Bradford Teaching Hospitals
NHS Foundation Trust

Meeting Title	Board Committee		
Date	12 September 2019	Agenda item	Bo.9.19.15

Annual Data Protection Officer Report

Presented by	Jenny Pope Head of Information Governance and Data Protection Officer	
Author	Jenny Pope Head of Information Governance and Data Protection Officer	
Lead Director	Cindy Fedell, Chief Digital and Information Officer and Senior Information Risk Owner	
Purpose of the paper	Data Protection Officer Annual Report	
Key control		
Action required	To note	
Previously discussed at/ informed by	IG Sub Committee	
Previously approved at:	**Committee/Group**	**Date**

Key Options, Issues and Risks

The General Data Protection Regulation (GDPR) requires the Trust to recruit a Data Protection Officer (DPO) who has autonomy to report directly to the Board of Directors. The Trust recruited a DPO in 2018. This is the first annual report by the DPO to the Board of Directors.

Analysis

There were no externally reportable Information Governance incidents in 2018/19.

In early 2019/20 there was a reportable incident the investigation of which is currently coming to a close. A second unrelated incident in August 2019 has been reported and is currently under investigation.

At the end of Quarter 4 of 2018/2019 Information Governance training compliance was 97%, combining both annual renewal and first-time training against an end of year target of 95%.

An improvement plan for 2019/20 is in place that encompasses the updated Data Security and Protection Toolkit Assertions, General Data Protection Regulation and Data Protection compliance.

The overall position of the Trust and the level of compliance with Information Governance related legislation and standards is good. However it is the opinion of the DPO that there is room for further maturity. This should take the form of a continuing rolling programme of checks and enhancements, where necessary with improvements to policy, procedures and guidance supported by the right tools and advice. This will enable staff to continue to carry out their duties in accordance with best practice Information Governance standards.

Recommendation

The group is asked to

- note the opinion of the Data Protection Officer regarding the position of Information Governance in the Trust
- consider the report and satisfy itself that the Data Protection Officer role is being effectively planned and discharged to provide the Board of Directors and Trust with the appropriate information and assurances regarding compliance with the General Data Protection Regulation and Data Protection Act 2018.

Meeting Title	Board Committee		
Date	12 September 2019	Agenda item	Bo.9.19.15

Risk assessment						
Strategic Objective	**Appetite (G)**					
	Avoid	**Minimal**	**Cautious**	**Open**	**Seek**	**Mature**
To provide outstanding care for patients		g				
To deliver our financial plan and key performance targets			g			
The level of risk against each objective should be indicated. Where more than one option is available the level of risk of each option against each element should be indicated by numbering each option and showing numbers in the boxes.	**Low**		**Moderate**	**High**	**Significant**	
	Risk (*)					
Explanation of variance from Board of Directors Agreed General risk appetite (G)	No variance.					

Benchmarking implications (see section 4 for details)	Yes	No	N/A
Is there Model Hospital data relevant to the content of this paper?	☐	☒	☐
Is there any other national benchmarking data relevant to the content of this paper?	☒	☐	☐
Is the Trust an outlier (positive or negative) for any benchmarking data relevant to the content of this paper?	☐	☒	☐

Risk Implications (see section 4 for details)	Yes	No
Corporate Risk register and/or Board Assurance Framework Amendments		X
Quality implications		X
Resource implications		X
Legal/regulatory implications		X
Diversity and Inclusion implications		X

Regulation, Legislation and Compliance relevance
NHS Improvement: (Risk assessment framework, quality governance framework, code of governance , annual reporting manual)
Care Quality Commission Domain: Well Led
Care Quality Commission Fundamental Standard: Good governance
Other (please state): General Data Protection Regulation (GDPR) and Data Protection Act 2018

Relevance to other Board of Director's Committee:					
Workforce	Quality	Finance & Performance	Partnerships	Major Projects	Other (please state)
	☒				

Meeting Title	Board Committee		
Date	12 September 2019	Agenda item	Bo.9.19.15

1 PURPOSE/ AIM

This report provides the annual update from the Trust's Data Protection Officer (DPO) regarding the discharging of the DPO role and the general approach to compliance with the requirements of the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018. It highlights key activities of the last year set against the national legislative landscape.

