Audit and Risk Assurance Committee

14 June 2023

Annual Information Governance Report

Executive Summary

The Annual Information Governance (IG) report is presented. The report covers the period 1 April 2022 to 31 March 2023.

Generally, there was a slight increase in compliance rates compared to last year, but there remains a potential delay in how FOI requests are received within other correspondence which may not be immediately identified. Work will continue to attempt faster response times in the new financial year. The number of requests per year continues to grow and challenges to refusal to provide information which the recipient is not entitled are ongoing via the internal review process.

We continue to operate the Subject Access Request / Freedom of Information process with the Lotus Notes solution originally built in around 2004, with subsequent upgrades. We await an update to the base software, and a potential replacement in future years.

The UK Government recently re-introduced the Data Protection and Digital Information Bill, which potentially moves away from EU GDPR / UK GDPR equivalence. This may impact how we react to data protection issues in future.

Previous consideration	The Committee reviews Information Governance activity annually. ELT looks at Information Governance activity on a monthly basis.
Decision	The Committee is asked to discuss and note the report.
Next steps	The next report will be received in June 2024.
Strategic priority	Build a resilient, healthy, capable and sustainable organisation.
Risk	SR5. The resources we require to achieve our strategy are not in place or are not sustainable.
Financial and resource implications	None

Author(s)	Maxine Noel, Information Governance Manager maxine.noel@hcpc-uk.org
ELT Sponsor	Claire Amor, Executive Director of Governance Assurance & Planning claire.amor@hcpc-uk.org

Audit and Risk Assurance Committee, 14 June 2023

Information Governance Annual Report - 1 April 2022 to 31 March 2023

Introduction

1.1 The Information Governance (IG) function within the Governance, Assurance & Planning Directorate is responsible for the HCPC's ongoing compliance with the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR), the Data Protection Act 2018 (DPA) and the UK General Data Protection Regulation (UK GDPR). The Department also manages the HCPC's relationship with the Information Commissioner's Office (ICO), the information rights body.

1.2 FOI and EIR legislation provide public access to information held by public authorities. Public authorities are obliged to publish certain information about their activities and members of the public are entitled to request information from public authorities. Both Acts contain defined exemptions to the right of access, which means that there are clear criteria on what information can and cannot be requested.

1.3 The DPA governs the protection of personal data in the UK. It also enables individuals to obtain their personal data from a data controller processing their data. This is called a subject access request. Data subjects also have certain other rights under data protection legislation. Namely:

- to be informed – the right to be informed about the collection and use of their personal data.
- to rectification – the right to have inaccurate personal data rectified or completed if it is incomplete.
- to erasure – the right to have personal data erased. The right is absolute and only applies in certain circumstances.
- to restrict processing - the right to request the restriction or suppression of their personal data. The right is not absolute and only applies in certain circumstances.
- to data portability – the right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
- to object – the right to object to processing based on the legitimate interests or performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processes for the purposes of scientific/historical research and statistics.

- in relation to automated decision making and profiling – the right to be provided with information about automated individual decision-making including profiling.

1.4 This report provides an update on IG activity for the period 1 April 2022 to 31 March 2023.

Information requests

2.1 During the reporting period we received a total of 506 requests for information. This is an increase to the total of 427 information requests received in the previous reporting year. A breakdown of the annual figures can be found at Appendix 1.

Freedom of information (FOI) requests

2.2 88% (227) of the 257 FOI requests completed within the reporting period were responded to within the statutory deadline of 20 working days. 88% is slightly higher than the 87% achieved last year. The ICO toolkit which is designed to help public authorities assess their current FOI performance and provide indicators of where efforts should be focused in order to improve, categorises as 'good' 95% or more of FOI requests that are responded to within the statutory timeframe. 90%-95% is assessed as 'adequate' and fewer than 90% is assessed as 'unsatisfactory'.

2.3 20% of the late responses were a result of delays in identifying an FOI request within an email and forwarding this to the Governance team.

2.4 Common FOI themes during the reporting period included information about international registrants with breakdown by country of origin/training, registrants with annotations, ethnicity of registrants, especially those who are subject to fitness to practise hearings.

