



---

**Parliamentary & Health Service Ombudsman**  
**Data Protection Audit Report**  
**Executive Summary**

**20 October 2010**

---

---

## **1. Background**

In May 2010, 80 documents belonging to the Parliamentary and Health Service Ombudsman (PHSO), including approximately 30 containing sensitive personal data, were misplaced, while being taken off-site. The PHSO reported this data security breach to the Information Commissioner's Office (ICO). The documents were subsequently recovered.

The ICO considered the circumstances surrounding the reported incident, including PHSO's willingness to take action to ensure that a similar breach cannot recur, and its invitation to ICO to carry out a review of its processes in this area. In view of this the ICO decided that formal regulatory action was not appropriate. Instead, the ICO agreed with the PHSO that they should complete an assessment of the relevant PHSO policies and procedures to determine their efficacy in meeting the requirements of the Data Protection Act 1998 (DPA), and their performance in practice.

Although PHSO has an electronic case tracking system which can store emails and scanned documents, the majority of personal data processed is in paper format. Operational requirements result in large volumes of data transfers to and from organisations being investigated, to third party experts providing professional opinions, and between PHSO offices.

It was agreed between ICO and PHSO to undertake the assessment at both of their sites, in London and Manchester.

---

## 2. Audit Scope

Following pre audit discussions with PHSO it was agreed that the review would focus on specific processes and activities to assess how their implementation contributes to compliance with the DPA principles within the following areas:

- a. Data Protection Governance – with reference to the arrangements and controls in place to ensure compliance with the DPA specifically in relation to personal data taken or sent off-site.
- b. The provision and monitoring of staff training and awareness of data protection requirements, relating to their roles and responsibilities, particularly in relation to personal data taken or sent off-site from PHSO offices.
- c. The processes in place to ensure adequate physical security is applied to the transfer of manual files
  - Between PHSO office sites by a third party contractor (manual only)
  - By PHSO employees working away from their office base
  - To and from Associates and External Reviewers working from their own base
- d. The processes in place to ensure adequate security is applied to the IT systems and mobile devices used for the electronic transfer of personal data as described in paragraph 'c' above.

---

### 3. Audit Opinion

The purpose and objective of the audit was to provide PHSO and the Information Commissioner with an assessment and assurance opinion on how PHSO is meeting its data protection obligations in respect of the security of personal data (held both manually and electronically) taken or sent off-site:

- by PHSO employees for the purpose of working on them away from PHSO's offices
- for work by Associate Caseworkers, Clinicians and Reviewers normally working from home
- while in transit by third party contractors between PHSO's sites

The recommendations made are primarily around enhancing processes and procedures relating to data governance and security.

<b>Overall Conclusion</b>	
<b>Reasonable Assurance</b>	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to enhance the likelihood that the objective of data protection compliance will be achieved.

---

## **4. Summary of Audit Findings**

### Areas of Good Practice.

PHSO employees generally have a good understanding of DPA principles, how to access associated policies and guidance and how these should be applied to work practices.

IT systems are designed to operate at Government standard CESG security levels and external IT auditors are employed to ensure compliance with these.

New secure terminals and access methods are being introduced for use by home and remote access workers offering high security access to PHSO applications and online case files.

Comprehensive procedures are in place to track paper files making use of both the case handling IT application and tracking systems from the main courier company.

### Areas for Improvement.

PHSO does not have a data protection policy or statement that underpins the standards required to comply with data protection law. Responsibility for applying and maintaining this policy is needed and measures introduced to ensure compliance is achieved. A forum for raising data protection issues for resolution can also facilitate the achievement of compliance. A Security Committee already exists to consider data security issues.

The transfer of personal data by PHSO staff between office and home or contractors' premises is a high risk area and consideration should be given to reviewing and updating procedures covering home working and associated data transfers.

Procedures are required to ensure all contractors are fully aware of the latest PHSO Security Policies and other policies related to personal data processing in order to comply with their own contractual as well as DPA obligations.

