Council, 14 May 2015

Information Governance Report

Introduction

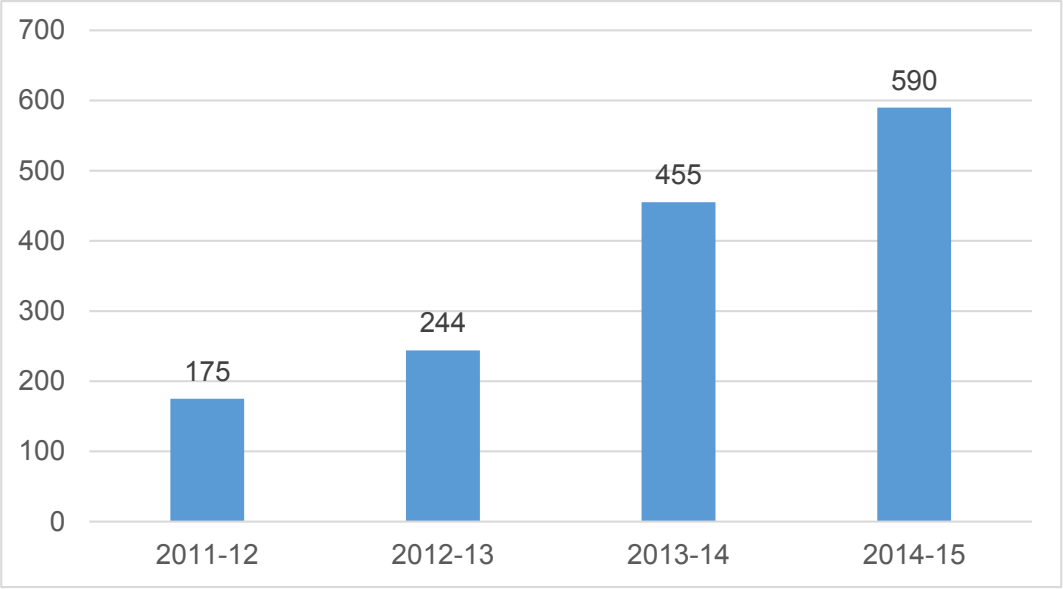
1.1 The Information Governance function within the Secretariat Department is responsible for the HCPC's ongoing compliance with the Freedom of Information Act 2000 (FOIA), the Environmental Information Regulations 2004 (EIR) and the Data Protection Act 1998 (DPA). The Department also manages the HCPC's relationship with the Information Commissioner's Office (ICO), the information rights body.

1.2 FOIA and EIR legislation provide public access to information held by public authorities. Public authorities are obliged to publish certain information about their activities and members of the public are entitled to request information from public authorities. Both acts contain defined exemptions to right of access, which means that there are clear criteria on what information can and cannot be requested.

1.3 DPA governs the protection of personal data in the UK. It also enables individuals to obtain their personal data from a data controller processing their data. This is called a subject access request

Background information

2.1 The number of information requests received by the HCPC has grown considerably following the on boarding of social workers to the HCPC Register in 2012. In 2011, the HCPC received 170 requests and in 2014, 579 requests were received.



2.2 Some of this increase can be attributed to employees being more aware of what an FOIA or DPA request looks like, as the quality of training in this area continues to improve. However, the majority of the increase is attributable to the HCPC regulating social workers in England.

2.3 The typical request for social work related information is complex. The complainants in social work cases are often service users and their families. These complainants often turn to FOIA and DPA to obtain information they have been unable to obtain elsewhere, for example from the local authority directly or from the HCPC fitness to practise department.

2.4 Statistical requests make up around half of all requests and their complexity has also increased. The HCPC also faces increased scrutiny from the ICO as more requestors pursue complaints via this route.

2.5 The HCPC achieves compliance with data access and protection legislation, whilst also sharing information for public protection purposes and transparency and reassuring those providing us with sensitive information that we are able to protect that information. Going too far in either direction can result in either damage to the regulatory function of the HCPC as third parties become unwilling to share information with us, or ICO regulatory action and damage to our reputation in not being seen to be transparent and open.

Information Governance departmental project

3.1 Due to the increasing complexity and volume of demands on the information governance function within the HCPC, a new dedicated resource has been put in place within the Secretariat Department. In 2015-16, a departmental project will be reviewing and improving this area of work.

