Report to:	Public Board of Directors	Agenda item:	14
Date of Meeting:	26 February 2020		

Title of Report:	**Data Security & Protection Toolkit (DSPT) Pre-submission Report**
Status:	**For Approval**
Board Sponsor:	**Libby Walters, Director of Finance & Deputy Chief Executive**
Author:	**Graeme Temblett-Willis, Head of Information Governance and Data Protection Officer**
Appendices	**Appendix 1: RUH Bath DSPT Status as at 28/01/2020**

1. Purpose of Report (Including link to objectives)

The purpose of this report is to update the Board on the Information Governance programme, confirming the results to date of the Toolkit assessment for 2019/20 and internal audit outcome. To provide an overview of the arrangements in place to manage information risks and improve compliance in the year ahead and to provide a progress summary of the activities undertaken by the Information Governance Team in-year.

2. Summary

The DSPT is a structured assurance framework and will provide the basis for compliance with the new General Data Protection Regulation (GDPR) and Data Protection Act 2018.

The DSPT is an online assessment tool produced by the Department of Health and hosted on their behalf by NHS Digital. It draws together the relevant information management legislation and national guidance under a single framework designed to enable an organisation to implement the relevant standards. It enables the Trust to measure its performance through an annual self-assessment audit process and report upon levels of compliance against a set number of assertions. The DSPT allows organisations to measure their performance against the National Data Guardian's 10 data security standards.

All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

The Trust was required during this assessment to measure itself against 44 assertions and 116 mandatory evidence items which represents an increase of 16 on the previous year's requirement. Organisations can only achieve a final overall score of "Standards Met" by providing evidence against each of the mandatory items and confirming all the necessary assertions. This mechanism equates to a standards met /standards not met outcome. It should be noted that this report is provided ahead of the required submission date of 31st March 2020. The assertions that are highlighted in the report as having not been met each have an action plan attached to them to drive accreditation by the end of March 2020.

During the collection of the evidence it was found that there was a significant increase in emphasis on IT protection, cyber security, and ensuring that the GDPR requirements in relation to data flows and data sharing including completion of Data Protection Impact

Assessments (DPIA's) have been adopted as routine practice.

The Trust's submission for 2019/20 will take place in or around the 31st March 2020. Prior to January 2020 the Trust's internal auditors, Grant Thornton, audited the DSP Toolkit submission for 2018/19 and the new mandatory items in this current version providing their overall opinion as **Significant Assurance** with some minor improvement. The Board can take assurance that the controls upon which the organisation relies to manage IG are suitably designed, consistently applied and effective but would benefit from undertaking a "deep dive" into the Trust to enhance the understanding of all information assets and data flows in and out of the organisation to provide even greater assurance.

3.	Recommendations (Note, Approve, Discuss etc)
Request to note and approve the DSP Toolkit return by the Trust for 2019/20.	

4.	Care Quality Commission Outcomes (which apply)
The DSP Toolkit helps demonstrate compliance with Regulation 17 – Good governance.	

5.	Legal / Regulatory Implications (ICO)

General Data Protection Regulation (GDPR) / Data Protection Act 2018

The General Data Protection Regulation (GDPR) came into force on 25 May 2018 supported by the Data Protection Act (2018), replacing the Data Protection Act (1998). The GDPR is applicable to any organisation that processes personal data – public, private and voluntary sectors. The key themes of the new legislation are more rights for individuals in relation to how their personal data is processed and more obligations for organisations that are processing personal data, whether of staff or patients / service users.

The Freedom of Information Act (FOIA)

Responding to requests under the Freedom of Information Act (2000) has been the responsibility of the Information Governance Team. The service is administered by one 1 WTE member of staff and managed by the Head of IG. FOI activity is monitored by the Information Governance Group and each request has Executive sign off by the SIRO / Deputy CEO Libby Walters. The FOI Act states that in order for a request to be compliant with the legislation then the information must be provided and responded to within 20 working days.

Under the FOI Act, anyone in the world can make a request to see information from Royal United Hospitals NHS Foundation Trust. The volume of requests we receive has increased as professionals, commercial companies, press, media and the public have become more familiar with the Act. Annual growth in request volume is listed below:

Year	Volume of requests
2017-18	724
2018-19	705
2019-20	763

Most requests are received for information held by Human Resources, the BIU, IT

and Finance with the Surgical Division also receiving a large number of requests. Some requests are complex and require detailed consideration to appropriately apply relevant exemptions under the Act. Delays in responses can occur when information is required from different specialities and departments.
It should be noted that the volume of requests can rarely give an indication of the amount of time spent in answering each one. Some requests involve reporting on data that we routinely collect and can be completed relatively quickly but others may involve large amounts of work by different departments and we frequently have to judge whether answering a request would exceed the 18 hours "appropriate cost limit".