---

**Parliamentary and Health Service Ombudsman**  
**Data Protection Audit Report**  
**Final**

---

**Auditors:** Alvin West      Team Manager - Audit  
David Simmons      Lead Auditor

**Distribution:**

Draft Report: Marie Cheek, Director of Service Delivery; Richard Selkirk, Facilities & Security Manager

Final Report: Bill Richardson, Deputy Chief Executive; Marie Cheek, Director of Service Delivery

**Report Issued:** 20th October 2010

# Contents

1. Background	page 2
2. Audit Opinion	page 3
3. Summary of Audit Findings	page 4
4. Audit Approach	page 6
5. Scope of the Audit	page 7
6. Audit Grading	page 8
7. Detailed Findings & Action Plan	page 9

---

## **1. Background**

- 1.1 In May 2010, 80 documents belonging to the Parliamentary and Health Service Ombudsman (PHSO), including approximately 30 containing sensitive personal data, were misplaced, while being taken off-site. The PHSO reported this data security breach to the Information Commissioner's Office (ICO). The documents were subsequently recovered.
- 1.2 The ICO considered the circumstances surrounding the reported incident, including PHSO's willingness to take action to ensure that a similar breach cannot recur, and its invitation to ICO to carry out a review of its processes in this area. In view of this the ICO decided that formal regulatory action was not appropriate. Instead, the ICO agreed with the PHSO that they should complete an assessment of the relevant PHSO policies and procedures to determine their efficacy in meeting the requirements of the Data Protection Act 1998 (DPA), and their performance in practice.
- 1.3 Although PHSO has an electronic case tracking system which can store emails and scanned documents, the majority of personal data processed is in paper format. Operational requirements result in large volumes of data transfers to and from organisations being investigated, to third party experts providing professional opinions, and between PHSO offices.
- 1.4 It was agreed between ICO and PHSO to undertake the assessment at both of their sites, in London and Manchester.

---

## 2. Audit Opinion

- 2.1 The purpose and objective of the audit was to provide PHSO and the Information Commissioner with an assessment and assurance opinion on how PHSO is meeting its data protection obligations in respect of the security of personal data (held both manually and electronically) taken or sent off-site:
- by PHSO employees for the purpose of working on them away from PHSO's offices
  - for work by Associate Caseworkers, Clinicians and Reviewers normally working from home
  - while in transit by third party contractors between PHSO's sites
- 2.3 The recommendations made are primarily around enhancing processes and procedures relating to data governance and security.

Overall Conclusion
Reasonable Assurance

The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to enhance the likelihood that the objective of data protection compliance will be achieved.

---

## **3. Summary of Audit Findings**

### **3.1 Areas of Good Practice.**

- 3.1.1 PHSO employees generally have a good understanding of DPA principles, how to access associated policies and guidance and how these should be applied to work practices.
- 3.1.2 IT systems are designed to operate at Government standard CESG security levels and external IT auditors are employed to ensure compliance with these.
- 3.1.3 New secure terminals and access methods are being introduced for use by home and remote access workers offering high security access to PHSO applications and online case files.
- 3.1.4 Comprehensive procedures are in place to track paper files making use of both the case handling IT application and tracking systems from the main courier company.

### **3.2 Areas for Improvement.**

- 3.2.1 PHSO does not have a data protection policy or statement that underpins the standards required to comply with data protection law. Responsibility for applying and maintaining this policy or statement is needed and measures introduced to ensure compliance is achieved. A forum for raising data protection issues for resolution can also facilitate the achievement of compliance. A Security Committee already exists to consider data security issues.
- 3.2.2 The transfer of personal data by PHSO staff between office and home or contractors' premises is a high risk area and consideration should be given to review and updating procedures covering home working and associated data transfers.
- 3.2.3 Procedures are required to ensure all contractors are fully aware of the latest PHSO Security Policies and other policies related to personal data processing in order to comply with their own contractual as well as DPA obligations.

---

## **4. Audit Approach**

- 4.1 In consideration of the circumstances leading to the audit it was agreed that the assessment would concentrate on processes related to general DPA awareness, security systems relevant to personal data transfers and data handling outside the PHSO offices. The audit concentrated on the processes associated with these transfers but further observations were made regarding general data security as well as others pertinent to DPA principles.
- 4.2 The audit was conducted following the Information Commissioner's Data Protection Audit Methodology and comprised a review of documents and evidence provided by PHSO and on-site visits and interviews with PHSO employees.
- 4.3 Interviews took place with staff at PHSO offices in Millbank Tower, London on 14<sup>th</sup> and 15<sup>th</sup> July and at The Exchange, Manchester on 22<sup>nd</sup> July 2010.

