The Royal Wolverhampton NHS Trust

# Information Governance (IG) Data Protection and Security Toolkit (DPST) 2018/19

## 1 April 2019

Agenda Item No: 11.8

Safe & Effective | Kind & Caring | Exceeding Expectation

The Royal Wolverhampton NHS Trust

# Trust Board Report

| | |
|---|---|
| **Meeting Date:** | 1st April 2019 |
| **Title:** | Information Governance (IG) Data Protection and Security Toolkit (DPST) 2018/19 |
| **Purpose of the Report:** | To provide assurances around the Trust compliance to national Information Governance standards. |
| **Summary:** | To keep the board informed on DPST Toolkit scores for submission to the Department of Health by 31st March 2019.<br><br>➢ RL4 - The Royal Wolverhampton NHS Trust<br>➢ Alfred Squire M92002<br>➢ West Park Surgery M92042<br>➢ Thornley Street M92028<br>➢ Ettingshall Y02735<br>➢ Lea Road M92007<br>➢ Penn Manor M92011<br>➢ Coalway Road M92006<br>➢ Warstones M92044<br>➢ Lakeside M83132<br><br>DPST Toolkit evidence has been ratified by IG Steering Group (IGSG) on 5th March 2019 and Compliance Oversight Group (COG) on the 15th March 2019, Quality Governance Assurance Committee 20th March 2019 and Trust Management Committee 22nd March 2019. |
| **Action required:** | For information: Scores will be ratified as per the above committees |
| **Clinical implications and view** | N/A |
| **Patient, carer, public impact and views** | N/A |
| **Resource implications** | N/A |
| **Report of:** | Dr Jonathan Odum<br><br>Medical: Director/ Caldicott Guardian |
| **Author + Contact Details:** | Tel Raz Edwards – Information Governance Manager / DPO<br>Tel 01902 307999 Email Raz.Edwards@nhs.net |
| **CQC Domains** | **Safe:** patients, staff and the public are protected from abuse and avoidable harm.<br>**Effective:** care, treatment and support achieves good outcomes, helping people maintain quality of life and is based on the best available evidence.<br>**Caring:** staff involve and treat everyone with compassion, kindness, dignity and respect.<br>**Responsive:** services are organised so that they meet people's needs.<br>**Well-led:** the leadership, management and governance of the organisation make sure it's providing high-quality care that's based around individual needs, that it encourages learning and innovation, and that it promotes an open and fair culture. |

| | |
|---|---|
| **Trust Strategic Objectives** | 1. Create a culture of compassion, safety and quality<br>3. To have an effective and well integrated local health and care system that operates efficiently |
| **Links to Assurances** | |
| **Resource Implications:** | N/A |
| **Equality and Diversity Impact** | N/A |
| **Risks:** | N/A |
| **Risk register reference:** | N/A |
| **Other formal bodies involved:** | N/A |
| **References** | N/A |

## Report Details

**1**

### Background detail on the IG Toolkit

The DSPT Toolkit is a Department of Health (DH) Policy delivery vehicle that NHS Digital is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DH policy and presents them in in a single standard as a set of information governance requirements. The new DSPT toolkit has also incorporated assurances around the General Data Protection Regulation 2016 and the national cyber security centre.

The purpose of the assessment is to enable the Trust to measure compliance against the law and central guidance and to see whether information is handled correctly and protected from unauthorised access, loss, damage and destruction.

Where non-compliance to mandatory evidence requirements is revealed, the Trust is required to take appropriate measures, (e.g. assign responsibility, put in place policies, procedures, processes and guidance for staff), with the aim of making cultural changes and raising information governance standards through year on year improvements. The ultimate aim is to demonstrate that the Trust can be trusted to maintain the confidentiality and security of personal information. This in-turn increases public confidence that the Trust can be trusted with personal data.

The Trust is also seeking assurance for the GP partnerships that are a part of Primary Care Directorate. Each GP Partnership is currently a registered data controller and therefore required to comply and submit their own toolkit submission.

