The Health and Care Professions Council (HCPC)

Data Protection

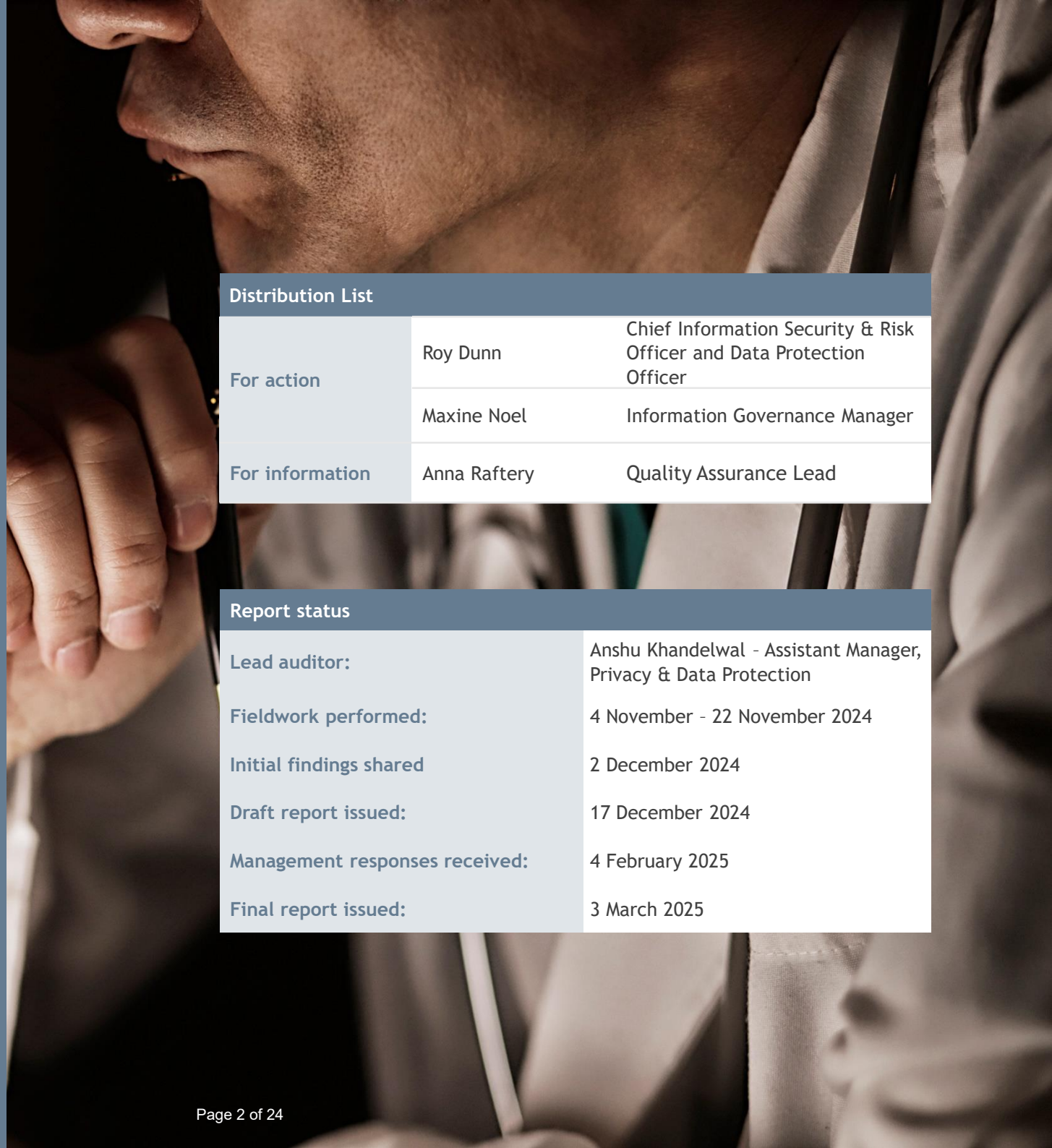
Internal Audit Report - Final

March 2025

Level of assurance:	
Design	Moderate
Effectiveness	Moderate

IDEAS | PEOPLE | TRUST

CONTENTS



Distribution List		
For action	Roy Dunn	Chief Information Security & Risk Officer and Data Protection Officer
	Maxine Noel	Information Governance Manager
For information	Anna Raftery	Quality Assurance Lead

Report status	
Lead auditor:	Anshu Khandelwal – Assistant Manager, Privacy & Data Protection
Fieldwork performed:	4 November – 22 November 2024
Initial findings shared	2 December 2024
Draft report issued:	17 December 2024
Management responses received:	4 February 2025
Final report issued:	3 March 2025

Executive summary

Level of Assurance: (see Appendix I for Definitions)		
Design	Moderate	Generally, a sound system of internal control designed to achieve system objectives with some exceptions.
Effectiveness	Moderate	Evidence of non-compliance with some controls, that may put some of the system objectives at risk.

Summary of findings (see appendix II)			# of agreed actions
H	-		-
M	2		TBC
L	5		TBC
Total number of findings: 7			

Purpose

The purpose of the internal audit was to assess how HCPC assures itself that it is compliant with the UK and EU GDPR and confirm that any exemptions are properly applied with appropriate oversight. We also assessed whether the data protection control environment has been adequately designed to mitigate inherent risks and whether these controls are operating effectively.

