9.7

# NHS DORSET CLINICAL COMMISSIONING GROUP

## GOVERNING BODY MEETING

## ANNUAL REVIEW OF THE DATA SECURITY AND PROTECTION TOOLKIT

| | |
|---|---|
| **Date of the meeting** | 17/07/2019 |
| **Author** | P Baker, Data Protection Officer |
| **Sponsoring Board member** | S Hunter, 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** | None |

### Monitoring and Assurance Summary

| | |
|---|---|
| **This report links to the following Strategic Objectives** | • Integrated Community and Primary Care Services<br>• One Acute Network<br>• Digitally Enabled Dorset<br>• 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

## 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 This is the first year of completion and publication of the new DSPT.

## 2. Data Security and Protection

### Data Security and Protection Internal Responsibility

2.1 The Data Security and Protection Group (DSPG) met on a bi-monthly basis during 2018/19. The group 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 representatives from each directorate. The group reports via the Audit and Quality Committee.

2.2 The DSPG has overseen the work plan for the CCG during 2018/19, in relation to the DSPT, training and review of the core Data Protection policies and procedures.

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

### Data Security and Protection Toolkit

2.4 There are 10 data security standards making up the DSPT, and each standard is broken down into a number of assertions (38 in total), which are further spoken down into specific evidence items required (131 in total). 70 of these specific evidence items are mandatory requirements.

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

**9.7**

### 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

2.6 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.

2.7 A full DSPT assessment was required to be submitted no later than 31 March 2019 by all NHS organisations. This involved uploading evidence to demonstrate compliance against the standards.

2.8 Organisations were required have met the 70 mandatory evidence items in order to achieve a final overall score of ‘Standards Met’. This was regardless of the amount of progress made against the remaining assertions.

**CCG DSP Toolkit Assessment 2018/19**

2.9 The CCG DSP Toolkit submission for 2018/19 was published on 29 March 2019. The CCG achieved an assessment status of ‘Standards Met (see Appendix 1 for further detail).

**DSP Toolkit 2019/20**

2.10 NHS Digital has reviewed the DSPT for 2019/20 and further changes have been made in order to:

- respond to lessons learned and direct feedback from users following the first year of the DSPT;
- rationalise some of the General Data Protection Regulation (GDPR) evidence items which are now considered ‘business as usual’;
- incorporate the requirements of Cyber Essentials and the Minimum Cyber Security Standard (MCSS) for relevant larger NHS organisations (this includes CCGs);
- incorporate key elements of the Network and Information Systems (NIS) Regulations 2018 Cyber Assessment Framework (CAF) as advised by the National Cyber Security Centre.

2.11 This means that there will be an increase from 70 to 116 mandatory evidence items for NHS organisations in the 19/20 Toolkit. This is due to additional evidence items being added to cover the above requirements.

2.12 Work on ensuring the CCG meets the requirements of the DSPT for 2019/20 is therefore continuing. The IT team and the Director of System Integration have been provided with details of the new requirements, as many of them will require input from the IT team which may require additional resourcing.

2.13 At present, the DSP Team are working on:

- implementing the Information Asset Owner framework and associated responsibilities;
- delivering cyber security training to all staff;
- updating information provided to the public;
- setting up an area on the intranet to hold information relevant to data security and protection;
- reviewing all data mapping across the CCG.

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

### Data Breaches

2.15 The CCG had no serious untoward incidents in relation to Data Protection for 2018/19 and has not been subject to any Information Commissioner Data Protection monetary penalties.

### Freedom of Information

2.16 The CCG received 284 FOI requests in the year 2018/19, a decrease from 2017/18 of 9%. 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 have to judge whether answering a request would exceed the 18 hours "appropriate cost limit".

2.17 The main themes of the requests have been identified as:

- Continuing Healthcare and Personal Health Budgets;
- Primary Care;
- Commissioning of Services, especially Mental Health;
- ICT expenditure;
- Individual Patient Treatments, especially Freestyle Libre;

### Requests for Internal Reviews

2.18 If an applicant is dissatisfied with the response the CCG has provided they can request an internal review. During 2018/19 one requests was received for an internal review but information needed to process the review, was not forthcoming when asked for.

