9.10

NHS DORSET CLINICAL COMMISSIONING GROUP

GOVERNING BODY MEETING

ANNUAL REVIEW OF THE DATA SECURITY AND PROTECTION TOOLKIT

Date of the meeting	16/09/2020
Author	P Baker - Data Protection Officer
Sponsoring Board member	N Rowland - Chief Finance Officer
Purpose of Report	To assure the Governing Body that the requirements of the Data Security and Protection Toolkit are being met and that significant improvements continue to be made across the CCG.
Recommendation	The Governing Body is asked to **note** the report.
Stakeholder Engagement	Patients/members of the public are involved in the management of complaints.
Previous GB / Committee/s, Dates	N/A

Monitoring and Assurance Summary

This report links to the following Strategic Objectives	• Integrated Community and Primary Care Services • One Acute Network • Digitally Enabled Dorset • Leading and Working Differently

	Yes [e.g. ✓]	**Any action required?**	
		Yes Detail in report	**No**
All three Domains of Quality (Safety, Quality, Patient Experience)	✓	✓	
Board Assurance Framework Risk Register	✓		✓
Budgetary Impact	✓		✓
Legal/Regulatory	✓		✓
People/Staff	✓		✓
Financial/Value for Money/Sustainability	✓		✓
Information Management &Technology	✓		✓
Equality Impact Assessment	✓		✓
Freedom of Information	✓		✓
I confirm that I have considered the implications of this report on each of the matters above, as indicated	✓		

Initials : PB

9.10

1. Introduction

1.1 The Data Security and Protection Toolkit (DSPT) replaced the Information Governance Toolkit from April 2018, as the standard for cyber and data security in healthcare organisations.

1.2 The DSPT is based on the National Data Guardian's (NDG) data security standards set out in the Data Security and Protection Standards for Health and Care.

1.3 The CCG is required to demonstrate that the organisation is working towards or is meeting the NDG standards by completing the DSPT self-assessment on an annual basis. This includes providing evidence and judging whether the CCG meets the standards of the assertions in the DSPT.

1.4 In accordance with the requirements of the DSPT, the purpose of this report is to provide the Governing Body with assurances in relation to data security and protection management and accountability, advise of any serious data protection incidents and to provide an update on the DSPT assessment.

1.5 The DSPT is not the same submission as 2019 and has been modified to become more IT-centric.

2. Data Protection Officers for General Practice

2.1 The CCG has recruited two Data Protection Officers to support General Practice. The two DPOs commenced their role on 1 October 2019 and will have been in post for six months at the end of March 2020.

2.2 The Dorset-wide service provided by the DPOs has been well received by Practices and use of the service has been growing:

Month	Contact from Practices
October	**33 contacts:** incl. 5 incidents queries, 1 request for training
November	**36 contacts:** incl. 4 incident queries, 6 requests for DPO visit
December	**22 contacts:** incl. 1 incident query, 1 request for DPO visit
January	**43 contacts:** incl. 3 incident queries, 2 requests for training, 6 requests for DPO visit
February	**56 contacts:** incl. 7 incident queries,5 requests for training,2 requests for DPO visit
March	**20 contacts (as at 6 March):** incl. 1 incident query, 2 requests for training

2.3 A Data Security and Protection site has been established on the GP Intranet where guidance documentation, templates, toolkit guidance and FAQs are available to support Practices. A monthly newsletter is sent out to all Practices to keep them up to date with the latest data protection news and highlight any new guidance and template documentation.

2.4 Three Data Security and Protection Toolkit workshops have also been hosted across the county to support Practices in the completion of their toolkits, with template documentation produced for many of the toolkit requirements.

2.5 Data Protection Audits have been completed at 21 Practices to date, with further audits booked over the coming months. A GDPR/IG training presentation has been produced and 5 Practices have requested and received training, with more sessions booked.

2.6 A GP DPO network group has been established with the Devon and Somerset GP DPOs which will meet on a quarterly basis, the first meeting having taken place in February.

2.7 Feedback on the new service is very positive and requests for visits and training are now received by word of mouth from Practice Managers.

3. Data Security and Protection at the CCG

Data Security and Protection Internal Responsibility

3.1 The Data Security and Protection Group (DSPG) has now been subsumed into the Information Asset Owners Group (IAOG). The IAOG is chaired by the Chief Finance Officer who is also the Senior Risk Owner (SIRO) for the CCG, and is attended by the Caldicott Guardian, the Data Protection Officer and IAOs from each directorate. The group reports via the Audit and Quality Committee.