---

## 5. Audit Scope

- 5.1 Following pre audit discussions with PHSO it was agreed that the review would focus on specific processes and activities to assess how their implementation contributes to compliance with the DPA principles within the following areas:
- a. Data Protection Governance – with reference to the arrangements and controls in place to ensure compliance with the DPA specifically in relation to personal data taken or sent off-site.
  - b. The provision and monitoring of staff training and awareness of data protection requirements, relating to their roles and responsibilities, particularly in relation to personal data taken or sent off-site from PHSO offices.
  - c. The processes in place to ensure adequate physical security is applied to the transfer of manual files
    - Between PHSO office sites by a third party contractor (manual only)
    - By PHSO employees working away from their office base
    - To and from Associates and External Reviewers working from their own base
  - d. The processes in place to ensure adequate security is applied to the IT systems and mobile devices used for the electronic transfer of personal data as described in paragraph 'c' above.

## 6. Audit Report Grading

6.1 Audit reports are graded with an overall assurance opinion, and any issues and associated recommendations are classified individually to denote their relative importance, in accordance with the definitions in the table below.

<b>Colour Code</b>	<b>Internal Audit Opinion</b>	<b>Recommendation Priority</b>	<b>Definitions</b>
	Good assurance	Minor points only are likely to be raised	The arrangements for data protection compliance with regard to governance and controls provide a good level of assurance that processes and procedures are in place and being adhered to and that the objective of data protection compliance will be achieved. No significant improvements are required.
	Reasonable assurance	Low priority	The arrangements for data protection compliance with regard to governance and controls provide a reasonable assurance that processes and procedures are in place and being adhered to. The audit has identified some scope for improvement in existing arrangements and appropriate action has been agreed to enhance the likelihood that the objective of data protection compliance will be achieved.
	Limited assurance	Medium priority	The arrangements for data protection compliance with regard to governance and controls provide only limited assurance that processes and procedures are in place and are being adhered to. The achievement of the objective of data protection compliance is therefore threatened. Actions to improve the adequacy and effectiveness of data protection governance and control have been agreed and timetabled.
	Very limited assurance	High priority	The arrangements for data protection compliance with regard to governance and controls provide very limited assurance that processes and procedures are in place and being adhered to. There is therefore a substantial risk that the objective of data protection compliance will not be achieved. Immediate action is required to improve the control environment.

## 7. Detailed Findings & Action Plan

Findings and recommendations from the audit will be risk categorised using the criteria defined in Section 6. The rating will take into account the impact of the risk and the probability that the risk will occur.

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.1	Data protection governance, – with reference to the arrangements and controls in place to ensure compliance with the DPA specifically in relation to personal data taken or sent off-site.			
a	A failure to identify and implement adequate arrangements and controls to ensure compliance with data protection requirements which are measured and reported on, raises the risk of PHSO being unaware of whether it is meeting its obligations,	<ul style="list-style-type: none"> <li>There is no overarching data protection policy or statement for PHSO that describes its position regarding processing complainants' personal data. There is a data protection policy in place for PHSO employee information.</li> <li>There is a Data Protection and Freedom of Information Team, whose role is to process requests for personal data under the DPA and requests for information under the FOI Act.</li> </ul>	A1 In order that staff and the general public understand PHSO's position consider the publication of a statement of PHSO's commitment to complying with the principles of the Data Protection Act 1998 to protect all personal data it holds and how that will be achieved.	<u>Recommendation Accepted</u> This will be included in our 'Information Promise' project and will be implemented in 2011/2012.  Claire Forbes, Director of Communications, is responsible for this project.