## 3. Conclusion

3.1 NHS Dorset CCG has 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.

3.2 The CCG has met the standards required for the DSPT submission for 2018/19. The DSP Team, with the assistance of representatives from IT and the DSP Group, will continue to ensure that the CCG complies with the requirements of the new Data Protection Act 2018 and will work to support directorates with the implementation of the changes to the forthcoming version of the DSPT.

3.3 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** |

**9.7**

**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 | Name of Senior Information Risk Owner. | Mandatory | COMPLETED |
| 1.1.2 | SIRO Responsibility for data security has been assigned. | Mandatory | COMPLETED |
| 1.1.3 | Name of Caldicott Guardian. | Mandatory | COMPLETED |
| 1.1.4 | Who are your staff with responsibility for data protection and/or security? | Mandatory | COMPLETED |
| 1.1.5 | Staff awareness- Leadership (Q1) I feel data security and protection are important for my organisation. | | |
| 1.1.6 | Name of Appointed Data Protection Officer. | 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 | There is a data security and protection policy or policies that follow relevant guidance. | Mandatory | COMPLETED |
| 1.2.2 | When were the data security and protection policy or policies last updated? | Mandatory | COMPLETED |
| 1.2.3 | Policy has been approved by the person with overall responsibility for data security. | Mandatory | COMPLETED |
| 1.2.4 | Data Security and Protection Policies available to the public. | | COMPLETED |
| 1.2.5 | Staff awareness - Policies (Q2). I know the rules about who I share data with and how. | | |

| | | | |
|---|---|---|---|
| 1.2.6 | Staff awareness – Policies (Q3). I know who to ask questions about data security in my organisation. | | |

| | | | |
|---|---|---|---|
| 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 | There is a staff procedure about how to provide information about processing and individuals’ rights at the correct time. | Mandatory | COMPLETED |
| 1.3.5 | There is an updated subject access process to meet shorter GDPR timescales. | Mandatory | COMPLETED |
| 1.3.6 | Provide details of how access to information requests have been complied with during the last twelve months. | Mandatory | COMPLETED |
| 1.3.7 | Total ICO Fines 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 | A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing. | Mandatory | COMPLETED |
| 1.4.2 | Have information flows been approved by the person responsible for data security? | Mandatory | COMPLETED |
| 1.4.3 | Date of when information flows were approved by the person with responsibility for data security. | Mandatory | COMPLETED |
| 1.4.4 | Provide a list of all systems/information assets holding or sharing personal information. | Mandatory | COMPLETED |
| 1.4.5 | List of systems which do not support individual login with the risks outlined and what compensating measures are in place. | 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 | Data Protection Compliance monitoring /staff spot checks are regularly carried out to ensure guidance is being followed. | Mandatory | COMPLETED |
| 1.5.3 | Results of staff spot checks and actions taken when data protection non-compliance is identified. | Mandatory | COMPLETED |
| 1.5.4 | Staff awareness Question - Used legally and securely (Q4) …. I am happy data is used legally and securely in my organisation. | | |

| | | | |
|---|---|---|---|
| 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 | Data Protection by design procedure has been agreed. | Mandatory | COMPLETED |
| 1.6.3 | There are technical controls that prevent information from being inappropriately copied or downloaded. | Mandatory | COMPLETED |
| 1.6.4 | There are physical controls that prevent unauthorised access to sites. | Mandatory | COMPLETED |
| 1.6.7 | There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance. | Mandatory | COMPLETED |
| 1.6.8 | The Data Protection Impact Assessment Procedure has been agreed by the person in the organisation with overall responsibility for data security. | | COMPLETED |
| 1.6.9 | The Data Protection Officer is consulted as a matter of routine when a Data Protection Impact Assessments is being carried out. | | COMPLETED |

| | | | |
|---|---|---|---|
| 1.6.10 | Have any unmitigated risks been identified through the Data Protection Impact Assessment process? | | COMPLETED |
| 1.6.11 | All high risk data processing has a Data Protection Impact Assessment carried out before processing commences. | Mandatory | COMPLETED |
| 1.6.12 | All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO. | Mandatory | COMPLETED |
| 1.6.13 | Data Protection Impact Assessments are published and available as part of the organisation’s transparency materials. | | |