In spite of the volume and complexities for some of the requests the FOI Coordinator has consistently maintained the Trust compliance level at an average of 94.3% for the last twelve months against the Regulatory requirement set by the ICO (Information Commissioner's Office) of 90%.

Access to Health Records requests made under the Data Protection Act (DPA)

During 2019/20, the Trust received 1298 requests for Access to Health Records. The response time was reduced from 40 days to 30 days on the 25/05/2018. This represent a fall of just 15 compared to this time in 2018/19. The service ensures that customers are made aware of any potential delays. The department is not aware of any complaints being received in relation to the service.

The right of access to health records is governed by rules set out under the DPA2018. Requests must be processed under their own individual merit and Data Controllers must consider whether each request meets the lawful requirements for provision. Many requests are straightforward but some are complex and require expert review to ensure the confidentiality rights of the data subject (and any associated third parties) are maintained.

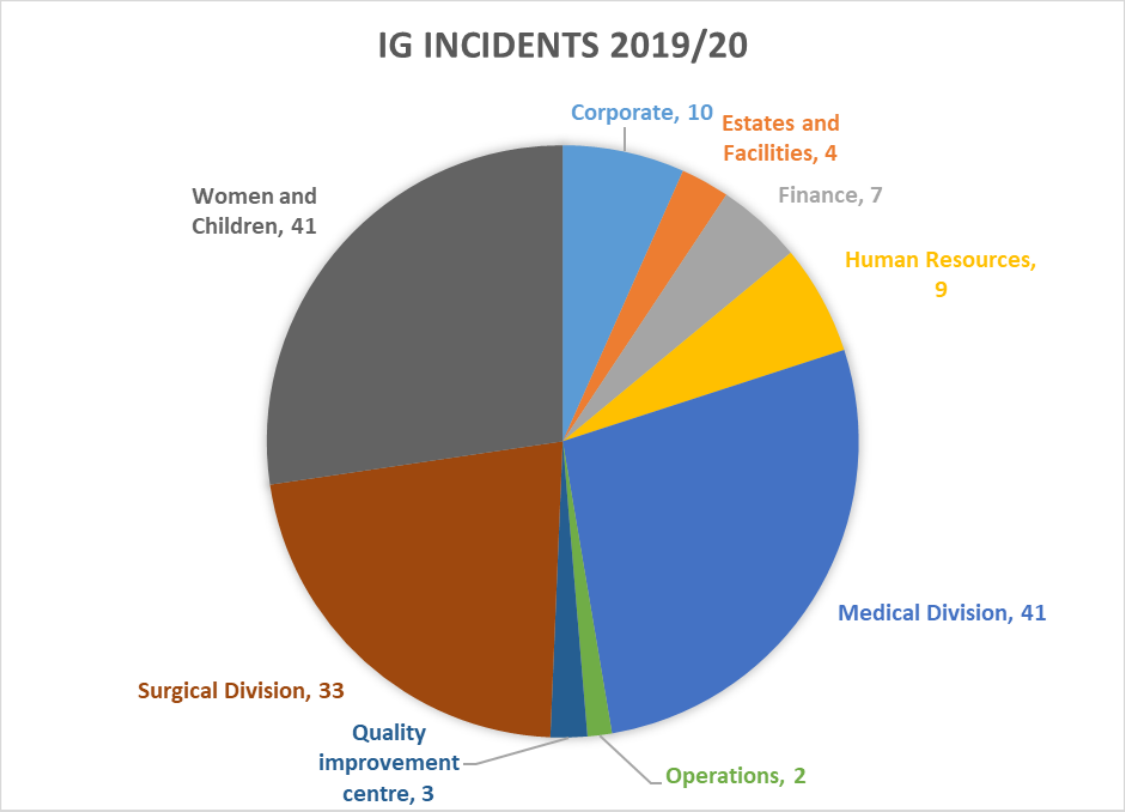
	Apr-19	May-19	Jun-19	Jul-19	Aug-19	Sep-19	Oct-19	Nov-19	Dec-19	Total
Medico Legal	92	105	99	114	88	72	95	104	86	855
Subject Access	24	23	28	35	38	39	26	30	28	271
Police	13	6	8	14	11	7	10	10	10	89
Healthcare Provider	9	7	4	5	8	7	21	12	10	83
	138	141	139	168	145	125	152	156	134	**1298**

Additionally, the Information Governance Team manage the SARs (Subject Access Requests) submitted from members of staff which are particularly time consuming and challenging for the organisation due to the issues of recovering emails held by other staff and the process of redaction which needs to be completed within 30 days. The Trust does not have a dedicated SAR Team to manage all requests and the sensitivities that can also surround them, especially in relation to the staff applications which has meant providing extra resource from other IM&T functions to assist with the compliance.