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
	<p>resulting in poor data protection practice or potential breaches of the Act not being identified or addressed and reputational damage to PHSO.</p>	<ul style="list-style-type: none"> <li>The Head of this team has involvement with policies relating to subject access requests and has recently been involved with agreeing a Memorandum of Understanding with the ICO regarding information requests from complainants.</li> <li>The Head is also consulted when new policies, guidance and public documents are being considered, although there was no indication that further polices concerning data protection were produced by this team. The job description of the Head of the team did not reflect this responsibility.</li> <li>Although PHSO is a major processor of personal data there did not appear to be a dedicated forum to discuss data protection issues except for data security issues which are discussed at the Security Committee.</li> <li>Policies and guidance are in place for IT Security, ICT Acceptable Use, Security and PHSO Employee Data Protection.</li> </ul>	<p>A2 It has been shown to be good practice for responsibility for ensuring there are data protection policies and statements in place and up to date to be vested in one position. The Head of DP and FOI would appear to be best placed to do this.</p>	<p><u>Recommendation Accepted</u></p> <p>We agree that this should be the responsibility of one person. We will consider who this is in tandem with our work on the 'Information Promises' project and the setting up of a centralised information and records management function. This may or may not be the current Head of FOI/DP whose role and responsibility will be revised.</p> <p>We will decide who will have the responsibility and implement the recommendation during 2011/2012. The Executive Board will be responsible for this decision.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<ul style="list-style-type: none"> <li>• Security Bulletin updates are distributed by email to all staff and contractors with a PHSO email account covering areas such as out of office working security requirements.</li> <li>• The Security Bulletins are used in team briefings to ensure staff are made aware of any new threats or procedures.</li> <li>• There does not appear to be a consistent version control system applied to the policies that ensures staff are aware of the latest data protection guidance.</li> <li>• PHSO contracts with various experts, such as Associate Clinical Advisers, External Professional Advisers and agency staff, on short and longer term contracts. At the time of the audit, only those with PHSO email accounts, such as agency staff have access to the latest data security guidance. Those without an email account receive some aspects of the security guidance when offered work, but they do not receive all of it.</li> </ul>	<p>A3 A formal approach to documentation control should be considered for policies including formal version controls</p>	<p><u>Recommendation Accepted</u>  We will ensure clearer version control, is added to our policies.  This will be implemented as follows: all future policies will be launched with appropriate version control and existing policies will be launched in this way when they are due for renewal.  Steve Brown, Head of Governance is responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<ul style="list-style-type: none"> <li>Contracts themselves did not include any comments regarding their obligations as data processors under the DPA although there are comments about the security of documents.</li> <li>Case files, which include sensitive personal data, are sent to the office or home address of contractors for assessments. The contracts for this work do not make specific reference to DPA requirements but do specify that the contractor must comply with PHSO security policy and guidance. However these standards and policies, including Employee Data Protection, are not included as part of the information packs sent to the contractors.</li> <li>PHSO has a Retention &amp; Disposal Policy for all paper and electronic documents. Disposal timescales are in place for all casework and clinical advice documents and are being developed for other corporate records. However, when asked, some staff were unaware of this policy.</li> </ul>	<p>A4 As the data controller PHSO should ensure that all contractors are aware of and comply with all DPA requirements and are given access to all relevant security, Employee Data Protection and other policies they are contractually required to comply with.</p>	<p><u>Recommendation Accepted</u>  We will put in place a process for ensuring that all contractors are issued with all relevant policies and guidance.  This will be implemented by 31 March 2011.  Ros Green, Head of HR Ops will be responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<ul style="list-style-type: none"> <li>• Policies are available from the PHSO Intranet and all staff and contractors with an email account are aware of how to access them.</li> <li>• IT audits have been carried out by KPMG with the last audit received in March 2009. This report identified one medium and one low IT risk area as well as one medium risk relating to the lack of a central registry for the control of paper files.</li> </ul>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.2	The provision and monitoring of staff training and awareness of data protection requirements, relating to their roles and responsibilities, particularly in relation to personal data taken or sent off-site from PHSO offices.			
b	<p>A failure to provide and implement staff training and awareness regarding the security of personal data in the circumstances described in paragraph 2, raises the risk of loss or inappropriate use of data, with the potential to cause damage and distress to individuals, and reputational damage to PHSO.</p>	<ul style="list-style-type: none"> <li>PHSO provides induction training for all staff and this includes security requirements. This is backed up by job specific desk training. Other data protection principles however do not appear to be included in the induction training programme although they are included as part of the caseworker training.</li> <li>There was no clear indication from some staff, when questioned, that they could remember having had any dedicated data protection training, or did not recognise it as such if they did have.</li> <li>Operational staff receive specific data security training from the PHSO FoI team.