| | | | |
|---|---|---|---|
| 1.7 | Effective data quality controls are in place. | | |
| 1.7.1 | There is policy and staff guidance on data quality. | Mandatory | COMPLETED |

| | | | |
|---|---|---|---|
| 1.8 | Personal information processed by the organisation is adequate (and not excessive) for the purposes. | | |
| 1.8.1 | There is guidance that sets out for staff the minimum retention periods for types of records and the action to be taken when records are to be securely destroyed or archived. | Mandatory | COMPLETED |
| 1.8.2 | A records retention schedule has been produced. | Mandatory | COMPLETED |
| 1.8.3 | Provide details of when personal data disposal contracts were last reviewed/updated. | 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 | When was the last review of the list of all systems/information assets holding or sharing personal information? | Mandatory | COMPLETED |

| | | | |
|---|---|---|---|
| 2.1.2 | The list of all systems/information assets holding or sharing personal confidential information has been approved as being accurate by the person with overall responsibility for data security. | Mandatory | COMPLETED |

| | | | |
|---|---|---|---|
| 2.2 | Personal Confidential Information is processed/shared legally and securely. | | |
| 2.2.1 | Staff awareness - Shared securely (Q5) …. I know how to use and transmit data securely. | | |
| 2.2.2 | Staff awareness - Used legally and securely (Q6) …. I feel that confidentiality is more important than sharing information for care. | | |
| 2.2.3 | Staff awareness - Processes (Q7) …. The tools and processes used by my organisation make it easy to use and transmit data securely. | | |
| 2.2.4 | Staff awareness - Raising concern (Q8) …. I can raise concerns about unsecure or unlawful uses of data, and I know that these will be acted on without personal recrimination. | | |

| | | | |
|---|---|---|---|
| 2.3 | Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards. | | |
| 2.3.1 | There is a data protection and security induction in place for all new entrants to the organisation. | Mandatory | COMPLETED |
| 2.3.2 | All employment contracts contain data security requirements. | Mandatory | COMPLETED |
| 2.3.3 | Staff awareness - Laws and principles (Q9) …. I understand the important laws and principles on data sharing, and when I should and should not share data. | | |
| 2.3.4 | Staff awareness - Data sharing questions (Q10) …. If I have a question about sharing data lawfully and securely I know where to seek help. | | |
| 2.3.5 | Staff awareness - Personal responsibility (Q11)…. I take personal responsibility for handling data securely. | | |

## 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 | A data security and protection training needs analysis has been completed. | Mandatory | COMPLETED |
| 3.1.2 | Date of last data security and protection training needs analysis. | Mandatory | COMPLETED |
| 3.1.3 | Training Needs analysis has been approved by the person with overall responsibility for data security. | Mandatory | COMPLETED |

| | | | |
|---|---|---|---|
| 3.2 | Staff receive suitable data security and protection training. | | |
| 3.2.1 | Staff awareness - Training (Q12) … The data security training offered by my organisation supports me in understanding how to use data lawfully and securely. | | |

| | | | |
|---|---|---|---|
| 3.3 | Staff pass the data security and protection mandatory test. | | |
| 3.3.1 | Percentage of Staff Successfully Completing the Level 1 Data Security Awareness training. | Mandatory | COMPLETED |
| 3.3.2 | Average mark of first attempt of Level 1 Training. | | |

| | | | |
|---|---|---|---|
| 3.4 | Staff with specialist roles receive data security and protection training suitable to their role. | | |
| 3.4.1 | Number of staff assessed as needing role specialist training. | Mandatory | COMPLETED |
| 3.4.2 | Number of staff completing advanced Data Security Training. | Mandatory | COMPLETED |
| 3.4.3 | Details of any Other data security and protection specialist training undertaken. | | COMPLETED |

| 3.5 | Leaders and board members receive suitable data protection and security training. | | |
|---|---|---|---|
| 3.5.1 | SIRO and Caldicott Guardian have received appropriate 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 | The organisation maintains a current record of staff and their roles. | Mandatory | COMPLETED |
| 4.1.2 | For each system holding personal and confidential data, the organisation understands who has access to the information. | Mandatory | COMPLETED |