Background

As part of the 2024/2025 internal audit plan for the Health and Care Professions Council (HCPC), as agreed by the Audit and Risk Assurance Committee (ARAC), we performed an audit over the design and operational effectiveness of the controls in place to comply with the UK and EU GDPR, in relation the processing of personal data.

The risks associated with non-compliance with the UK and EU GDPR are significant, amounting to a maximum of £17.5 million (€20 million) or 4% of global turnover (whichever is greater), although the associated reputational damage of enforcement action is also a significant risk.

The Information Commissioner's Office (ICO) is a very active regulator (when compared with European counterparts) and has issued enforcement action as a result of non-compliance, in the healthcare sectors in the last 12 months.

HCPC regulates 15 health and care professions, and is therefore exposed to the processing of personal data as part of;

Background (continued)

1. Core Business – administering registrations, investigating concerns, administering fitness to practice (FTP) hearings, Continuing Professional Development (CPD) records and running events and consultations.
2. Day to day operations - regarding current/former employees and recruitment applicants.

The Executive Director of Corporate Affairs was appointed as the Data Protection Officer (DPO) and returned from maternity leave at the start of 2025. During this period, the Chief Information, Security & Risk Officer was appointed as Interim DPO leading on the data protection compliance at HCPC.

The DPO is supported by the Information Governance Manager and an Improvement & Compliance Specialist who looks after the day-to-day compliance activities, such as updating and reviewing the Records of Processing Activities (RoPA), privacy notices, policies and procedures and managing data subject rights requests and data breaches when required.

In the last 12 months (from November 2023 to October 2024), HCPC has recorded a total of 54 data breaches internally. One of which was deemed high risk and sufficiently serious to warrant reporting to the ICO, although the ICO did not take any further action.

HCPC has received a total of 171 data subject rights requests in the last 12 months, of which, 91% were processed within the prescribed one calendar month.

Executive summary

Good practice

We identified areas of good practice in relation to data protection compliance at HCPC:

- The Information Governance Manager develops a monthly Information Governance report, which is presented to the Executive Leadership Team, and includes updates on data subjects rights request received, complaints from ICO and data breaches reported.
- The Information Governance Manager presents an Annual Information Governance (IG) report to Audit and Risk Assurance Committee on Data subject rights requests, data breaches, complaints from ICO etc.
- HCPC has established an Information Security Management System Board (ISMSB), chaired by the Chief Information Security Risk Officer (CISRO) which meets quarterly. The DPO presents a report to ISMSB on internal developments i.e. pipeline projects that require a Data Protection Impact Assessments (DPIAs), the number of breaches reported internally, etc.

Summary of findings

Despite the good practice identified, we have noted two Medium priority findings:

1. **Records of Processing Activity (RoPA), third-part data transfers and lawful basis of processing:** The RoPA forms the foundation of data protection governance and compliance. It is also the basis of other areas of data protection compliance, including the accuracy of privacy notices and data subject rights procedures. To meet transparency requirements, organisations usually publish data processing activity via the privacy notices, however HCPC has taken the decision to also publish the RoPA online, (even though this is not a regulatory requirement) which has therefore limited the granularity of the information contained in the RoPA, and in turn means that HCPC cannot evidence complete oversight of data processing activities, third-party data transfers (including international transfers) and the lawful basis for processing, (Article 6).
2. **Data subject rights requests:** 16 data subject rights requests (9%) were not processed within the prescribed one calendar month, with no further extension applied. We found a gap in the Frink system as it records the wrong start date for monitoring data subject rights requests and does not distinguish between data subject rights requests and Freedom of Information (FOI) requests.

We also noted five Low priority findings which relate to the following;

1. The Data Protection Policy and privacy notice are two separate documents with distinct purposes; however, these have been combined, making it more difficult for individuals to understand how their personal data is processed.
2. Improvements are needed in the information security training material and the accuracy of the training completion reports.
3. Complete implementation of data retention periods.
4. The requirement to complete DPIAs has not been incorporated in centralised processes, notably, the Project Management guide.
5. HCPC has not defined the process for assessing the severity of a data breach and notifying the ICO and affected individual (in the event of a reportable breach

Executive summary

Conclusion

Overall, we identified two Medium and five Low priority findings within this audit. These findings relate to both design and control, resulting in 'Moderate' assurance over the design and 'Moderate' assurance over the operational effectiveness of data protection compliance processes.

If the findings identified in the audit are left unaddressed, this could ultimately expose HCPC to financial penalties, reputational damage, and increased regulatory scrutiny.

91%
Of the Data subject rights requests were processed within prescribed time limits

14
DPIAs complete by HCPC in last 12 months

1
Data breach (of 54) reported to the ICO in last 12 months, though the ICO took no further action

92%
Of employees completed mandatory Protection Personal data training

Detailed findings

Detailed findings

Risk: HCPC cannot evidence complete oversight of organisation-wide data processing activity, third-party data transfers or transfers of personal data outside of the UK or EU/EEA and an appropriate lawful basis, which has an impact on the ability to comply with additional compliance requirements when relying on consent or legitimate interest.

