Kingston Hospital
NHS Foundation Trust

Information Governance Annual Report 2018/19

Trust Board	**Item:** 16
Date: 25th September 2019	**Enclosure:** L
Purpose of the Report: To present the annual report on information governance to the Trust Board.	
For: Information ☐ **Assurance** ☒ **Discussion and input** ☒ **Decision/approval** ☐	
Sponsor (Executive Lead):	Susan Simpson, Director of Corporate Governance
Author:	*Janice Sorrell, Head of Information Governance*
Author Contact Details:	020 8973 5292 **Janice.sorrell@khft.nhs.net**
Risk Implications – Link to Assurance Framework or Corporate Risk Register:	Report identifies significant risks and actions taken
Legal / Regulatory / Reputation Implications:	Regulatory and reputational implications
Link to Relevant CQC Domain: **Safe** ☒ **Effective** ☒ **Caring** ☐ **Responsive** ☐ **Well Led** ☐	
Link to Relevant Corporate Objective:	Strong foundations - good governance
Document Previously Considered By:	Information Governance Committee Executive Management Committee
Recommendations: The Trust Board is asked to note the content of this report.	

Information Governance Committee
Annual Report
(April 2018 to March 2019)

Executive Summary

This reports covers the period for the financial year 2018/19.
The highlights

- KPMG Internal Audit rating for General Data Protection Regulation (GDPR) readiness (Amber – Green) Significant Assurance with minor improvement opportunities.
- Despite increasing numbers and complexity of Freedom of information Requests, compliance with target rose from 83% to 88% in 2018/19.
- The Trust meets national data quality targets.
- Kingston Hospital templates are used by other organisations across SW London to meet statutory requirements.
- Privacy Notice updated to GDPR Standards and published

Challenges

- New Data Security and Protection Toolkit rating - Standards not fully met – plan agreed
- Further IG SIRIs (Serious Incidents Requiring Investigation)

1. Dates of Meetings

The Information Governance Committee met on the following dates:-

21 May 2018
16 July 2018
10 September 2018
12 November 2018
28 January 2019
11 March 2019

Quorum for meetings is four members. All meetings were quorate.

2. Membership

Position	Attended	Out of Possible	%
Director of Finance/SIRO/ CHAIR	5	6	83%
Medical Director/Caldicott Guardian	4	6	67%
Director of IM&T	3	6	50%
Assistant Director of IM&T (IT Installation Security Officer)	4	6	67%
Head of Business Intelligence (or Deputy)	5	6	83%
Nursing Representative	2	6	33%
Workforce Representative	1	6	17%
Health Records Manager	4	6	67%
Director of Corporate Governance	5	6	83%
Head of Information Governance - Secretary	6	6	100%

ToR require 67% to be attended.

3. Compliance with Terms of Reference

The terms of reference for the Committee identify objectives under the overarching headings of Data Accreditation, Statutory Requirements and Information Security. The Committee also has responsibility for overseeing the following CQC Key Lines of Enquiry (KLOE) requirements. These are encompassed within the actions taken under the overarching headings.

W6.7 Are there robust arrangements (including appropriate internal and external validation) to ensure the availability, integrity and confidentiality of identifiable data, records and data management systems, in line with data security standards? Are lessons learned when there are data security breaches?
S3.1 Are people's individual care records, including clinical data, written and managed in a way that keeps people safe?
S3.2 Is all the information needed to deliver safe care and treatment available to relevant staff in a timely and accessible way? (This may include test and imaging results, care and risk assessments, care plans and case notes.)
S3.3 When people move between teams, services and organisations (which may include at referral, discharge, transfer and transition), is all the information needed for their ongoing care shared appropriately, in a timely way and in line with relevant protocols?

Data Accreditation

- **To achieve and maintain data accreditation.**

The Trust has won an award in the annual CHKS Clinical Coding Awards each year.

The Trust meets national data quality targets e.g. use of NHS number. The Information Department has a service catalogue of data quality reports which are available and are in use across the Trust. Many of these reports are readily available through the Trust Intranet as DISCO reports. This Department also strives to maintain and improve data quality through improving practice by users. This year saw further work on reporting of data quality issues to the initial point of creation to support the Trust initiative of getting the data right first time.