| 4.2 | Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. | | |
|---|---|---|---|
| 4.2.1 | Date last audit of user accounts held. | Mandatory | COMPLETED |
| 4.2.2 | List of data security incidents in the last 12 months caused by a mismatch between user role and system accesses granted. | | COMPLETED |
| 4.2.3 | Staff awareness - Access to information (Q13): The level of access I have to IT systems holding sensitive information, is appropriate. | | |

| 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 | The person with responsibility for IT confirms that IT administrator activities are logged and those logs are only accessible to appropriate personnel. | | COMPLETED |

| | | | |
|---|---|---|---|
| 4.3.3 | Acceptable IT usage banner displayed to all staff when logging into system, including a personal accountability reminder. | | COMPLETED |
| 4.3.4 | List of all systems to which users and administrators have an account, plus the means of monitoring access. | | COMPLETED |
| 4.3.5 | Staff have provided explicit understanding that their activity of systems can be monitored. | Mandatory | 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 | Dates of process reviews held to identify and manage problem processes which cause security breaches. | Mandatory | COMPLETED |
| 5.1.2 | List of actions arising from the process review, with names of actionees. | | 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 person with overall responsibility for data security. | | COMPLETED |

## 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.

| | |
|---|---|
| 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 | List routes available for staff to report data security and protection breaches and near misses. | | COMPLETED |
| 6.1.3 | List of all data security breach reports in the last twelve months with action plans. | Mandatory | COMPLETED |
| 6.1.4 | The person with overall responsibility for data security is notified of the action plan for all data security breaches. | Mandatory | COMPLETED |
| 6.1.5 | Individuals affected by a breach are appropriately informed. | Mandatory | COMPLETED |

| 6.2 | Users know how to spot an incident and where to report it, and incidents are effectively reported. | | |
|---|---|---|---|
| 6.2.1 | Number of security and personal information breaches recorded. | | COMPLETED |
| 6.2.2 | Speed of data security and protection breach reporting. | | COMPLETED |
| 6.2.3 | Staff awareness - Reporting (Q14) - I know how to report a data security breach. | | |
| 6.2.4 | Number of breaches that have been reported to the Information Commissioner. | Mandatory | COMPLETED |

| 6.3 | All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway. | | |
|---|---|---|---|
| 6.3.1 | Name of anti-virus product. | Mandatory | COMPLETED |
| 6.3.2 | Number of alerts recorded by the AV tool in the last three months. | Mandatory | COMPLETED |
| 6.3.3 | Name of spam email filtering product. | | COMPLETED |
| 6.3.4 | Number of spam emails blocked per month. | Mandatory | COMPLETED |
| 6.3.5 | Number of phishing emails reported by staff per month. | | COMPLETED |

| | | | |
|---|---|---|---|
| 6.4 | Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses. | | |
| 6.4.1 | Number and details of incidents caused by a known vulnerability being exploited. | | COMPLETED |
| 6.4.2 | Have you had any repeat data security incidents of the same issue within the organisation. | | COMPLETED |
| 6.4.3 | Staff awareness - Incidents (Q 15) - When there is a data security incident my organisation works quickly to address it. | | |
| 6.4.4 | Staff awareness - Learning Lessons (Q16) - When there is a data security incident, or near miss, my organisation learns lessons and makes changes to prevent it happening again. | | |

## 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 | There is a continuity plan in place for data security incidents, and staff understand how to put this into action. | | |
| 7.7.1 | There is an incident management and business continuity plan in place for data security and protection. | Mandatory | COMPLETED |
| 7.1.2 | The incident plan has been approved by the person with overall responsibility for data security. | | COMPLETED |
| 7.1.3 | Staff awareness - Contingency plan (Q17) - If a data security incident was to prevent technology from working in my organisation, I know how to continue doing the critical parts of my job. | | |

| | | | |
|---|---|---|---|
| 7.2 | There is an effective annual test of the continuity plan for data security incidents. | | |
| 7.2.1 | Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held. | | |
| 7.2.3 | From the business continuity exercise which issues and actions were documented, with names of actionees listed against each item. | | |
| 7.2.4 | All emergency contacts are kept securely, in hardcopy and are up-to-date. | Mandatory | COMPLETED |
| 7.2.5 | Location of hardcopy of emergency contacts. | Mandatory | COMPLETED |
| 7.2.6 | Date emergency contact list updated. | Mandatory | COMPLETED |
| 7.2.7 | Date emergency contact list printed/shared. | | COMPLETED |
| 7.2.10 | Document any re-defined processes to respond to common forms of cyber-attack in the last twelve months. | | COMPLETED |