2 BACKGROUND/CONTEXT

The GDPR that came into force on 25 May 2018, alongside a new DPA, set out the requirement for the Trust to appoint a DPO. The DPO is responsible for ensuring that the application of data protection and confidentiality legislation is consistently observed and any weaknesses in current practices are identified and remedied where possible. This report is the first annual DPO report.

The DPO has provided advice on data protection and confidentiality across the Trust. Common themes have included clarity around internal and cross-organisational information sharing and risk and Data Protection Impact Assessments (DPIAs).

In 2018 the Trust identified its need to address compliance with the more exacting GDPR and Data Protection legislation, alongside existing Confidentiality obligations. The profile of IG awareness has been successfully raised within the Trust. The Trust successfully implemented GDPR and DPA.

The work undertaken by the Information Governance (IG) Team and colleagues is to be commended. The extent of readiness and compliance achieved is testament to their expertise, drive and commitment. An IG Improvement Plan for 2019/20 has been drafted which the team will work to throughout 2019/20.

3 PROPOSAL

Monitoring and Compliance

The GDPR resulted in increased public awareness of privacy and data uses but also some misunderstanding. IG in the NHS overall is mature. The Data Security and Protection Toolkit (DSPT), Caldicott Guardian, Senior Information Risk Owner arrangements and medical ethics around confidentiality have been in place for some years.

Within the Trust there is evidence of internal processes are working in multiple ways. The DSPT provides considerable assurance but also staff queries are an indicator of awareness. There are more queries with more complex questions.

Evidence of controls includes policy and procedures, Data Protection Impact Assessments (rationale, risks, assurance of security, legal basis for processing), contract clauses (data processors), and Data Sharing and Data Processing Agreements. Business change means assurance is at a point in time and requires continual checks against these controls. To keep gaining assurance that staff are engaged with changes we test, maintain and improve them.

Meeting Title	Board Committee		
Date	12 September 2019	Agenda item	Bo.9.19.15

The IG Team monitors requests from staff to help identify gaps and learning needs. The team is pro-active in engaging with other teams who seek advice, or who are relied on for evidence. Regular IG walkrounds are undertaken around the Trust. To further augment controls and compliance work took place to update policies and procedures. In early 2019 the Data Protection Impact Assessment (DPIA) template was revised and piloted. The Trust does not embark on new or changed processes without having considered privacy impacts and a number of DPIA reviews have been done. The DPO has met with stakeholders regarding the consultation process for the new DPIA and there is guidance that communicates the process which is also currently being revised. We will continue to work with business units to help ensure IG requirements are considered at the outset in line with Privacy by Design principles under GDPR.

Work has been undertaken to ensure that Trust contracts include the necessary updated IG clauses and where applicable there are written data sharing or processing agreements, assisted by the IG Team and the DPO to complete this important activity.

In 2018/19 the IG Toolkit became the new Data Security and Protection Toolkit (DSPT). It provides assurance of good practice, i.e., that an IG framework is in place with the necessary controls, governance, and policies. The DSPT is based on the 10 National Data Guardian Security Standards. The end of year report on 26 March 2019 confirmed Trust compliance of 'Standards MET' against all mandatory Assertions-items. Internal Audit opinion from its review of the Assessment provided Significant Assurance.

The Trust's information assets, what happens to them, and the controls surrounding them, inform a multitude of other areas. Poor quality, loss or damage, or inadequate controls for information and systems being used to process it could impact patient care. Thus the role Information Asset Owners (IAOs) play in ensuring such controls are in place is key to our information asset management framework and mitigating information risk. The Trust has improved its intelligence of its processing activities through phases of work on its Information Asset Register. An annual refresh of the Register took place and an internal audit is planned for September 2019. A mapping exercise was also undertaken in 2018 to understand the personal data processed across the organisation and flows of that data. This 'data flow map' will be maintained on an ongoing basis. It also informs our notification and register of processing activity obligations. IAOs are given guidance and training in order that they understand and address risks to the information asset they 'own'. Training was delivered in Quarters 1 and 2 of 2018 as part of a rolling programme that will continue in 2019. With the new structure training will be re-delivered to align with the business units. A pilot training session is planned for a September 2019 regular Performance meeting. Training helps to provide assurance to the Senior Information Risk Owner (SIRO) on the security, reliability, and integrity of assets plus reinforces their responsibilities and accountabilities.