Statutory Requirements

- **To ensure full compliance with Caldicott guidelines to ensure that patient-identifiable information is only shared for justifiable purposes and that only the minimum necessary information is shared in each case.**

Caldicott Provisions - The Trust is signatory to a range of Information Sharing Protocols. The Trust has worked with the South West London IG Group to provide an Overarching Information Sharing Protocol and Purpose Specific Information Sharing Agreement for the Connecting your Care project which will share information for direct care between health and social care organisations across South West London, including the four Acutes, Mental Health, Adult Social Care and GP Practices. These are based on the Kingston templates. We also collaborated in a Data Privacy Impact Assessment for the project. These are all hosted on the Data Controller Console by Kingston Hospital and at the time of writing 189 organisations have signed up. There have been no incidents which required the intervention of the Medical Director in her capacity as Caldicott Guardian.

Our Purpose Specific Information Sharing Agreement (PSISA) template has also been used for a number of other projects across the Trust and has been adopted by other Trusts as well. We have also developed a template for Data Privacy Impact Assessments and these are in use for high risk processing.

- **To ensure full compliance with legal requirements for storing and handling requests for information (eg GDPR/Data Protection, Human Rights, Freedom of Information)**
- **To comply with Public Records Office requirements and ensure a systematic and planned approach to the management of records within the organisation from creation to disposal**

Compliance with legal requirements around requests for information – The Trust currently is not fully compliant with all provisions of the information access legislation. We fall short of the Information Commissioner's Office target of 90% of all FOIs being responded to within 20 working days. However we have exceeded the Trusts' target of 85%. 88.2% of the 669 requests were responded to within the statutory timeframe for the year.

The Data Protection Act (DPA) compliance target is 85% responded to within the legal timeframes. DPA Subject Access Requests achieved compliance in 90% of the 1170 requests received by Health Records, and Radiology achieved c100% compliance from 1865 requests.

- **To monitor, oversee and approve the Data Security and Protection Toolkit**

Although it has broad compliance across all ten assurances standards of the Data Security and Protection Toolkit v1.0, after initial submission and review by NHS Digital the assessment was graded as Standards Not Fully Met – plan agreed. We had already submitted improvement plans for four of the IM&T Assertions but a further plan was required to bring Data Protection and Security Mandatory Training up to the target 95% within 6 months (end of September 2019).

Information Security (IS)

- **To comply with ISO/IEC 27001 for information security, through achieving Met rating on the annual Data Security and Protection Toolkit**

See reference above to level of compliance with DSP Toolkit.

- **To develop and implement appropriate supporting policies and procedures**

The Trust has a suite of supporting policies and procedures available through the Intranet under the Clinical Guidelines and Trust Policies Button. These are reviewed every three years as a minimum. Policies and procedures are approved through the Information Governance Committee and ratified by EMC.

- **To develop appropriate reporting mechanisms (eg IT security/ IG incidents)**
- **To review and approve Reports on IG SIRIs (Serious Incidents Requiring Investigation) and to monitor action plans on these.**

A report listing Information Security incidents is prepared for the IG Committee by the Head of Information Governance. The information is gathered from the Ulysses Safeguard System. Incidents are also brought to the attention of the SIRO and Caldicott Guardian outside of the Committee by the Head of Information Governance when required. IG Serious Incidents Requiring Investigation (SIRIs) are first logged as Incidents or Complaints on Ulysses then, if required, logged through the Incident Reporting Tool on the DSP Toolkit. Incidents of significant severity are automatically notified to the Information Commissioner's Office. All SIRI's undergo full investigation and root cause analysis. They are reported to the Information Governance Committee.

Reporting Lines

The Information Governance Committee reported to the Executive Management Committee (EMC) by exception during 2018/19 and through this annual report. The terms of reference for the Information Governance Committee were reviewed and approved unchanged by EMC during the year.

The Information Governance Committee oversees and receives reports from:

- **Health Records Management Group -** provided reports to the Information Governance Committee on four occasions during the year. The Terms of Reference for this group are currently under review.
- **Data Quality Group** - provided reports to the Information Governance Committee on six occasions during the year. The Group receives Data Quality reports from which the SIRO reports to the Trust Board. The Terms of Reference for this group are under review.

4. Principal Activities

Data Security and Protection Toolkit version 1 – As mentioned above the Trust achieved " Standards not fully met – plan agreed" across the ten assurance standards of the Toolkit. Unlike previous years there are no scores. As part of the Toolkit we have submitted plans on how we intend to improve.

