to supplier related issues, these issues should be raised at the board.				
The organisation understands and manages security risks to networks and information systems from your supply chain	Text	10.5.2	**10.5.1**	No changes	Where appropriate, you offer support to suppliers to resolve incidents.			Where appropriate, you offer support to suppliers to resolve incidents.								
		1.3.5	**N/A**	Removed												
		1.6.7	**N/A**	Removed												
		1.6.8	**N/A**	Removed												
		3.2.2	**N/A**	Removed												
		3.4.2	**N/A**	Removed												
		4.4.5	**N/A**	Removed												
		4.5.6	**N/A**	Removed												
		5.1.2	**N/A**	Removed												
		6.1.2	**N/A**	Removed												
		4.4.1	**N/A**	Removed												
		6.2.2	**N/A**	Removed												