</li> <li>Specific security issues are highlighted by use of Security Bulletins sent to all staff. Some line managers use these as a basis for refresher training but this is not a</li> </ul>	<p>B1 To ensure all staff are aware of all aspects of the Data Protection Act 1998 include more in the induction training package indicating how the principles affect the work carried out within PHSO.</p> <p>B2 A monitoring system would go some way to ensuring Security Bulletins are effectively disseminated and</p>	<p><u>Recommendation Accepted</u> We will review our induction programme to ensure they contain details of our Data Protection Principles and their impact on the work of PHSO. This will be implemented by 31 March 2011. Jon Ward, Director of People &amp; Organisational Development is responsible for this.</p> <p><u>Recommendation Accepted</u> We will put in place a process to ensure that information contained in Security Bulletins is</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>uniform practice.</p> <ul style="list-style-type: none"> <li>There is no formal procedure in place to distribute Security Bulletins to Associate Clinical Advisers and External Professional Advisers on short term contracts who handle case files containing sensitive personal data.</li> </ul>	<p>understood by all affected staff.</p> <p>B3 Introduce a means of ensuring that all contractors have access to Security Bulletins.</p>	<p>disseminated to and understood by staff and contractors. This will be discussed and agreed with the Security Committee before implementation. This will be completed by 31 December 2010.</p> <p>Richard Selkirk, Facilities, Security &amp; Business Continuity Manager is responsible for this.</p> <p><u>Recommendation Accepted</u></p> <p>We will put in place a process for ensuring that all contract staff have access to Security Bulletins. This will be done in conjunction with the work for Recommendation A4.</p> <p>This will be completed by 31 December 2010</p> <p>Richard Selkirk, Facilities, Security &amp; Business Continuity Manager is responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.3	<p>The processes in place to ensure adequate physical security is applied to personal data taken or sent off-site in manual files both in terms of transit and when such data is used outside of PHSO offices by employees or at home by contractors.</p>	<p>Since the reported data loss PHSO have reinforced the system to control files taken home by staff. Line managers provide authority for this by email and files must then be booked out and back in using a log book for each case team.</p> <ul style="list-style-type: none"> <li>PHSO has provided staff with security guidance (Security Bulletin March 2009) requiring them to "Only take PHSO documentation off site if absolutely essential for business reasons e.g. take key documents on a file rather than the whole file." It was indicated that this guidance is not always complied with due either to lack of awareness or time constraints.</li> <li>PHSO's Visualfiles case management software is used to track paper file movements.</li> <li>Visualfiles tracking relies on</li> </ul>	<p>C1 To minimise the risk of the loss of excessive personal data introduce checks to ensure compliance with the security guidance prior to files being taken home by staff.</p>	<p><u>Recommendation Accepted</u> The checks will form part of the programme of audit and compliance to be undertaken by our new central information and records management function. This will be implemented in 2011/12. Iain Ogilvie, Head of Archive Project Team is responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>individual staff updates but it was indicated that this procedure is not always complied with leading to files being misplaced occasionally. The process in these circumstances is to deploy a localised office search with individual line managers then being required to search all possible missing file locations for their own teams and reporting back to the Security Officer. At the time of the audit it was advised that this had always proved effective.</p> <ul style="list-style-type: none"> <li>• PHSO case files are transported, using a tracked courier service: <ul style="list-style-type: none"> <li>- to and from PHSO offices and an archive site</li> <li>- to and from homes of Homeworkers</li> <li>- to and from homes or offices of contractors.</li> </ul> </li> <li>• Different contracts are in place for the different assessment services but common tracking systems are in place using both Visualfiles entries and TNT consignment notes. The transfer and receipt of files is confirmed by email.</li> </ul>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<ul style="list-style-type: none"> <li>• Top sheets of files are photocopied and scanned into the PHSO server to provide evidence of files dispatched by the PHSO mail rooms.</li> <li>• Files are transported using secure standard TNT cardboard boxes for large transfers between offices or to the TNT Archive site in Derbyshire or else using TNT A3 size plastic courier pouches.</li> <li>• PHSO staff applying to work from home must comply with a process that includes a Health and Safety assessment of their premises. Physical security issues are referenced but there is no formal assessment system to confirm compliance with PHSO Physical Security requirements if paper files are to be processed at the home location.</li> <li>• Case files are sent by courier to staff working from home using TNT's tracking service. The same service is provided for contractors</li> </ul>	<p>C2 An assessment of staff premises, possibly a self-assessment, would be beneficial to confirm compliance with PHSO physical security requirements prior to agreement to home working with paper files containing personal data. Such compliance would not be required if home working is to be restricted to IT based working only, using the new remote working</p>	<p><u>Recommendation Accepted</u>  We are about to launch a new Flexible Working Policy. This is supported by new Health &amp; Safety &amp; Security requirements and an Assessment for home workers that cover the issues identified.  This will be implemented in line with the launch of the Flexible Working Policy during 2010/2011.  Richard Selkirk, Facilities, Security &amp; Business Continuity Manager is responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>working in their own offices or at home. This service provides tracking of the pouches used and is backed up by Visualfiles entries.</p> <ul style="list-style-type: none"> <li>The TNT courier service only guarantees delivery by 12:00 noon next day. Alternatively, to ensure that work files are available to staff the following morning, it was indicated that they might take files home with them the previous day.