Data Protection Act Subject Access Requests (SARs) – Health Records and Radiology are compliant with the statutory timeframe which changed from 40 calendar days under Data Protection Act 1998 to one month under GDPR2016 / DPA 2018. The Trust has adopted the shortest month of 28 calendar days. Both Health Records and Radiology exceed the Information Commissioner's Office (ICO) target. The RAG scores below for SARs show Trust target of >=85% of requests handled within statutory timeframe as Green. Amber represents 50-84%. Red <50%

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total
Radiology													
Received	150	122	143	151	254	98	201	209	109	131	184	113	1865
Completed in 40cd %	100%												**100%**
Completed in 28cd %		100%	99%	100%	98%	100%	98%	100%	100%	100%	99%	100%	**99%**
Health Records													
Received	99	33	86	91	95	98	122	123	78	126	116	103	11170
Completed in 40cd %	87%												**87%**
Completed in 28cd %		92%	87%	95%	93%	93%	94%	97%	88%	91%	92%	91%	**92%**
Workforce													
Received		1	1					1				1	**4**
Completed in 40cd %													
Completed in 28cd %		100%	100%					0%				0%	**50%**

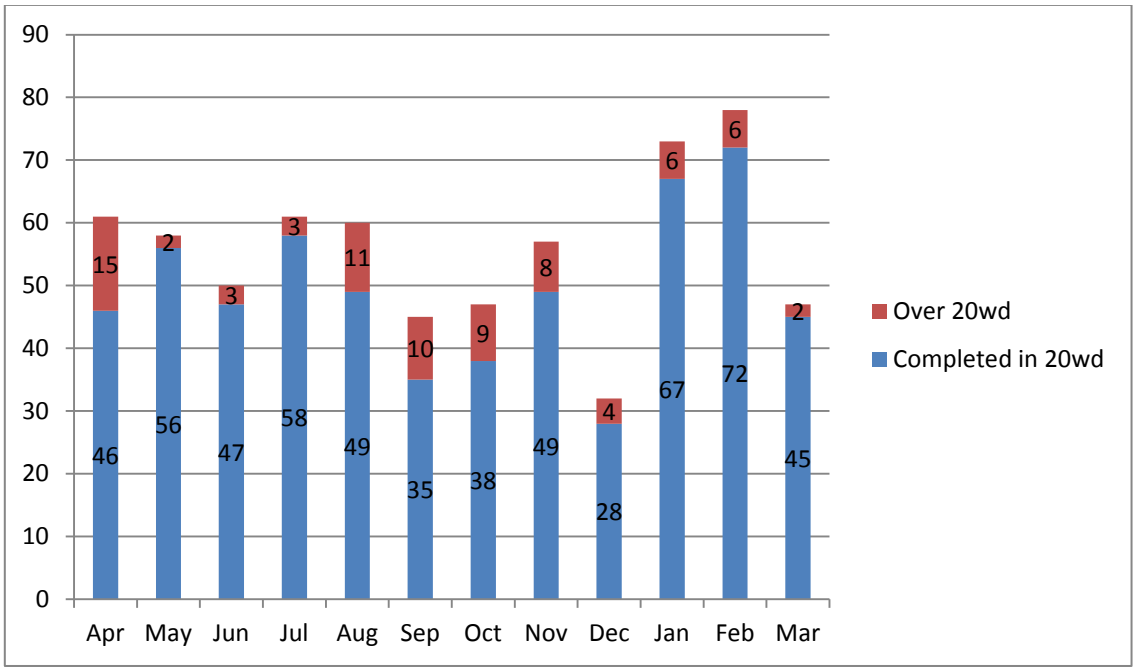
	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Total
Wolverton													
Received	1				1			1	3		2	1	**9**
Completed in 40cd %	100%												**100%**
Completed in 28cd %					100%			100%	100%		100%	100%	**100%**
Data Protection Officer													
Received		2				1	1						**4**
Completed in 40cd %													
Completed in 28cd %		50%				100%	100%						**75%**

Training – At 79.43% for the year, the Trust did not meet the NHS Digital target of 95% of all staff being trained in information governance annually, and this was down from 86% in 2017/18. Much was done during the year to introduce access to e-learning for all staff through the Electronic Staff Record (ESR). This will facilitate access to the training, automatic logging of test results and a dashboard keeping each member of staff sighted on their own compliance. Pre-employment training for new starters has also been introduced. Face-to-face training is available by departmental request. A Managers portal is also now available, facilitating managers tracking compliance of their teams. The new pay deal will link compliance with pay point progression. All of these measures should ensure improved training compliance is achieved in 2019/20.