For the purposes of this report we are seeking assurances on the following toolkit submissions for the following organisation codes for the October position statement:

- RL4 - The Royal Wolverhampton NHS Trust
- Alfred Squire M92002
- West Park Surgery M92042
- Thornley Street M92028
- Ettingshall Y02735
- Lea Road M92007
- Penn Manor M92011
- Coalway Road M92006
- Warstones M92044
- Lakeside M83132

This is the first full submission of the new Data Protection and Security Toolkit (DPST) hosted by NHS digital. The approach has changed from 45 requirements for a large acute trust to 10 national data standards comprising of 40 assertions. Within these assertions there are currently 100 **mandatory** evidence requirement for a large organisation, which the Trust is required to demonstrate they do or they don't comply with. The levels of compliance have been removed and replaced by mandatory and non-mandatory requirements. Large organisations are required to demonstrate compliance against 100 of the mandatory requirement.

As with the old toolkit, GP practices will continue to submit their own separate toolkits (after advice sought from NHS digital) which means that in total the Trust will have to monitor compliance against 10 toolkits in total. All GP practices are working to harmonise their evidence so all practices submit the same evidence, and where possible this will be harmonised with the RL4 Trust toolkit. GP practices have 10 data standards with 30 assertions and 52 mandatory evidence requirements. GP practices are not required to submit in October but will still provide the same level of assurance.

Appendix 1 shows a breakdown of the RL4 Trust toolkit submission and the GP submissions with mandatory requirements shown and where not achieved any actions that are required to achieve compliance for the March 2019 submission.

In summary the RL4 submission currently has 96 completed mandatory elements with 4 outstanding. For GP practices 52 mandatory completed with no outstanding requirements.

It is important to emphasise that a non-mandatory submission may have impact on contractual relationships with other providers in terms of the level of assurance they require. Any requirement that are not met by March 2019 will automatically be reported by NHS digital to CQC, which will feature in the inspection framework, under well led. 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 DSP Toolkit 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 DSP Toolkit. Many information sharing projects and partnerships use the completion of DSP Toolkit to a status of 'Standards met' as a pre-qualification question for joining.

Summary of the IG Toolkit position to be approved.

| | | | | | |
|---|---|---|---|---|---|
| **Assessment DSPT toolkit 2018/19** | | **requirement achieved** | **Requirement not achieved** | **Total mandatory requirements** | **Overall Result** |
| | Performance Update RWT – March 2019 | 96 | 4 | 100 | **Standards Not met** |
| | Performance Update GP practices - Oct 2018 | **52** | **0** | **52** | **Standards met** |

**Not all mandatory requirements met**

**Mandatory standards met**

**2**

**Action required by Committee**

DPST Toolkit evidence has been ratified by IG Steering Group (IGSG) on 5th March 2019 and Compliance Oversight Group (COG) on the 15th March 2019, Quality Governance Assurance Committee 20th March 2019 and Trust management Committee 22nd March 2019. All GP submissions will be submitting as **'Standards Met'** The RL4 Trust

| | |
|---|---|
| | submission will be looking to achieve a status of **Standards Not Met (Improvement Plan)**, which will mean that an agreed action plan will be submitted for approval by NHS digital for the 4 standards that have not been achieved by the 31st March 2019.<br><br>All evidence will be reviewed and assurance will be requested from internal audit on evidence submitted to achieve compliance. |