Subject access requests (SAR)

2.5 93% (107) of the 115 subject access requests (SAR) completed within the reporting period were responded to within the statutory deadline of one month. This is higher than the 87% achieved last year.

2.6 Subject access requests (SARs) most often related to fitness to practise cases. For example, a request from the complainant for a copy of the registrant's response to the matters raised in their complaint. We often receive widely scoped SARs for 'a copy of all personal data held' which requires a search of more than one system.

2.7 Details of the organisation's obligations for dealing with such requests is covered in the annual information security training.

2.8 Under the FOIA organisations are required to carry out an internal review of an initial response where someone expresses dissatisfaction. Whilst not specified in the DPA, we also conduct internal reviews of subject access requests where asked. We received 39 internal review requests (16 FOIs and 23 SARs were referred for internal review). This compares to 38 internal review requests received in the previous year.

2.9 The team responded to four data erasure requests. This compares to three data erasure requests received in the previous year.

Information incident management

3.1 The HCPC encourages an open incident reporting culture, with an emphasis on analysis and learning in order to identify any weaknesses in our processes and make appropriate changes.

3.2 Since February 2015, all incidents, regardless of how minor they may initially appear, are reported centrally and risk scored. A breakdown of the number of incidents that were reported can be found at Appendix 2.

3.3 In the reporting period, we recorded 34 incidents. This is lower than the 48 incidents recorded for the previous year. It's also the lowest number of incidents recorded over the past 3 years.

3.4 The majority of incidents reported occurred in FTP followed by Registration. These areas of the organisation handle large volumes of personal data.

3.5 The main cause of incidents was human error; for example, sending personal data to an incorrect email address. Many of the incidents categorised as 'system/IT issues' occurred due to the auto-complete function in Outlook. This feature suggests names when typing in the To, Cc and Bcc fields for the user to select from a list of previously used email addresses. Where incidents have happened due to the auto-complete function, the user has been advised to disable this in their Outlook.

3.6 One incident was reported to the ICO:

- One of our suppliers of legal services tried to extract a copy of the complainant's statement from an exhibits bundle. The exhibits were not extracted properly and instead the whole draft exhibit bundle was uploaded to their portal and the complainant was given access. The bundle included the registrant's personal information and also included reference to her health. This incident was reported to the ICO by both the HCPC and the law firm.

3.7 The ICO determined there was no further action required and closed the matter.

ICO Complaints and decisions

4.1 Part of the role of the Information Commissioner's Office (ICO) is to improve the information rights practices of organisations by gathering and dealing with concerns raised by members of the public about information rights issues.

4.2 We received five complaints from the Information Commissioner as follows:

- We were asked to revisit the way we handled a complaint regarding a data incident. The incident was in relation to the disclosure of inaccurate personal data in a published report. Under the 'upcoming hearings' section we had incorrectly included allegations that were found as no case to answer by an ICP. The ICO recognised that the HCPTS took the correct steps to correct the errors and raise the errors with the relevant teams once the original complaint had been received from the registrant. However, we failed to provide the registrant with a copy of the risk assessment that was carried out following their complaint to us. This we did on receipt of the ICO complaint.
- An FTP complainant's complaint to the ICO was that in our response to their subject access request we refused to release a copy of the registrant's response to the allegations. An ICP determined no case to answer and the case was closed. Where complaints about a registrant do not progress to a public hearing or to sanctions, then the information is treated as the confidential personal data of the registrant. The ICO supported our decision to withhold this information in their published decision notice (IC-174748-T0X9). We were subsequently notified by the ICO that this decision notice has been appealed to the First-Tier Tribunal (General Regulatory Chamber). The Tribunal's task is to consider if the Information Commissioner's decision is in accordance with the law or if any discretion he exercised should have been exercised differently. At the time of writing, a date has yet to be set for this hearing, which will be decided on papers.
- An FOI requester's complaint to the ICO was that we refused to release any FTP information regarding two radiographers. For the first registrant, a not well founded decision at final hearing held over 10 years ago. We therefore refused to release the information requested (all available information including the pleadings, nature of the complaints, any witness statements). For the second registrant, the request was for details of any FTP complaints received about the registrant. We used the FOIA exemption to neither confirm nor deny that we hold the information requested. The ICO supported our decision to withhold this information in their published decision notice (IC-168818-C5M4).
- The ICO asked us to review how we handled a complaint from an FTP complainant regarding the sharing of a confidential Family Court document by the registrant in this case. The ICO felt that we should have explained our lawful basis for processing the document in our original response. The complainant's FTP concerns were regarding the preparation and content of a report provided by the registrant for a private family law matter. As part of the evidence the complainant submitted to the HCPC to support her