Data Quality – The Data Quality (DQ) Group continues to meet to look in-depth at Data Quality Issues. The comprehensive Data Quality suite of KPI reports goes to the DQ Group and this Committee. The KPIs include details on elective, outpatient, A&E, Coding and 18 Week Referral To Treatment data quality issues.

Freedom of Information - This year saw an increase in the number of FOIs the Trust received - 669 requests – up from 622 last year. The complexity of requests continues to increase, often involving co-ordination across multiple departments to gather the requested information. Compliance has risen from 83% last year to 88.2% in 2018/19.

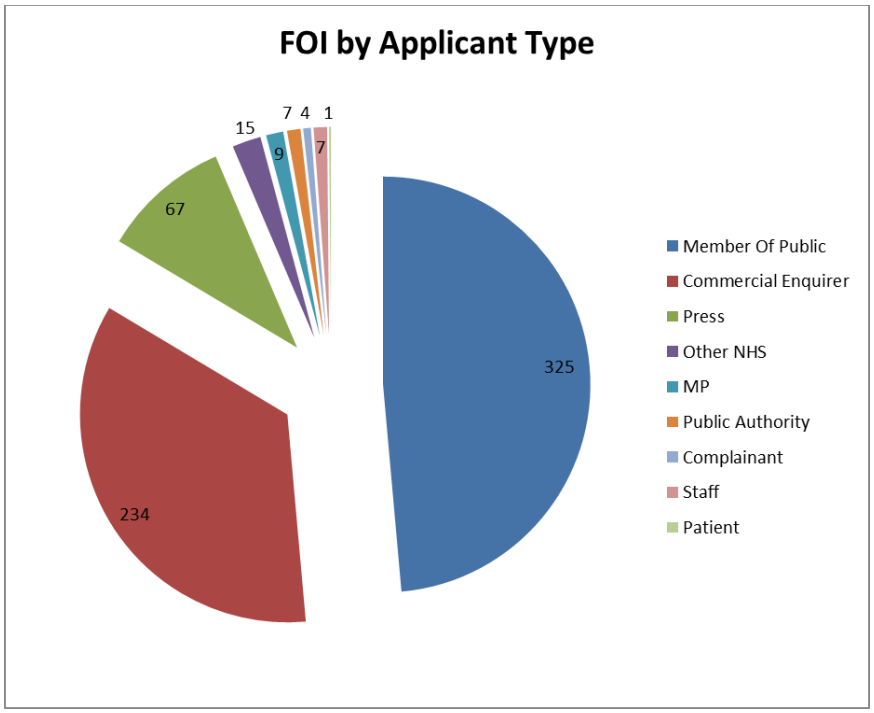
The graph overleaf presents overall FOIs per month differentiated into those received each month completed within the 20 working day statutory limit and those which exceeded the limit.



The following table provides a further breakdown on the time taken to close FOIs and the percentage that this represents. Although we have not met the 20 working day target this demonstrates that we do try to answer requests as quickly as possible

Row Labels	Completed 20wd	21-40wd	41-80wd	81+	Still open	Total	%20wd	%>20wd
Apr	46	7	7	1		61	75.4%	24.6%
May	56	1	1			58	96.6%	3.4%
Jun	47	2	1			50	94.0%	6.0%
Jul	58	1	1	1		61	95.1%	4.9%
Aug	49	8	2	1		60	81.7%	18.3%
Sep	35	3	3	4		45	77.8%	22.2%
Oct	38	6	2	1		47	80.9%	19.1%
Nov	49	4	3	1		57	86.0%	14.0%
Dec	28	4				32	87.5%	12.5%
Jan	67	6				73	91.8%	8.2%
Feb	72	3	2		1	78	92.3%	6.4%
Mar	45	1			1	47	95.7%	2.1%
Grand Total	590	46	22	9	2	669	88.2%	11.5%

Our FOI applicants fall into the following categories:



Only one request could be identified as coming from a patient. Almost half of all requests now come from Members of the Public but this category could be obfuscating applicants from other categories. Commercial Enquirers make up the next highest type of applicant, followed by Press, followed by MPs or their assistants.

