NHS
The Royal Wolverhampton
NHS Trust

Information Governance (IG) Data Protection and Security annual update 2018/19

5 August 2019

Agenda Item No: 7.9

Safe & Effective | Kind & Caring | Exceeding Expectation

The Royal Wolverhampton NHS

NHS Trust

Trust Board Report

Meeting Date:	August 2019
Title:	Information Governance (IG) Data Protection and Security annual update 2018/19
Purpose of the Report:	To provide assurances around the Trust compliance to national Information Governance standards.
Summary:	The purpose of this report is to update members on progress of the Information Governance agenda for 2018/19, including : • Data protection and Security Toolkit • IG incident patterns 2018/19 • General Data Protection Regulation 2016 (update on progress) • National Opt Out requirements • Freedom of Information Compliance • IG Risk profile
Action required:	For information
Clinical implications and view	N/A
Patient, carer, public impact and views	N/A
Resource implications	N/A
Report of:	Dr Jonathan Odum Medical: Director/ Caldicott Guardian
Author + Contact Details:	Tel Raz Edwards – Information Governance Manager / DPO Tel 01902 307999 Email rwh-tr.IG-Enquiries@nhs.net
CQC Domains	**Safe:** patients, staff and the public are protected from abuse and avoidable harm. **Effective:** care, treatment and support achieves good outcomes, helping people maintain quality of life and is based on the best available evidence. **Caring:** staff involve and treat everyone with compassion, kindness, dignity and respect. **Responsive:** services are organised so that they meet people’s needs. **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 3. To have an effective and well integrated local health and care system that operates efficiently
Links to Assurances	
Resource Implications:	
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. Executive Summary

The purpose of this report is to update members on progress of the Information Governance agenda, including the IG toolkit, incident trends, FOIs and IG national developments including the General Data Protection Regulation 2016 (GDPR).

1.1 IG Toolkit final submission 2018/19 & the new Data Protection and Security Toolkit (DPST)

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.

2018/19 saw the first full submission of the new Data Protection and Security Toolkit (DPST) hosted by NHS digital. The approach changed from 45 requirements for a large acute trust to 10 national data standards comprising of 40 assertions. Within these assertions there were 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. For GP practices there were also 10 data standards with 30 assertions and 52 mandatory evidence requirements

The Trust submission in March 2019 was submitted at 'standards not met – improvement plan agreed'. All GP practices submitted at 'Standards met' with all 52 mandatory requirements being met. Below is a summary of the Trust position for 2018/19. Standards that were not met with action plans include:

- **1**.42 & - When were information flows approved by the Board or equivalent.
- 1.43 - Provide a list of all systems/information assets holding or sharing personal information**.**
- 4.1.2 – For each system holding personal and confidential data, the organisation understands who has access to the information.
- 7.2.1 - Scanned copy of data security business continuity exercise registration sheet with attendees signatures and roles held.

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

🟥 **Not all mandatory requirements met**
🟩 **Mandatory standards met**

1.1.1 High level analysis of other Trusts submissions

Based on the information published to date on the toolkit, the Trust position can be comparted other acute Trusts.

- In total there are 156 registered acute trusts on the DSP toolkit (this excludes FTs).
- 3 Trusts were 'standards not met' – non compliant
- 70 were standards not fully met but had action plans agreed (of which RWT is one)
- 77 standards met – compliant
- 6 Trusts submitted as standards exceeded

1.1.2 2019/20 Toolkit position

The Trust is preparing for the 2019/20 submission which has again changed in scope from last year's submission. Nearly 80% of the toolkit assertions have changed.

The Trust is now required to meet **116 mandatory** evidence items which has increased by 16 from the last submission. In addition to this, 50% of the mandatory evidence items have changed, which means that the 116 evidence requirement won't be the same as what was asked for last year. GPs submission has decreased from 52 mandatory requirements to 42, but these are also changed from the previous submission. As a result of this the Data Security and Protection Team (IG team) are working to ensure all new evidence is mapped to an owner and there is an agreed reporting structure in place, which has further increased the workload of the team.

The Trust is working towards a baseline submission in October which will highlight any areas of concern in terms of compliance, and IG Steering group are working with internal audit to ensure a robust review of evidence and compliance for this financial year.

