Audit and Risk Assurance Committee

Meeting Date	11 June 2025
Title	Annual Information Governance Report
Author(s)	Maxine Noel, Information Governance Manager
Executive Sponsor	Claire Amor, Executive Director of Corporate Affairs

Executive Summary

The Annual Information Governance (IG) report is presented. The report covers the period from April 2024 to 31 March 2025.

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

Appendix 1 – Annual information requests 2024/2025

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

Appendix 2 – Annual information incidents 2024/2025

- Data incidents quarterly breakdown
- Data incidents by category

Action required	The Committee is asked to review the information provided and seek clarification on any areas.
Previous consideration	The draft report was discussed at the ISMS Board on 13 May 2025.
Next steps	Ongoing monitoring of trends in information governance.

Financial and resource implications	There is no direct financial impact.
Associated strategic priority/priorities	Build a resilient, healthy, capable and sustainable organisation
Associated strategic risk(s)	5.a The resources we require to achieve our strategy are not in place or are not sustainable
Risk appetite	Compliance - measured
Communication and engagement	Not applicable
Equality, diversity and inclusion (EDI) impact and Welsh language standards	Not applicable
Other impact assessments	• Data protection • Sustainability
Reason for consideration in the private session of the meeting (if applicable)	Not applicable

Information Governance Annual Report - 1 April 2024 to 31 March 2025

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 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.
- 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 2024 to 31 March 2025.

2. Information requests

2.1 During the reporting period we received a total of 565 requests for information. This is an increase to the total of 534 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 93% (224) of the 240 FOI requests completed within the reporting period were responded to within the statutory deadline of 20 working days. 93% is lower than the 96% achieved last year. A number of requests have been located within other matters after the response deadline has been passed.

2.3 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’.

2.4 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) and other data subject information requests

2.5 93% (136) of the 146 data subject requests 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 higher than the 90% 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 Section 45 of the FOI Code of Practice 2018, it is good practice for organisations to conduct 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

46 internal review requests (7 FOIs and 39 SARs were referred for internal review). This compares to 41 internal review requests received in the previous year.

2.9 The team responded to five data erasure requests. This compares to six 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 86 incidents. This is double the 43 incidents recorded for the previous year. We are unsure why there has been an increase in the number of reported incidents. However, it should be noted that we record information incidents (and not just data breaches). Some incidents were reported by data subjects, but were part of the fitness to practise (FTP) process.

3.4 The majority of incidents reported occurred in FTP followed by Registration and Tribunal Services. These areas of the organisation handle large volumes of personal data. Generally most incidents are of the same general level of risk, although five were of sufficient risk to require reporting.

3.5 Human error continues to be the main cause of many incidents, with some weaknesses in processes and systems also highlighted.

3.6 Following the Committee's comments on last year's report, we have developed additional analysis and categorisation of data incidents. Our analysis tries to identify the underlying cause of human error incidents. This can be found at Appendix D.

3.7 One of the recommendations from last year's BSI audit of ISO27001:2022 was that we should improve our ability to track and manage information incidents. We intend to make changes to the current IT helpdesk system to incorporate logging of information incidents. It is envisaged that staff will use the IT helpdesk to log their information incident and complete the information that we currently capture on the information incident report (IIR) form. This will assist with tracking, data analysis and reporting of incidents. Go live for this is planned for the first quarter of the 2025-26 financial year.

3.8 Five information incidents were assessed as meeting the threshold for reporting to the ICO. All were closed by the ICO with no further action.

4. 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:

- The ICO contacted us to advise that they had received a complaint from a solicitor that we had inappropriately disclosed sensitive and special category personal data relating to a third party. The solicitor represents registrants subject to FTP investigations. The incident arose from an error in updating Nexus because the solicitor moved from one law firm to another. The cases that needed to be updated were identified by profession and registrant surname alone from the list that the solicitor provided to the FTP team. This resulted in the file for the third party, who had the same surname as one of the solicitor's clients, being incorrectly assigned to the solicitor.
    - The ICO determined that we had failed to comply with our data protection obligations and that our approach to updating case files was inadequate and led to the breach. However, the ICO are satisfied that we have identified the inadequacy that caused the issue and that we have put procedures in place to prevent similar issues in the future. They were also satisfied that we were right not to report the incident to them (we advised the solicitor at the time of the incident that we would not report the incident to the ICO because we considered the level of risk to be low as the material had been sent to a solicitor/law firm with understanding of the requirements of data protection law and the information had not been shared further).
    - ICO outcome: no further action. However, the ICO will keep a record of the incident on file.