The Trust categorises the requests into what types of information are requested. This is applied to the whole request, even though some requests cover multiple categories. The table below shows the top categories, accounting for 493 of the 669 requests.

no	Category
83	Staff Information
57	Statistics e.g. Length of Stay, Numbers of Procedures etc
53	IT Infrastructure / Software Etc
46	Agency And Bank
42	Service Performance
40	Policies / Procedures / Guidelines
30	Drug Information - Drugs prescribed, numbers of patients prescribed for etc
24	Contract Information
21	Finance
19	Private Patients / Foreign Patients
16	Clinical Services
16	Patient Information
13	Brexit
13	Equipment
10	Births
10	Estates / Maintenance

With regards the outcome of the requests, the Trust is maintaining the spirit of the Act by providing either all the information or as much as we can in over 87% of requests. Here is a breakdown of the Outcomes:

Outcome	No	%
All Information Delivered	326	48.7%
Info. Available Elsewhere	12	1.8%
Info. Partially Delivered	253	37.8%
Information Not Held	54	8.1%
No Information Delivered	19	2.8%
No Response From Appliant	1	0.1%
Withdrawn	2	0.3%
stiil open (at time of extract)	2	0.3%
Grand Total	669	

Where information is not provided or only partially provided then exemptions in the Act must be engaged. The Request For Information (RFI) module of Ulysses Safeguard allows us to group exemptions into Subjects which then apply to the request. Please note that in some cases the Subjects would only apply to part of the request where information was partially delivered. Therefore it would not be appropriate to provide percentages verses the total number of requests.

Row Labels	No
Not Held	105
Appropriate Limit	53
Person Identifiable Information	38
Not Held And Elsewhere	30
Information Available Elsewhere	16
Commercially Sensitive	14
Not Held, Appropriate Limit	8
Information Provided In Confidence	6
Not Held, Elsewhere, Appropriate Limit	6
Personal Info And Appropriate Limit	6
Commercial And Not Held	5
H & S And Law Enforcement	5
Appropriate Limit and Available Elsewhere	4
Available Via Other Means	4
Personal And Commercial	4
FOI 31 38 41 43 *	3
Personal Information & Available Elsewhere	3
Personal Information And Not Held	3
Appropriate Limit & Commercial	2
Available Elsewhere And Future Publication	2
Dead With No Next Of Kin	2
Not a FOI	2
Not Held Person Identifiable And Elsewhere	2
Appropriate Limit, H&S, Law, Commercial	1
Available Elsewhere & Commercial	1
Available Elsewhere and In Confidence	1

Row Labels	No
Commercial, In Confidence, Not Held	1
FOI - 1 21 31 38 43 *	1
H & S	1
H&S And Commercial	1
Law Enforcement H&S And Commercial	1
Not Held, Person Identifiable, In Confidence	1
Personal And In Confidence	1
Personal Info, Available Elsewhere, Appropriate Limit	1
Personal, Appropriate Lim, Confidential, Commercial	1
Vexatious Or Repeated Requests	1

*FOI Exemptions
1 – Not held
21 – Available elsewhere
31 – Law Enforcement
38 – Health and Safety
43 – Commercial Interests

The Appropriate Limit applies when the cost of fulfilling a request would exceed £450 (or 18hrs at £25 per hour) according to the Fees Regulations. The exemption at Section 12 of the Act then does not oblige us to fulfil this part of the requests.

SWL Health Information Exchange / SWL Overarching ISA / PSISA – Connecting your Care

The Trust is actively engaged with the South West London Information Governance Group, chaired by our Director of IM&T, and has helped to create a new GDPR compliant Overarching Information Sharing Agreement, which does not in its own right allow information sharing but sets out the framework with which Purpose Specific Information Sharing Agreements must comply. This has been passed by the Group, the LMC (Local Management Committee) and legal review. The Group has also taken the Kingston Tier 2 Purpose Specific Information Sharing Agreement Template and updated this to be GDPR compliant. This work has been done to facilitate a Health Information Exchange across the whole of South West London, to have information from the Acute Trusts, Mental Health Trust, GP practices and Adult Social Care available to access for direct patient care – the Connecting your Care project. A full Data Privacy Impact Assessment was also created. A Privacy Notice was set up for the project and launched in February 2019 which contains FAQ's as well as the opt-out procedure for patients who do not wish their information to be shared in this way. Our Kingston Hospital Privacy Notice links to this. Kingston Hospital is hosting the Overarching Information Sharing Protocol, the PSISA and the DPIA on the Data Controller Console and 189 organisations have signed up.