3.2 The IAOG has had oversight of the Data Security work at the CCG during 2019/20, especially in relation to the DSPT, training and review of the core Data Protection policies and procedures.

3.3 It is essential to ensure that the Governing Body and the senior management of the organisation are assured of continued compliance, and changes in performance both within the CCG and commissioned services.

Data Security and Protection Toolkit

3.4 There are 10 data security standards making up the DSPT, and each standard is broken down into a number of assertions (43 in total), which are further broken down into specific evidence items required (158 in total). 106 of these specific evidence items are mandatory requirements.

3.5 The data security standards that the CCG is required to complete a self-assessment against are:

Data Security Standard 1: Personal Confidential Data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

Data Security Standard 2: Staff Responsibilities

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3: Training

All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the Data Security and Protection Toolkit.

Data Security Standard 4: Managing Data Access

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5: Process Reviews

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6: Responding to Incidents

Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7: Continuity Planning

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Data Security Standard 8: Unsupported Systems

No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9: IT Protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proved cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10: Accountable Suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

Consequences of Not Meeting Data Security Standards

3.6 At the beginning of 2019, NHS Digital provided a briefing on arrangements for the DSPT which advised that:

- the status of health and care organisations' DSPT will be shared with the Care Quality Commission, NHS England and NHS Improvement. The DSPT status is important evidence for the key line of enquiry on information in a CQC well-led inspection;

- NHS providers' DSPT status will be notified through NHS England/Improvement to the Cyber Risks and Operations group and if appropriate they will be flagged as a trust of concern;

- organisations will be listed on the DSPT with their status displayed and available for commissioners, partner organisations and the public;

- if organisations are applying for research data through DARS or HRA CAG or demographics data from NHS Digital, each organisation applying for data has their DSPT reviewed as part of the data security assurance process. A key element of this process is that the organisation is required to demonstrate good levels of data security and protection through the DSPT;

- many information sharing projects and partnerships use the completion of the DSPT to a status of 'Standards met' as a pre-qualification question for joining;

- where organisations fail to meet the Standards required, an improvement plan will be required and must be agreed with NHS Digital. The organisation will then display as 'Standards not fully met (Plan Agreed)';

- organisations failing to make adequate progress in their improvement plans may have their status changed to 'Standards not met' and will be notified through NHS England/Improvement to the Cyber Risks and Operations Group. If appropriate they will be flagged as a Trust of concern.

3.7 A full DSPT assessment was required to be submitted no later than 31 March 2020 by all NHS organisations. However, due to the current national crisis, the deadline for submission has been extended until the 30th of September 2020.

3.8 Organisations are required to meet the 106 mandatory evidence items in order to achieve a final overall score of 'Standards Met'. This is regardless of the amount of progress made against the remaining assertions.

CCG DSP Toolkit Assessment 2019/20

3.9 The CCG DSP Toolkit submission for 2019/20 has not yet been published, due to the demands, particularly on our IT Department (see appendix 1 for further detail). NHS Digital has extended the submission date to the 30th of September 2020. At the time of writing this report the CCG has achieved 104 of the 106 mandatory requirements and 40 of the 43 assertions.

3.10 Notably the CCG has achieved 99% staff attendance for mandatory training this year with the average score of the mandatory test reported as 90%.

DSP Toolkit 2020/21

3.11 NHS Digital has reviewed the DSPT for 2020/21 and the planned changes are:

- To ensure achieving ‘Standards met’ on the DSPT is equivalent to Cyber Essentials PLUS for NHS Trusts, CCGs and CSUs.
- To respond to lessons learned and direct feedback from users of the DSPT.
- To rationalise the evidence items which are now considered “business as usual” or where there is overlap between evidence items.
- To migrate some evidence items to compliance statements to be clearer on the response required.

3.12 The new DSPT work plan will be produced once the new toolkit has been issued.

Data Breaches

3.13 The CCG had no serious untoward incidents in relation to Data Protection for 2019/20 and has not been subject to any Information Commissioner Data Protection monetary penalties.

Freedom of Information

3.14 The CCG received 278 FOI requests in the year 2019/20, a decrease from 2018/19 of 2%. It should be noted that the volume of requests does not give an indication of the amount of time spent in responding to each one. Some requests involve reporting on data that is routinely collected and can be completed relatively quickly, but others involve large amounts of work by different departments and the FOI team must judge whether answering a request would exceed the 18 hours “appropriate cost limit”.