3.2 Whilst the progress of this project will depend upon 'business as usual demands', it is expected that the review will focus on the following areas :

- Correspondence templates;
- Case law review;
- Publication scheme and website;
- Data collection and retention policies;
- Information incident management;
- Employee Training;
- Privacy Impact Assessments; and
- HCPC wide compliance and Communications Strategy.

3.3 Information requests were around twenty percent higher than average in March and April 2015, however progress has been made on the project. A cross departmental Information Security and Governance Group (ISGG) has been formed from key members of staff to share ideas and arising issues. The

process for reviewing case-specific data has been streamlined. However, the main area of activity so far has been information incident management.

Information Incident Management

4.1 The HCPC encourages an open reporting culture, with an emphasis on analysis and learning in order to engineer-out any weaknesses in our processes, much like the feedback and complaints function. The HCPC is currently undergoing ISO27001 pre-certification audits. As part of the preparation for this, policies around information incident management have been reviewed.

4.2 From January 2015, all incidents, regardless of how minor they may initially appear are now reported centrally and the information security group (which includes key EMT members and the CEO) is notified on the day they are detected. A detailed report is completed for each incident and a severity score is allocated to the incident. Please see appendix one for an example of an information incident report.

4.3 The incident severity scoring procedure is based on the Data Protection Act and the ICO's criteria for reporting incidents. Please see appendix two for this procedure. Severity is measured according to the risk of harm to the data subject and to the HCPC and the scale is aligned with HCPC's Risk Matrix. Five factors are taken into account, these are the risk of harm to the data subject, the number of data subjects involved and the number of people the data has been disclosed to, the nature of the HCPC's relationship with the recipients of the data and the recovery status of the data.

4.4 Sometimes an incident will have special circumstances which will affect the scoring outside of the five factors, for example if a vulnerable service user's data is involved. Incidents are classified as either green, amber or red with differing actions associated with each. Incident scores are presented to the Executive Management Team at their monthly meeting and future mitigations and improvements are discussed, agreed and tracked. Please see appendix three for a copy of the April 2015 report discussed by EMT.

4.5 The new process is a first step and, as its use becomes established, improvements will inevitably be identified. For example, the Information Governance Manager and Head of Business Process Improvement sit on the Health Regulators Information Security Specialist Interest Group. The HCPC will host the quarterly meeting in June 2015, and this will focus on data breach management and reporting. The Group has agreed to share policies and data in this area. It is hoped that the sharing of data and processes could lead to improvements in the HCPC's approach

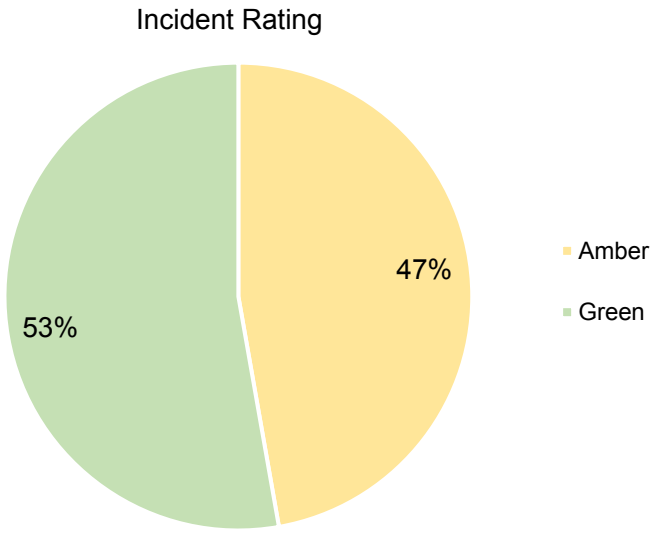
Information Incidents 2014-15

5.1 The HCPC is required to report on fitness to practise and registration-related data incidents to the PSA each year as part of the performance review process. In 2014-15 the HCPC reported 38 incidents to the PSA. Out of the

38, one of these incidents was reported to the ICO in February 2015 although to date the HCPC has received no communication from the ICO regarding this incident.

5.2 There were a further three information incidents recorded in 2014-15 which did not involve fitness to practise or registrations data. Of this number one incident was reported to the ICO in September 2014. No response has been received from the ICO regarding this notification.