Forward App

The Forward App is a communication tool to provide smoother communication than bleeps, phones, pagers or email. The App is downloaded to the Doctor's or other Staff's mobile phone but requires direct login each time it is used. It has been evaluated by NHS Digital and the Trust has piloted and is now rolling it out across the Trust. From initial feedback there is strong demand for secure, compliant instant messaging and photosharing between the junior firms and their consultants as well as nursing, allied healthcare professionals and Multi-Disciplinary teams CRS still remains the electronic patient record and Forward takes pains to point out that relevant clinical information should be documented in CRS.

Data Privacy Impact Assessments (DPIAs)
Under GDPR, Data Privacy Impact Assessments became mandatory for high risk processing of personal information. This is part of the Privacy by Design ethos. The Trust had previously been using DPIAs where new technologies were introduced and they are becoming commonplace for the Trust as we mostly deal with health information which is a special category of information (similar to DPA 1998 sensitive data) under GDPR. We currently use a tool derived from the Information Commissioner's guidance.

5. Constraints

Freedom of Information requests – The number as well as complexity of requests continues to increase. In most cases the complexity requires the IG Team to request information from multiple departments and combine the results. This has an impact on the capacity of the Information Governance team to respond within the required time limits.

Information Sharing – as many organisations progress towards a shared care model more requests are being received to develop Purpose Specific Information Sharing Agreements (PSISAs). When these requests first come in they often lack basic details on why information should be shared i.e. the purpose, as well as lacking details on which patients and what data. This then necessitates significant work to be done to bring the project to fruition. Similarly with Data Privacy Impact Assessments, which in many cases are used to underpin PSISAs

6. Significant Risks Identified and Actions Taken

Serious Incidents Requiring Investigation (SIRIs)
During 2018-19 there were five Serious Incidents (SIs) relating to information governance reported though the Data Security and Protection Toolkit. All received Root Cause Analysis Investigation. Three involved emails sent to external organisations who have all deleted the information. One involved information stored on a camera for an extended period of time. The final SI involved information about another patient being sent out on CD to the wrong recipient which was promptly returned. None of the SIs required reporting to the Information Commissioner's Office. No further action was required to the mitigations that had already been put in place.

Information Governance Risk Register
There are four risks on the IG Risk Register. All are being treated on an ongoing basis. They range from very low to moderate in scale

1. Risk to Satisfactory rating on the IG/DSP Toolkit and increased risk of IG incidents due staff not being up-to-date with annual IG Training – Moderate Risk
2. Risk of fines from Information Commissioner's Office of up to £500,000 (from 25th May 2018 up to £17,000,000) for breaches of Data Protection Act – Moderate Risk
3. Risk of Actions/Fines from Information Commissioner's Office for Inappropriate Charging for Subject Access Requests – Very Low Risk
4. Risk of Information Commissioner's Office fines for breaches where there is lack of Data Privacy Impact Assessment for high risk processing. – Low Risk

7. Procedural Documents Approved

The following policies, procedures and guidelines have been approved by the Committee during the period:

7.1. Medical Photography Policy
7.2. Data Protection Policy
7.3. Health Records Subject Access Procedure (inc Access to Health Records)

7.4. Staff Subject Access Procedure
7.5. Code of Confidentiality
7.6. Clinical Coding Policy
7.7. Third Party Confidentiality Agreement

8. Objectives / Forward Plans

The introduction of GDPR and the Data Protection Act 2018 required a number of Trust policies and procedures to be re-written, most importantly the Data Protection Policy and the Subject Access Procedures. The Code of Confidentiality has also been updated. The rest of the IG pantheon will be updated in due course in the usual review cycle.

Electronic Document Management System (EDM)
The Trust is currently finalising contracts for the procurement of an Electronic Document Management System and a Scanning Bureau solution. These contracts were offered as two lots under OJEU. The Trust has reviewed responses to the Invitations To Tender, invited suppliers onsite to provide demonstrations, and has sent delegates out to view and assess the EDMs working at other Trusts and also to view and assess the Scanning Bureaus. The aim is that the Trust will scan and ingest to EDM all active patient health records and ongoing dayfiles. The records of patients who present whose records have not so far been ingested will then be scanned.

