

Information Governance Annual Report 2017-18

Trust Board	Item: 17
3rd October 2018	Enclosure: J
Purpose of the Report:	
The Information Governance Committee Annual Report 2017-18 is presented for the information of the Trust Board.	
FOR: Information <input checked="" type="checkbox"/> Assurance <input checked="" type="checkbox"/> Discussion and input <input type="checkbox"/> Decision/approval <input type="checkbox"/>	
Sponsor (Executive Lead):	Susan Simpson, Director of Corporate Governance
Author:	Janice Sorrell, Head of Information Governance
Author Contact Details:	Ext. 5292
Risk Implications – Link to Assurance Framework or Corporate Risk Register:	none
Legal / Regulatory / Reputation Implications:	Compliance with Information Governance Legislation - GDPR 2016, DPA 2018, FOI 2000 et al
Link to Relevant CQC Domain:	
Safe <input checked="" type="checkbox"/> Effective <input type="checkbox"/> Caring <input type="checkbox"/> Responsive <input type="checkbox"/> Well Led <input checked="" type="checkbox"/>	
Link to Relevant Corporate Objective:	
Recommendations and action required:	
The Board is asked to: <ul style="list-style-type: none"> • Note that the Information Governance Toolkit remains satisfactory • Note the increase in Freedom of Information KPI to 83% • Note two SIRs in year • Note the Trust's GDPR compliance and increase in Notification fee to £2,900 	

Information Governance Committee Annual Report (April 2017 to March 2018)

Executive Summary

This report covers the period for the financial year 2017/18.

The highlights

- IG Toolkit remains Satisfactory
- Completion of ICO Audit and Follow-up Audit

Challenges

- Further IG SIRIs (Serious Incidents Requiring Investigation)

1. Dates of Meetings

The Information Governance Committee met on the following dates:-

22 May 2017
25 September 2017
11 December 2017
22 January 2018
12 March 2018

Quorum for meetings is four members. All meetings were quorate. No meeting was held in July 2017.

2. Membership

Name	Position	Attended	Out of Possible
Jo Farrar	Director of Finance/SIRO/ CHAIR	5	5
Jane Wilson	Medical Director/Caldicott Guardian	2	5
Kevin Fitzgerald	Director of IM&T	4	5
David Edwards	Assistant Director of IM&T	3	5
Stephen Piper	Head of Business Intelligence	4	5
	Nursing Representative	0	5
	Workforce Representative	3	5
Ursula Kingsley	Deputy Head of Business Intelligence	4	5
Theresa Hogan	Health Records Manager	1	5
Susan Simpson	Director of Corporate Governance	3	3
Janice Sorrell	Information Governance Manager - Secretary/CHAIR	5	5
Wendy Kelly	Minute taker	2	
Matthew Wilson	Minute taker	3	

ToR require 67% to be attended.

3. Compliance with Terms of Reference

Compliance with the Objectives of the Group was as follows:

Enclosure M

• **Data Accreditation**

The Trust has broad compliance across all six assurances of the Information Governance Toolkit and is a regular winner of the CHKS Clinical Coding Awards.

As a comparison, here are the IG Toolkit Version 14.1 Scores for Kingston Hospital and other local Trusts.