concerns, it included a copy of the registrant's report. We received a copy of the Court judgement from the registrant to support her evidence that the report she prepared for the Court received no judicial criticism. On receiving the complaint from the ICO we dealt with this complaint as a data erasure request. We recognised the sensitivity of the Court judgement and determined that the document should be erased from the FTP case records and deleted completely from our systems.

- An FOI requester's complaint to the ICO was that we refused to release any FTP information regarding a clinical psychologist. The request was for details of any FTP complaints received about the registrant. As above, we used the FOIA exemption to neither confirm nor deny that we hold the information requested. The ICO supported our decision to withhold this information in their published decision notice (IC-220700-X7T2).

Information Governance

5.1 During the reporting period the Information Governance team continued to develop and improve the information governance framework; the way we manage and dispose of information, identify and respond to data security incidents and ensure compliance with the FOIA, DPA and UK GDPR.

5.2 FOI responses are reviewed, and appropriate data is published online on our FOI disclosure log.

5.3 Since January 2021, we have published on the HCPC website on a quarterly basis our FOI compliance statistics. It is good practice to publish these statistics as detailed in the Freedom of Information Code of Practice 2018, Section 8 Publication Schemes (paragraphs 8.5 and 8.6).

5.4 During the year, we updated our privacy notice. These changes include:

- strengthening our statement on data sharing with public bodies. We now specifically explain that we will only share personal data where a specific data sharing agreement or memorandum of understanding (MOU) is place.
- the sharing of registrant information with Health Education England (HEE), to enable them to undertake analysis of trends in the workforce of allied health professionals registered by the HCPC. This will enable them to develop better workforce planning.

5.5 Data privacy impact assessment (DPIA) is a process to help identify and minimise the data protection risks of a project or new way of processing personal data. A DPIA must be carried out for processing that is likely to result in a high risk to individuals. The team has advised, and assisted colleagues complete the screening questions and on those pieces of work requiring a full DPIA, as follows:

- KPMG (Business Central re-implementation)

- Monthly data feed with Health Education England (HEE)
- Generic regulation (for general use where registrant data sharing is proposed)

5.6 We continue to review all our older MOUs. We have updated a total of 3 MOUs as follows:

- Disclosure & Barring Service (DBS)
- Regulation and Quality Improvement Authority (RQIA)
- Health Improvement Scotland

5.7 In May 2021, BSI recertified HCPC's ISO27001:2013 registration. This covers all aspects of information security, including having knowledge of our data repositories, the sensitivity of data, and the legal aspects of collection, use, storage and eventual archiving or destruction. The standard requires that we respond to information security incidents and continually improve our Information Security Management System (ISMS), our data security and management.

5.8 Annual information security training is delivered to all staff (including contractors) as part of mandatory staff training. Partners and Council members are also asked to complete the training. At the time of writing, 88% of staff have completed this year's information security training.

Decision

The Committee is requested to discuss the report.

Appendices

Appendix 1 – Annual information requests 2022/2023

- Quarterly breakdown of information requests received
- FOIs and SARs completed

Appendix 2 – Annual information incidents 2022/2023

- Data incidents quarterly breakdown
- Data incidents by category

Date of paper
31 May 2023

Appendix 1 – Annual information requests

Table A - Breakdown of information requests received

	Q1	Q2	Q3	Q4	Total 2022/23	Total 2021/22
FOI	62	52	58	95	**267**	**205**
SAR	28	30	39	41	**138**	**120**
Disclosure requests	16	11	11	19	**57**	**59**
Internal reviews	9	4	14	12	**39**	**38**
ICO	1	1	1	2	**5**	**5**
Total requests received	**116**	**98**	**123**	**169**	**506**	**427**
Total closed	**118**	**88**	**116**	**151**	**473**	**422**