### 8 Unsupported Systems

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

| | | | |
|---|---|---|---|
| 8.1 | All software has been surveyed to understand if it is supported and up to date. | | |
| 8.1.1 | What software do you use? | Mandatory | COMPLETED |

| | | | |
|---|---|---|---|
| 8.2 | Unsupported software 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 | Where it is not possible to upgrade/update software, reasons are given. | | COMPLETED |
| 8.2.3 | The person with overall responsibility for data security 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 | Provide your strategy for security updates. | Mandatory | COMPLETED |
| 8.3.2 | How regularly do you apply security updates to desktop infrastructure? | Mandatory | COMPLETED |
| 8.3.3 | How often, in days, is automatic patching typically being pushed out to remote endpoints? | | COMPLETED |
| 8.3.4 | How many times, in the last twelve months has the person with overall responsibility for data security been notified where patches have not been applied for longer than two months, with reasons why? | | COMPLETED |
| 8.3.5 | List of where software updates have not been applied for longer than two months, with reasons why. | | 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 person with overall responsibility for IT infrastructure confirms all networking components have had their default passwords changed. | Mandatory | COMPLETED |
| 9.1.2 | A Penetration test has been conducted in the last 12 months, which confirmed that all networking components have had their default passwords changed. | | COMPLETED |

| | | | |
|---|---|---|---|
| 9.2 | Web applications owned by the organisation are secured against OWASP Top 10 vulnerabilities. | | |
| 9.2.1 | A penetration test has been conducted in the last 12 months, which confirmed web applications were not vulnerable to the Open Web Application Security Project (OWASP) Top 10 vulnerabilities. | | COMPLETED |
| 9.2.2 | The person with overall responsibility for IT has reviewed the results of latest penetration | | COMPLETED |

| | | | |
|---|---|---|---|
| | testing, with action plan against outstanding OWASP findings. | | |

| | | | |
|---|---|---|---|
| 9.3 | All organisations receive a penetration test annually, whether commercially sourced or in-house. The scope of the pen-test is articulated to the SIRO and signed by them. | | |
| 9.3.1 | The annual IT penetration testing is scoped in negotiation between the business and the testing team, and uploaded. | | COMPLETED |
| 9.3.2 | The SIRO confirms the scope of the annual IT penetration testing is adequate, and that actions from the previous penetration testing are complete or ongoing (with reasons for non-completion). | | COMPLETED |

| | | | |
|---|---|---|---|
| 9.4 | A data security improvement plan has been put in place on the basis of the assessment and has been approved by the SIRO. | | |
| 9.4.1 | The person with overall responsibility for data security confirms the organisation has a data security improvement plan. | | COMPLETED |
| 9.4.2 | What are your top three data security and protection risks? | | COMPLETED |
| 9.4.3 | Evidence that your management team has discussed your top three data security and protection risks and what is being done about them? | | COMPLETED |
| 9.4.4 | Date for full implementation of the data security improvement plan. | | |
| 9.4.5 | Data security improvement plan status. | | 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 | Mandatory | COMPLETED |

| | | | |
|---|---|---|---|
| | services they deliver, their contact details and the contract duration. | | |
| 10.1.2 | Contracts with all third parties that handle personal information are compliant with GDPR. | | |

| | | | |
|---|---|---|---|
| 10.2 | Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance. | | |
| 10.2.1 | Basic due diligence has been undertaken against each supplier according to ICO guidance. | Mandatory | COMPLETED |
| 10.2.2 | The person with overall responsibility for data security is assured that suppliers who are Data Processors are prepared for GDPR. | | |

| | | | |
|---|---|---|---|
| 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. | | COMPLETED |