3.15 The main themes of the requests have been consistent with last year:

- Continuing Healthcare and Personal Health Budgets;
- Primary Care;
- Commissioning of Services, especially Mental Health;
- ICT expenditure;

Requests for Internal Reviews

3.16 If an applicant is dissatisfied with the response the CCG has provided, they can request an internal review. During 2019/20 two requests were received for review. One required further information from the requester which was not forthcoming, and the request was closed, the second was dealt with by the DPO to the requester’s satisfaction.

4. Conclusion

4.1 NHS Dorset CCG does have robust processes for managing Data Security and Protection and the associated responsibilities that come with the commitment to adopt best practice policy and procedures in order to protect patient and service users’ information.

4.2 The CCG will meet the standards required for the DSPT submission for 2019/20. The DSP Team, with the assistance of representatives from IT and the IAO Group, will continue to work to ensure the last of the work is completed and submitted before the September deadline.

4.3 The Governing Body is asked to **note** this report.

Author Name and Title: Paddy Baker, Data Protection Officer
Telephone Number: 01305 213567

APPENDICES	
Appendix 1	Data Security and Protection Toolkit Final Assessment Summary 2018-19

9.10

Appendix 1

Data Security and Protection Toolkit
Final Assessment 2018-19

1 Personal Confidential Data

All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

1.1	There is senior ownership of data security and protection within the organisation.		
1.1.1	Has SIRO Responsibility for data security been assigned?	Mandatory	COMPLETED
1.1.2	List the names and job titles of your key staff with responsibility for data protection and/or security.	Mandatory	COMPLETED
1.1.3	Are there clear lines of responsibility and accountability to named individuals for data security?	Mandatory	COMPLETED
1.1.4	Is data security direction set at board level and translated into effective organisational practices?	Mandatory	COMPLETED

1.2	There are clear data security and protection policies in place, and these are understood by staff and available to the public.		
1.2.1	Are there Board approved data security and protection policies in place that follow relevant guidance?	Mandatory	COMPLETED
1.2.2	When were each of the data security and protection policies last updated?	Mandatory	COMPLETED
1.2.3	How are Data Security and Protection Policies available to the public?		COMPLETED

1.3	Individuals’ rights are respected and supported (GDPR Art 12-22)		
1.3.1	ICO Registration Number.	Mandatory	COMPLETED
1.3.2	Transparency information is published and available to the public.	Mandatory	COMPLETED

1.3.3	How have Individuals been informed about their rights and how to exercise them?	Mandatory	COMPLETED
1.3.4	Provide details of how access to information requests have been complied with during the last twelve months.	Mandatory	COMPLETED
1.3.5	Total ICO fines, enforcement notices or decision notices in last 12 months.		COMPLETED

1.4	Records of processing activities are documented for all uses and flows of personal information (GDPR Article 30 and Data Protection Bill 2017 Schedule 1 Part 4)		
1.4.1	Provide details of the record or register that details each use or sharing of personal information.	Mandatory	COMPLETED
1.4.2	When were information flows approved by the Board or equivalent?	Mandatory	COMPLETED
1.4.3	Provide a list of all systems/information assets holding or sharing personal information.	Mandatory	COMPLETED
1.4.4	Is your organisation compliant with the national data opt-out policy?	Mandatory	COMPLETED

1.5	Personal information is used and shared lawfully.		
1.5.1	There is approved staff guidance on confidentiality and data protection issues.	Mandatory	COMPLETED
1.5.2	What actions have been taken following Confidentiality and Data Protection monitoring/spot checks during the last year?	Mandatory	COMPLETED

1.6	The use of personal information is subject to data protection by design and by default.		
1.6.1	There is a procedure that sets out the organisation’s approach to data protection by design and by default, which includes pseudonymisation requirements.	Mandatory	COMPLETED

1.6.2	There are technical controls that prevent information from being inappropriately copied or downloaded.	Mandatory	COMPLETED
1.6.3	There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed.	Mandatory	COMPLETED
1.6.4	Provide the overall findings of the last data protection by design audit.	Mandatory	
1.6.5	There is a staff procedure, agreed by the SIRO, on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance.		COMPLETED
1.6.6	Is a Data Protection Impact Assessment carried out before high risk processing commences?	Mandatory	COMPLETED
1.6.7	Have any unmitigated risks been identified through the Data Protection Impact Assessment process and notified to the ICO?		COMPLETED
1.6.8	Data Protection Impact Assessments are published and available as part of the organisation’s transparency materials.		COMPLETED

