Annual Report – Information Governance

Executive Director	Lisa Marie Williams, Executive Director, Legal and Governance
Author(s)	**Luke Whiting, Information Governance Manager & Data Protection Officer**
Type of business	To note
For Council only:	Public Session
Issue	To provide the Council with the annual information update for 2019.
Recommendation	The Council is asked to **note** the annual information update for 2019.

1. Introduction

1.1 Throughout 2019, and going into 2020, there remains a strategic risk on the GDC's register in relation to data breaches, Risk CP1 - "Failure to comply with the requirements of the GDPR and Data Protection Act 2018 leading to enforcement action". The residual risk score for CP1 is currently 12, which is on the risk appetite limit.

1.2 The GDC's Information Governance Team, working with colleagues across the GDC, ensures this risk is appropriately managed and mitigated by developing and improving the GDC's information governance framework, the way it manages and disposes of information, identifies and responds to data security incidents, and ensures compliance with the Freedom of Information Act 2000 (the FOI Act) and the Data Protection Act 2018 (the DPA).

2. The work of the Information Governance Team in 2019

2.1 During 2019, the Information Governance Team has managed a complex caseload of information requests, the GDC's DSI reporting process, and the GDC's relationship with the Information Commissioner. As part of this core work, the team has also continued to train and support staff while completing project work aimed at strengthening the GDC's information governance framework.

2.2 Significant improvement work completed during the year included a review of records held in offsite storage, implementation of the GDC's retention schedule, implementation of an email deletion/retention policy which reduced emails held in outlook from 10m to 2m, and the creation of a records management policy.

2.3 The team's performance against KPIs remains high. During the year of 2019 **98% of FOI requests** completed (182 requests) and **96% of SAR requests** completed (185 requests) were responded to within the statutory deadline. This translates to missing four FOI and seven SAR deadlines. This is a significant achievement given the additional work the team completed during the year.

2.4 Another critical measure of performance across the organisation and reported on by the team is in relation to Data Security Incidents (DSIs). **114 incidents** occurred (142 in 2018)

and **two of these were reported to the ICO** in 2019 (**five in 2018**), although no enforcement action was taken.

2.5 Please see Appendix 1 for a summary of the core work of the team.

2.6 A summary of other work completed by the team is set out below:

Area	Work Undertaken	To note
Training	The team have run monthly induction training sessions (twice monthly when the new casework staff in Birmingham joined) for new staff and ensured GDC staff completed annual data protection training on the GDPR. Workshops were also run in relation to the email deletion policy and the use of a document library storage solution.	
Disclosure log	We have continued to review and publish appropriate FOI responses on a quarterly basis in the GDC's online disclosure log.	
Legal Advice	The GDC's information law solicitor, provided more than **200** pieces of formal legal advice (in addition to advice provided informally and supporting the team more widely) to internal clients on matters relating to the disclosure of information under the FOI, DPA and our own legislation (mainly in relation to FTP).	Disclosure requests for clinical advice reports have been particularly challenging to manage. Requests for advice in relation to contracts and procurement and specifically the role of the supplier as a data processor/controller have also been complex to resolve.
Objections to processing	The Data Protection Officer received **four formal complaints** and objections to the way in which the GDC has processed personal data. Two have been responded to and two are open.	These related to: • the description of a conviction in a determination; • the sharing of registrant history with the NHS for the performers list; • a data breach; • sanction information no longer on the GDC's website still being available via google.

Information Governance Group (the IGG)	The IGG is part of the GDC's information governance framework and has, at its quarterly meetings, helped shape the development of the data security incident reporting, policy, and support framework; the offsite records review project; and the records management policy.	
Records management	The GDC's Records Manager completed a review of boxes held in offsite storage that had been identified as being ready for review and disposal under the GDC's Retention Policy. A 'lift the lid' exercise was also completed on the **1068** boxes where the contents and/or business owner was unknown.	As a result of this work, the GDC now has a complete inventory of the records it holds in offsite storage and has for the first time, reviewed and destroyed records in line with its published retention and disposal schedule. Discussion is underway with the BDA about donating books to their library and papers of historical interest to their archive.
Data Privacy Impact Assessments (DPIAs)	During the year, DPIAs became a more formal part of the GDC's procurement and project management processes. The team have advised and assisted colleagues completing the screening questions and on those pieces of work requiring a full DPIA.	Full DPIAs were completed for health tests in FtP and are underway for the DARTs technology and people services IT systems procurement.
Internal audit of GDPR compliance	Audit of GDC's GDPR work programme and compliance completed by Mazars.	The audit provided **substantial assurance.** The auditor concluded that the GDC's implementation of the GDPR project demonstrated good VfM and that the GDC addressed GDPR to a greater level of compliance than organisations in the same sector in areas.
NHS toolkit assessment	Working with the GDC's Risk Management and Internal Audit team we completed an assessment of the GDC's IG risk management framework using the NHS Data Security and Protection Toolkit. Of the **112 criteria** we could evidence **meeting 106**. Of the **55 mandatory** criteria we could evidence **meeting 51.**	The assessment will provide a basis for the team's 2020 work plan. This is the first time the GDC has assessed itself using an objective measure of performance aligned with the ISO27k suite of policies, but it will now take place on an annual basis.