1.2 Incident patterns

Analysis of Trust wide patterns 2018/19 reviewed by Quality Governance Assurance Committee (QGAC) shows the following patterns of incidents which remains consistent with previous years:

  - o Lost ward handovers has increased
  - o Social media disclosures
  - o Disclosed in error email both internally and externally
  - o Disclosed in error other – including verbal disclosures and handing information to incorrect patients on discharge data quality incidents have also increased despite better reporting introduced

- Serious incident patterns

  - o Despite unauthorised access decreasing as a pattern the serious unauthorised access incidents appear to have remained the same as last year
  - o Disclosed in error in all categories is a consistent theme for serious incidents
  - o Non secure disposal has been an increased theme this year for serious incidents (electronic devices and paper)

Areas that have had increased patterns of incidents have been selected for audit in 2019/20. It is currently being assessed what audit approach should be taken this year by IGSG, in order to understand what is contributing to the incidents. It has been agreed that all areas will be asked to self-audit and then receive an unannounced follow up audit.

1.3 General Data Protection Regulation (GDPR)

The GDPR came into force across the EU on 25 May 2018 and applies to the Trust as data controller, where we determine the purposes and means of processing personal data for both employees and patients, and also as data processors where we are responsible for processing personal data on behalf of another data controller.

The GDPR represents a step change in the way that data is protected and managed. The UK has adopted the GDPR and the new EU Law Enforcement Directive into UK statute via the newly enacted Data Protection Act 2018. GDPR introduces new rights for data subjects and strengthens existing rights available under previous laws. The IG Steering group delegated responsibility to the GRPR implementation group to oversee the implementation and ongoing compliance to the GRPR, chaired by the Trust Caldicott Guardian/Medical Director. QGAC has reviewed the Trust GDPR implementation plans to ensure compliance.

The Trust has appointed a Data Protection Officer (DPO) and is continuing to review what resources are required to support ongoing implementation and compliance. Since the 25th May 2018 the Trust has seen an expected increase in requests for information which is also increasing in complexity. The Trust is also seeing an increase in rectification requests and queries relating to the use of patient data. Processes will continue to develop to ensure systems are able to ensure rights of both patients and staff are balanced with the need to have access to good quality information to continue to provide high quality care.

Development of asset registers and a supporting asset owner structure will be a key priority to ensure the Trust is able to manage its information risk, supported by the Senior Information Risk Owner (SIRO). Systems for monitoring and compliance are currently being investigated.

1.4 National opt out program (update position)

The national data opt-out was introduced on 25 May 2018, providing a facility for individuals to opt-out from the use of their data for research or planning purposes. This is provided in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs. By March 2020 all health and care organisations are required to apply national data opt-outs where confidential patient information is used for research and planning purposes. NHS Digital have been applying national data opt-outs since 25 May 2018. For details of when opt out applies see appendix 1.

All provider organisations, including the Trust, have been contacted and have been asked to demonstrate compliance to the nation opt out. There must be evidence of its implementation no later than March 2020. This would be supported by a compliance statement being published on the Trusts fair processing notice for patients to see. The Trust is currently looking into resource to support the implementation, with areas such as information team and research being the primary focus of compliance.

1.5 FOI compliance

In the period of 2018/19, FOIs have increased in volume and complexity, contributing to the Trust's compliance. FOIs have increased year on year with 2018/19 being the highest levels to date. July 2018 and Jan 2019 have seen FOI numbers of 80 + which is nearly double what has been seen in previous years which has impacted the Trust ability to respond to FOIs within the 20 day statutory timescale. It should be noted that despite the above, the Trust has not has any complaints logged with the ICO in relation to FOI.

1.6 IG Risk Profile

Through the work that is being carried out in the above programmes of work, the Trust is able to outline the areas that are currently of risk in the area of IG. More work will be done in the financial year to better understand how these risks develop and how they compare to the national picture.

1.6.1 **People and process risk** – through IG incident monitoring we can see that disclosed in error via various means (verbal, email, post, fax and in person), is a risk to the organisation in terms of the way in which people work. This is always a risk in large organisations such as health. Lost ward handovers continue to be an issue, with paper handovers being a contributory factor to the issue. Unauthorised access has also risen as a theme again in the last financial year due to the open access approach to systems supporting the way we work; proactive monitoring of user access continues to be a challenge for a Trust our size.