## Appendix 1

| Assertion | Order | Evidence required | Director responsible for req. | RL4 Trust Mandatory | GP Mandatory | Outstanding actions to achieve compliance |
|---|---|---|---|---|---|---|
| 1.1 There is senior ownership of data security and protection within the organisation. | 1.1 | Name of Senior Information Risk Owner. | Dr Odum | Yes | | |
| | 1.12 | SIRO responsibility for data security has been assigned. | Dr Odum | Yes | | |
| | 1.13 | Name of Caldicott Guardian. | Dr Odum | Yes | Yes | |
| | 1.14 | Who are your staff with responsibility for data protection and / or security? | Dr Odum | Yes | Yes | |
| | 1.16 | Name of Appointed Data Protection Officer. | Dr Odum | Yes | Yes | |
| 1.2 There are clear data security and protection policies in place and these are understood by staff and available to the public. | 1.21 | There is a data security and protection policy or policies that follow relevant guidance. | Dr Odum | Yes | Yes | |
| | 1.22 | When were the data security and protection policy or policies last updated? | Dr Odum | Yes | Yes | |
| | 1.23 | Data Security and Protection policy has been approved by the SIRO | Dr Odum | Yes | Yes | |
| 1.3 Individuals' rights are respected and supported (GDPR Article 12-22). | 1.31 | ICO registration number. | Dr Odum | Yes | Yes | |
| | 1.32 | Transparency information is published and available to the public. | Dr Odum | Yes | Yes | |
| | 1.33 | How have Individuals been informed about their rights and how to exercise them? | Dr Odum | Yes | Yes | |
| | 1.34 | There is a staff procedure about how to provide information about processing and individuals' rights at the correct time. | Dr Odum | Yes | Yes | |
| | 1.35 | There is an updated subject access process to meet shorter GDPR timescales. | Dr Odum | Yes | Yes | |
| | 1.36 | Provide details of how access to information requests have been complied with during the last twelve months. | Dr Odum | Yes | | |
| 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). | 1.41 | A record (e.g. register or registers) that details each use or sharing of personal information including the legal basis for the processing and if applicable, whether national data opt outs have been applied. | K Stringer | Yes | Yes | |
| | 1.42 | Have information flows been approved by the SIRO or equivalent local method? | K Stringer | Yes | Yes | RL4 – Action plan submitted. Asset owners have been asked to confirm data flows have been mapped; results awaited and will be analysed. (SP) |
| | 1.43 | Date of when information flows were approved by the board or equivalent. | K Stringer | Yes | | RL4 – Action plan submitted. Asset owners have been asked to confirm data flows have been mapped; |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | results awaited and will be analysed. (SP) |
| | 1.44 | Provide a list of all systems / information assets holding or sharing personal information. | K Stringer | Yes | Yes | |
| | 1.45 | List of systems which do not support individual login with the risks outlined and what compensating measures are in place. | K Stringer | Yes | Yes | |
| 1.5 Personal information is used and shared lawfully. | 1.51 | There is approved staff guidance on confidentiality and data protection issues. | Dr Odum | Yes | Yes | |
| | 1.52 | Data protection compliance monitoring / staff spot checks are regularly carried out to ensure guidance is being followed. | Dr Odum | Yes | Yes | |
| | 1.53 | Results of staff spot checks and actions taken when data protection non-compliance is identified. | Dr Odum | Yes | Yes | |
| 1.6 The use of personal information is subject to data protection by design and by default. | 1.61 | There is a procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements. | K Stringer | Yes | Yes | |
| | 1.62 | Data Protection by design procedure agreed by local governance process. | K Stringer | Yes | | |
| | 1.63 | There are technical controls that prevent information from being inappropriately copied or downloaded. | K Stringer | Yes | Yes | |
| | 1.64 | There are physical controls that prevent unauthorised access to sites. | K Stringer | Yes | Yes | |