1.7	Effective data quality controls are in place.		
1.7.1	There is policy and staff guidance on data quality.	Mandatory	COMPLETED
1.7.2	Was the scope of the last data quality audit in line with guidelines.	Mandatory	COMPLETED
1.7.3	A data quality forum monitors the effectiveness of data quality assurance processes.		
1.7.4	Has a records retention schedule been produced?	Mandatory	COMPLETED
1.7.5	Provide details of when personal data disposal contracts were last reviewed/updated.	Mandatory	COMPLETED
1.7.6	When was the date of last audit being made on data disposal contractors/other arrangements to ensure security is of the appropriate agreed standard?	Mandatory	COMPLETED

1.8	There is a clear understanding and management of the identified and significant risks to sensitive information and services		
1.8.1	Does your organisation operate and maintain a risk register that follows an acceptable Information Security risk framework which links to the corporate risk framework?	Mandatory	COMPLETED
1.8.2	Senior management have visibility of key risk decisions made throughout the organisation.	Mandatory	COMPLETED
1.8.3	What are your top three data security and protection risks?	Mandatory	COMPLETED

2 Staff Responsibilities

All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

2.1	There is a clear understanding of what Personal Confidential Information is held.		
2.1.1	The organisation has identified and catalogued personal and sensitive information it holds.	Mandatory	COMPLETED
2.1.2	When did your organisation last review the list of all systems/information assets holding or sharing personal information?	Mandatory	COMPLETED

2.2	Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards.		
2.2.1	Is there a data protection and security induction in place for all new entrants to the organisation?	Mandatory	COMPLETED
2.2.2	Do all employment contracts contain data security requirements?	Mandatory	COMPLETED
2.2.3	The results of Staff awareness surveys on staff understanding of data security are reviewed to improve data security.		COMPLETED

3 Training

All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.

3.1	There has been an assessment of data security and protection training needs across the organisation.		
3.1.1	Has an approved organisation wide data security and protection training needs analysis been completed in the last twelve months?	Mandatory	COMPLETED

3.2	Staff pass the data security and protection mandatory test.		
3.2.1	Have at least 95% of all staff, completed their annual Data Security awareness training in the period 1 April to 31 March?	Mandatory	COMPLETED
3.2.2	What is the average mark of staff completing the Data Security Awareness Training?		COMPLETED

3.3	Staff with specialist roles receive data security and protection training suitable to their role.		
3.3.1	Provide details of any specialist data security and protection training undertaken.	Mandatory	COMPLETED
3.3.2	The organisation has appropriately qualified technical cyber security specialist staff and/or service.	Mandatory	COMPLETED
3.3.3	The organisation has nominated a member of the Cyber Associates Network.	Mandatory	COMPLETED

3.4	Leaders and board members receive suitable data protection and security training.		
3.4.1	Have your SIRO and Caldicott Guardian received appropriate data security and protection training?	Mandatory	COMPLETED
3.4.2	What percentage of Board Members have completed appropriate data security and protection Training?	Mandatory	COMPLETED

4 Managing Data Access

Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

4.1	The organisation maintains a current record of staff and their roles.

4.1.1	Your organisation maintains a record of staff and their roles.	Mandatory	COMPLETED
4.1.2	Does the organisation understand who has access to personal and confidential data through your systems, including any systems which do not support individual logins?	Mandatory	COMPLETED
4.1.3	Are users in your organisation only given the minimum access to sensitive information or systems necessary for their role?		COMPLETED

4.2	Organisation assures good management and maintenance of identity and access control for it's networks and information systems.		
4.2.1	When was the last audit of user accounts held?	Mandatory	COMPLETED
4.2.2	Provide a summary of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted.		COMPLETED
4.2.3	There is a corporate policy on log retention, the secure centralised storage and management of log information?		
4.2.4	Explain how logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity.		COMPLETED

4.3	All staff understand that their activities on IT systems will be monitored and recorded for security purposes.		
4.3.1	All system administrators have signed an agreement which holds them accountable to the highest standards of use.	Mandatory	COMPLETED
4.3.2	Are users, systems and where appropriate, devices, always identified and authenticated prior to being provided access to information or system?	Mandatory	COMPLETED
4.3.3	Is an acceptable IT usage banner displayed to all staff when logging in, including a personal accountability reminder?		COMPLETED