	Organisation	Overall Score 14.1	Information Governance Management	Confidentiality and Data Protection Assurance	Information Security Assurance	Clinical Information Assurance	Secondary Use Assurance	Corporate Information Assurance	V14
A C C U T E	Kingston Hospital NHS Foundation Trust	80	80	74	73	86	100	77	80
	Royal Surrey County Hospital NHS Trust	71	80	70	68	73	66	77	69
	Ashford St Peter's Hospital NHS Trust	72	80	74	71	80	66	66	71
	Epsom St Helier Hospital NHS Trust	71	66	70	68	80	75	66	72
	Frimley Health NHS Foundation Trust	73	93	66	71	73	70	77	76
	Surrey & Sussex Healthcare Trust	80	93	92	75	73	70	77	79
	St Georges University Hospitals NHS Foundation Trust	66	66	66	66	66	66	66	68
	West Middlesex Hospital NHS Trust		now part of Chelsea and Westminster						
	Barts Health NHS Trusts	74	80	74	71	80	75	77	77
	Croydon Health Services	66	66	66	66	66	66	66	69
	Chelsea and Westminster Healthcare Foundation NHS Trust	71	80	66	66	73	79	66	66
	North Middlesex University Hospital NHS Trust	74	80	77	66	73	83	77	74
	Royal Free London NHS Foundation Trust	68	80	66	66	66	66	66	66
	The Royal Marsden NHS Foundation Trust	88	100	81	82	100	91	88	88
	Barnet & Chase Farm		Now part of Royal Free (joined 1st July 2014)						
C o m m u n i t y	YourHealthcare CIC	82	93	85	71	93	100	83	80
	Achieving For Children	not started							not started
	Hounslow and Richmond Community Healthcare NHS Trust	78	86	79	73	86	66	77	66
	Wandsworth Community Health	not started							not started
	Central London Healthcare CIC	77	86	75	73	80	66	77	66
	Central Surrey Health	66	66	66	66	66	66	66	78
M H T	Surrey And Borders Partnership NHS Foundation Trust	74	66	70	66	86	83	88	88
	South West London & St Georges Mental Health Trust	72	73	74	68	73	79	66	72
C C G	Kingston CCG	92	100	85	91	100			88
	Richmond CCG	91	100	91	90	66			94
	Wandsworth CCG	92	100	95	88	66			88
	Sutton CCG	97	100	100	96	66			93
	Merton CCG	86	100	95	74	66			97
	South London Commissioning Support Unit								
	NHS South West London PCT CLUSTER								
	London Ambulance Service NHS Trust	81	86	71	82	91		77	83
C O U N C I L	Royal Borough of Kingston upon Thames	none	none	none	none	none			82
	Richmond	none	none	none	none	none			69
	Wandsworth	67	66	72	66	66			69
	Elmbridge	none	none	none	none	none			not started
	Sutton	82	93	77	82	75			79
	Merton	82	73	72	89	83			80

- **Data Quality**

The Trust meets national data quality targets e.g. use of NHS number. The Information Services 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.

The Data Quality Group, chaired by the SIRO, has met during the period. The Group receives Data Quality reports from which the SIRO reports to the Trust Board.

- **Statutory Requirements**

Caldicott Provisions - The Trust is signatory to a range of Information Sharing Protocols including the Kingston Overarching Information Sharing Protocol (KOISP). The Trust is now working with the South West London IG Group to provide an overarching Information Sharing protocol to provide the framework for information sharing across South West London. The Tier 2 Purpose Specific Information Sharing Agreement (PSISA) template has also been used for a number of projects. The PSISA is also being adapted to provide a GDPR compliant template for South West London and together with the Overarching will be used for the South West London Health Information Exchange and other projects.

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 90% Information Commissioner's Office target of all FOIs being responded to within 20 working days but we did achieve 83% of the 622 requests within the statutory timeframe for the year. The DPA compliance is 90% responded to within 40 calendar days legal timeframe. DPA Subject Access Requests were in excess of 99% of the 1268 requests received by Health Records, and Radiology achieved 100% of 1690 requests.

- **Information Security-**

ISO/IEC 27001 – The Trust's IG Toolkit serves as assurance against this international standard.

IS Policies and Procedures – The Trust has these available through the Policy Information Management System (PIMS). This is available under the Clinical Guidelines and Trust Policies Button on the intranet.

IS Reporting Mechanisms – The Committee receives the IG Report from the Head of Information Governance and/or lists of Information Security Incidents. These are gathered from the Ulysses Safeguard System (which, in addition to risk incidents also has modules for Customer Services (PALS and Complaints), Litigation (Claims), Risk Registers and Request for Information (DPA, FOI etc.)). 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 IG Toolkit. Scores of 2 or above 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.

- **Subgroups**

The Health Records Management Group has met during this period. The Terms of Reference are currently under review.

Enclosure M

A Data Quality Group has met during the period, see above. The Terms of Reference have been reviewed.

• Reporting

The Committee reported to the Executive Management Committee (EMC) during 2017/18. IG KPI's (Key Performance Indicators) and IGC minutes are provided to this Committee.