5.3 As the incident severity scoring procedure began in 2015, and was not retrospectively applied to previous incidents, the full year's data cannot be reported on according to severity. The number of incidents according to severity from January to March 2015 is shown below:



5.4 Recent corrective actions and improvements agreed by EMT in response to information incident reports include redaction training for all fitness to practise case managers, changes to the way recorded mail is tracked and distributed, undertaking a supplier audit and changes to the way files are named on CMS.

Decision

The Council is requested to discuss the document.

Appendices

- Appendix one – example information incident report
- Appendix two – Information Incident Rating Procedure
- Appendix three – Information Incident Report April EMT

Date of paper

5 May 2015

Information Incident Report Form

Part A and B to be completed by the person reporting an incident.
Part C to be completed by the Information Governance Manager.

The form should be completed as soon as possible after an event and returned to the Information Governance Manager. If you do not know the details requested please leave these sections blank.

Please contact the Information Governance Manager or Head of Business Process Improvement if you require assistance completing the form.

Part A – Incident details

1. Name	Admin (ongoing investigation)
2. Department	FTP Admin
3. Report Date	30/04/15
4. Summary of incident	
Cross departmental process failure – ongoing investigation Council sent documents to HCPC (council confirm that they may have used generic address). Documents are received and signed for in the HCPC on the 17/4/15. CM Case Team 4 is alerted by Council and sends email out to 'all' to chase the location. 30/04/15 CM from CT6 confirms the documents have been scanned onto another bundle and attached to his case on CMS. CM [redacted] is in a hearing at present I do not have FTP number. I spoke to CSO Manager and he was unaware of the issue, he will look into the incident. Update The missing bundle was located on FTP[redacted] [redacted] this case belongs to CT6, the papers were embedded in the middle of another bundle of documents and could have been missed, if the appropriate checks were not in place.	
5. When did the incident happen?	
Between 17/04/15 – 29/04/15	
6. When was the incident detected?	
30/04/15	
7. Please list any relevant HCPC reference numbers	

8. Who was the data disclosed to? Please indicate the number of individuals.
Internal incident
9. Whose personal information was disclosed? (e.g witness, applicant.) Please indicate the number of people affected.
Internally misplaced N/A
10. Please indicate the type of information disclosed (e.g. name, date of birth, email address etc.)
Council records
11. What are the potential consequences and adverse effects on those individuals? For example; • Emotional / physical harm • Identify theft • Financial loss • Loss of business or employment opportunities
Emotional / physical harm
12. Are you in the process of recovering the data or has this already happened? If so, please provide details of how and when this occurred.
Yes – FTP reference TBC instructions to remove the information scanned to other documents in the wrong case on CMS
13. Are the affected individuals aware that the incident has occurred?
No
14. Have any affected individuals complained to the HCPC or another body about the incident? If so please attach these complaints.
No
FTP [redacted] other case ref TBC

Part B

Actions

Action	Owner	Date to be completed by
CSO – to ensure the documents are removed from the wrong case and subsequently scanned to the relevant case on CMS	Case Support Manager	Immediate action

Future improvements

Learning point	Proposed improvement	Directors response
CA and SH have reviewed the recorded delivery process within facilities. Admin – process in place ensure robust checks to add assurance to postal and scanning process	Review admin scanning process are relevant checks completed to avoid papers being scanned or attached to other documents and imported into wrong FTP case	This action was agreed and implemented.

Part C

Incident Rating

A	B	C	D	E	Rating
3	1	0	1	1	2

Comments
A number of incidents of this type have occurred recently. The process for accepting and distributing signed for post has been amended to prevent future occurrences.

Notification

Date information Security Group informed	30/04/2015
Date reported to EMT	26/05/2015
ICO notification (Y/N)	N
Legal advice sought (Y/N)	N

Information Incident Rating Procedure

Purpose

This procedure aims to enable to the HCPC to assess the severity of information incidents in a consistent and comparable way and to strike the right balance when self-reporting to the ICO.

Rating Formula

An incident severity rating formula has been developed based on the Data Protection Act and the ICO's criteria for reporting incidents. Severity is measured according to the risk of harm to the data subject and to the HCPC. The scale is compatible with HCPC Risk Matrix.

The formula is based on the three main components of a data incident. These are the nature of the data, the impact of the disclosure and containment of the incident. Each component of a data incident is given a score out of five. The following formula is used to obtain the rating. Division by 1.2 converts the score to match the HCPC Corporate Risk Register scale.