</li> <li>Policy is for staff to take files home in PHSO issued rucksacks or lockable briefcases Anecdotal evidence suggested that staff were not always able to obtain these cases and consequently personal data could be transported using unapproved bags.</li> </ul>	<p>terminals and secure network access.</p> <p>C3 To minimise the risk of data loss of files when using public transport, alternative and more secure arrangements should be considered including the scanning of files that would otherwise be taken home to work on. The new home working IT infrastructure could then be used to view the documents.</p>	<p><u>Recommendation Accepted</u></p> <p>We have already implemented a new Remote Working IT solution for home workers during 2010/2011.</p> <p>We are conducting a retendering for courier service and the new contract will include improved focus on security issues.</p> <p>This will be completed during 2010/2011.</p> <p>Richard Selkirk, Facilities, Security &amp; Business Continuity Manager is</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>Outcomes &amp; Learning</p> <ul style="list-style-type: none"> <li>• Sharepoint is used in this section to record if case files are taken home for casework quality review.</li> <li>• Packs of documents, including copies of papers from case files, are made up for each member of an advisory panel for discussion at the Recommendations panel.</li> <li>• Papers are often taken away by panel members after they have met. These papers are uncontrolled and may contain sensitive personal data.</li> </ul> <p><u>Proofreading</u></p> <ul style="list-style-type: none"> <li>• Files are received in this section and logged onto a paper schedule. Visualfiles is checked to verify it has been tracked to this team.</li> <li>• Files transferred for proofreading are recorded on Visualfiles by the person sending the file, although it was indicated that this process is</li> </ul>		<p>responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>not always followed.</p> <ul style="list-style-type: none"> <li>To ensure no files are held longer than necessary, staff in the team pick up the next file available with the earliest receipt date and they record on the log who is working with that file.</li> <li>No files are taken home to work on but individual reports from the file may be. Post-it notes are stuck to the front of the file to indicate what has been taken out.</li> </ul> <p><u>Health Investigations</u></p> <ul style="list-style-type: none"> <li>This team send files out to health investigators working from home and to Associates via the clinical advice team.</li> <li>In most cases, documents in files sent to Associate Clinical Advisers are copies of PHSO file documents which themselves are copies of the originals. However, in some instances, they are sent the original documents.</li> </ul>	<p>C4 A permanent record of reports taken out of files to be worked on at home would provide a more secure means of tracing documents.</p>	<p><u>Recommendation Accepted</u> As part of the launch of the new Flexible Working Policy and supporting H&amp;S &amp; Security guidance, we will reiterate the correct procedure for taking paper corporate documents out of the office. We will do this in conjunction with the launch of the Flexible Working Policy in 2010/2011 Richard Selkirk, Facilities, Security &amp; Business Continuity Manager, is responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<ul style="list-style-type: none"> <li>• Case files can be held up to 2 months after the case has finished being investigated so that any further correspondence from the complainant can be captured. After that period they are sent to the Post Opening &amp; Archive Team who determine where they will be stored dependant upon the size of the file.</li> <li>• PHSO keeps electronic records of investigations on the Visualfiles system in addition to paper files. There was no indication that checks were carried out to verify information on Visualfiles with actual paper file holdings held in separate storage areas.</li> </ul> <p><u>Parliamentary Investigation</u></p> <ul style="list-style-type: none"> <li>• There are currently no case workers working permanently from home although some occasionally work part time from home.</li> <li>• A log is maintained of papers that are taken out of the office as</li> </ul>	<p>C5 Consideration should be given to introducing a system of checks, between Visualfiles records and physical case files, to verify the accuracy of the records and the existence of files. This will also facilitate the identification of missing files that could contain personal data.</p>	<p><u>Recommendation Accepted in Principle</u></p> <p>We will consider introducing checks to verify the location of files against the Visualfiles record as part of the programme of audit and compliance to be undertaken by our new central information and records management function. This will be implemented in 2011/2012 as part of the new programme.</p> <p>Iain Ogilvie, Head of Archive Project Team is responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		authorised in the log by the manager.		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
7.4	<p>The processes in place to ensure adequate security is applied to the IT systems and mobile devices used for the electronic transfer of personal data as described in 7.3.</p> <p>A failure to implement security measures which adequately protect electronically held personal data taken or sent off-site raises the risk of loss, damage or inappropriate access to data resulting in distress to the affected individuals, non-compliance with the DPA and reputational damage to PHSO.</p>	<ul style="list-style-type: none"> <li>PHSO IT systems are designed to meet UK Government CESG / GSI code of compliance standards and are subject to Information Security Standard 1 (IS1) risk assessment which is the recognised standard for GSI access approval.</li> <li>Staff mainly use standard PCs in the London office and Wyse Thin Client terminals in the Manchester office. Standard builds for these disable USB ports and DVD/CD write facilities in order to prevent unauthorised file copying.</li> <li>IT application access control list systems are in place to restrict access rights for contractors. In response to previous KPMG audit recommendations, contractors now have access to case files related to the contract only rather than blanket access</li> <li>All access control lists for users are reviewed quarterly to</li> </ul>		
d				

