Bradford Teaching Hospitals
NHS Foundation Trust

Meeting Title	Board of Directors		
Date	8.11.18	Agenda item	Bo.11.18.31

Senior Information Risk Owner 2018/19 Quarter 2 Update

Presented by	Cindy Fedell, Chief Digital and Information Officer and Senior Information Risk Owner	
Author	Jenny Pope, Head of Information Governance Nadine Boczkowski, Head of Business Intelligence Steve Pearson, Network and Security Services Manager	
Lead Director	Cindy Fedell, Chief Digital and Information Officer	
Purpose of the paper	Information Risk Update	
Key control		
Action required	To note	
Previously discussed at/ informed by	Information Governance Sub-Committee 25 October 2018	
Previously approved at:	**Committee/Group**	**Date**
	Quality Committee	30 October 2018

Key Options, Issues and Risks

The Senior Information Risk Owner (SIRO) is required to regularly report to the Board of Directors to identify information governance risks and action taken. This paper is the 2018/19 Quarter 2 update.

Analysis

There were no externally reportable information governance or cyber security incidents in Quarter 2.

At the end of September 2018 training compliance was 83%, combining both annual renewal and first time training.

An improvement plan for 2018/19 has been drafted which encompasses the new Toolkit Assertions and General Data Protection Regulation.

Recommendation

The Board of Directors is asked to note the current position of Information Governance in the Trust.

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.					

Meeting Title	Board of Directors		
Date	8.11.18	Agenda item	Bo.11.18.32

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

Regulation, Legislation and Compliance relevance
NHS Improvement: (Risk assessment framework, quality governance framework, code of governance , annual reporting manual)
Care Quality Commission Domain: *(Safe, caring, effective, responsive, well led drop down)*
Care Quality Commission Fundamental Standard:
Other (please state):

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

Meeting Title	Board of Directors		
Date	8.11.18	Agenda item	Bo.11.18.32

1 PURPOSE/ AIM

The Senior Information Risk Owner (SIRO) is required to regularly report to the Board of Directors to identify information governance risks and action taken. This paper is the 2018/19 Quarter 2 update.

2 BACKGROUND/CONTEXT

Risk Incidents

There were no externally reportable Information Governance or cyber security incidents this quarter. The new National Information Governance incident reporting requirements and guidance for grading information governance incidents has been introduced. Incidents are no longer graded by level but are now graded on effect and likelihood. The number of reported incidents in this quarter is similar to the number of incidents which were reported in the previous quarters. Over the last few years there has been a decrease overall in incidents. There are currently no particular 'hot spots' of teams or services. There is one open incident with the Information Commissioner's Office (ICO) from December 2017. The investigation for this incident has been completed and the final report is awaited for review by the Information Governance Sub-Committee in October 2018.

Table 1: Number of Incidents by rating pre-GDPR

Incidents	2017/18									2018/19		
	Q2			Q3			Q4			Q1		
	Jl	Ag	Sp	Ot	Nv	Dc	Jn	Fb	Mr	Ap	My	Jn
SIRI High Risk Level 2 (reportable)	0	0	0	0	0	1	0	0	0	0	0	0
SIRI Level 1	18	13	8	7	6	2	5	4	2	1	4	3
SIRI Level 0 and below	5	3	5	7	14	13	15	13	14	16	21	17
No Trust involvement	2	1	0	0	0	0	0	0	0	0	1	1
Not rated	0	1	0	2	2	0	0	0	0	0	2	1

Table 2: Number of Incidents by rating post-GDPR

Incidents	2018/19		
	Q2		
	Jl	Ag	Sp
No impact has occurred	7	30*	28**
An impact is unlikely	5	10	6
Reportable to the ICO	0	0	0
Reportable to the ICO. DHSC notified	0	0	0
No Trust involvement	1	0	1
Not rated	0	0	0

* Eight of these incidents were reported by one consultant whereby patients had been transferred from A&E to a ward and the incorrect consultant had been allocated through EPR.
** Eleven of these incidents were reported by one consultant whereby patients had been transferred from A&E to a ward and the incorrect consultant had been allocated through EPR.

Security

The Trust has continued to ensure that the systems and processes to identify, intercept and manage attacks are robust and raising staff awareness is ongoing. NHS Digital regularly issues alerts to Trusts which are reviewed and, if relevant, actioned. No breaches have been reported this quarter. The Information Governance Sub-Committee continues to receive regular updates on the security position and supporting Key Performance Indicators.