The incident rating scale is set out below;

Category	Score	Colour Code	Action
Incident	1-5	Green	Review if similar incidents are occurring and consider if departmental processes can be improved
Significant incident	6-11	Amber	Departmental and organisation wide learning points to be considered and possibly implemented
Serious incident	12-25	Red	ICO notification likely. NMR to be initiated

The rating score is a guideline only, sometimes un-quantifiable aspects of an incident may cause the level of risk to increase or decrease, for example the involvement of a vulnerable service user.
The resultant action has been suggested above. However actions and learning points will be case specific and are beyond the scope of this process. The process is

focused on determining if ICO notification is required and on obtaining a clear picture of the severity of data incidents across the HCPC.

The tables below outline the criteria for each formula component.

Data Details

A – Risk of Harm to data subject		B – Number of data subjects involved	
1	Any non-identifiable personal data	1	1
2	Any identifiable personal data such as name and DOB.	2	2 – 10
3	Any identifiable personal data such as name, DOB, address confidential and / or sensitive material or sensitive personal data.	3	11 – 100
4	Any identifiable data such as name, DOB, address confidential and / or sensitive material or sensitive personal data. Level 4 will usually include significant volumes of information that could be harmful to the individual.	4	101 – 1000
5	Significant volumes of sensitive personal data that is likely to cause serious harm to the individual and / or organisation involved.	5	more than 1000

Impact

C – Number of people disclosed to		D – Who was the information disclosed to?	
1	1 person.	1	Internally within the HCPC.
2	2 – 10 people.	2	Internally but outside of HCPC system control eg. Disclosing information to a colleague's hotmail address.
3	11 – 100 people.	3	A third party where the HCPC has a relevant contract or information sharing agreement detailing DPA and information security requirements.
4	101 – 1000 people.	4	NHS or organisations or professions that we have a level of understanding with and / or they are bound by patient confidentiality or solicitors' code of conduct.
5	More than 1000 people.	5	A person / persons with whom the HCPC does not have a contract with.

Containment

E – Data recovery status	
1	The information has been recovered, deleted or securely destroyed.
2	Lost within the HCPC premises
3	Lost in a controlled environment eg. A third party where the HCPC has a relevant contract or information sharing agreement detailing DPA and information security requirements.
4	Lost in a controlled environment eg. A special delivery item lost within Royal Mail systems
5	The information has not been recovered. This score is also assigned to any incident where data is in the process of being recovered. The rating score is updated once the data is recovered or securely destroyed.

There will be incidents where it is difficult to allocate a specific category score. For example, in some circumstances it can be difficult to ascertain how many people may have had access to disclosed material. In such cases the higher score will be used to ensure we are giving the incident an appropriate level of priority.

How the formula will be used

- When an incident is reported the Information Governance Manager (IGM) will analyse the circumstances and record an initial score. This will be notified to the information security group (ISG). Any initial red scores will also be alerted to EMT.

- When the investigation report is complete, the IGM will review the score based on its findings. Any revision to a score will be alerted to the ISG.

- The IGM will record the incident rating score in the Information Incident spreadsheet and will update the scores if for example disclosed information has been securely destroyed or deleted.

- Statistics on incidents will be reported to EMT on a monthly basis.

- This forms an essential part of the ISO27001 process for incident management.

Working examples

1. A HCPC hearing bundle is lost on a train by a Partner. The case relates to record keeping. The bundle was redacted and only the registrant can be identified from the information. The bundle is not recovered. The scoring for this case would be as follows;

    - A - The data is confidential but not likely to cause the registrant harm, though it may cause distress. It is not sensitive information. Therefore this scores a 3.

    - B - The information identifies one person only and so this scores a 1.

    - C - It is difficult to determine the number of people disclosed to as it is never recovered. A score of 3 is reasonable.

    - D - It is unknown who has possession of the information and therefore this scores a 5.

    - E - The information was not recovered and therefore this scores a 5.

    The incident rating would therefore be as follows;

    ((3+1)/2 x (3+5)/2) + 5) / 1.2 = 11

    This means that the incident is deemed to be a significant incident (amber) but ICO notification is not considered necessary.