- The ICO received a complaint from a solicitor representing a registrant subject to FTP. The complaint to the ICO was that they had requested an internal review of their SAR but we had not responded. The ICO asked us to provide further details of our handling of this SAR.
    - As there is no statutory requirement to provide internal reviews of SARs and we responded to the SAR within the relevant timescale the ICO determined that we had complied with our data protection obligations.
    - ICO outcome: The ICO noted that we had advised the requester that we would respond to the internal review request.

- The ICO received a complaint about our refusal to release information in response to an FOI request. The FOI request was for the contact address of a registrant. The ICO supported our decision to withhold this information in their published decision notice (ic-330081-q9n4/).

- The ICO received a complaint that we did not respond to an SAR from an FTP complainant. The SAR asked specific questions about the evidence that we had made available to the registrant and the ICP and our lawful basis under the DPA to process the complainant's personal data. The ICO asked us to write to the requester and comply with the SAR by answering the specific questions that they asked.

- The ICO received a complaint about the way we had handled a SAR from a registrant. The complaint to the ICO was that we had refused to release the personal information requested. The ICO asked us to revisit and review the SAR. The registrant had not asked us to conduct an internal review of their SAR. Therefore, in response to the ICO complaint we conducted an internal review of their SAR. Their original request was for a copy of all personal data held about them. We noted that we had not refused to release any personal information to them. We provided them with a copy of the personal data held, except for some documents held on their current FTP cases. Our original response explained why we thought an exemption applied to the withheld information, and we provided further explanation of this when we wrote to them following their complaint to the ICO.

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 Since January 2021, we have published our FOI compliance statistics on the HCPC website on a quarterly basis. 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).

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

- explaining that all external outbound and inbound telephone calls received into a HCPC number are recorded. This was later removed when the decision was made to stop recording all external outbound/inbound telephone calls; and

- amending the details of our Data Protection Officer (changed from Executive Director of Corporate Affairs to Chief Information Security & Risk Officer).

5.4 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:

- online concerns form enhanced;
- CONTINIA payment processing;
- data platform – Reporting-HASURA;
- FTP testing cycle anonymisation;
- FTP mVine upgrade or replace;
- phone call recording;
- hard disk wiping and recycling;
- SimplyMeet;
- online employee feedback form;
- diversity dashboard;
- BottomLine (BACS software);
- NALYTICS redaction software; and
- ENHESA (health and safety legislation portal).

5.5 We continue to review all our older memorandums of understanding (MOUs). We have updated or newly signed a total of seven MOUs as follows:

- the Williams Review (Investigating healthcare incidents where suspected criminal activity may have contributed to death or serious life-changing harm);
- the Education department have established a number of MOUs with professional bodies including the British Association of Art Therapists, the College of Paramedics, the Institute of Biomedical Science, the College of Operating Department Practitioners, the Royal College of Occupational Therapists and the Chartered Society of Physiotherapy; and
- a number of MOUs are in the process of being updated with the appropriate authorities, including Care Quality Commission, which reports that the average time to renegotiate is two years. Some requests have been refused, including the Department of Work and Pensions.

5.6 In April 2024, the BSI undertook a six and a half day recertification and transition audit of the HCPC's ISO27001:2013 registration spread over the month. This resulted in the successful transition to ISO27001:2022 standard. 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. Opportunities for improvement were highlighted around "Supplier Management including use of Cloud Services"; "Information Security Incident Management" (automating the incident reporting process via the IT helpdesk); "Information Security during disruption including ICT readiness for business continuity" scheduling more disaster recovery/business continuity management tests in advance. The three day surveillance audit for April 2025 was planned.

5.7 A total of 38 information security related audits were completed in the 2024-25 financial year. Further audits are ongoing as they require to evidence change over time.

5.8 All Information Security Management System documentation was updated by the ISMS Board over December 2024/ January 2025, and the Information Security Computer Based Training package updated to include selected recommendations from the BDO Data Privacy Audit (see below).

5.9 During the year, data protection was subject to internal audit. The internal auditors (BDO) report was presented to the Committee at its meeting in March 2025.