Team restructure	The Deputy Information Governance Manager and DPO and two Information Officer posts were, following consultation, moved and recruited to in Colmore Square.	

3. Review and analysis of Data Security Incidents 2019

3.1 There was a decrease in the number of DSIs reported during 2019, compared with 2018. Although as new staff joined and got up to speed work flow may have been a factor, in the coming months we will also be running awareness raising exercises to ensure visibility of the process remains high.

3.2 As in previous years the majority of incidents reported occurred in FTP Casework, and in areas of the office that handle large volumes of personal data. But all areas of the organisation reported incidents, indicating that awareness and use of the reporting system was generally good. The main cause of incidents continued to be human error. This was often where checks failed to prevent a DSI occurring. Causes of these lapses are being reviewed and include where people were working under pressure or too quickly and across multiple cases at once.

4. Data Security Incidents referred to the ICO

4.1 In 2019, **two incidents** (one involving the loss of records on a USB and one where mental health information was included in a public determination) were considered serious enough that we self-reported them to the Information Commissioner. This is a decrease from the five incidents reported in 2018.

4.2 In the two incidents the Information Commissioner concluded that the framework the GDC already had in place was appropriate, that the incidents were due to human error, but they nonetheless welcomed the actions taken in response and further improvements made as a result of the incident. On that basis, the Commissioner decided that they should not take any enforcement action.

5. Information requests

5.1 During the year 367 information requests were also completed. This is an increase of 55 on 2018. 98% (178) of the 182 FOI requests responded to in 2019 were responded to within the statutory timeframes (20 working days) or an extension was appropriately claimed to carry out a public interest test. 96% (178) of the 185 subject access requests responded to in 2019 were responded to within the statutory timeframes (30 calendar days) or an extension was appropriately claimed. This is a considerable achievement given the volume and complexity of the project work the team also undertook in 2019.

5.2 FOI requests of note received during 2019, included hearing transcripts and information relating to cases overturned following appeal by the PSA, requests in relation to overseas trained dentists registering as dental therapists via s36C of the Dentists Act 1984 (as amended), the use and cost of in-guise visits in FTP, and information relating to the component parts of the Overseas Registration Examination (ORE). This was part of a concerted campaign about the ORE.

5.3 The number of subject access requests received in 2019 was significantly higher than previous years, although inflated by requests from people who had failed the ORE. We also regularly received requests from people involved in the FTP process. These requests often related to a single FTP complaint, for example a copy of the case file usually from the

patient (informant) but also from the registrant. We have though received a volume of requests for, expert reports, including clinical advice, and individual medical records. Requests for information during the FTP process were frequently complex.

6. Internal Reviews of our decisions

6.1 Under the FOI Act organisations are required to carry out an internal review of an initial decision where someone expresses dissatisfaction. 9 reviews were received and completed in total for 2019 (six in relation to FOI and three in relation to a SAR). This compares to 12 in 2018 and 19 reviews in 2017).

7. ICO FOI Complaints and Decisions

7.1 Of the 367 information requests the GDC responded to in 2019, **one** FOI response was appealed to the Information Commissioner (zero in 2018, two in 2017 and seven in 2016). In this case the ICO upheld the GDC's decision not to disclose FTP casework guidance. These low numbers speak of the quality of the team's initial responses and the effectiveness of the internal review process.

7.2 Three subject access cases were referred to the Information Commissioner. One complaint of delay was upheld but overall in all three cases the ICO found that the GDC had disclosed information appropriately and no further action was recommended.

Recommendation

7.3 The Council is asked to **note** the information update.

Luke Whiting, Information Governance Manager and Data Protection Officer
LWhiting@gdc-uk.org
Tel: 0207 167 6309

06 January 2020

Appendix 1

	Q1	Q2	Q3	Q4	Annual Total 2019	Annual Total 2018	Annual Total 2017	Annual Total 2016
DSIs	27	30	26	31	114	142	94	129
FOI Requests Received	50	36	38	53	177	207	234	369
FOI Requests Completed	42	40	40	60	182	218	228	391
SAR Requests Received	49	52	30	56	187	98	107	102
SAR Requests Completed	34	56	40	55	185	94	113	80
Internal Reviews	0	3	6	0	9	12	19	14
Complaints to the Information Commissioner (FOI and SAR)	0	1 (FOI)	3 (SAR)	0	4	1	3	7