Improvements to cyber security are continuous. A number of external assurances are sought and received each year. In addition the Trust conducted a Go Dark exercise and undertook an Internal Audit review. The current annual plan has been reviewed by the IG Sub-Committee and a Board of Director's development session was held sharing the current position. The Trust will continue to update its plan as new information becomes available.

In my opinion the Trust has well established governance in place with engaged membership. Assurance comes from the IG Sub-Committee (by way of the Quality Committee) provided through quarterly updates from the SIRO. The IG Sub-Committee (IGSC), chaired by the Chief Digital and Information Officer who is the SIRO and Deputy Chaired by the Caldicott

Guardian, receives progress reports in relation to all matters of IG and cyber security. The IGSC has strong representation from clinical and non-clinical areas plus key technical officers from IT, the IG Team, and DPO. The Trust should be assured that the DPO is afforded free access to senior management as is required of the role and is able to undertake the role independently without management direction.

Awareness

Mandatory training provides a level of assurance but is complemented in other ways. In 2018 separate additional training was also delivered to different staff groups, such as Information Asset Owners, Project Search, volunteers, clinical areas, Bank staff plus to the Board of Directors. Training materials were updated and new materials developed for face to face sessions, and induction. The IG Team worked with colleagues in IT, Education Services and Communications to develop tailored messaging, for example a new screensaver. Take up of the national e-learning package has been high as this is a mandatory piece of training. The Trust achieved a position of comprehensive awareness (97% of employees undertaking IG training).

In my opinion, this is a considerable achievement to be applauded.

The IG staff survey completed in 2018 returned positive feedback and will inform us of areas where further attention may be needed.

Whilst largely well received; it is recognised that the training material can be shorter and relate more to people in their workplace. Options have been explored including a Trust produced video for use at Induction.

Incidents and data breaches

Changes to the way the Trust is required to assess and report Information Governance or data breach incidents took effect in 2018. Processes have been implemented and embedded.

The Trust saw approximately 280 incidents reported by staff in 2018/19. The majority were lower level 'minor' incidents or near misses. Reports are presented monthly to the IG Sub-Committee and included in the SIRO Report to the Quality Committee and Board of Directors.

The volume of incidents reported reinforces the value of continuing training and raising of data protection awareness.

For 2018/19 the Trust saw no data breaches reportable externally. In early 2019/20 there was a reportable incident the investigation of which is currently coming to a close. A second unrelated incident in August 2019 has been reported and is currently under investigation.

Despite this, it is the opinion of the DPO that the vast majority of staff have embraced the need for honesty and transparency with regards to the management of personal information.

The IG Team is invited to the Trust's Learning Hub meetings and is exploring other ways it can extend learning. Unfortunately benchmarking of incidents with other Trusts is not easily

accessible but further work will be undertaken by the DPO in 2019 to analyse our incidents, whether we can predict or establish any trends or themes.

It is unrealistic to expect low level incidents and near misses to be eradicated entirely. The Board will be acutely aware of the spectre of the massively increased fines that the ICO can impose for information breaches and serious non-compliance issues.

The privacy and processing of personal data consciousness still shows occasional lapses. Reporting of low level incidents is encouraging as it demonstrates awareness but conversely may indicate complacency and is something that is monitored. I am confident that the Trust is an 'honest' reporter from continued reporting by staff of lower level breaches and near misses. It is however important to be watchful of accumulated 'minor' incidents, themes or trends, so that we learn from our mistakes, and potential issues are addressed before they become more serious. The changes in 2018 to the way incidents are assessed means there is an increased likelihood of organisations having reportable incidents. Where previously external reporting was based on numbers of subjects affected, the criteria now is likely harm, whether to one or many, and so an incident affecting only one individual could be externally reportable. The two recent reportable incidents reflect this.

Whilst no guarantees can ever be made that the Trust will not be subject to fines or censure, the robust approach being taken is reducing the risk.

