Audit and Risk Assurance Committee

9 June 2022

Information Governance Annual Report

Executive Summary

This paper provides an update on information governance activity for the period 1 April 2021 to 31 March 2022.

Appendices

1 – Annual information requests

2 – Annual information incidents

Previous consideration	This report was considered by ELT on 16 May 2022 and presented to ARAC annually as a standing report.
Decision	The Committee is invited to discuss the report.
Next steps	The Committee will receive the next report at its meeting in June 2023.
Strategic priority	Strategic priority 1: Continuously improve and innovate Strategic priority 4: Be visible, engaged and informed
Financial and resource implications	None as a result of this paper
EDI impact	N/A
Author	Maxine Noel, Information Governance Manager maxine.noel@hcpc-uk.org
Sponsor	Claire Amor, Head of Governance claire.amor@hcpc-uk.org

Audit Committee, 9 June 2022

Information Governance Annual Report - 1 April 2021 to 31 March 2022

Introduction

1.1 The Information Governance (IG) function within the Governance 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 2021 to 31 March 2022.

Information requests

2.1 During the reporting period we received a total of 427 requests for information. This is an increase to the total of 367 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 87% (177) of the 203 FOI requests completed within the reporting period were responded to within the statutory deadline of 20 working days. 87% is lower than the 95% 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 46% of the late responses were a result of delays in identifying an FOI request within an email and forwarding this to the Governance team. This delay was due to the large volume of correspondence the Registration team received over the summer and beyond and the impact this had on processing times.

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

Subject access requests (SAR)

2.5 87% (102) of the 117 subject access requests (SAR) completed within the reporting period were responded to within the statutory deadline of one month. This is lower than the 91% achieved last year. Delays in forwarding requests as noted in 2.3 also impacted SARs.

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 38 internal review requests (11 FOIs and 27 SARs were referred for internal review). This compares to 19 internal review requests received in the previous year.

2.9 The team responded to three data erasure requests and one request to restrict processing. This compares to five 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 48 incidents. This is lower than the 51 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 or not applying redactions. These errors are caused sometimes due to working across multiple cases at once.

3.6 Two incidents were reported to the ICO:

- A professional body contacted us to explain that a member of their legal and governance staff, who was on parental leave, had contacted us without the organisation's authorisation. The individual contacted us for personal reasons. They sought information pertaining to complaint(s) raised about a named registrant. This person would normally be in touch with us about FTP matters and we disclosed the information they requested. The individual who contacted us for disclosure is also on the Solicitors Regulation Authority (SRA) Register. As the incident involved deception, we also reported the matter to the SRA.
- An interim order application was made. The bundle of documents, sent to the registrant's representative and ICP Panel, included documents received from the registrant's employer, including witness statements. The employer did not state that these could not be shared with the registrant. The names of colleagues were not redacted from the witness statements which the registrant received. This was in breach of our current redaction guidance. The employer later contacted us to say that they were

concerned that the names of their staff witnesses were shared with the registrant. The employer had also reported the FTP incident to the Police who had also informed them that the employer's witness statements should not have been shared with the registrant.

3.7 For both incidents reported to the ICO, the ICO determined there was no further action required and closed both matters.

3.8 As a result of these incidents, we provided specific training and guidance to FTP on the level of detail and point in the FTP process when information can be shared with professional bodies.

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 asked us to review how we handled a complaint regarding sending sensitive confidential information (health-related) to a registrant by email without encryption. The registrant's complaint to the ICO also included that we sent some letters to an incorrect address. This incident had been reported centrally by the FTP department prior to us receiving correspondence from the ICO. Our investigation documents showed that the member of staff who had sent the health-related document to the registrant had known that the document should have been password protected, prior to sending. However, a lapse in concentration was the cause of this error. At the time of the incident, a reminder email was sent to the member of staff that confidential and/or sensitive information should be password protected prior to sending by email. We could find no evidence of letters being sent to an incorrect address.
- The ICO asked that we review how we handled a request for our internal process documents (or standard operating procedures) that staff follow when processing fitness to practise cases. Our initial response was to withhold the information on the grounds that the documents we hold detail how to process cases within our case management system. We felt disclosure would be likely to prejudice the effectiveness of our case management system or expose it to security attacks. On further review we determined that we could release redacted copies of our FTP operational manual (the manual comprises of two documents: FTP case management manual and the Post ICP manual).
- We were asked to revisit the way we handled a complaint regarding a data incident. The incident was in relation to the taking of a direct debit payment earlier than scheduled. We wrote to the registrant to further address his complaint and explained that the direct debit instalment which was scheduled for collection from their bank account on 4 January 2021, was taken a week earlier than expected on 24 December 2020 due to a system

error. The incident happened due to issues associated with moving to a new registration and payment system.

