Audit and Risk Assurance Committee

19 June 2024

Information Governance Annual Report 2023-24

Executive Summary

The Annual Information Governance (IG) report is presented. The report covers the period 1 April 2023 to 31 March 2024.

The number of requests per year continues to grow and challenges to refusal to provide information which the recipient is not entitled to are ongoing via the internal review process.

Appendices:

1 – Annual information requests

2 – Annual information incidents

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 the report.
Next steps	The next report will be submitted to the Committee in June 2025.
Strategic priority	Strategic priority 1: Continuously improve and innovate Strategic priority 4: Be visible, engaged and informed
Financial and resource implications	None
EDI impact and Welsh Language Standards	No impact
Author	Maxine Noel, Information Governance Manager Maxine.noel@hcpc-uk.org

Information Governance Annual Report - 1 April 2023 to 31 March 2024

1. Introduction

1.1 The Information Governance (IG) function within the Corporate Affairs 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 Freedom of Information (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 not 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; and
- 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 2023 to 31 March 2024.

2. Information requests

2.1 During the reporting period we received a total of 534 requests for information. This is an increase to the total of 506 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 96% (234) of the 243 FOI requests completed within the reporting period were responded to within the statutory deadline of 20 working days. 96% is higher than the 88% 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 33% 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 (FTP) hearings.

Subject access requests (SARs)

2.5 90% (145) of the 161 SARs completed within the reporting period were responded to within the statutory deadline of one month (or in the case of complex SARs within the additional two months). This is lower than the 93% achieved last year. However, the overall number of SARs received this year (161) is higher than last year (115).

2.6 SARs most often related to FTP 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 41 internal review requests (eight FOIs and 33 SARs were

referred for internal review). This compares to 39 internal review requests received in the previous year.

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

3. 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 43 incidents. This is higher than the 34 incidents recorded for the previous year.

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.

3.6 No information incidents were assessed as meeting the threshold for reporting to the ICO.

4. 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 two complaints from the Information Commissioner as follows:

- We were asked to provide further explanation of a data incident. The incident was in relation to the disclosure of the complainant's name to the registrant in an FTP case, where the complainant had asked for anonymity. The ICO asked us to explain how the error happened and the steps we were taking to guard against further similar errors in the future. In our explanation to the ICO we explained that the incident occurred because in responding to the registrant who had asked for an update in relation to four linked matters, the case manager identified each FTP case by the HCPC reference number and the name of the complainant. One of the four cases was reported by a complainant (the data subject) that requested to remain anonymous. We further explained that it is usual for us to inform the registrant of the name of the complainant in FTP matters unless the complainant has asked to remain anonymous. We outlined to

the ICO the measures we have put in place to prevent reoccurrence, which is to make better use of the Nexus case management system technology. The process that FTP has implemented is to add a note on the home page of each individual case in the Nexus system where the complainant has requested anonymity. This will serve as a reminder to anyone viewing the case as previously a complainant's anonymity wishes were less visible. Prior to implementing this change, anyone accessing a case would need to review the documentation held on the case to see if a complainant requested anonymity. The ICO was satisfied with our explanation and closed the case.

- 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. 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-271819-F9M3).

4.3 During the reporting period, we received the outcome of the ICO decision notice which had been appealed to the First-Tier Tribunal (General Regulatory Chamber). This was a request from an FTP complainant for a copy of the registrant's response to the allegations where an ICP determined no case to answer. The First-Tier Tribunal dismissed the appeal and upheld the ICO decision notice (IC-174748-T0X9).

5. 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:

- adding plagiarism detection services to our list of the types of suppliers who are contracted data processors; and
- making it clearer that where registrants, employees or partners require us to correct inaccurate personal data we hold for them we will need documented official evidence.

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:

- CoreHR-Volcanic portal
- Turnitin - registration anti-plagiarism
- Professional body data sharing
- FTP front loading - inhouse legal
- CoreHR App4employees
- Welsh language scheme
- Redaction by AI POC
- AI assisted email responses (registration)
- General Chiropractic Council sharing tribunal space

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

- Disclosure and Barring Service (DBS)
- Health Inspectorate Wales
- NHS Counter Fraud and Department of Health and Social Care Health Improvement Scotland
- A number of other MoUs are in the process of being updated with the appropriate authorities

5.7 One organisation, Disclosure Scotland, has declined to sign an MOU with the HCPC. This was initially a recommendation from our internal auditors (BDO) as part of the safeguarding audit in 2021.

5.8 In May 2023, the British Standards Institution (BSI) undertook a surveillance audit of the 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.

5.9 The BSI audit found no non-conformances. In January 2024 the BSI undertook a readiness audit with the CISRO to determine if we were likely to be ready for the transition from ISO27001:2013 to the 2022 iteration of the standard. The audit suggested that the HCPC would be ready for transition, with appropriate evidence of project management and key employee training in place.