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, 97% 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 2024-2025

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

Appendix 2 – Annual information incidents 2024-2025

- Data incidents quarterly breakdown
- Data incidents by category

Date of paper: 15 May 2025

Contact for further information:

Name: Maxine Noel
Role: Information Governance Manager
Email: Maxine.Noel@hcpc-uk.org

Appendix 1 – Annual information requests

Table A - Breakdown of information requests received

	Q1	Q2	Q3	Q4	Total 2024/25	Total 2023/24
FOI	63	64	54	64	**245**	**248**
SAR	43	42	26	45	**156**	**156**
EIR	0	0	1	0	**1**	
Disclosure requests	23	29	31	28	**111**	**87**
Internal reviews	13	12	4	17	**46**	**41**
ICO complaints	0	3	0	2	**5**	**2**
Total requests received	**142**	**150**	**116**	**156**	**564**	**534**
Total closed	**131**	**145**	**133**	**114**	**523**	**523**

Table B – FOIs and SARs completed

	Q1	Q2	Q3	Q4	Total 2024/25	Total 2023/24
FOI						
Total closed	57	64	62	57	**240**	**243**
- Response within statutory timescale	52	61	58	53	**224**	**234**
- Response in breach of statutory timescale	5	3	4	4	**16**	**9**
- % within statutory timescale	**91%**	**95%**	**94%**	**93%**	**93%**	**96%**
SAR						
Total closed	36	44	31	35	**146**	**161**
- Response within statutory timescale	34	43	26	33	**136**	**145**
- Response in breach of statutory timescale	2	1	5	2	**10**	**16**
- % within statutory timescale	**94%**	**98%**	**84%**	**94%**	**93%**	**90%**

Appendix 2 – Annual information incidents

Table C- Data incidents quarterly breakdown

	Q1	Q2	Q3	Q4	Total 2024/25	Total 2023/24
No. of data incidents	19	16	24	27	**86**	**43**

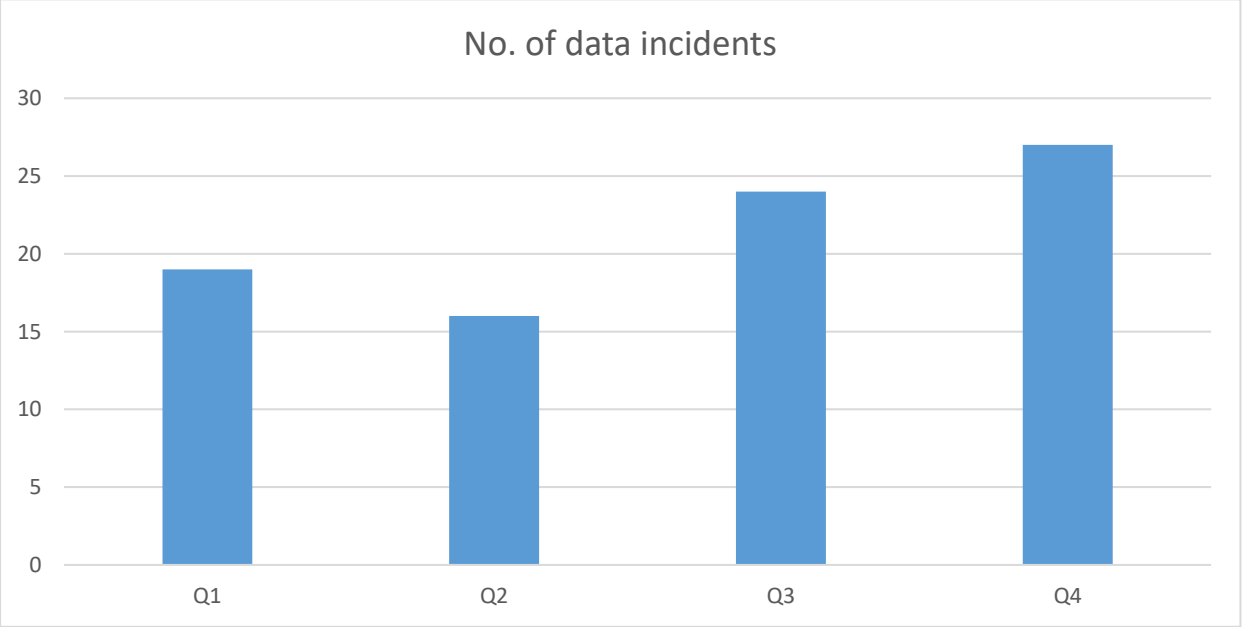

Table D - Data incidents by category

Data incident categories - Total 2024/25											
CAUSE MATRIX	**Human Error**	**System/IT issue**	**Supplier Error**	**Process not followed**	**Process Weakness**	**Malicious Activity / Attempted Fraud**	**Paper Loss**	**Verbal Disclosure**	**Redaction failure**	**Internal Loss**	**Lack of suitable Training**
Human Error		4	3	2	1				1		
System / IT Issue	13					5					
Supplier Error	3										
Process not Followed	14		1					1			
Process Weakness	12	4	1								
Malicious Activity / Attempted Fraud											
Paper Loss											
Verbal Disclosure	1										
Redaction failure	4		1								
Internal Loss	3		1				1				
Lack of suitable Training	4	1									