Training

The Toolkit compliance requires 95% of staff to be in date with training. The Trust has sustained relatively high levels of training compliance. Training compliance overall, both annual renewal and first time, as at 30 September 2018 is 83%. The teams have evaluated

different methods to deliver training this year to both recognise the high level of compliance and to ensure the training is practical, i.e., cyber security and information governance good practice supporting day-to-day working. A number of options have been considered and a blended approach of online modules, video presentation, face-to-face and workbook materials is being taken. A communication campaign will be supported by a suite of informative documents. This blended approach ensures there are suitable alternatives to the nationally mandated e-learning training, essential for compliance with the Toolkit.

Data Quality Current State
Progress continues to fill vacant positions in the Data Quality Team substantively, post Electronic Patient Record (EPR) implementation, by the end December 2018. To date data quality has focussed almost exclusively on the EPR and roles and responsibilities have transferred from the EPR implementation to substantive teams across the Trust. External experts have delivered a training programme for operational staff to correct their own data entry errors in the EPR. Work continues to embed this training to prevent errors and correct data at source. Data quality correction meetings continue weekly as part of the Income Recovery Programme. A series of Point of Delivery (POD) meetings took place with each specialty throughout September 2018 to gain a detailed understanding of the impact of EPR recording errors on the Trust's financial position. The POD meetings exposed a mixed range of issues caused either by; user error, process failures, system configuration or a combination of all three. Work is progressing to prioritise actions.

Data Quality Maturity
To date the data quality indicators being monitored has focussed on the EPR. The Information Governance Sub-Committee approved a suite of high-level indicators intended to provide a boarder perspective on the maturity of data quality across the Trust. These indicators plan to be reported from November 2018. Further work will be undertaken to review and assess the appropriateness of these and potential additional metrics in coming months.

Data Security and Protection Toolkit 2018/19
The Data Security & Protection Toolkit (DSPT) is a self-assessment tool managed and hosted by NHS Digital on behalf of the Department of Health. It replaced the Information Governance Toolkit. The DSPT has ten standards beneath which sit 32 mandatory Assertions the Trust must declare compliance with. Owners for the ten standards (formerly called Requirements) have responsibility for evidencing against the relevant Assertions. All owners have subject matter expertise related to the Assertions and will attend the Sub-Committee to provide assurance against the evidence they are providing. 12 of the 32 mandatory Assertions have been completed ready for review.

General Data Protection Regulation and new Data Protection Act
The General Data Protection Regulation (GDPR) and Data Protection Act 2018 came into effect on 25 May 2018. Ongoing improvement work will continue to ensure that the Trust develops information governance for ongoing GDPR compliance and maturity. The newly appointed Information Governance Manager supported by the Data Protection Officer (DPO) and Information Governance Officer will manage the work to ensure the Trust approaches data protection issues and compliance seriously, and will provide a report to the Board of Directors.

Meeting Title	Board of Directors		
Date	8.11.18	Agenda item	Bo.11.18.32

Information Governance Maturity
The Trust continues to mature information governance understanding and practices in the Trust in keeping with learning from the Information Commissioner's Office Best Practice review and in pursuit of a high depth of compliance to the new General Data Protection Regulation and Data Protection Act. This maturity has focussed on Information Asset Owners (IAO) and their management of information assets. Over 100 IAOs have been trained and a programme to provide assurance to the SIRO was implemented over the summer period. The work to update the Information Asset Register with details of 970+ assets must continue to ensure that there are no gaps. Further work will involve, for example, ensuring Data Protection Impact Assessments (DPIAs) are in place where required, ensuring IAOs have access to appropriate guidance and communications campaign to ensure all IAOs are aware of their responsibilities.

Information Commissioner's Office
There has been no ICO enforcement action against NHS organisations in this quarter. The ICO continue to update their GDPR guidance. This will enable the Trust to introduce and implement policies, guidance and processes to improve the information governance provision and ensure compliance against the relevant legislation and standards.

3 PROPOSAL

The report presented the current position of information governance at the Trust and does not contain a proposal.

4 RISK ASSESSMENT

This report provides positive assurance on the current information governance position of the Trust, notwithstanding the need to increase the overall training compliance level. The risk position of the Trust in this regard is unchanged.

5 RECOMMENDATIONS

The Board of Directors is asked to note the current position of information governance in the Trust.

6 Appendices

NA