2. An incomplete direct debit form for Registrant A is returned to Registrant B by mistake. The form contains the name, date of birth home address and bank details of the Registrant A. Registrant B has confirmed that they have securely destroyed the form. The scoring for this case would be as follows;

    - A - The information is sensitive as there is a risk it could enable Registrant A's identity to be stolen, resulting in harm. However the information is not voluminous. This scores a 3.

    - B - The information relates to one person only and so this scores a 1.

    - C - The information was disclosed to one person only and so this scores a 1.

    - D - Registrant B must follow the SCPE and therefore it is reasonable for us to assume that the information will not be misused. This scores a 4.

    - E - The information was securely destroyed and so the score is 1.

    The incident rating would therefore be as follows;

    ((3+1)/2 x (1+4)/2 + 1)/1.2 = 5

This means that the case is deemed to be an incident (green) but ICO notification is not considered necessary.

3. The monthly payroll package goes missing in transit. The package contains the name, address, date of birth and national insurance numbers of over 200 people. The scoring for this case would be as follows;

   - A - The information is sensitive as it could lead to identity theft, score is 3.
   - B - There are over 200 data subjects affected therefore the score is 4.
   - C - This information is unknown to us. It is reasonable to score this as a 3.
   - D - The personal holding the information is unknown to the HCPC. This scores 5.
   - E - The information is not recovered, scoring a 5.

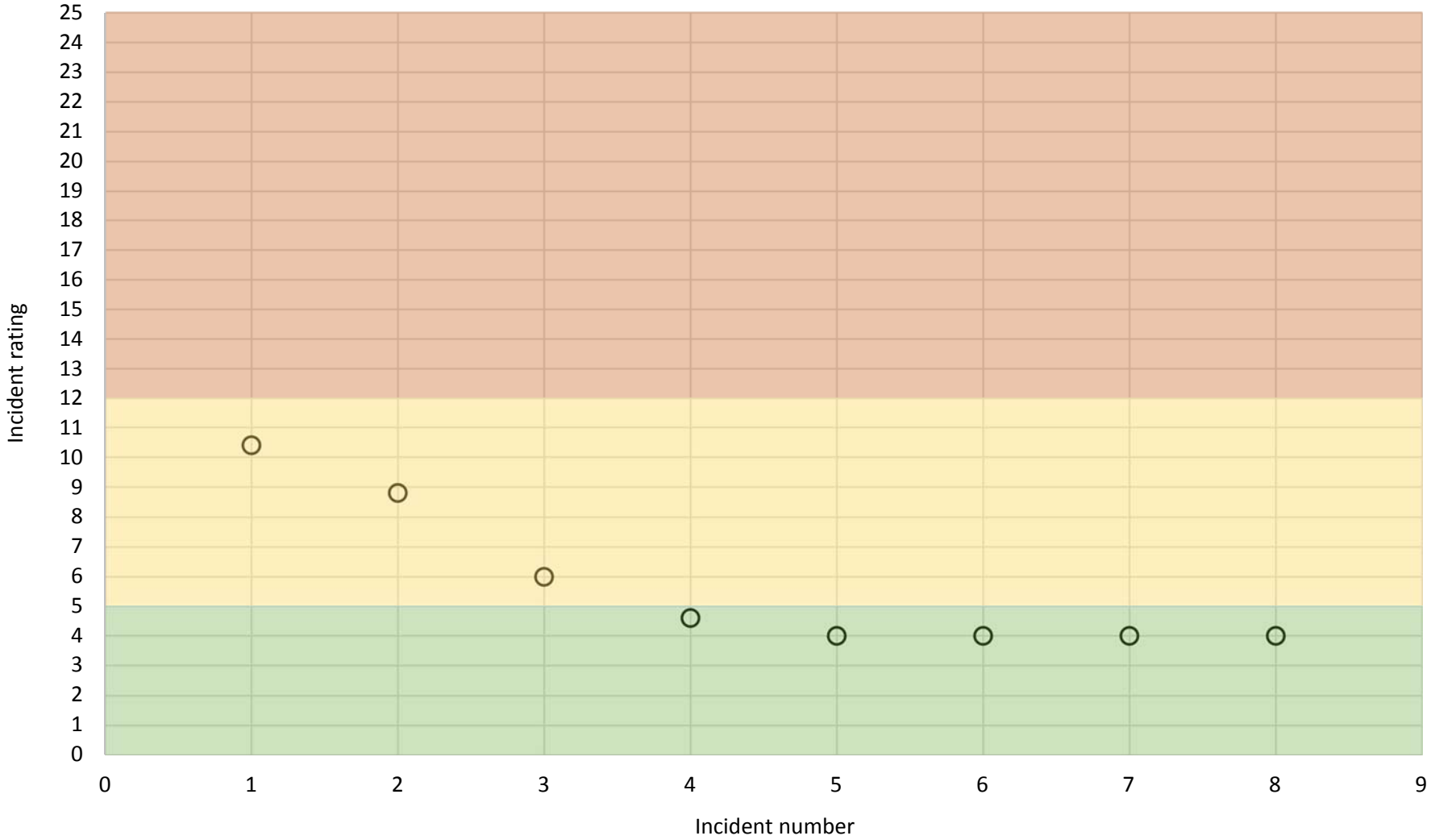
   The incident rating would therefore be as follows;