4. Proposals for any changes to the Terms of Reference

None.

5. Achievements

IG Toolkit version 14.1 – As mentioned above the Trust achieved a "Satisfactory" score across all six assurances of the Toolkit, scoring 80% (the same as V14). V14.1 was not subject to internal review. This is the last year of the IG Toolkit in its current form. Next year it is being replaced by the Data Security and Protection (DSP) Toolkit which is cyber focused.

Data Protection Act Subject Access Requests (SARs) – Health Records and Radiology are compliant with the statutory timeframe of 40 calendar days. Both exceed the Information Commissioner's office (ICO) target.

	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	YTD
Radiology													
Received	118	158	143	127	147	125	142	164	108	140	139	179	1690
Completed in 40 cd %	100 %	100 %	99%	100 %	100 %	100 %	100 %	100 %	99%	100 %	100 %	100 %	100 %
Health Records													
Received	98	100	114	116	114	93	105	116	81	116	101	114	1268
Completed in 40 cd %	99%	97%	99%	100 %	100 %	100 %	99%	100 %	100 %	100 %	100 %	99%	99%
Wolverton													
Received					1		2		1	2			6
Completed in 40 cd %					100 %		100 %		100 %	100 %			100 %
Workforce													
Received								1	1	1		1	4
Completed in 40 cd %								100 %	0%	100 %		100 %	75%
Data Protection Officer													
Received												1	1
Completed in 40 cd %												100 %	100 %
A&E													
Received	Not Available												
Claims*													
Received		5	4	4	9	5	6	8	3	8	7	9	68
Completed in 40 cd %		100 %	100 %	100 %	100 %	100 %	100 %	88%	100 %	100 %	100 %	100 %	99%

*Standard disclosure window in legal cases is 40 days. Civil Procedure Rules via the Ministry of Justice allows flexibility as long as the Trust provides reasonable explanations as to any delays. If there are issues with disclosure and disagreements between the Trust and that of the legal representative a 'Statement of Truth' can be

Enclosure M

provided (in a court format) to facilitate protection from court fines. In general approximately 70% of cases are disclosed within the standard limit. The remainder will fall outside of this parameter due to reasons involving access, complexity and clarification of existence of the data required

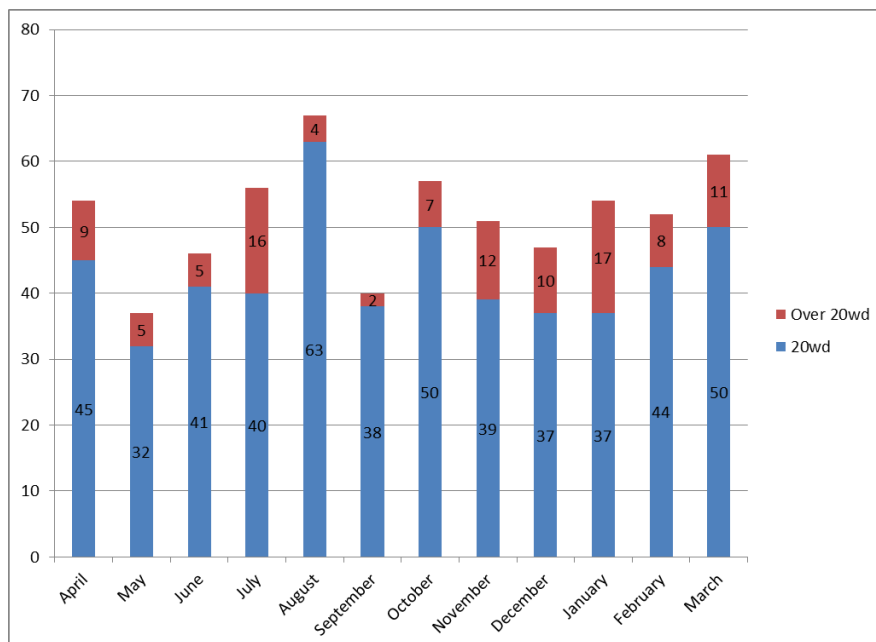
The RAG scores both in SARs and FOIs (above) comes from the Information Commissioner's Office (ICO) target of 90% of requests handled within statutory timeframe for green. Amber represents 50-89%. Red <50%

Training – Although the Trust did not meet the NHS Digital 95% target of all staff being trained annually, we did manage to achieve 86%, up from 85% last year. This is deemed Green by the Trust. The Training provision by Workforce was altered to include Online pre-employment training for new starters with testing. E Learning For Health is expected to come on-stream later in the 2018 for existing staff, again with testing. Face-to-face training continues for new nursing staff and a test is to be introduced to this as well. The Head of Information Governance will also be providing training for Esher Green Surgery and potentially more GP practices in the next financial year.