Finding 1 - The Record of Processing Activity (RoPA) does not accurately reflect organisation-wide data processing.	TYPE
Article 30 of the UK Data Protection Act 2018 and EU General Data Protection Regulation requires organisations to document organisation-wide data processing activities in a Records of Processing Activity(RoPA). The RoPA should be a live document which forms the foundation of data protection governance and is the basis of other compliance areas, including the accuracy of privacy notices and data subject rights procedures. Organisations are also required to document and appropriately justify a lawful basis for each processing activity as required by Article 6 of the UK GDPR to demonstrate that personal data is processed 'lawfully, fairly and transparently.' Data controllers should also have complete oversight of third-parties with whom personal data is shared, to ensure that contracts are in place which include the relevant data processing clauses, as well as oversight of international data transfers (outside the UK or EU/EEA) to ensure that appropriate safeguards are in place, where applicable. HCPC developed a RoPA using Microsoft Excel and has taken the decision to publish via the website, even though this is not a regulatory requirement. Typically, Organisations primarily comply with the transparency principle by communicating data processing activity via the privacy notices. Overall, we noted that the HCPC RoPA is high level and the concern is that the desire to publish the RoPA via the website limits the granularity of the information contained within the document, (for example systems in which personal data is stored, and the names of third-party processors, which could be considered commercially sensitive). We also noted the following: 1. The RoPA was developed using categories of data subjects as the driver, rather than the purpose for processing, which impacts on HCPC's ability to define the lawful basis for processing, identify third-party data transfers and systems in which data is stored. Furthermore, the lawful basis for processing in the RoPA has been allocated against the category of personal data (i.e. name, title, date of birth) rather than the purpose of processing (required by Article 6 of the UK GDPR (and Articles 9 and 10, if processing special category or criminal offence data). As a result, HCPC is unlikely to have an accurate view of the lawful bases for processing across the organisation. 2. Column D in the RoPA requires HCPC to define internal and external data transfers, however HCPC has not defined third-parties or their location in the RoPA, to evidence oversight of international transfers, where additional safeguards may apply. Although, the procurement team maintains a list of contracts which includes the names of the vendors and contract details, this is not linked to data processing activities in the RoPA. 3. The RoPA does not include version control, to evidence regular review.	Design & Effectiveness
Implication	**Significance**
▶ If the RoPA does not accurately define the purpose of processing in sufficient detail, HCPC cannot evidence complete oversight of organisation-wide data processing activity, in-keeping with the accountability principle. This also increases the risk that HCPC will not comply with other requirements, such as ensuring the accuracy of privacy notices, in-keeping with the transparency principle.	Medium

Detailed findings

Risk: HCPC cannot evidence complete oversight of organisation-wide data processing activity, third-party data transfers or transfers of personal data outside of the UK or EU/EEA and an appropriate lawful basis, which has an impact on the ability to comply with additional compliance requirements when relying on consent or legitimate interest.

Implication	Significance
▶ If HCPC does not have organisation-wide oversight of third-party transfers, it cannot ensure that contracts are in place which include the relevant data processing clauses. There is also an increased risk that in the event of a notifiable third-party data breach (at a third party), HCPC will not be notified promptly to communicate this to the ICO within 72 hours ▶ If the RoPA does not define the lawful basis for processing personal data (Article 6) and additional conditions for processing special category data (Article 9) for each processing activity, HCPC cannot evidence that personal data is being processed lawfully and fairly. Furthermore, the DPO will not have complete oversight of data processing activities based on consent or legitimate interest, where additional compliance requirements apply.	Medium

Recommendations	Action owner	Management Response	Completion Date
1. HCPC should reconfigure the RoPA to document; a. Purpose of processing b. Data processed c. Categories of data subjects d. Single most appropriate lawful basis for processing e. Additional conditions for special category data f. Name of third-party data processors and joint controllers g. Locations of third-party data processors and joint controllers h. Systems in which personal data is stored.	*Roy Dunn, CISRO*	*We accept the findings. Elements a-h will be documented in the Risk Info Assets document.*	*30 April 2025*
2. Incorporate version control in the RoPA to evidence regular review and to ensure that the RoPA is updated on an on-going basis (at a minimum annually).	*Roy Dunn, CISRO*	*We accept the findings. A version control tab will be incorporated in the Risk Info Assets document.*	*30 April 2025*

Detailed findings

Risk: Data subject rights requests are not managed within prescribed timescales, leading to individual complaints to HCPC and/or directly to the supervisory authority.

Finding 2 - Data subject rights requests are not managed within prescribed timescales, and gaps identified in the Frink system.	TYPE
Individuals have several rights in relation to their personal data, which include the right to access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object and rights related to automated decision-making including profiling. Organisations are required to process data subject rights requests as soon as possible or within one calendar month of receipt. HCPC has developed a 'Dealing with Personal Data Requests' procedure which defines the internal process to follow when a data subject access rights request is received. HCPC has developed a process map using Visio that documents the flow of the internal process for managing data subject rights requests. However, we noted that the procedure does not include the following : 1. The process to follow when any data subject rights request is received (such as the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling). 2. Key timescales i.e. as soon as possible or within one calendar month (extended by a further two month in certain circumstances). 3. Version control details to evidence regular review. Once received, data subject rights requests are managed by the Information Governance Manager with support of the Compliance Officer and recorded in Frink (system). We noted that: 1. Between November 2023 to October 2024, in 9% of cases (16 out of 171 instances), data subject rights request were not processed within one calendar month, with no further extension applied. The Information Governance Manager confirmed that delays occur due to various reasons, such as complex requests, late identification of data subject requests, or delay in forwarding of data subject rights request received by other departments to Information Governance Manager. 2. Frink records the date the ticket was created within the system as a start date for the request, however, this is not always the date when the requestor's identity was confirmed (and when the one calendar month deadline starts). 3. Frink does not distinguish between data subject rights requests and Freedom of Information (FOI) requests which have different deadlines for completion. However, we understand that the Information Governance Manager manually distinguish the data subject rights requests and FOI.	Design & Effectiveness
Implication	**Significance**
▶ In the absence of a documented procedure, which outlines the step-by-step process for managing all types of data subject rights requests, there is an increased risk that in the event of staff absence and/or turnover, HCPC will not be able to process requests within one calendar month, which could increase the risk of complaints, either to HCPC or directly to the Information Commissioner's Office (ICO).	Medium