4.3.4	Provide a list of all systems to which users and administrators have an account, plus the means of monitoring access.	Mandatory	COMPLETED
4.3.5	Have all staff been notified that their system use could be monitored?		COMPLETED
4.4	You closely manage privileged user access to networks and information systems supporting the essential service.		
4.4.1	Has the Head of IT, or equivalent, confirmed that IT administrator activities are logged and those logs are only accessible to appropriate personnel?	Mandatory	COMPLETED
4.4.2	Privileged user access is removed when no longer required or appropriate.	Mandatory	COMPLETED
4.4.3	The organisation does not allow users with wide ranging or extensive system privilege to use their highly privileged accounts for high-risk functions, in particular reading email and web browsing.	Mandatory	COMPLETED
4.4.4	The organisation only grants privileged access on devices owned and managed by your organisation.		COMPLETED
4.4.5	You record and store all privileged user sessions for offline analysis and investigation.		COMPLETED

4.5	You ensure your passwords are suitable for the information you are protecting		
4.5.1	Do you have a password policy giving staff advice on managing their password?		COMPLETED
4.5.3	Multifactor authentication is used [wherever technically feasible].		COMPLETED
4.5.4	Passwords for highly privileged system accounts, social media accounts and infrastructure components shall be changed from default values and shall not be easy to guess. Passwords which would on their own grant extensive system access, should have high strength.	Mandatory	COMPLETED
4.5.5	Does your organisation grant limited privileged access and third party access for a limited time period or is planning to?		COMPLETED

5 Process Reviews

Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

5.1	Process reviews are held at least once per year.		
5.1.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident.	Mandatory	COMPLETED
5.1.2	Provide summary details of process reviews held to identify and manage problem processes which cause security breaches.	Mandatory	COMPLETED
5.1.3	List of actions arising from each process review, with names of actionees.		COMPLETED
5.1.4	You use lessons learned to improve security measures, including updating and retesting response plans when necessary.		COMPLETED
5.1.5	Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.		COMPLETED

5.2	Participation in reviews is comprehensive, and clinicians are actively involved.		
5.2.1	Scanned copy of the process review meeting registration sheet with attendee signatures and roles held.		COMPLETED

5.3	Action is taken to address problem processes as a result of feedback at meetings or in year.		
5.3.1	Explain how the actions to address problem processes are being monitored and assurance given to the Board or equivalent senior team?		COMPLETED
5.3.2	Post testing findings should inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again.	Mandatory	COMPLETED

5.3.3	Systemic vulnerabilities identified in process reviews shall be remediated as soon as practicable.		COMPLETED

6 Responding to Incidents

Cyber-attacks against services are identified and resisted and security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

6.1	A confidential system for reporting security breaches and near misses is in place and actively used.		
6.1.1	A data security and protection breach reporting system is in place.	Mandatory	COMPLETED
6.1.2	How can staff report data security and protection breaches and near misses?		COMPLETED
6.1.3	List of all notifiable data security breach reports in the last twelve months.	Mandatory	COMPLETED
6.1.4	How is the Board or equivalent notified of the action plan for all data security and protection breaches?	Mandatory	COMPLETED
6.1.5	Individuals affected by a breach are appropriately informed.	Mandatory	COMPLETED

6.2	All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway.		
6.2.1	Name of anti-virus product.	Mandatory	COMPLETED
6.2.2	Number of alerts recorded by the AV tool in the last three months.	Mandatory	COMPLETED
6.2.3	Has anti-virus or malware protection software been installed on all computers that are connected to or capable of connecting to the Internet?		COMPLETED
6.2.4	Anti-malware and Anti-Virus is kept continually up to date.		COMPLETED
6.2.5	Anti-malware (Anti Virus) software scans files automatically upon access.		COMPLETED

6.2.7	Name of spam email filtering product.	Mandatory	COMPLETED
6.2.8	Number of spam emails blocked per month.	Mandatory	COMPLETED
6.2.9	Number of phishing emails reported by staff per month.		COMPLETED
6.2.11	You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) records in place for their domains to make email spoofing difficult.	Mandatory	COMPLETED
6.2.12	You have implemented spam and malware filtering and enforce DMARC on inbound email.	Mandatory	COMPLETED