8.1. Information Governance Toolkit -> Data Security and Protection Toolkit

Version 2 of the DSP Toolkit has been launched. Whilst similar to V1, V2 now has 180 Assertions of which 116 are mandatory, though 5 are exempt for the Trust as we use nhs.net. Information carried forward from v1 will be subject to amendment and updating where necessary. Each Assertion requires a response. For some this will be a tick box and free text field, some where data is entered as well as a free text field, and some that requires evidence to be uploaded or a link to a web or internet page again with a free text field for comments. The excel spreadsheet as before was made available in order for organisations to be able to track their progress, actions and owners for each Assertion. In V2 the Toolkit has become more IM&T focused. As with the previous version there are no Assertions around manual health records which, like most other Trusts, Kingston Hospital NHS Foundation Trust still has.

Data Security Standard 3 (Assertions 3.11- 3.53) - Training
"All staff complete appropriate annual data security training and pass a mandatory test, provided linked to the revised Information Governance Toolkit.

All staff should complete an annual security module, linked to 'CareCERT Assurance'. The course is followed by a test, which can be re-taken unlimited times but which must ultimately be passed. Staff are supported by their organisation in understanding data security and in passing the test. The training includes a number of realistic and relevant case studies."

By "All" this is defined as 95% of all staff. In V2 the Trust is encouraged to show how the 95% target is achieved as some Trusts begin by discounting staff turnover rate and other factors which affect whether staff are available to have completed training. The full Board (including non-Execs) are referenced as having to complete this training. SIRO and Caldicott are also to receive appropriate data protection and security training. Specialist staff are also highlighted for appropriate training on a Training Needs Analysis and this should be recorded on the local training system (ESR).

Information Flow Mapping
This is refreshed annually and is referenced by a number of Assertions. We have included the legal basis for the flows (GDPR articles Six and Nine as well as Common Law of Confidentiality)

Staff IG Quiz
The Department aims to run two quizzes per year.

Quiz 1 – Halloween 2018

The Halloween quiz received a grand total of 195 entries. We would like to thank the Charity for donating three £25 Gift Vouchers which added to the other prizes donated by the IG Team. The results of this quiz were very positive with the average score being 9.22, and 111 participants scoring a full 10/10.

The results showed that 99.5% of staff completing the quiz knew that you should not share your CRS smartcard at any time, and 99% knew that patients could not just request to see their medical notes without a written request on a subject access form.

In contrast, 78.5% knew that the Trust's Senior Information Risk Owner (SIRO) was the Director of Finance, and 81.5% knew that patients do have a right to request a list of everyone who has accessed their CRS record. Overall, the quiz showed that staff's knowledge of Information security was good.

Quiz 2 – Spring 2019

The Spring quiz received a grand total of 219 entries. We would like to thank Jackie Kerkham as well as the IG team for donating prizes. The results were very positive with the average score being 9.73, and 169 participants scoring a full 10/10.

The results showed that 100% of staff completing the quiz knew that you should not share your CRS smartcard at any time, and 99% knew that no one could just request to see their medical notes without a written request on a subject access form. We are particularly pleased that 98.6% of staff knew who to inform if a confidential waste bin is full. 97.7% knew how to send secure emails to patients and 94.5% knew that the Trust's Caldicott Guardian is the Medical Director. Overall, the quiz showed that staff's knowledge of Information security was good.

8.2. Freedom of Information requests

The numbers of requests received has been increasing every year despite considerable amounts of information already being available on the Trust's website. There is no way to control the number of requests we receive as the legislation makes it clear that any person, anywhere in the world, has the right to have information which the Trust holds communicated to him unless suitable exemption(s) apply. Each FOI request must be handled individually and requirements in terms of time and resources can vary considerably. The complexity of requests is also increasing year on year requiring information to be collated across a number of departments. Compliance with the 20 working day statutory limit is still a Key Performance Indicator (KPI).

8.3. GDPR/Data Protection Act Subject Access Requests

The work here will mostly be monitoring compliance with the new one month statutory limit. This is a KPI. The Head of Information Governance as Data Protection Officer for the Trust continues to deal with any complex issues. GDPR expands the range of information

available to data subjects to what previously had been considered non-relevant filing systems e.g. email. However, the Public Sector has already had this requirement in place since the inception of the Freedom of Information Act. It is expected that more applicants will request this type of information. The Head of Information Governance also ensures DPA Notification.