5.10 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, 92% 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 2023/2024

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

Appendix 2 – Annual information incidents 2023/2024

- Data incidents quarterly breakdown
- Data incidents by category

Date of paper
29 May 2024

Appendix 1 – Annual information requests

Table A - Breakdown of information requests received

	Q1	Q2	Q3	Q4	Total 2023/24	Total 2022/23
FOI	63	74	58	53	**248**	**267**
SAR	37	36	48	35	**156**	**138**
Disclosure requests	19	16	28	24	**87**	**57**
Internal reviews	10	14	7	10	**41**	**39**
ICO	1	0	1	0	**2**	**5**
Total requests received	**130**	**140**	**142**	**122**	**534**	**506**
Total closed	**151**	**139**	**121**	**112**	**523**	**473**

Table B – FOIs and SARs completed

	Q1	Q2	Q3	Q4	Total 2023/24	Total 2022/23
FOI						
Total closed	73	72	54	44	**243**	**257**
- Response within statutory timescale	70	68	54	42	**234**	**227**
- Response in breach of statutory timescale	3	4	0	2	**9**	**30**
- % within statutory timescale	**96%**	**94%**	**100%**	**95%**	**96%**	**88%**
SAR						
Total closed	44	36	40	41	**161**	**115**
- Response within statutory timescale	36	34	38	37	**145**	**107**
- Response in breach of statutory timescale	8	2	2	4	**16**	**8**
- % within statutory timescale	**82%**	**94%**	**95%**	**90%**	**90%**	**93%**

Appendix 2 – Annual information incidents

Table C- Data incidents quarterly breakdown

	Q1	Q2	Q3	Q4	Annual Total 2023/24	Annual Total 2022/23
No. of data incidents	10	14	11	8	**43**	**34**

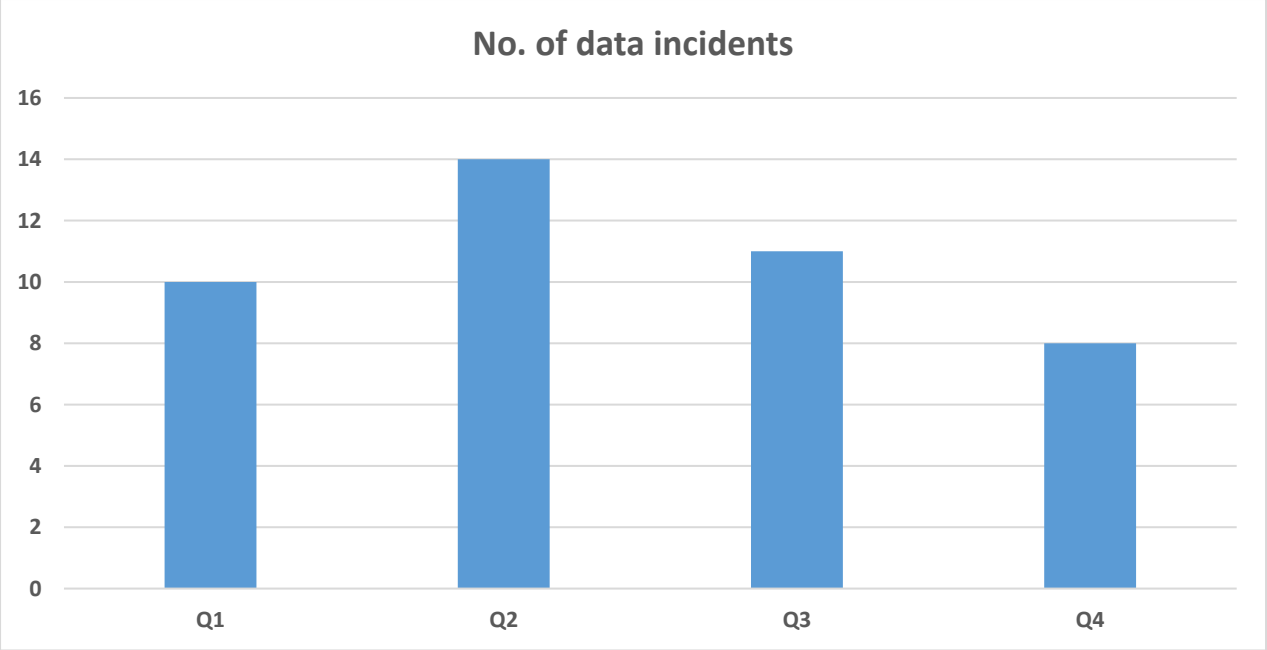

Table D - Data incidents by category