Data Quality – The Data Quality Group (DQG) continues to meet to look in-depth at Data Quality Issues. The comprehensive Data Quality suite of KPI reports goes to the DQG and to the Executive Management Committee. The KPIs include details on elective, outpatient, A&E, Coding and 18 Week Referral To Treatment data quality issues. Patient Identifiable Data has been removed from all reports apart from ones where a strong business case has been presented to the Head of Information Services and Information Governance Manager

Freedom of Information – This year the Trust received 622 FOI requests, compared to 618 in the previous year. The complexity of requests continues to increase, often involving co-ordination across multiple departments to gather the requested information. Compliance has risen from 63% last year to 83% this year.

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

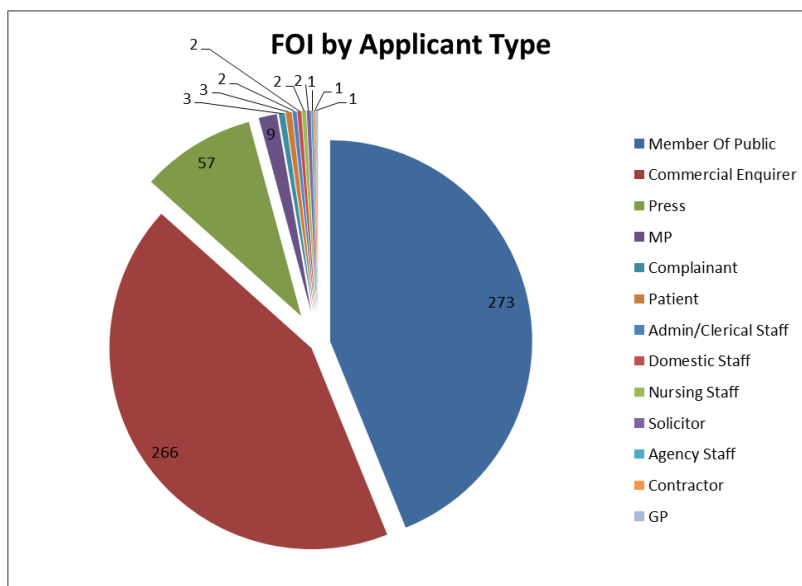


Enclosure M

The following table provides a further breakdown on the time taken to close FOIs and the percentage that this represents.

	20wd	21-40wd	41-80wd	80+ wd	still open	total	% in 20 wd
April	45	6	2	1	0	54	83%
May	32	2	2	1	0	37	86%
June	41	2	3	0	0	46	89%
July	40	10	5	1	0	56	71%
August	63	3	1	0	0	67	94%
September	38	1	1	0	0	40	95%
October	50	3	3	1	0	57	88%
November	39	8	4	0	0	51	76%
December	37	2	4	2	2	47	79%
January	37	8	7	0	2	54	69%
February	44	3	5	0	0	52	85%
March	50	7	0	0	4	61	82%
Total	516	55	37	6	8	622	83%

Our FOI applicants fall into the following categories:



Only three requests could be identified as coming from patients. 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 then MPs or their assistants.

The Trust has been categorising the requests into what types of information have been requested. This is applied to the whole request, even though some requests cover multiple categories, sometimes seemingly at random. The table below shows the top categories.