Table B – FOIs and SARs completed

FOI						
Total closed	65	47	54	91	**257**	**203**
- Response within statutory timescale	57	43	52	75	**227**	**177**
- Response in breach of statutory timescale	8	4	2	16	**30**	**26**
- % within statutory timescale	88%	91%	96%	82%	**88%**	**87%**
SAR						
Total closed	25	23	37	30	**115**	**117**
- Response within statutory timescale	23	22	33	29	**107**	**102**
- Response in breach of statutory timescale	2	1	4	1	**8**	**15**
- % within statutory timescale	92%	96%	89%	97%	**93%**	**87%**

Appendix 2 – Annual information incidents

Table C- Data incidents quarterly breakdown

	Q1	Q2	Q3	Q4	Annual Total 2022/23	Annual Total 2021/22
No. of data incidents	8	8	9	9	**34**	**48**

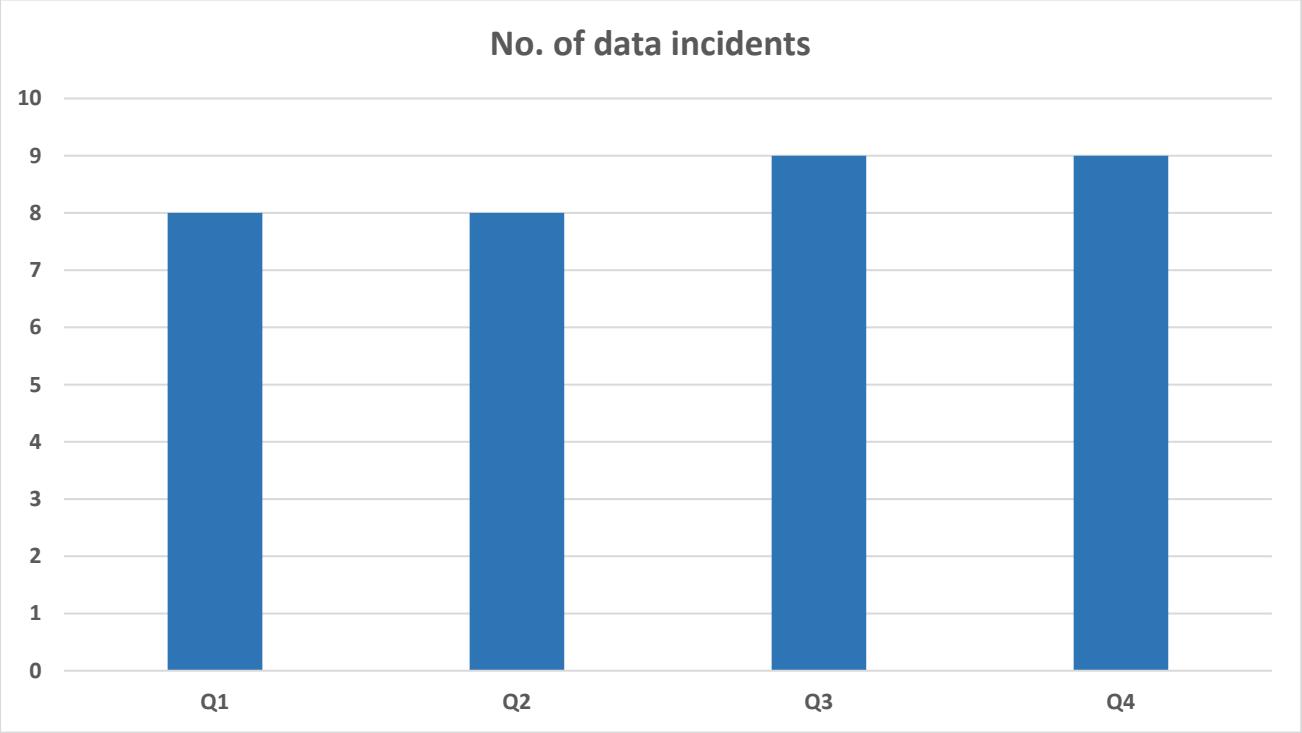

Table D - Data incidents by category