6.3	Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.		
6.3.1	If you have had a data security incident, was it caused by a known vulnerability?	Mandatory	COMPLETED
6.3.2	The organisation has responded to high severity CareCERT alerts within 48 hours over the last twelve months.	Mandatory	COMPLETED
6.3.3	The Organisation has a proportionate monitoring solution to detect cyber events on systems and services.	Mandatory	COMPLETED
6.3.4	When did the last review of monitoring solutions take place?	Mandatory	COMPLETED
6.3.5	Are all new Digital services that are attractive to cyber criminals for the purposes of fraud, implementing transactional monitoring techniques from the outset?	Mandatory	COMPLETED
6.3.6	Have you had any repeat data security incidents of the same issue within the organisation?		COMPLETED

9.10

7 Continuity Planning

A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

7.1	Organisations have a defined, planned and communicated response to Data security incidents that impact sensitive information or key operational services.		
7.7.1	Organisations understand the health and care services they provide.	Mandatory	COMPLETED
7.1.2	Do you have well defined processes in place to ensure the continuity of services in the event of a data security incident, failure or compromise?		COMPLETED
7.1.3	You understand the resources and information that will likely be needed to carry out any required response activities, and arrangements are in place to make these resources available.		COMPLETED
7.1.4	You use your security awareness, e.g. threat intelligence sources, to make temporary security changes in response to new threats, e.g. a widespread outbreak of very damaging malware.		COMPLETED

7.2	There is an effective test of the continuity plan and disaster recovery plan for data security incidents.		
7.2.1	Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan.	Mandatory	COMPLETED
7.2.2	Which scenario/s were tested during the business continuity exercise, why, and when?	Mandatory	COMPLETED
7.2.3	Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held.	Mandatory	COMPLETED

7.2.4	From the business continuity exercise, which issues and actions were documented, with names of actionees listed against each item.	Mandatory	COMPLETED

7.3	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.		
7.3.1	On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary.	Mandatory	COMPLETED
7.3.2	All emergency contacts are kept securely, in hardcopy and are up-to-date.	Mandatory	COMPLETED
7.3.3	Are draft press materials for data security incidents ready?		COMPLETED
7.3.4	Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed.	Mandatory	COMPLETED
7.3.5	When did you last successfully restore from backup?		COMPLETED

8 Unsupported Systems

No unsupported operating systems, software or internet browsers are used within the IT estate.

8.1	No unsupported operating systems, software or internet browsers are used within the IT estate.		
8.1.1	Provide evidence of how the organisation tracks and records all software assets and their configuration?	Mandatory	COMPLETED
8.1.2	Does the organisation track and record all end user devices and removeable media assets?	Mandatory	COMPLETED

8.2	Unsupported software and hardware is categorised and documented, and data security risks are identified and managed.		
8.2.1	List of unsupported software prioritised according to business risk, with remediation plan against each item.	Mandatory	COMPLETED

8.2.2	The SIRO confirms that the risks of using unsupported systems are being treated or tolerated.	Mandatory	COMPLETED

8.3	Supported systems are kept up-to-date with the latest security patches.		
8.3.1	How do your systems receive updates and how often?	Mandatory	COMPLETED
8.3.2	How often, in days, is automatic patching typically being pushed out to remote endpoints?	Mandatory	COMPLETED
8.3.3	What is your approach to ensuring patches for critical or high-risk vulnerabilities are applied within 14 days of release?	Mandatory	COMPLETED
8.3.5	Is the organisation is actively managing Active Threat Prevention (ATP)?		COMPLETED

8.4	You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service.		
8.4.1	Is all your infrastructure protected from common cyber-attacks through secure configuration and patching?	Mandatory	COMPLETED
8.4.2	All infrastructure is running operating systems and software packages which are patched regularly, and as a minimum in vendor support.	Mandatory	COMPLETED
8.4.3	You maintain a current understanding of the exposure of your hardware and software to publicly-known vulnerabilities.		COMPLETED

9 IT Protection

A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

9.1	All networking components have had their default passwords changed.		
9.1.1	The Head of IT, or equivalent role confirms all networking components have had their default passwords changed.	Mandatory	COMPLETED

9.2	A penetration test has been scoped and undertaken		
9.2.1	The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including checking that all networking components have had their default passwords changed.	Mandatory	COMPLETED
9.2.2	The date the penetration test was undertaken.	Mandatory	COMPLETED
9.2.3	Where critical and high-risk vulnerabilities have been detected, and have not been resolved within 14 days, the risk is understood, documented, and has been agreed by the SIRO.	Mandatory	COMPLETED