1.6.2 **Protecting information assets (cyber risk) –** due to the increase cyber risk seen to the health sector , knowing what the organisation holds and how this should be protected continues to be a challenge for an organisation the size of the Trust. As well as protecting against threats to large scale assets such as CWP portal and MMS for example, we also need to understand what local information assets are held, how these are managed and protected and what happens in the even they are compromised. A Trust wide information asset mapping exercise is taking place to better understand this issue through the GDPR and DSPT toolkit assurance work.

1.6.3 **Third party/ supplier assurance** – whilst the Trust has worked to better understand which data processors are handling data on behalf of the Trust, there is still more work to be done ensuing that there are clear contractual stipulations in place to ensure there is explicit instructions in place between the Trust and a third party. This should be supplemented by data sharing/ processing agreements. Robust contract monitoring to ensure these instructions are being followed continues to be a risk, and the Trust currently have a reactive approach to contract monitoring in the event of a data incident. This work also forms part of the DSPT toolkit assurance and GDPR work streams.

Appendix 1 - National opt out program

1.0 When does opt -out apply?

The national data opt-out will apply when:

• Confidential patient information is used for purposes beyond an individual's care and treatment,

AND

• The legal basis to use the data is approval under regulation 2 or 5 of the Control of Patient Information Regulations 2002, section 251 of the NHS Act 2006

2.0 The national data opt-out will not apply to uses beyond individual care and treatment in the following circumstances:

(1) When the data being used is anonymised such that it is considered to meet the requirements of the Information Commissioner's Office (ICO) anonymisation code of practice

(2) When data is provided under a mandatory legal requirement. - such as when there is a court order, when the Care Quality Commission (CQC) use their statutory powers to request information in support of their inspection role, NHS Digital's powers to collect information when directed (Health and Social Care Act 2012) or sharing for safeguarding cases (The Children Act 1989). For further examples of mandatory legal requirements when a national data opt-out would not apply, see the Operational Policy Guidance document published at: https://digital.nhs.uk/national-data-opt-out.

(3) When there is an overriding public interest- there are a small number of exceptional circumstances when Caldicott Guardians can decide to share information based on public interest.

(4) When the patient has given explicit consent to the use of their data for the specific purpose e.g. they have consented to participate in a medical research study

(5) When data is provided to the services below, which operate a separate opt-out mechanism:

   a. The National Cancer Registration Service

   b. The National Congenital Anomalies and Rare Diseases Registration Service.

(6) When the data is not confidential patient information

(7) Data is provided for the purposes of risk stratification for case-finding, when carried out by a provider involved in an individual's care.

(8) Information to support payments and invoice validation

(9) Data is provided for the oversight and provision of population health screening programmes (This refers to screening programmes that an independent expert group, the UK National Screening Committee (UK NSC), have advised that the NHS should offer. See below for NHS screening programmes offered in 2018 in England)

NHS screening programmes offered in 2018 in England - screening programmes currently offered in England in 2018 are listed below.

Screening in pregnancy

- screening for infectious diseases (hepatitis B, HIV and syphilis)
- screening for Down's syndrome, Patau's syndrome and Edwards' syndrome
- screening for sickle cell disease and thalassaemia

- screening for physical abnormalities (mid-pregnancy scan)

Screening for new-born babies

- a physical examination, which includes the eyes, heart, hips and testes
- a hearing test
- a blood spot test to check if the baby has any of nine rare conditions

Diabetic eye screening

- From the age of 12, all people with diabetes are offered an annual diabetic eye test to check for early signs of diabetic retinopathy.

Cervical screening

- Cervical screening is offered to women aged 25 to 64 to check the health of cells in the cervix. It is offered every three years for those aged 26 to 49, and every five years from the ages of 50 to 64.

Breast screening

- Breast screening is offered to women aged 50 to 70 to detect early signs of breast cancer. Women over 70 can self-refer.

Bowel cancer screening

- There are two types of screening for bowel cancer.
- A home testing kit is offered to men and women aged 60 to 74.
- Bowel scope screening uses a thin, flexible tube with a tiny camera on the end to look at the large bowel. It is offered to men and women at the age of 55 in some parts of England.

Abdominal aortic aneurysm (AAA) screening

- AAA screening is offered to men in their 65th year to detect abdominal aortic aneurysms (a dangerous swelling in the aorta). Men over 65 can self-refer.