- A registrant's complaint to the ICO was that in our response to his SAR we had not included a copy of the transcripts of the calls he made to the Registration department. We explained to the registrant (in our response to his SAR) and later to the ICO that we were not able to record telephone calls made to the Registration Department during the dates the registrant had called (Jan-Feb 2021). We did provide a copy of the notes taken of his telephone calls that are held on his registration record in response to his SAR. However, as we do not hold a copy of the call transcripts, we were unable to provide these.
- A registrant's complaint to the ICO was that we had unlawfully disclosed their personal data when we contacted a legal representative (a solicitor) who never acted for them in relation to their fitness to practise cases. Our investigations into this incident showed that the registrant had advised us that we would be contacted by a legal representative (the registrant did not provide the name of their legal representative in their correspondence to us). Four days later, the legal representative contacted us to advise that they were acting for the registrant. We therefore concluded there had been no unlawful disclosure or data breach.

4.3 For all five complaints, the ICO determined there was no further action required.

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 now include our use of personal data for research purposes. We make it clear to our data subjects that we conduct research only for purposes that fall within our statutory function. To be lawful it must be research that is necessary for our statutory functions and is carried out in the public interest. We also made changes to include our processing of personal data included in the pass lists we receive from HCPC approved course providers.

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:

- Moving paper-based registration applications to online applications
- Data sharing/memorandum of understanding with other regulators where FTP concerns are raised
- Transport of hard copy international applications to an outsourced data processor

5.6 Our template data sharing agreements and memorandum of understanding (MOU) were updated with legal input. These templates enable us to have a HCPC start point when entering into agreements with third party organisations. We have started a project to review all our older MOUs.

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, 86% 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 2021/2022

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

Appendix 2 – Annual information incidents 2021/2022

- Data incidents quarterly breakdown
- Data incidents by category

Date of paper
10 May 2022

Appendix 1 – Annual information requests

Table A - Breakdown of information requests received

	Q1	Q2	Q3	Q4	Total 2021/22	Total 2020/21
FOI	52	55	39	59	**205**	**191**
SAR	36	35	24	25	**120**	**103**
Disclosure requests	12	14	11	22	**59**	**51**
Internal reviews	10	7	9	12	**38**	**19**
ICO	1	3	1	0	**5**	**3**
Total requests received	**111**	**114**	**84**	**118**	**427**	**367**
Total closed	**107**	**110**	**97**	**108**	**422**	**346**

Table B – FOIs and SARs completed

FOI						
Total closed	48	54	44	57	**203**	**174**
- Response within statutory timescale	37	49	41	50	**177**	**165**
- Response in breach of statutory timescale	11	5	3	7	**26**	**9**
- % within statutory timescale	77%	91%	93%	88%	**87%**	**95%**
SAR						
Total closed	37	30	27	23	**117**	**97**
- Response within statutory timescale	31	27	26	18	**102**	**88**
- Response in breach of statutory timescale	6	3	1	5	**15**	**9**
- % within statutory timescale	84%	90%	96%	78%	**87%**	**91%**

Appendix 2 – Annual information incidents

Table C- Data incidents quarterly breakdown

	Q1	Q2	Q3	Q4	Annual Total 2021/22	Annual Total 2020/21
No. of data incidents	14	11	15	8	**48**	**51**

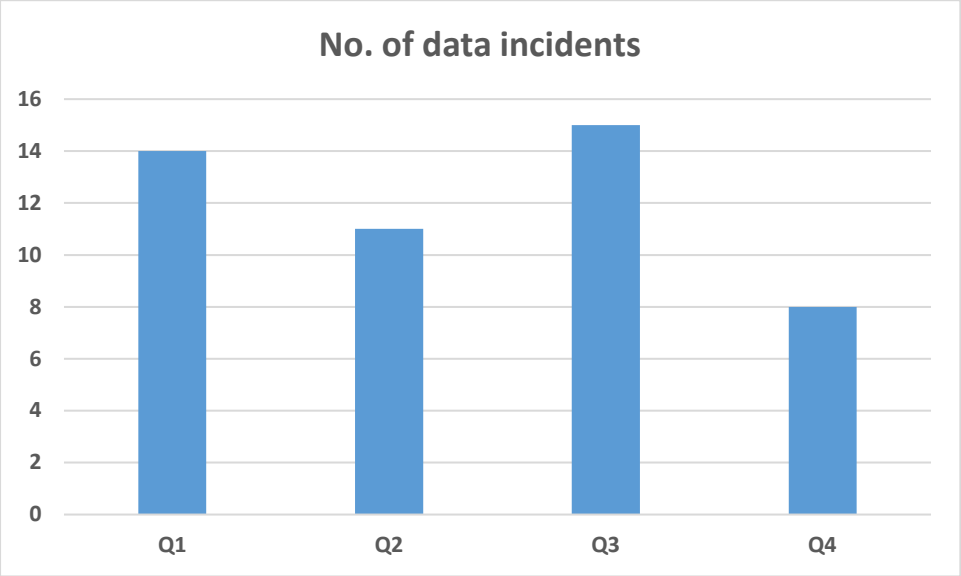

Table D - Data incidents by category