9.3	Systems which handle sensitive information or key operational services shall be protected from exploitation of known vulnerabilities.		
9.3.1	All web applications are protected and not susceptible to common security vulnerabilities, such as described in the top ten Open Web Application Security Project (OWASP) vulnerabilities.	Mandatory	COMPLETED
9.3.2	The SIRO or equivalent senior role has reviewed the results of latest penetration testing, with action plan against outstanding OWASP findings.		COMPLETED
9.3.3	The organisation uses the UK Public Sector DNS Service to resolve internet DNS queries.	Mandatory	COMPLETED
9.3.4	The organisation ensures that changes to your authoritative DNS entries can only be made by strongly authenticated and authorised administrators.	Mandatory	COMPLETED
9.3.5	The organisation understands and records all IP ranges in use across your organisation.	Mandatory	COMPLETED
9.3.6	The organisation is protecting data in transit (including email) using well-configured TLS v1.2 or better.	Mandatory	COMPLETED
9.3.7	The organisation has registered and uses the National Cyber Security Centre (NCSC) Web Check service for your publicly visible applications.	Mandatory	COMPLETED

9.3.8	The organisation has suitable perimeter security device.		COMPLETED

9.4	You have demonstrable confidence in the effectiveness of the security of your technology, people, and processes relevant to essential services.		
9.4.1	You validate that the security measures in place to protect the networks and information systems are effective, and remain effective for the lifetime over which they are needed.		COMPLETED
9.4.2	You understand the assurance methods available to you and choose appropriate methods to gain confidence in the security of essential services.		COMPLETED
9.4.3	Your confidence in the security as it relates to your technology, people, and processes has been demonstrated to, and verified by, a third party in the last twelve months.	Mandatory	COMPLETED
9.4.4	Security deficiencies uncovered by assurance activities are assessed, prioritised and remedied when necessary in a timely and effective way.	Mandatory	COMPLETED
9.4.5	The methods used for assurance are reviewed to ensure they are working as intended and remain the most appropriate method to use.		COMPLETED
9.4.6	What level of assurance did the independent audit of your Data Security and Protection Toolkit provide to your organisation?	Mandatory	COMPLETED

9.5	A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO.		
9.5.1	What is the status of your data security improvement plan?	Mandatory	
9.5.2	Date for full implementation of the data security improvement plan.		

9.6	You securely configure the network and information systems that support the delivery of essential services.		
9.6.1	All devices in your organisation have technical controls which manage the installation of software on the device.	Mandatory	COMPLETED

9.6.2	Confirm all data is encrypted at rest on all mobile devices and removeable media and you have the ability to remotely wipe and/or revoke access from an end user device.	Mandatory	COMPLETED
9.6.3	You closely and effectively manage changes in your environment, ensuring that network and system configurations are secure and documented.		COMPLETED

10 Accountable Suppliers

IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

10.1	The organisation can name its suppliers, the products and services they deliver and the contract durations.		
10.1.1	The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.	Mandatory	COMPLETED
10.1.2	Contracts with all third parties that handle personal information are compliant with ICO guidance.		COMPLETED

10.2	Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance.		
10.2.1	Organisations ensure that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.	Mandatory	COMPLETED
10.2.2	Organisations should, as part of their risk assessment, determine whether the supplier certification is sufficient assurance.	Mandatory	COMPLETED
10.2.3	Percentage of suppliers with data security contract clauses in place.		COMPLETED
10.2.4	Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility.	Mandatory	COMPLETED

10.2.5	All Suppliers that process or have access to health or care personal confidential information have completed a Data Security and Protection Toolkit, or equivalent.		COMPLETED

10.3	All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.		
10.3.1	List of data security incidents – past or present – with current suppliers who handle personal information.		COMPLETED

10.4	All instances where organisations cannot comply with the NDG Standards because of supplier-related issues are recorded and discussed at board		
10.4.1	List of instances of suppliers who handle health and care data not complying with National Data Guardian standards, with date discussed at board or equivalent level.		COMPLETED

10.5	The organisation understands and manages security risks to networks and information systems from your supply chain.		
10.5.1	Your organisation's approach to risk management includes the risks to your services arising from supply chain.		COMPLETED
10.5.2	Where appropriate, you offer support to suppliers to resolve incidents.		COMPLETED