No.	Categories
73	Statistics E.G Length of Stay, number of procedures etc.
72	Staff Information
48	IT Infrastructure / Software Etc.
43	Drug Information – Drugs prescribes, numbers of patients prescribed for etc.
36	Agency and Bank
35	Contract Information
33	Service Performance
25	Equipment
21	Policies / Procedures / Guidelines

Enclosure M

No.	Categories
18	Private Patients / Foreign Pat
17	Finance
12	Radiology and Imaging
11	Cancer, Cancer Unit (Sir William Rous Unit)
11	Car Parking
11	Patient Information
10	Staffing Levels
10	Supplies

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. The table below shows a breakdown of the Outcomes:

Outcome	No.	%
All Information Delivered	360	58%
Info. Partially Delivered	182	29%
No Information Delivered	29	5%
Information Not Held	27	4%
Info. Available Elsewhere	9	1%
Still open	8	1%
Withdrawn	5	1%
Closed - Dormant 3 Months	1	0%
Info. No Longer Available	1	0%
Grand Total	622	

Where information is not provided or only partially provided then exemptions in the Act must be engaged. The 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 versus the total number of requests.

Subject	No
Appropriate Limit	59
Not Held	47
Person Identifiable Information	32
Not Held And Elsewhere	24
Commercially Sensitive	17
Information Available Elsewhere	12
Not Held, Approp Limit	7
Appropriate Limit And Available Elsewhere	6
H & S And Law Enforcement	4
Available Elsewhere & Commercial	3
Commercial And Not Held	3
Personal Info And Appropriate Limit	3
Available Elsewhere And Future Publication	2
Available Via Other Means	2
Personal And Commercial	2
Personal, In-Confidence, Law Enforcement	2
Approp Limit & Commercial	1
Approp Limit A& Future Publish	1
Approp Limit, H&R, Law Enforcement	1
Available Elsewhere AND Approp Limit	1
Available Elsewhere And In Confidence	1
Commercial, In Confidence, Not Held	1
Elsewhere, Law Enforcement, H&S	1
Future Publication	1
H&S Law Enforce Personal Vexatious	1
Information Provided In Confidence	1
Not Held & In Confidence	1
Personal Info & Available Elsewhere	1
Personal Info And Not Held	1

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.

Cancer Data Exchange

The Trust contributed to the formation of a Purpose Specific Information Sharing Agreement for a repository of information from KHFT and The Royal Marsden NHS Foundation Trust. This repository was to provide information from both organisations to be available to one another for direct patient care. At the time of writing further information was being added to the Data Privacy Impact Assessment which is to underpin the Information Sharing Agreement.

SWL Health Information Exchange / SWL Overarching ISA / PSISA

The Trust is actively engaged with the South West London Information Governance Group, chaired by our Director of IM&T, 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 Agreement must comply. This has been passed by the Group and is to go to the Local GP Boards prior to 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 is being 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. This work is in the design stage and is subject to a full Data Privacy Impact Assessment and has engagement with focus groups.

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 mobile phone but requires direct login each time it is used. It has been evaluated by NHS Digital and the Trust is currently piloting it with a view to rolling it out across the Trust. From initial feedback there is strong demand for secure, compliant instant messaging and photo sharing between the junior doctors and their consultants. CRS still remains the electronic patient record and “Forward” emphasises that relevant clinical information should be documented in CRS.

Data Privacy Impact Assessments (DPIAs)

Under GDPR, Data Privacy Impact Assessments become mandatory for high risk processing of personal information. This is part of the Privacy by Design ethos. The Trust had previously been using these where new technologies were introduced and they will become 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 which was refined by Dilys Jones Associates and which we are further refining.

6. Constraints

Freedom of Information requests – The number, as well as complexity of requests continues to increase. In most cases this requires the IG Team to request information from multiple departments and combine the results. The Head of Information Governance is the Trust Freedom of Information Lead who signs the requests off.

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

Enclosure M

and what data which then necessitates significant work to be done to bring the project to fruition.

7. Significant Risks Identified and Actions Taken

There were two Serious Incidents Requiring Investigation that involved IG this year. In both cases Patient Identifiable Data (PID) was sent by unencrypted email to other NHS organisations. In both cases the Information Commissioner's Office (ICO) required no further action by the Trust as the lessons learned had already been followed up.

The ICO also required no further action on the remaining case from the previous year where staff had breached Trust policy again with an unencrypted email.