8.4. Audits

KPMG – GDPR Privacy Diagnostic Review
This review, carried out by our internal auditors KPMG, focused on how Kingston Hospital NHS Foundation Trust has addressed specific key aspects of the General Data Protection Regulations (GDPR) that came into force from May 2018. Overall, KPMG gave this review an assurance rating of 'Significant assurance with minor improvement opportunities' (AMBER-GREEN).
In carrying out similar reviews at other Trusts, KPMG had found no other Trust which had completed their GDPR action plan, and therefore Kingston Hospital NHS Foundation Trust is in a similar position to other Trusts in the UK.

Areas of Good Practice Identified

- The DPO is sufficiently qualified to perform the role and has a direct line of reporting to the Executive through the Director of Corporate Governance, SIRO and the Caldicott Guardian.
- The Trust has identified 476 data flows of personal information and Data Flow Maps are annually updated and has documented 387 data asset in an annually updated Information Asset Register that details the purpose of record for all assets listed.
- A DPIA template has been created that enables a risk rating to be captured.
- A process has been documented to include enhanced data protection clauses are included in standard clauses for new third party contracts.
- The Trust has prioritised 54 existing contracts with suppliers who process personal information as part of a documented exercise to update existing contracts with GDPR-complaint provisions.
- A Training Needs Analysis has been created to align various staff groups to GDPR-focused training according to their privacy risk profile and GDPR responsibilities.

Areas for improvement

- Several versions of the external facing privacy statement are accessible on the Trust's external website and they inconsistently address the requirements of the GDPR. This has now been rectified to link to the one Privacy Notice.
- Due to the Trust having discrete budget lines in place, departments are able to engage with third parties without central procurement oversight. As a result there is a risk that Trust management does not have oversight of content of contracts agreed with all third party suppliers, which may also result in data assets being shared without being captured in the Trust's IAR. Procurement is addressing the recommendations.
- The Trust does not currently capture the legal basis for processing personal information and categories of recipients to whom the personal information will be disclosed. This was addressed as part of the Information Flow Mapping for 2018/19 Toolkit.
- One low priority recommendation was raised in relation to more detailed Board level GDPR training. This has also been addressed.

P2 Sentinel is available to the Head of Information Governance and the Caldicott Guardian as well as key staff in Business Intelligence Unit and IM&T. P2 Sentinel is the Privacy Office/Caldicott Guardian audit tool for CRS Cerner Millennium. It has been used by the

Head of Information Governance to investigate incidents at the behest of Complaints, HR, Risk Management and Departments as well as patients.

MPI Tool will be available to monitor use of Connecting Your Care as well as investigate potential breaches.

IG Walkabouts – The IG team will continue the work from the ICO audit and perform regular IG inspections around the Trust. The emphasis will be on locking computers when not in use, deterring sharing of CRS SmartCards, ensuring that paper records are securely stored when not in use.

8.5. CRS

The roll out of Clinical Documentation and E-Prescribing, documenting directly into the system rather than in paper records, continues to proceed and is complete across inpatient areas. Outpatients remains the focus for rollout. This is part of the overall plan to make CRS the patient record and for the Trust to be paper-light. The system itself continues to be hardened to prevent data entry/data quality errors. BigHand Digital Dictation where patient letters are digitally recorded, transcribed as Word Documents, approved by the clinician, then stored in the patient's CRS record as well as an electronic copy going directly by GP Link to the GP's own system, is now well embedded within the Trust.

The Trust continues its EDM (Electronic Documents Management) procurement through the Official Journal of the European Union (OJEU). This procurement is in two lots – for EDM software system and for a scanning bureau to digitise the paper records for ingestion to the EDM system. It is envisaged that this will integrate/be available through CRS. Contracts are currently being negotiated.

8.6. GDPR

The General Data Protection Regulations (GDPR) came into effect on 25 May 2018 along with the Data Protection Act 2018. The GDPR Data Protection Officer role has been incorporated into the job description of the Head of Information Governance. The Fair Processing Notice, the "Your Information" booklet, has been updated to a GDPR compliant Privacy Notice and this has been published on the Trust Website. The main areas which have changed

- Sharing health information for Direct Care no longer relies on consent but is conducted through our responsibilities under the Health and Social Care Act and for Medical Purposes.
- Subject Access Requests are now Free of Charge unless manifestly unfounded, excessive or repetitive and that the legal time frame is reduced to one month.
- The cost of Data Protection Notification will increase to £2900 at the next renewal.
- Data breaches must be reported within 72 hours and that the data subjects must be notified of the breach.
- Data Privacy Impact Assessments are mandatory for high risk processing.