Information Governance Data Incidents

The Trust reported two externally reportable serious Information Governance incidents to the ICO during 2019/20. Both of these were satisfactorily investigated and the Trusts IG team were commended by the ICO at the expeditious approach to each incident and the thorough reporting and actions undertaken in each case. This resulted in no further action being taken.

Confidentiality or information governance issues continue to be well reported via the Trust's Incident Reporting process, Datix. 150 incidents were reported during 2019/20 which compares to 170 during the same reporting period for 2018/19. Incidents are disseminated to the SIRO, Caldicott Guardian, the Head of IG / DPO and the CIO simultaneously (in real time, as they are reported). This enables prompt response where needed. They are also provided as a standing agenda item at the IG Group where wider awareness can be disseminated by the Group membership.



Most incidents are minor but the national reporting and assessing of IG incidents has changed since 2018. The main reporting has been the transmission of emails to incorrect recipients but the majority have all been in 'trusted organisations' which has resulted in low risk to the data subjects. The other main reporting is through documentation sent to the wrong patient often as a result of incorrect NHS Spine detail and this is a National trend not just within the Trust.

Serious incidents formerly referred to as SIRIs are now assessed and judged for seriousness and therefore externally reportable according to new criteria based on likelihood and impact on the data subject(s) affected. The very low number of incidents (2) is testament to the positive culture of IG awareness cultivated in the

Trust over recent years and the ongoing reporting of lesser breaches reassures that staff have embraced the need for honesty and transparency with regards to the management of personal information. The volume of IG incidents reported reinforces the value of continuing training and raising of data protection awareness.

Risk Management & Assurance

The SIRO is responsible for overseeing the development and implementation of the information risk strategy. The SIRO is supported in this by the IG team and by Information Asset Owners (IAO) within each business area. The IAO is responsible for managing information risks to the assets within their control. This involves developing system security policies (SLSP) and business continuity plans as well as documenting their personal data information flows and conducting regular information risk assessments.

The IG and the IT Management team support IAOs in achieving these objectives. Whilst progress has been made again during 2019/20, further work is required to embed these processes. A review of the IAO structure has taken place and is in the process of being taken forward by the IG team with the support of both the SIRO and CIO. This will provide assurance that the correct members of staff have good control and knowledge of the data assets in their Specialities but also to enable collaborative working between clinical teams, Information Governance and the IM&T to remove the obstacles sometimes encountered by not engaging at an early stage of any project or new technology.

Mandatory IG Training

IG training is available in several different formats to suit individual needs. Staff may choose to undertake the e-learning IG module provided by NHS Digital, attend a trainer-led classroom session or they may complete the IG assessment that is available via the new IG intranet page (https://RUH Bath IG Assessment 2020) which would appear to be the easiest method for staff in busy clinical areas and who have difficulty in gaining access to a PC.

Figures from ESR state that IG Training Compliance is at 84.4%. RUH Bath is currently short of the national target of 95% staff compliance expected of NHS Trusts so there is additional progress to make, although training is regarded as ongoing throughout the year and compliance will fluctuate as individuals' annual completion dates occur. Factors also to be taken into control include absence and turnover rates. Support from the Trust leadership and HR services continues and is critical to ensure the Trust continues to improve and to steadily close the IG training compliance gap throughout the year.

However, there is a risk that with not being able to achieve the 95% national target this will mean that the Trust has not met the required Satisfactory standard for the years DSPT submission. Our contracts with the CCG's and external suppliers require that we have reached a satisfactory level against the mandatory evidence items of the toolkit to be able to satisfy due diligence checks carried out by those organisations and stakeholders. Achieving the minimum status for the mandatory annual IG training is important should there be any breaches of patient

confidentiality, as this is an area that the Information Commissioners Office would form part of their investigations on, and could have a bearing on any potential enforcement action to be taken against the Trust and individual. It is therefore imperative that managers take responsibility for ensuring their staff complete all mandatory. It also forms part of the CQC inspection process.

Audits (Spot Checks)

The IG Team has continued to undertake spot check audits throughout the Trust services during 2019/20. IG Audits take the form of a brief visit to a service area, use of an IG & Security checklist tool and supporting conversation with staff on duty in the service. Both clinical and corporate areas are audited. Services which report higher than usual numbers of IG incidents are also visited so that the IG service may offer additional support to improve practice.
This work is efficient in increasing awareness of IG requirements and celebrating good practice in situ. Such audits are part of ensuring compliance with the national Data Security and Protection Toolkit.

Cyber Security

The Trust continues to use NHS Digital's CareCERT Programme, including both the Advisory service and CareCERT Collect portal to monitor and report on vulnerabilities. Between them they provide details of known vulnerabilities, how they are remediated and allow the Trust to respond to medium and high vulnerabilities respectively with central visibility and reporting.