Information Sharing

The Trust has a responsibility to work with partners to minimise the burden of data collection, and ensure that it uses data effectively to support the overall aims of health and social care. The Trust is a signatory to the Bradford Interagency Information Sharing Protocol. The Trust knows there is a need to share for care but the Trust does not overshare in the interests of transparency. As more organisations progress towards a shared care model more requests are being received by IG to develop or contribute to purpose specific Information (or Data) Sharing Agreements.

The National Data Opt Out Programme will not affect sharing for direct care but the DPO and Trust lead made contact with the National programme leads in 2018 and began to consider actions required in readiness for March 2020 when opt-outs must be upheld.

The Trust is responding to the Opt Out programme appropriately.

The planned 2018 EU Exit involved IG assessing and advising the Trust of potential risks to information flows. Once the UK leaves the EU it will no longer be subject to the GDPR, however, the UK government has committed to full alignment with it.

The Trust has undertaken analysis of potential risks arising from a no deal EU Exit scenario in relation to our processing and receipt of personal data. No immediate challenges are foreseen but will be closely monitored over the coming months.

Meeting Title	Board Committee		
Date	12 September 2019	Agenda item	Bo.9.19.15

Risks

The SIRO and IG Team monitors and reports incident related and other Information Governance related risks reported on the Trust risk register routinely via the IG Sub-Committee.

In my opinion the Trust has a robust system and governance structure for identifying, assessing and monitoring IG associated risks.

Networking and Collaboration

Internally, the DPO and IG Team are represented at various groups and committees on both ad-hoc and regular bases, for example, the Learning Hub and Security Steering Group.

Externally, the DPO contributes to the IG sector sharing of advice, guidance and working practices in relation to the application of new legislation and general data protection compliance. New links with peers at Bradford District Care Trust have been established as well as the National SIGN chair (Senior IG Network), other Trusts, and with the Yorkshire and Humber Care Record exemplars programme.

In November 2018 the DPO attended the annual North Yorkshire and Humber Directors of Informatics (NYHDIF) conference and is a longstanding member of the NYHDIF regional SIGN (Senior IG Network). The latter holds monthly meetings and is a well-established and respected forum represented by senior IG professionals from across the North with the emphasis on IG in a health and care setting. Some of the key issues and themes during the course of the year have been:

- GDPR and DPA compliance, e.g., implications of and clarity on subject rights
- New DSPT
- Developments in relation to the National Data Opt Out Programme
- Use of cloud and NHS Digital guidance
- Recording, e.g., by patients of consultations and/or surveillance of NHS staff.

The DPO role is a joint role between the Trust and Airedale NHS Foundation Trust. The IG Team staff at each Trust have begun working more closely to align or replicate processes and guidance where possible. Work took place during 2018 on a joint Information Governance Improvement Plan, processes for respective Toolkit (DSPT) assessments, and shared lessons learned from the 2018/19 DSPT assessment. Internal audits were co-ordinated to gain maximum benefit from the reviews in terms of avoiding or reducing duplication and adopting shared approaches to evidencing good practice.

External Updates

Prior to the introduction of GDPR in May 2018 the maximum penalty that could be imposed was £500,000 for serious IG/data security breaches. The maximum penalty now is 20 million euros (or 4% of annual turnover) for the most serious breaches of DPA principles (individual rights and third country transfers) and up to 10 million euros (or 2% of annual turnover) for standard infringements (administrative requirements).

Between 1 April 2018 and 31 March 2019 the Information Commissioner's Office (ICO) imposed monetary penalties on 39 organisations. Of those, two were health related organisations. Bayswater Medical Centre received a penalty of £35,000 in May 2018 due to

highly sensitive patient information being left in an empty building for more than 18 months. BUPA received a penalty of £175,000 in September 2018 for a failure to have effective security measures to protect personal information. Additionally, there were three prosecutions on individuals, all involving patient records being inappropriately accessed

Although according to the ICO's latest annual track report people have become slightly more confident in how public authorities store and use their personal information, far more non-health related organisations than the above figures were affected by enforcement action from the ICO during 2018.