Detailed findings

Risk: Data subject rights requests are not managed within prescribed timescales, leading to individual complaints to HCPC and/or directly to the supervisory authority.

Recommendations	Action owner	Management Response	Completion Date
3. HCPC should update the data subject rights procedure to include: a. The process to follow when any data subject rights requests is received (such as the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object, rights in relation to automated decision making and profiling). b. Key timescales for completion i.e. as soon as possible or within one calendar month (extended by a further two month in certain circumstances). c. Version control details to evidence regular review.	*Roy Dunn, CISRO*	*We Accept the findings. The process for managing all types of data subject rights requests will be updated. The procedure will be updated to reference key timescales for completion and version control.*	*31 May 2025*
4. HCPC should promote the data subject rights process internally by: a. Incorporating the process (for reporting rights requests internally) in mandatory training b. Periodic employee awareness initiatives to remind them of internal processes when a data subject rights request is received. c. Asking team leaders to cascade information about the process to their teams.	*Roy Dunn, CISRO*	*We accept the findings.* *The process for recognising and escalating SARs is included in mandatory training which is being rolled out (February 2025).* *Intranet post raising awareness of SAR processes will be published.* *Team Leaders will be contacted to cascade this information to their teams. Furthermore, specific departmental training is planned for roll out in August 2025.*	*31 March 2025*

Detailed findings

Risk: HCPC does not accurately communicate data processing activity to individuals via the privacy notices, in-keeping with the transparency principle.

Finding 3 - HCPC has combined the data protection policy and privacy notice into one document.	TYPE
To comply with the transparency principle, data controllers are required to communicate data processing activities to individuals accurately, in a clear, concise, digestible, accessible format, and communicated in a way that is effective for the target audience. This is typically documented in the privacy notice, which should be provided to individuals at the point of data capture. In addition, privacy notices should be developed based on a complete, comprehensive and organisation-wide RoPA, to enable an organisation to accurately communicate data processing to individuals. It is important to ensure that privacy notices are regularly reviewed to reflect any changes in the RoPA. HCPC has published the data protection policy and privacy notice via the website which communicates data processing activities to all categories of data subjects including employees, education visitors, registrants, job applicants and council members. However, we noted the following: 1. The Data Protection Policy and Privacy Notice are two documents which have separate purposes, however HCPC has combined them. The data protection policy should set out how HCPC complies with the requirements of UK GDPR, which is distinct from a privacy notice which should communicate data processing activities to data subjects. 2. We also noted that the privacy notice communicates data processing activities to all categories of data subjects, including employees, education visitors, registrants, job applicants and council members. In practice however these categories of data subject personal data will be processed in very different ways by HCPC, and combining this into one document, in reality, can make the privacy notice difficult for an individual to understand how their data is processed.	Design
Implication	**Significance**
▶ If privacy notices group together categories of data subjects or are not written in a clear, accessible way that is easy for a data subject to understand, there is an increased risk that data subjects will not easily understand how HCPC processes their personal data which is not keeping in line with the transparency principle. This could lead to an increase in the number of complaints to HCPC, or directly to the ICO.	Low

Recommendations	Action owner	Management Response	Completion Date
5. HCPC should separate the privacy notice from the data protection policy and develop: a. A Data Protection Policy which sets out how HCPC complies with the requirements of the UK GDPR b. HCPC should reformat the existing privacy notice, to reflect a layered approach so that individuals can easily navigate to the section of the privacy notice which is applicable to then.	*Roy Dunn, CISRO*	*We accept the findings.* *a) The Privacy Notice and Data Protection Policy will be separated. The Data Protection Policy will define how HCPC complies with UK GDPR requirements.* *b) The privacy notice will be reformatted to make it more accessible.*	*31 March 2025*

Detailed findings

Risk: Employees are not aware of key data protection compliance requirements.