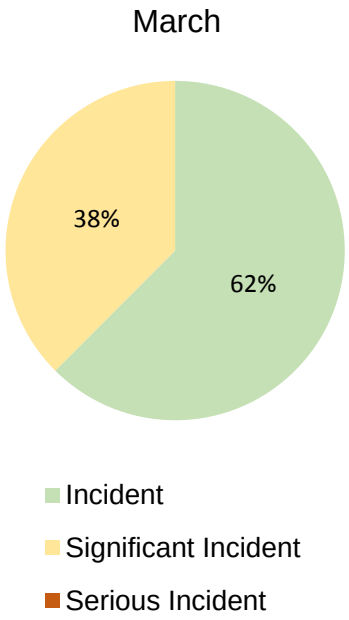
   ((3+4)/2 x (3+5)/2 + 5)/1.2 = 16

   This means that the case would be deemed a serious incident. The HCPC would notify the ICO in this instance.

Information Incident Report – March 2015

The graph below shows the number of reported information incidents in March 2015 and their position on the rating scale. Please see the information incident rating process for further information on the scale. Details of each incident, and future mitigations, follow the graph.





No.	Date	Dept	Summary of incident	Key factors	Score	Root analysis
1	March	FTP	ICP bundle was issued with inadequate redactions, enabling the identification of several service users. The case contained sensitive personal data.	The bundle is now with KN for redactions for the final hearing. The CM delegated the redactions to a CSO. The CM check of the redactions did not catch the error. FTP confidentiality FOG states that case team managers are responsible for checking the ICP/Obs redactions of their team. There was no CTM check documented for this case, is there a standard form to evidence the quality check? Anecdotally it seems that this check does not take place as the norm. If the information had been requested in a redacted form initially this incident may have been avoided.	10.4	HCPC error Human error Process issue
			<u>Information Governance Manager recommendations</u> CTM checks of ICP/Obs bundle redactions should take place as outlined in the FOG. These checks should be documented. <u>Management response</u> The information and confidentiality FOG has been revised and includes further detail regarding redactions. Training to support the roll out of the FOG is scheduled to take place at the end of April. Due to the time consuming nature of checking bundles further thinking is needed on how to continue to ensure that the resources devoted to checking redactions remains proportionate to the risk. This may include only requiring Case Team Managers to check those bundles which could be consider 'high risk' in terms of the sensitivity of the information contained in the bundle.			
2	March	FTP	Registrant A received the ICP decision notice for registrant B. Redactions to ICP bundle were not adequate. This is in part due to the poor partial redactions made by the local authority supplying the documents, however this should have been caught by HCPC. Child protection case.	The case was audited in August 2014 before it went to ICP and it was recommended to the CM at that time that the bundle required further attention due to the quality of the redactions and the disclosure issues. Unfortunately this advice was not acted on.	8.8	HCPC error Third party error Human error Process issue
			<u>Information Governance Manager recommendations</u> Training has been arranged for all CMs and CSOs as per the agreed recommendation in the March information incident report. However this training is not specifically redaction focused and only two time slots of around an hour have been allocated which means that the group sizes for the two sessions will not enable a 'workshop' format. One session per case team would be more focused and helpful to CMs. <u>Management response</u>			