8. Procedural Documents Approved

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

- Registration Authority Policy and Procedure
- Clear Desk and Clear Screen Policy
- Code of Confidentiality

9. Other Issues

None

10. Objectives / Forward Plans

The introduction of GDPR and the Data Protection Act 2018 requires a number of Trust policies and procedures to be re-written, most importantly the Data Protection policy and the Subject Access Procedures. The Head of Information Governance is currently reviewing these. This will be a key feature of the IGC Workplan for the coming year and will inform a renewed 5 year Information Governance Strategy.

10.1 Information Governance Toolkit -> Data Security and Protection Toolkit

The Data Security and Protection Toolkit replaces the Information Governance Toolkit. It is still a self-assessment device comprising 157 Assertions which are either met or not met. Of these 97 are mandatory, 3 are not applicable as we have nhs.net and 57 are currently not mandatory but these include a staff survey which we will be conducting this year.

Deadlines for the new DSP Toolkit are as follows:-

October 2018 Baseline of current compliance against each Assertion

March 2019 Final submission/publication of scores.

It is to be expected that CQC and NHS Resolution will have access to the DSP Toolkit and this will be used to cross reference their own requirements.

Although the Toolkit does not require evidence to be uploaded, an excel spreadsheet which is available through the Toolkit website has provision for evidence to be linked in. The Head of Information Governance will therefore revert to the old practice of gathering the evidence

Enclosure M

in a folder and linking it to the spreadsheet. We have also reverted to having an Assertion Owner (responsible for collating whatever information is required to meet the Assertion) and an Overseer who is responsible for ensuring the Owner completes the Assertion.

The aim for the Data Security and Protection Toolkit submission in March 2019 is to have all of the Mandatory Assertions Met as well as having conducted the staff survey.

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 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 refined to 95% of all staff. 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 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 and is now linked to the Information Asset Register.

Staff Quiz

This 2017/18 Information Governance Quiz, boosted by the donation of prizes by the Information Governance department, received 173 entries. With 102 entrants achieving the modal score of 10/10 and an 8.85 average the results are positive.

The results revealed strong knowledge in the areas that each individual encountered. 99.4% knew that they should not lend their CRS card to other employees or volunteers, whereas only 76.3% knew that the maximum fine to you for failing to provide the information for a FOI request is £5,000. Overall the quiz results were positive. General understanding of information security issues is good and a wide range of staff attempted the questions.

We will be repeating the Quiz this year.

10.2 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. Compliance with the 20 working day statutory limit is still a Key Performance Indicator (KPI).

10.3 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

Enclosure M

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 from the inception of the Freedom of Information Act. It is expected that more applicants will request this type of information. The IGM also ensures DPA Notification which from the next renewal in 2018 will cost £2,900.

10.4 Audits

Information Commissioner's Office (ICO) Data Protection Audit – The ICO conducted a voluntary audit onsite from 21st to 23rd February 2017. The ICO wrote to the Chief Executive in December 2015 proposing a Data Protection Audit to help the Trust achieve best practice. The ICO has automatic powers of entry and inspection on NHS sites. The Scope of the Audit was agreed to cover the following areas –

- Records Management
- Security of Personal Data
- Subject Access Requests

The ICO conducted a desktop exercise the week before they came in to inspect. As well as documents and other evidence requested directly from the trust they had Auditor Access to our IG Toolkit. Further evidence was directly submitted to them both during and after the visit.

The Overall Conclusion was that the Trust had Limited Assurance (scored Amber on the Green, Yellow, Amber, red scale). This is in line with many other Trusts who had voluntary audits. The Executive Summary has been published on the Information Commissioner's Website - <https://ico.org.uk/action-weve-taken/audits-advisory-visits-and-overview-reports/kingston-hospital-nhs-foundation-trust/>

The Trust worked on the Recommendations which have come out of the Audit to improve compliance. The ICO has since conducted a Desktop Follow-up Audit in January 2018. Most of the recommendations from the first audit had been completed by that stage and the Trust has now completed the revisions of staff training provision and Subject Access Pack to GDPR standards.

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.

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 the sharing of CRS SmartCards,
- Ensuring that paper records are securely stored when not in use.

10.5 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

Enclosure M

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 has now started an 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.

10.6 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 interim 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.