Finding 4 - Gaps identified in mandatory training materials and in the training completion report.	TYPE
Data Protection training and awareness throughout the employee lifecycle is a key control to ensure that employees are aware of key processes such as managing data subject rights requests and reporting data breaches, where strict time limits apply. HCPC delivers mandatory Information Security training to employees including HCPC partners (HCPC registrants, members of the public and legal professionals who are required to complete HCPC Partner Information Security Training) and new joiners as a prerequisite to passing their probation. However, we noted that the training focuses on information security with some focus on how to recognise and report breaches and working from home securely. As a result, the mandatory training does not include, at the very least, key data protection topics such as data protection principles, data subject rights requests, DPIAs etc. The completion rates for the Information Security training was 92%. However, we noted that the training completion report also reflects employees on long-term absence (i.e. maternity/paternity leave) and those who have left the organisation who don't have access to HCPC data, therefore reporting does not provide accurate oversight of training completion rates for the *current* workforce.	Design & Effectiveness 
Implication	**Significance**
▶ If the training material does not include data protection topics, there is an increased risk that staff will not be aware of key GDPR concepts, leading to non-compliance with the key requirements of GDPR where strict timescales apply. ▶ If the training completion rates are not accurate there is an increased risk that the report may not accurately reflect the true completion rates, potentially leading to incorrect assessments of compliance and readiness.	Low

Recommendations	Action owner	Management Response	Completion Date
6. HCPC should update the training to include the key data protection topics such as data protection principles, data subject rights requests (and timescales for processing), DPIAs etc.	*Roy Dunn* *CISRO*	*Accept - Principles, timescales and DPIA's have been added to the 2025 training pack.*	*24 February 2025*
7. HCPC should review training completion reporting arrangements, to reflect current employees only.	*Tehmina Ansari* *Learning & OD Lead*	*Accept - Management has reviewed reporting arrangements, and those on Maternity/paternity leave are still required to complete training upon their return, these names must be retained within the IT system. The L&D dept will manually remove those names of those not available for training for reporting purposes.*	*14 March 2025*

Detailed findings

Risk: HCPC cannot demonstrate compliance with the 'Data Protection by Design and Default' principle, by evidencing that consideration of data protection risk has been incorporated into business as usual.

Finding 5 - Requirement to complete a DPIA has not been included in centralised processes.	TYPE
Organisations are required to embed data protection by design and by default into business as usual. This is evidenced through the completion of Data Protection Impact Assessments (DPIAs) which identify the risks associated with data processing activities and mitigations. DPIAs should be reviewed and updated on an on-going basis to highlight the identification of new or emerging risks and mitigations as projects develop and should be included as part of any project initiation, change, or software onboarding that impacts on the processing of personal data. HCPC has developed DPIA screening questions that employees are required to complete as part of the project initiation phase, however we noted that HCPC has not developed a standalone DPIA procedure which governs the process for the completion, approval and on-going review of DPIAs. We also noted that although the DPIA is completed as part of the project initiation or onboarding of system/software, the requirement to complete DPIAs is not documented in the Procurement Manual.	Design
Implication	**Significance**
▶ If the requirement to complete DPIAs are not incorporated in centralised processes (notably the Project Management Guide and Information Security Project Management guide, there is an increased risk that DPIAs will not be completed, or, that DPIAs will be completed with the appropriate review/approvals and kept up to date.	Low

Recommendations	Action owner	Management Response	Completion Date
8. HCPC should develop a standalone DPIA procedure which governs the process for completing DPIAs, including the identification of the requirement to complete a DPIA and allocating the responsibilities for completion, approval and on-going review.	*Roy Dunn, CISRO* *Paul Cooper, Head of Business Change*	*We accept the findings. A high level process will be linking to the existing process forms. Also now included in annual training. A process has been designed. All demonstrated projects had a DPIA*	*31 March 2025*
9. HCPC should incorporate the requirement to complete the DPIA in the Procurement Manual and.	*Tarek Hussien, Procurement Manager*	*We accept the findings. The DPIA requirement will be included in the next iteration of the Procurement Manual and is already included in the Project Checklist.*	*31 March 2025*

Detailed findings

Risk: Data breaches are not reported to the Information Commissioner's Office (ICO) and/or affected data subjects within prescribed timescales, prompting financial penalties, reputational damage and increased regulatory focus.

Finding 6 - HCPC has not defined the process for assessing the severity of a data breach and notifying the ICO and affected individual (in the event of a reportable breach).	TYPE
The UK and EU GDPR requires data controllers to report certain types of data breaches to the relevant supervisory authority within 72 hours of discovery. In some instances, in the event of a high risk to the rights and freedoms of individuals, there is an additional requirement to inform the affected data subjects. HCPC has developed an Information Security Policy which sets the standards and guidelines for ensuring the confidentiality, integrity, and availability of information with some references to breaches that involve personal and sensitive data. We also noted that HCPC has developed an Information Security Incident Management process map which documents the internal process to follow in the event of a data breach. We reviewed the Information Security Incident Management Process Map and noted that HCPC has not defined the step-by-step process for how to assess the severity of a data breach (using the Information Incident Rating Tool) and, depending on the outcome of the tool, report a breach to the ICO and affected data subject (if required) within prescribed timescales.	Design
Implication	**Significance**
▶ If HCPC does not define the process for assessing the risk of a data breach and notifying the ICO and/or affected data subject, there is an increased risk that data breaches will not be managed within prescribed timescales, in the event of staff absence of turnover. If this risk were left to crystallise, it could lead to financial penalties, reputational damage and increased regulatory focus.	Low

Recommendations	Action owner	Management Response	Completion Date
10. HCPC should define the process for assessing the severity of a data breach (using the Information Incident rating tool) and reporting to the ICO and affected individual (if appropriate) in the helpdesk system.	*Roy Dunn, CISRO*	*We accept the finding. For context, currently, the response to information incidents is the sole responsibility of the Information Governance Team who have been trained and have experience in this area. A process flow exists that flags each potential type of incident and the business lead. The Information Gov Mgr reports breaches to ELT & ARAC annually in a lessons learned section of her annual report. Employees and Partners have been trained to flag incidents to allow us to respond in appropriate time scales reporting issues to informationsecurity@hcpc-uk.org*	*31/08/2025*

Detailed findings

Risk: HCPC cannot evidence complete oversight of organisation-wide data processing activity.