The IG landscape is continuously evolving, no more so than over the last year with the added complexities brought by the changes in data protection legislation. Throughout 2018 there were updates to national guidance and policy, with new publications from the Information Commissioner's Office, NHS Digital, the Health Research Authority, British Medical Association and others. The Information Governance Alliance rebranded itself as NHS IG early in 2019. It is developing guidance and will pull health sector guidance from other bodies together to make it consistent.

A review of the Records Management Code of Practice was instigated and a new Health and Social Care (National Data Guardian) Act passed by Parliament in 2018. The latter came into effect on 1 April 2019 and places the office of the National Data Guardian on a statutory footing. The Act has a number of implications for the NHS and organisations who contract with it, such as imposing a duty to have regard to any Guidance published by the National Data Guardian.

Early in 2019 NHS England published the NHS Long term plan. Information Governance points of interest including digitising community services, digital ways for patients to access care, the NHS app, integrated care, digital care records and population health management. National bodies are still lagging in provision of guidance; GDPR was only the start of change.

The Information Commissioner has begun to impose fines under its new powers although to date, there have been no large fines imposed on NHS organisations. It is difficult to predict whether this will change and to what degree. We will continue to monitor developments nationally and make sure that we keep appraised of any potential 'flashpoints'.

Future Plans and Key Activities

Areas for continued development are much the same for every Trust - transparency and the need to ensure patients are fully informed about what the Trust does with their data through clear privacy notices, having a strong understanding of our processing activities, ensuring we follow the rules of privacy by design.

As DPO, I expect to see ongoing maturity of the IG Improvement Plan alongside a clear IG Strategy. The existing Strategy is being reviewed during 2019.

A service catalogue will be drafted to provide clarity for staff across services and sites. Additionally, a suite of updated and improved staff guidance will be developed and made available to help improve awareness and further embed good practice. The IG Team will develop and deploy a range of communication methods and materials to engage and support staff including use of newsletters and presentations. New channels will be considered, such as a blog to engage other staff with IG. Enhancements and updates will be

made to the IG and DPO Intranet pages. The website should be sufficiently clear to be the first point of contact for any member of staff with a query in relation to data protection, records management, confidentiality and information security.

Compliance testing and assurance work will take place in 2019/20 also utilising specific days set aside in the main Internal Audit plan. I am developing an 'audit programme' of activity to ensure the DPO role is fully discharged. This will focus on the higher risk areas of data protection and test awareness and compliance across all parts of the Trust.

4 RISK ASSESSMENT

This report does not contain a risk assessment.

5 RECOMMENDATIONS

The level of compliance with the GDPR and DPA 2018 is evidenced as having progressed in the Trust. This can be seen for example by the favourable Internal Audit opinion of the Trust's DSPT assessment review and consistent compliance with Subject Access and Freedom of Information Act requests plus high levels of mandatory training compliance.

Support from the Trust leadership and education services continues and is critical to ensure the Trust continues to maintain or improve training compliance throughout the year.

I believe that the Board can take assurance that the controls upon which the Trust relies to manage IG are suitably designed, applied and effective. However, as set out in this report, there is room for further continual improvement across different areas of IG. The IG resources available to the Trust are limited and so more needs to be done to align policy, procedures and guidance between the Trusts and Airedale NHS Foundation Trust, which will enable staff to help themselves with the right tools, advice and support.

Because the landscape is changing and evolving constantly, alongside a fast paced path towards a truly digital NHS, the Trust will need to keep pace with and attribute the necessary resources and attention to its Information Governance obligations. Both the IG Service and Caldicott Guardian regularly receive requests for advice and direction on a variety of work streams; most notably with regard to new initiatives, new suppliers, partners and data sharing and contractual elements which underpin each. It is an emerging challenge for the Trust to continue to meet the demand and assure the Board that work in this area is safe, legal, efficient and stands up to scrutiny.

The group is asked to

- note the opinion of the Data Protection Officer on the position of IG in the Trust
- consider the report and satisfy itself that the Data Protection Officer role is being effectively planned and discharged to provide the Board of Directors and Trust with the appropriate information and assurances regarding compliance with the GDPR and Data Protection Act 2018.

.

6 Appendices

NA