| | 1.65 | Date of last audit of pseudonymisation, anonymisation or de-identification controls. | K Stringer | Yes | | |
| | 1.66 | Overall findings of last audit of [pseudonymisation, anonymisation or de-identification] controls. | K Stringer | Yes | | |
| | 1.67 | There is a staff procedure on carrying out a Data Protection Impact Assessment that follows relevant ICO guidance. | K Stringer | Yes | Yes | |
| | 1.68 | The Data Protection Impact Assessment Procedure has been agreed by the Board or equivalent. | K Stringer | Yes | | |
| | 1.6.10 | Have any unmitigated risks been identified through the Data Protection Impact Assessment process? | K Stringer | Yes | | |
| | 1.611 | All high risk data processing has a Data Protection Impact Assessment carried out before processing commences. | K Stringer | Yes | Yes | |
| | 1.612 | All Data Protection Impact Assessments with unmitigated risks have been notified to the ICO. | K Stringer | Yes | Yes | |
| | 1.613 | Data Protection Impact Assessments are published and available as part of the organisation's transparency materials. | K Stringer | Yes | | |
| 1.7 Effective data quality controls are in place | 1.7.1 | There is policy and staff guidance on data quality. | K Stringer | Yes | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1.72 | The scope of the data quality audit was in line with guidelines. | K Stringer | Yes | | |
| | 1.73 | Date of last data quality audit. | K Stringer | Yes | | |
| 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. | Dr Odum | Yes | Yes | |
| | 1.82 | A records retention schedule has been produced. | Dr Odum | Yes | Yes | |
| | 1.83 | Provide details of when personal data disposal contracts were last reviewed / updated. | Dr Odum | Yes | | |
| | 1.84 | Date of last audit being made on data disposal contractors to ensure security is of the appropriate agreed standard. | Dr Odum | Yes | | |
| 2.1 There is a clear understanding of what Personal Confidential Information is held. | 2.11 | When was the last review of the list of all systems / information assets holding or sharing personal information? | K Stringer | Yes | Yes | |
| | 2.12 | The list of all systems / information assets holding or sharing personal confidential information has been approved as being accurate by the SIRO or equivalent local method. | K Stringer | Yes | | |
| 2.3 Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards. | 2.31 | There is a data protection and security induction in place for all new entrants to the organisation. | Dr Odum | Yes | Yes | |
| | 2.32 | All employment contracts contain data security requirements. | Dr Odum | Yes | Yes | |
| 3.1 There has been an assessment of data security and protection training needs across the organisation. | 3.11 | A data security and protection training needs analysis has been completed. | Dr Odum | Yes | | |
| | 3.12 | Date of last data security and protection training needs analysis. | Dr Odum | Yes | | |
| | 3.13 | Training needs analysis has been approved by the SIRO or equivalent. | Dr Odum | Yes | | |
| 3.3 Staff pass the data security and protection mandatory test. | 3.31 | Percentage of staff successfully completing the Level 1 Data Security Awareness training. | Dr Odum | Yes | Yes | |
| 3.4 Staff with specialist roles receive data security and protection training suitable to their role. | 3.41 | Number of staff assessed as needing role specialist training. | Dr Odum | Yes | | |
| | 3.42 | Number of staff completing specialist Data Security Training. | Dr Odum | Yes | | |
| | 3.43 | Details of any specialist data security and protection training undertaken . | Dr Odum | Yes | | |
| 3.5 Leaders and board members receive suitable data protection and security training. | 3.51 | SIRO and Caldicott Guardian have received appropriate data security and protection training. | Dr Odum | Yes | | |
| | 3.52 | List of board members. | Dr Odum | Yes | | |
| | 3.53 | Percentage of board members completing appropriate data security and protection training. | Dr Odum | Yes | | |
| 4.1 The organisation maintains a current record of staff and their | 4.11 | Confirmation that the organisation maintains a current record of staff and their roles. | A Duffell | Yes | Yes | |