There have been no identified significant Cyber or Information Security issues during 2019/20. As part of further ongoing security enhancements to the Trust's core IT infrastructure, site firewalls have been upgraded and incorporate the latest security enhancements to detect and reduce security threat whilst also improving capacity and demand. The annual Penetration test, as a requirement of the DSPT, is planned and scheduled for March 2020 but it is unclear if this will be achievable due to the capacity of the IT Infrastructure team and current ongoing work.

There has been an improved training agenda for staff across the Trust in relation to the Cyber threat and includes Board cyber awareness training delivered by Templar Executives via NHS Digital Cyber Services, RCUU (Regional Cyber Crime Unit A&S Police) cyber awareness for staff, Red Goat GCHQ approved social engineering course for data specialists and SIRO training also delivered by Templar Executives via NHS Digital.

A separate Cyber Security report is provided to Board by the Head of Infrastructure and provides greater detail on the current Cyber Essentials Plus programme.

Networking and Collaboration

Internally, the Head of IG/DPO and IG Team are represented at various groups and committees on both ad hoc and regular bases, for example, the Informatics Board, Non-Clinical Digital Strategy Group, Data Quality Steering Group, and Information Governance Group. Externally, the Head of IG/DPO contributes to the West of

England Strategic Information Governance Network (SIGN), the WiSC (Wiltshire information Sharing Charter), WIGF (Wessex Information Governance Forum) and the BSW STP sharing advice, guidance and working practices in relation to the application of new legislation and general data protection compliance. The Head of IG/DPO has also been instrumental in driving forward the BSW STP data sharing agreement for the eWorkforce programme which is hoped to be achieved in the very near future which will be the first level of extensive data sharing for the BSW STP programme.

National Data Opt Out

NHS Digital has developed a new system to support the National Data Opt-out Programme which will give patients more control over how identifiable health and care information is used. The system will offer patients and the public the opportunity to make an informed choice about whether they wish their personally identifiable data to be used just for their individual care and treatment or also used for research and planning purposes. Patients and the public who decide they do not want their personally identifiable data used for planning and research purposes will be able to set their national data opt-out choice online. All health and care organisations will be required to uphold patient and public choices by March 2020 using the new system. The Trust has managed this requirement throughout the year and has reached the standards necessary for compliance with communications being rolled out during February – July to ensure staff and patients are aware of this National Programme.

Conclusion

The Trust has a robust process for managing IG and the associated responsibilities that come with its commitment to adopt best practice processes and procedures in order to protect patient and service users' information. It has a dynamic action plan to refresh and improve its compliance with the Data Security and Protection Toolkit standards. Evidence for many of the standards is refreshed as part of established daily business or monitoring activities. However, some objectives are more challenging and for this reason are being targeted already.

Key areas identified below:

Area	Rationale
Promote and monitor the uptake of mandatory IG training	An organisations approach to IG training is often a key factor when the ICO consider enforcement action during their investigations of IG breaches or incidents, ***regardless*** of the nature of the actual incident. Compliance with DSPT criteria.
Work with IAO's to embed good information risk management activities	To protect patient information, other associated Trust assets and to mitigate against potential fines or other enforcement action.
Expand on the sharing of data securely and wider collaborations	To inform and improve the National programme for more joined up approaches

	across the Trust network and BSW STP / LHCR	and ensure patient data is secure. Compliance with DSPT criteria
	Review the Trust workflow in respect of patient and staff data through robust DPIA and Data Sharing Agreements.	Compliance with DSPT criteria.
	Support the Trusts Digital Strategy and assist the IG process within this business area.	To improve compliance with legislation when and where required to reduce the risk of enforcement action.

6.	NHS Constitution
This report shows that the Trust is committed to maintaining patient confidentiality and patient's right to privacy, as well as complying with the Data Protection principles.	

7.	Risk
There is a risk that with not being able to achieve the 95% national target this will mean that the Trust has not met the required Satisfactory standard for the years DSPT submission. Our contracts with the CCG's and external suppliers require that we have reached a satisfactory level against the mandatory evidence items of the toolkit to be able to satisfy due diligence checks carried out by those organisations and stakeholders.	

8.	Resources Implications
NA	

9.	Equality and Diversity
NA	

10.	Communication
NA.	

11.	References to previous reports
NA	

12.	Freedom of Information
Public	

APPENDIX 1 – DSPT Status as at 28/01/2020

It should be understood that those outstanding items are relating to dates that papers are approved by a Board, IG Group or SIRO and will be undertaken prior to final submission on 31st March 2020.

National Data Guardian Standards

The National Data Guardian (NDG) standards have been calculated for your organisation based on the responses provided in your organisation profile.