### Action
To note

### Purpose
The Data Protection Officer is responsible for monitoring and advising on the GMC’s compliance with data protection legislation. This report summarises the past year’s actions and highlights future developments.

### Decision trail
This is a standing annual report.

### Recommendation
To consider the Data Protection Officer’s Annual report.

### Annexes

### Author contacts
**Andrew Ledgard**, Head of Information Policy  
[andrew.ledgard@gmc-uk.org](mailto:andrew.ledgard@gmc-uk.org), 020 7189 5418

**Thomas Oppé**, Information Governance Manager  
[thomas.oppe@gmc-uk.org](mailto:thomas.oppe@gmc-uk.org), 0161 923 6410

### Sponsoring director/Senior Responsible Owner
**Neil Roberts**, Director of Resources  
[neil.roberts@gmc-uk.org](mailto:neil.roberts@gmc-uk.org), 0161 923 6230
Introduction

1 Over the course of the last year, the Information Policy Section have been involved in both conventional business-as-usual activities as well as specific initiatives associated with the coronavirus pandemic. We have supported a range of external pandemic research requests. We have also supported GMC and MPTS colleagues in introducing pandemic-related measures.

Activities in 2020

Supporting the pandemic response

2 We ensured that the GMC’s response to the coronavirus was compliant with our GDPR obligations, while working within a fast-moving and challenging environment. Colleagues across the GMC were proactive in engaging with the Data Protection Officer, and this collaborative approach meant that information governance concerns did not act as a barrier, especially where collaboration with external organisations was required.

3 We worked with the Registration team while they re-registered doctors using the GMC’s emergency powers. Despite concerns being raised by a small number of doctors about the re-registration process, we were able to ensure that the GMC could demonstrate its information governance compliance measures.

4 At the start of the pandemic, we provided Public Health England with access to information about registrants to assist them with their response planning. We also supported the NIHR-funded UKREACH study, which is monitoring the disproportionate impact of COVID on BME Healthcare workers. This study is likely to expand to include the impacts of “long-covid” and vaccine hesitancy among the same cohort. This important research raised complex information governance issues but we were able to draw on our experience of similar projects, particularly the GMC’s own UKMED research programme, to put appropriate controls in place.
Publication and disclosure

5 We supported the Registration and Revalidation directorate in drafting a new publication and disclosure policy. The policy will strengthen the GMC’s compliance with the GDPR’s accountability principles by making our use of data more transparent.

6 The policy sets out the overarching principles which will apply when we publish registration information on the GMC website (for example through LRMP) and when we disclose information to support our statutory functions. This will help GMC staff to make consistent decisions in response to requests and when developing policy.

7 The policy will sit alongside a similar policy already established for Fitness to Practise information, so the majority of the GMC’s publication and disclosure is now set out in established policy.

Data breaches and information security

8 In 2020, we saw a 14% decrease in reported disclosure incidents (137 reported in 2020) and a 36% decrease in reported security incidents in general (267 reported in 2020).

9 In October 2020 we passed our annual assessment for BS10008. Our annual internal audit was also performed in July, receiving positive results.

10 The information security team also carried out a Phishing exercise on behalf of the Audit and Risk Committee, which has been followed by additional guidance and the introduction of new Phishing e-learning for staff.

11 The full Information security management system annual review 2020 can be found at Annex A of this paper.

Data Protection Impact Assessments

12 We received 28 requests for Data Protection Impact Assessments from colleagues in 2020. 100% of submissions received an initial response on whether a DPIA was necessary within 5 working days.

13 In 2021 we will work with the Quality Assurance team to audit the DPIA process, which was introduced in 2019. We will reflect on how it is working in practice.
Data subject rights

14 In terms of processing subject access requests (SARs), the work of the Information Access Team has been significantly impacted by the pandemic. For the period from mid-March to July 2020 we placed a considerable number of requests ‘on hold’ as we were unable to carry out the necessary action to complete those requests. This was usually because we were required to seek a view on disclosure from either an NHS body or a registered doctor and a decision was taken that it was inappropriate to make contact with them at that point due to the pandemic-related pressure on the profession. The vast majority of those ‘on hold’ requests failed to meet the statutory timeframe for response due to the pause in activity.

15 Additionally at the time of the first lockdown the team were in the middle of a recruitment campaign to fill vacancies at Officer level. The temporary postponement of the campaign meant that the team were significantly below headcount for the vast majority of 2020. Consequently, for the twelve-month period from March 2020 to February 2021 we met the statutory deadline for response in 73.6% of SARs. This is set against an SLA of 80%.

16 While the intake of requests declined considerably in the period from mid-March to May 2020 it soon recovered to reach pre-pandemic levels during the remainder of 2020. For the twelve-month period from March 2020 to February 2021 we received 438 SARs compared with 498 requests over the same period in 2019/20. This marks a 12% decrease overall.

17 We also received 24 requests related to other data subject rights under the GDPR. The majority of these were requests for the erasure of personal data (the ‘right to be forgotten’). 71% of these requests were responded to within the target timescale, with the reason for delay usually relating to the complexity of the requests and the need to develop policy lines.

18 Most requests for the deletion of data are refused on the grounds that retention is necessary for the GMC to carry out its statutory functions. For example, the right cannot be used to override existing publication periods for FTP sanctions. A small number of requests were granted in circumstances where the publication of designated body or training information might disclose the location of a vulnerable doctor.
Future work

Legislative reform

19 The legislative reform programme provides an opportunity for the GMC to improve clarity on its powers to obtain and disclose personal data. We are leading a workstream in the programme looking at information governance and data sharing reform. In particular, we are addressing some of the challenges posed by the GDPR. When processing personal data, we are required to establish a clear association with our Medical Act statutory functions. This sometimes poses a challenge when we wish to make disclosures that are not clearly or specifically identified in our primary legislation.

20 The information governance priorities for legislative reform are to:

- retain our existing data acquisition and disclosure powers if they are still required
- extend existing powers to enable a wider approach to using personal data to support our statutory objectives
- ensure we are not restricted to only publishing or disclosing data about currently registered doctors
- make it easier to obtain data for research and operational purposes through enabling powers to obtain data

21 The legislative reform programme also presents some information governance risks if our powers are amended in ways which make it more difficult to obtain or disclose information. We are actively engaging with DHSC officials to address our data processing requirements.

Automated processing and Artificial Intelligence

22 Automated processes and AI are an increasingly prominent part of the GMC’s IS strategy. This presents the GMC with new opportunities but also creates new compliance risks as we begin to explore new ways of using personal data. The Information Commissioner’s Office has published more detailed guidance on this topic and it is likely to be an area of increased regulatory scrutiny. We will be working closely with IS colleagues to ensure the necessary compliance controls are in place.