			The revised Confidentiality and Information Security FOG coupled with the training will ensure that case teams have more detailed guidance on the importance of appropriate redaction and how to redact documents effectively. Whilst it is acknowledged that the time set aside for the initial training is limited, the training should be viewed as the start of a process of ongoing and regular training. Further training at an individual or case team level can be considered in light of an evaluation of the planned training or where a manager assesses this may be helpful.			
3	March	FTP	The FTP cases of registrant A and B were originally linked due to the allegations. However registrant B's case was no case to answer. Registrant A's case bundle was not then reviewed to remove data about registrant B	Registrant A and B are known to each other so the harm of this incident is low. However as registrant B is no longer under any investigation and is not being called as a witness to the events their identity should be anonymised in future hearings.	6	Supplier error Human error Process issue
			<u>Information Governance Manager recommendations</u> As outlined in 1 and 2 above. <u>Management response</u> Please see response to points 1 and 2.			
4	March	FTP	Registrant has two live cases. Registrant emailed HCPC from his wife's email address cc'ing his own email address. The email said that he would not be submitting a response to case 1. KN then used this email address to send the notice of allegation for case 2 to the registrant. The registrant complained about this and feels this is a data breach.	There is no evidence to suggest that the CM provided the wife's email address as a contact for the registrant, indicating that KN took this direct from the bundle. HCPC provide KN with a contact list when sending the initial instruction. KN have undertaken an internal investigation which identifies staff not following agreed procedures as the cause. Allegations are published on our website 28 days before a hearing so this information will be public. Allegations can be disclosed before this on request. There was a delay in KN notifying us of the registrant's complaint (i.e that an incident had occurred) as a HCPC member of staff was on leave.	4.6	Supplier error Human error Process issue
			<u>Information Governance Manager recommendations</u> Agree an operational process with KN in relation to notification of information incidents in line with our own to avoid future delays. <u>Management response</u> The contract with KN requires that they inform the HCPC immediately if they become aware or suspects that personal information may be disclosed to an unauthorised person. This will be addressed through the regular Service Level Agreement meetings and may include sharing our			

			operational guidance on confidentiality and the data security reporting framework to ensure there is a consistent understanding of incidents that should be reported and when. Under the terms of the contract with KN HCPC may conduct an audit. An audit is planned for 22 April and will include a review of their data security arrangements.			
5	March	FTP	A concern was received about an unregistered therapist. The complainant provided the registration number of one of our registrants who had the same name. ID checks were inadequate and the address details of our registrant were changed according to the complainant's information. A case was logged. Email address was not changed and so registrant received an email relating to the case. Non registrant's solicitor was cc'd in to email and forwarded this to the non-registrant, disclosing the email of the registrant	The address and work details provided by the complainant did not match those of our registrant but we amended them to match. Change of address form submitted to CEO. NMR called. We should not change someone's personal details without first trying to make contact with them unless we are confident that the information provided is factually correct, for example information provided by a 'trusted source'.	4	HCPC error Human error Process issue
			<u>Information Governance Manager recommendations</u> NMR report will be more comprehensive, however the change of address form should require more detail on the justification and CTM sign off before being submitted to the CEO. <u>Management response</u> Await the outcome of the NMR.			
6	March	FTP	A letter intended for the complainant was sent to the registrant, disclosing the complainant's home address.	Human error. Registrant has been informed of the complaint but was not aware of the details as the matter. CMS enhancement completed on the 5/01/15 which removed the default population issue discussed in the March information incident report. This incident was human error only.	4	HCPC error Human error
			<u>Information Governance Manager recommendations</u> None, appears to be purely human error based. <u>Management response</u> This appears to be an isolated incident resulting from human error. The importance of taking care that documents are sent to the correct recipient will continue to be reinforced to employees. Going forward, if there is evidence to suggest particular individuals are repeating the same			

			error then further analysis will be undertaken to establish why this is the case; and to identify any additional remedial measures that may be required.			
7	March	FTP	Letter to registrant was sent to the complainant. Letter was not confidential but did contain the home address of the registrant.	The complainant was the registrant's previous employer so it is very likely that this information was known.	4	HCPC error Human error
			<u>Information Governance Manager recommendations</u> None, appears to be purely human error based. <u>Management response</u> See response to 6.			
8	March	FTP	A letter of instruction intended for KN was emailed to the complainant. This contained the home address of the registrant.	Complainant is the employer of the registrant so the home address of the registrant would have been known to them.	4	HCPC error Human error
			<u>Information Governance Manager recommendations</u> None, appears to be purely human error based. <u>Management response</u> See response to 6.			