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>determine validity.</p> <ul style="list-style-type: none"> <li>• At the time of audit, homeworking arrangements for staff and contractors allow the use of remote web based email (Outlook Web Access OWA) to check emails, as well as local printing using personal IT equipment.</li> <li>• A new standard IT homeworking package was due to be introduced from July 2010 using portable Wyse Thin Client devices only with no local storage or printing capabilities. This new standard will comply with Government CESG standards and eliminate security risks such as use of WiFi networking, use of personal PCs and local printing.</li> <li>• It was indicated that emails, that have not been authorised by the Security Officer have been used, contrary to PHSO security guidance, to send personal data as attachments to facilitate home working. This is a security risk raising the possibility of</li> </ul>		

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>unauthorised access to personal data held on unsecure personal PCs.</p> <ul style="list-style-type: none"> <li>• The homeworking IT package is expected to be made available for use by contractors and nominated staff working for the Local Authority Ombudsman services to provide secure access to email and other authorised applications.</li> <li>• Individual paper files may be scanned and then sent as attachments to caseworkers PHSO email accounts for transfer to Visualfiles case entries. However, there is no large scale bulk scanning capability.</li> <li>• The Security Guidance prohibits sending unencrypted personal data by email to email accounts unless they are on GSI accredited</li> </ul>	<p>D1 Consideration should be given to complete document scanning and the collection and processing of electronic data rather than paper files reduces the risk of loss of personal data.</p>	<p><u>Recommendation Accepted in Principle</u>  We have begun to consider increasing the amount of document scanning and the options for improved electronic working. This would be a major change in working practice and may not be feasible for all aspects of all work.  This will be considered further in 2011/2012.  Discussion of this recommendation will be taken by our Executive Board.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date
		<p>networks. However, there are no controls in place to ensure compliance with this policy for small attachments sent to contractors' email accounts not GSI accredited.</p> <ul style="list-style-type: none"> <li>• Any email sent externally with an attachment larger than 5 MB is automatically logged and added to a report sent to the IT Manager for review. This is to check for any possible unauthorised system use.</li> <li>• Some staff are issued with Blackberry mobile devices. The standard builds for these prevent access to Internet sites and opening of email attachments as these are known security risk areas.</li> <li>• IS1 audits have been carried out by KPMG with the last audit received in March 2009. This report identified one medium and one low IT risk area.</li> </ul>	<p>D2 In the case of sending small attachments via e-mail to contractors, a check is required to ensure only secure email addresses are used or only encrypted personal data attachments are sent to non-secure mailboxes.</p>	<p><u>Recommendation Accepted in Principle</u></p> <p>We are unable to use encryption for emails as this is not permitted by CESG as part of the conditions for GSI connectivity</p> <p>We will investigate the feasibility of checks on email attachments to contractors to ensure they do not include personal data.</p> <p>We will do this by 31 March 2011.</p> <p>Marie Cheek, Director of Service Delivery is responsible for this.</p>

Ref	Compliance Risk	Issues / Findings	Recommended Solution	Management Comments, Responsibility for Action and Due Date

The agreed actions may be subject to a follow up audit to establish whether they have been implemented.

7.6 Any queries regarding this report should be directed to Alvin West, ICO Audit Group.

7.7 During our audit, all the employees that we interviewed were helpful and co-operative. This assisted the audit team in developing an understanding of PHSO, their policies and procedures.