Finding 7 - Defined retention periods have not been implemented across all systems.	TYPE
Storage limitation is one of the key principles of the UK Data Protection Act 2018 and EU General Data Protection Regulation (Article 5) whereby organisations should not retain personal data for longer than required. To comply with the requirements of the storage limitation principle, organisations should define organisation-wide retention periods and subsequently operationalise across systems. Personal data is currently stored across multiple systems, and HCPC has developed a Record Retention and Disposal Policy which defines record types and retention periods which is published via the HCPC website. Whilst we recognise that the HCPC has applied retention periods to some systems such as Outlook (where all the data is archived automatically after 2 years) and PeopleXD (HR system with in-built data deletion which is aligned to defined retention periods). However, a number of systems are reliant on data being manually deleted, such Optimizely, SharePoint, Kallidus 360 etc.	Design & Effectiveness
Implication	**Significance**
▶ If there is an overreliance reliance on manual deletion of personal data from systems (when it reaches the end of the retention period), there is an increased risk that personal data will be retained in excess of defined retention periods, and for longer than required, increasing the organisation's exposure in the event of a data breach e.g. an external cyber-attack.	Low

Recommendations	Action owner	Management Response	Completion Date
11. HCPC should implement defined data retention periods and automated deletion process (where possible) across organisation-wide systems to ensure personal data is not retained for longer than required.	*Roy Dunn CISRO on behalf of system owners*	*Partial accept - a review of retention requirements is due in FY 2025/2026.* *A technology road map has been defined for most business areas and the requirement will be added to backlogs where required, but this does not guarantee implementation.*	*31 March 2026*

Observations

Observation 1 - Data Breach log
HCPC maintains a data breach log where all data breaches reported internally are recorded by the Data Protection Officer or Information Governance Team members. HCPC should consider incorporating the following fields in the log which would enhance overall oversight of the number and nature of data breaches reported: 1. The number of individuals affected 2. Whether special category data is compromised 3. Whether the breach was deemed to be reportable to the ICO 4. Whether the 72-hour time limit for reporting a breach to the ICO was adhered to.
Observation 2 - Data protection compliance plan
HCPC should consider defining and implementing an annual data protection compliance plan which formalises periods for reviewing and updating key compliance documents, such as the RoPA, privacy notices, policies procedures and on-going employee awareness initiatives.
Observation 3 - Data subject rights requests
We noted that the Frink system does not distinguish between data subject rights requests and Freedom of Information (FOI) requests which have different deadlines for completion. However, we understand that the Information Governance Manager manually distinguish the data subject rights requests and FOI. Therefore, HCPC should explore whether there is capability within the existing (Frink) system or new system to: 1. Record the date when identity of the data subject was confirmed as a start date of processing data subject rights requests. 2. Distinguish between data subject rights requests and Freedom of Information (FOI) requests. This will help automate the process and reduce the need for manual workarounds and the maintenance of separate Excel spreadsheets for managing deadlines.
Observation 4 - Data Breach Procedure
HCPC has developed Information Security Policy which sets the standards and guidelines for ensuring the confidentiality, integrity, and availability of information with some references to data breaches. The Information Security Policy provides the overarching guidelines for protecting information, while a Data Breach Procedure is a targeted response plan for managing data breaches. Therefore, HCPC should consider separating the Data Breach Procedure from the Information Security Policy which to specifically define the step-by-step process to be followed in the event of a data breach. This will complement the Information Security Policy by providing clear, actionable steps to handle data breaches effectively.

Appendices

Appendix I: Definitions

Level of assurance	Design of internal control framework		Operational effectiveness of controls	
	Findings from review	Design opinion	Findings from review	Effectiveness opinion
Substantial	Appropriate procedures and controls in place to mitigate the key risks.	There is a sound system of internal control designed to achieve system objectives.	No, or only minor, exceptions found in testing of the procedures and controls.	The controls that are in place are being consistently applied.
Moderate	In the main there are appropriate procedures and controls in place to mitigate the key risks reviewed albeit with some that are not fully effective.	Generally, a sound system of internal control designed to achieve system objectives with some exceptions.	A small number of exceptions found in testing of the procedures and controls.	Evidence of non-compliance with some controls, that may put some of the system objectives at risk.
Limited	A number of significant gaps identified in the procedures and controls in key areas. Where practical, efforts should be made to address in-year.	System of internal controls is weakened with system objectives at risk of not being achieved.	A number of reoccurring exceptions found in testing of the procedures and controls. Where practical, efforts should be made to address in-year.	Non-compliance with key procedures and controls places the system objectives at risk.
No	For all risk areas there are significant gaps in the procedures and controls. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Poor system of internal control.	Due to absence of effective controls and procedures, no reliance can be placed on their operation. Failure to address in-year affects the quality of the organisation's overall internal control framework.	Non-compliance and/or compliance with inadequate controls.

Recommendation significance	
High	A weakness where there is substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such risk could lead to an adverse impact on the business. Remedial action must be taken urgently.
Medium	A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.
Low	Areas that individually have no significant impact, but where management would benefit from improved controls and/or have the opportunity to achieve greater effectiveness and/or efficiency.