| | | | | | | |
|---|---|---|---|---|---|---|
| roles. | 4.12 | For each system holding personal and confidential data, the organisation understands who has access to the information. | A Duffell | Yes | Yes | **RL4 action-** Information around who has access to personal and confidential data will be requested from all asset owners on asset register (DL) |
| 4.2 Staff roles are linked to IT accounts. Staff moves in, out or across the organisation are reflected by IT accounts administration. | 4.21 | Date last audit of user accounts held. | K Stringer | Yes | | |
| 4.3 All staff understand that their activities on IT systems will be monitored and recorded for security purposes. | 4.31 | All system administrators have signed an agreement which holds them accountable to the highest standards of use. | K Stringer | Yes | Yes | |
| | 4.34 | List of all systems to which users and administrators have an account, plus the means of monitoring access. | K Stringer | Yes | | |
| | 4.35 | Staff have provided explicit understanding that their activity of systems can be monitored. | K Stringer | Yes | Yes | |
| 5.1 Process reviews are held at least once per year. | 5.11 | Dates of process reviews held to identify and manage problem processes which cause security breaches. | Dr Odum | Yes | Yes | |
| 6.1 A confidential system for reporting security breaches and near misses is in place and actively used. | 6.11 | A data security and protection breach reporting system is in place. | Dr Odum/ K Stringer | Yes | Yes | |
| | 6.13 | List of all data security breach reports in the last twelve months with action plans. | Dr Odum/ K Stringer | Yes | Yes | |
| | 6.14 | The board or equivalent is notified of the action plan for all data security breaches. | Dr Odum/ K Stringer | Yes | | |
| | 6.15 | Individuals affected by a breach are appropriately informed. | Dr Odum/ K Stringer | Yes | Yes | |
| | 6.24 | Number of breaches that have been reported to the Information Commissioner | Dr Odum/ K Stringer | Yes | Yes | |
| 6.3 All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway. | 6.31 | Name of anti-virus product. | K Stringer | Yes | Yes | |
| | 6.32 | Number of alerts recorded by the AV tool in the last three months. | K Stringer | Yes | Yes | |
| | 6.33 | Name of spam email filtering product. | K Stringer | Yes | | |
| | 6.34 | Number of spam emails blocked per month. | K Stringer | Yes | Yes | |
| | 6.35 | Number of phishing emails reported by staff per month. | K Stringer | Yes | | |
| 6.4 Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses. | 6.41 | Number and details of incidents caused by a known vulnerability being exploited. | K Stringer | Yes | | |
| 7.1 There is a continuity plan in place for data security incidents, and staff understand how to put this into action. | 7.11 | There is an incident management and business continuity plan in place for data security and protection. | G Nuttall | Yes | Yes | |
| 7.2 There is an effective annual test of the continuity plan for data security incidents. | 7.21 | Scanned copy of data security business continuity exercise registration sheet with attendee signatures and roles held. | G Nuttall | Yes | | **RL4 action** - We have not done a specific test for data security incidents but have for other business continuity issues like loss of premises. The Trust is yet to undertake a specific data security incident exercise/include as part of next business continuity exercise.(July 2019) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 7.24 | All emergency contacts are kept securely, in hardcopy and are up-to-date. | G Nuttall | Yes | Yes | |
| | 7.25 | Location of hardcopy of emergency contacts. | G Nuttall | Yes | Yes | |
| | 7.26 | Date emergency contact list updated. | G Nuttall | Yes | Yes | |
| | 7.210 | Document any re-defined processes to respond to common forms of cyber attack in the last twelve months. | G Nuttall | Yes | | |
| 8.1 All software has been surveyed to understand if it is supported and up to date. | 8.11 | What software do you use? | K Stringer | Yes | | |
| 8.2 Unsupported software is categorised and documented, and data security risks are identified and managed. | 8.21 | List of unsupported software prioritised according to business risk, with remediation plan against each item. | K Stringer | Yes | | |
| | 8.22 | Where it is not possible to upgrade / update software, reasons are given. | K Stringer | Yes | | |
| | 8.23 | The SIRO confirms that the risks of using unsupported systems are being treated or tolerated. | K Stringer | Yes | | |
| 8.3 Supported systems are kept up-to-date with the latest security patches. | 8.31 | Provide your strategy for security updates. | K Stringer | Yes | Yes | |
| | 8.32 | How regularly do you apply security updates to desktop infrastructure. | K Stringer | Yes | Yes | |
| | 8.33 | How often, in days, is automatic patching typically being pushed out to remote endpoints? | K Stringer | Yes | | |
| | 8.34 | How many times, in the last twelve months, has the SIRO or equivalent senior role been notified where patches have not been applied for longer than two months, with reasons why? | K Stringer | Yes | | |
| | 8.35 | List of where software updates have not been applied for longer than two months, with reasons why. | K Stringer | Yes | | |
| 9.1 All networking components have had their default passwords changed. | 9.11 | The Head of IT, or equivalent role, confirms all networking components have had their default passwords changed. | K Stringer | Yes | Yes | |
| | 9.12 | A penetration test has been conducted in the last 12 months, which confirmed that all networking components have had their default passwords changed | K Stringer | Yes | | |
| 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. | 9.31 | The annual IT penetration testing is scoped in negotiation between the business and the testing team, and uploaded. | K Stringer | Yes | | |
| | 9.32 | 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). | K Stringer | Yes | | |
| | 9.33 | The date the penetration test was undertaken. | K Stringer | Yes | | |
| 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. | 9.41 | The SIRO or equivalent senior role confirms the organisation has a data security improvement plan. | Dr Odum/ K Stringer | Yes | | |
| | 9.42 | What are your top three data security and protection risks? | Dr Odum/ K Stringer | Yes | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | 9.43 | Evidence that your board has discussed your top three data security and protection risks and what is being done about them. | Dr Odum/ K Stringer | Yes | | |
| | 9.45 | Data security improvement plan status. | Dr Odum/ K Stringer | Yes | | |
| 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. | K Stringer | Yes | Yes | |
| 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. | K Stringer | Yes | Yes | |
| | 10.2 2 | Percentage of suppliers with data security contract clauses in place. | K Stringer | Yes | | |