Appendix II: Terms of reference

Background

As part of the 2024/2025 internal audit plan for the Health and Care Professions Council (HCPC), and agreed by the Audit and Risk Assurance Committee (ARAC) we will perform an audit over the design and operational effectiveness of the controls in place to comply with the Data Protection Act 2018 (UK GDPR) in relation the processing of personal data.

Following the UK's departure from the European Union, UK-based organisations are subject to UK GDPR (Data Protection Act 2018) for any data processing in the UK, however, HCPC should also be aware of the need to apply the EU GDPR for any processing of EU based data subjects. For UK organisations, the changes are minimal, the UK GDPR almost mirrors the EU GDPR in full. The risks associated with non-compliance with UK and EU GDPR are significant, amounting to a maximum of £17.5 million (€20 million) or 4% of global turnover (whichever is greater), although the associated reputational damage will be the most likely adverse impact for HCPC.

HCPC regulates 15 health and care professions, and is therefore exposed to the processing of personal data as part of;

- Core Business – administering registrations for designated titles which are protected by law, investigating concerns, administering fitness to practice (FTP) hearings, administering Continuing Professional Development (CPD) records and running events and consultations.
- Day to day operations - regarding current/former employees and recruitment applicants.

By virtue of its role as the regulator of Healthcare professionals, HCPC can rely on exemptions outlined in Schedules 2-4 of the UK GDPR, specifically in relation to

- the right to be informed,
- all other individual rights (except rights related to automated individual decision-making including profiling), and
- all the principles, but only so far as they relate to the right to be informed and other individual rights

Data Protection Compliance at HCPC is led by the Chief Information, Security & Risk Officer (and DPO), with support from the Information Governance Manager for day to day compliance activities. HCPC typically receives a high number of Subject Access Requests, which are usually linked to Fitness to Practise (FTP) hearings.

The Information Commissioner's Office (ICO) is a very active regulator, particularly in the healthcare sector, given the volume and sensitivity of personal data processed, but we have also seen an increase in enforcement action issued to public bodies.

Scope

The review considered the scope areas outlined on pages 3 and 4, which also details our approach to the testing.

Fieldwork conducted remotely through review of key compliance procedures and documents, and discussions and walkthroughs with management, to understand the control environment

Internal Audit brought to the attention of management any points relating to other areas that come to their attention during the audit. A closing meeting was held to discuss findings emerging from the review prior to issue of the draft report. Once the report and recommendations have been agreed following discussions with management, a summary of the findings will be presented to the ARAC at its next meeting.

Purpose

The purpose of the review was to assess how HCPC assures itself that it is compliant with the UK GDPR, and confirm that any exemptions are properly applied with appropriate oversight. We also assessed whether the data protection control environment has been adequately designed to mitigate inherent risks and whether these controls are operating effectively.

Appendix II: Terms of reference

The table below, which outlines the areas which will be covered as part of this review, the key inherent risks associated with the areas under review and our approach to test the design and operational effectiveness (where applicable) of the controls in place to mitigate the risks outlined:

Scope Area	Key Risks	Approach
Awareness	• Employees are not aware of key data protection compliance requirements.	We checked employee awareness of corresponding data protection regulations, in particular, we confirmed that: • Data protection awareness training is mandatory for all employees throughout the employee lifecycle and incorporates an assessment to measure its effectiveness and that the results of any assessment and tracked and recorded. • Training materials address, at the very least, key data protection topics. • Employees have access to a regularly reviewed data protection policy. • Materials provided take account of the specific requirements and circumstances as healthcare professions regulator and areas such as handling data relating to non-UK nationals.
Information you hold	• HCPC cannot evidence complete oversight of organisation-wide data processing activity.	We verified whether HCPC can demonstrate oversight of personal data processed, by confirming that: • HCPC maintains a Record of Processing Activity (ROPA) which documents organisation-wide data processing activities. We will discuss ROPA completeness with HCPC management and verify that it is up to date, sufficiently detailed, regularly reviewed and incorporates the minimum information required. • The documented content is of sufficient quality for HCPC to demonstrate oversight of data processing activity. • HCPC has implemented defined data retention procedures across systems which store personal data. *Please note that this review not included a substantive assessment of whether the retention periods documented are reasonable*
Data Processors	• HCPC cannot evidence oversight of third-party data processors with whom personal data is shared.	We confirmed whether HCPC can demonstrate oversight of data processor relationships, by reviewing whether this is documented in the ROPA. *Please not that this review not included a substantive review of data processor agreements or contractual clauses contained therein.*
Joint Controllers	• HCPC cannot evidence oversight of third-party Joint Controllers with whom personal data is shared.	We confirmed whether HCPC can demonstrate oversight of joint controller relationships, by reviewing whether this is documented in the ROPA. *Please note that this audit not included a substantive review of joint controller arrangements, including of any contracts in place.*

Appendix II: Terms of reference

The table below, which outlines the areas which will be covered as part of this review, the key inherent risks associated with the areas under review and our approach to test the design and operational effectiveness (where applicable) of the controls in place to mitigate the risks outlined:

Scope Area	Key Risks	Approach
International data transfers	• HCPC transfers personal data outside of the UK or EU/EEA without appropriate safeguards in place, and/or without notifying data subjects, in-keeping with the transparency principle.	We verified whether the ROPA defines the country location of third parties, (specifically those located outside the UK or EU/EEA) to determine whether appropriate transfer mechanism/safeguard have been documented. *Please not that the review not included a substantive review of the international data transfer contractual clauses, or of the safeguards relied on in each case.*
Lawful basis for processing	• HCPC does not cite an appropriate lawful basis for processing, which has an impact on the ability to comply with additional compliance requirements, when relying on consent or legitimate interest, as the lawful basis for processing.	We confirmed whether the ROPA cites a lawful basis for data processing activities (including additional bases for the processing of special category data). *Please note that this review not included a substantive review of whether the lawful basis cited is appropriate.*
Transparency	• HCPC does not accurately communicate data processing activity to individuals via the privacy notices, in-keeping with the transparency principle.	We reviewed published privacy notices and determine whether they include the relevant sections, are easily accessible and are regularly reviewed/updated. *Please note that this review not include a substantive review of whether the detail published within each privacy notice is deemed to be fit for purpose in direct relation to HCPC data processing activities.*
Individual rights	• Data subject rights requests are not managed within prescribed timescales, leading to individual complaints to HCPC and/or directly to the supervisory authority.	To demonstrate that HCPC complies with data subjects' rights, we determined whether HCPC has implemented data subject rights procedures and maintains a record of data subject rights requests received. *Please note that this review not included a substantive review or sample testing of whether the data subject rights requests received have been managed appropriately*
Data breaches	• Data breaches are not reported to the Information Commissioner's Office (ICO) and/or affected data subjects within prescribed timescales, prompting financial penalties, reputational damage and increased regulatory focus.	With a view to confirming that HCPC can demonstrate complete oversight of data breaches, we determined whether HCPC has implemented data breach procedures, and a record of data breaches is maintained. *Please note that this review not included a substantive review of whether data breaches have been appropriately dealt with or reported.*
Data Protection Impact Assessments (DPIA)	• HCPC cannot demonstrate compliance with the 'Data Protection by Design and Default' principle, by evidencing that consideration of data protection risk has been incorporated into business as usual.	We determined whether HCPC has implemented DPIA procedures to embed data protection by design and default. *Please note that this review not included a substantive review of DPIA processes or whether DPIAs have been appropriately completed.*
Governance & Accountability	• HCPC cannot demonstrate on-going compliance with regulatory compliance.	We confirmed that responsibilities for data protection compliance are formally allocated within HCPC. Taking account of the findings above, we determined whether HCPC can demonstrate continued compliance with applicable data protection regulatory requirements.

Appendix III: Staff Interviewed

BDO LLP appreciates the time provided by all the individuals involved in this review and would like to thank them for their assistance and cooperation.	
Roy Dunn	Chief Information Security & Risk Officer and Data Protection Officer
Maxine Noel	Information Governance Manager
Nicole Jones	Improvement & Compliance Specialist
Jamie Hunt	Head of Education
Rick Welsby	IT Support Manager
Jagana Abubacarr	System Accountant
Aihab Al Koubaisi	Financial Controller
Jessica Daly	Partner Officer
Uta Pollmann	Partner Project Lead
Karen Flaherty	Head of Governance
Madalina Botezatu	Payroll Manager
Tarek Hussien	Procurement Manager
Paul Cooper	Head of Business Change
Kayleigh Birtwistle	Programme Manager
Paul Douglas	Interim Head of Case Progression and Quality
Claire Baker	Head of Adjudication Performance
Mark Robinson	Registration Manager
Adam Mawson	Registration Manager
Matthew Peck	Head of Communications, Engagement and Public Affairs
Fatma Ali	Head of HR

Appendix IV: Limitations and Responsibilities

Management Responsibilities

The Board is responsible for determining the scope of internal audit work, and for deciding the action to be taken on the outcome of our findings from our work.

The Board is responsible for ensuring the internal audit function has:

- The support of the Company's management team.
- Direct access and freedom to report to senior management, including the Chair of the Audit Committee.
- The Board is responsible for the establishment and proper operation of a system of internal control, including proper accounting records and other management information suitable for running the Company.

Internal controls covers the whole system of controls, financial and otherwise, established by the Board in order to carry on the business of the Company in an orderly and efficient manner, ensure adherence to management policies, safeguard the assets and secure as far as possible the completeness and accuracy of the records. The individual components of an internal control system are known as 'controls' or 'internal controls'.

The Board is responsible for risk management in the organisation, and for deciding the action to be taken on the outcome of any findings from our work. The identification of risks and the strategies put in place to deal with identified risks remain the sole responsibility of the Board.

Limitations

The scope of the review is limited to the areas documented under Appendix II - Terms of reference. All other areas are considered outside of the scope of this review.

Our work is inherently limited by the honest representation of those interviewed as part of colleagues interviewed as part of the review. Our work and conclusion is subject to sampling risk, which means that our work may not be representative of the full population.

Internal control systems, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making, human error, control processes being deliberately circumvented by employees and others, management overriding controls and the occurrence of unforeseeable circumstances.

Our assessment of controls is for the period specified only. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that: the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or the degree of compliance with policies and procedures may deteriorate.

FOR MORE INFORMATION:

Sarah Hillary, PARTNER

Sarah.Hillary@bdo.co.uk

Bill Mitchell, DIRECTOR

Bill.Mitchell@bdo.co.uk

www.bdo.co.uk

0459956