Irish Journal of Psychological Medicine (2014), **31**, 125–130. © College of Psychiatrists of Ireland 2014
doi:10.1017/ipm.2014.12

ORIGINAL RESEARCH

Compliance with the Data Protection Acts in a psychiatric department: a complete audit cycle

A. Hassab Errasoul[1,*], **M. Cannon**[2] and D. Cotter[2]

[1] *Coolock Community Mental Health Service, Coolock Health Center, Coolock, Dublin, Ireland*
[2] *Department of Psychiatry, Education and Research Centre, Royal College of Surgeons in Ireland, Dublin, Ireland*

Aim. 1) to assess compliance with the Data Protection Acts (DPA) by a Department of Psychiatry in a general hospital, 2) to implement measures that are likely to maximize compliance with the hospital data protection policy, 3) to close the audit cycle by assessing the impact of such measures on departmental compliance with the DPA over five months period.

Method. An individual, anonymised staff questionnaire on data collection practices, procedure of disclosure of data to third parties and previous training on DPA was used to collect information from the department staff. The premises were inspected at different times over a week period using structured checklist. Default points were recorded during each inspection. Post-audit interventions included a mixture of educational interventions and practical solutions. A re-audited took place five months later using the same method.

Results. The baseline audit demonstrated significant lack of compliance with the DPA among staff members and lack of staff training on the DPA. Following the interventions, staff awareness of the requirements of the act rose which in turn lead to better adherence to recommend practices in data handling and to mean default points dropped significantly. Management of manual files appears to constitute the biggest problem in this audit. Daytime breaks were found to pose higher risk to stored data compared with before and after working hours.

Conclusions. A combination of educational and practical interventions including training of staff on the DPA results in overall improvement in compliance and reduction in default points. However, management of manual (physical) data proves to be more difficult and hence will need more input.

Received 20 September 2012; Revised 21 February 2013; Accepted 18 March 2014

Key words: Act, audit, compliance, data, protection.

Introduction

People's right to personal privacy is recognised both by the Constitution of Ireland (Bunreacht Na hEireann 1937) and European legislations (European Union 2000). The Data Protection Acts (DPA) (2003) provide a legal framework that safeguards this basic human right and confers rights on individuals as well as placing responsibilities on those persons processing personal data. In the DPA, special consideration is given to certain categories of 'sensitive data' and hence is granted special protection. This 'sensitive data' include data on physical and mental health. Table 1 provides definitions to some of the key terminologies used in the DPA.

The Code of Practice for Healthcare Records Management (The National Hospitals Office 2007) stresses the responsibility of each hospital in establishing and maintaining policies and procedures to ensure that patients are assured that their medical information is treated in confidence and not shared inappropriately. Maintaining patients' confidentiality is considered not only an issue of professionalism but also a legal obligation. This document also recognises education and training and audit as key procedures in healthcare record management.

Conviction of an offence under the DPA may result in forfeitures or destruction of data material, fine up to €100 000 or subjectivity to civil sanctions by the person (s) affected in compensation for injury (defamation, breach of confidentiality or mental distress).

The DPA encompass eight principles regulating personal data handling. These include:

1. Fair obtaining and processing of information.
2. Keeping data only for specified and lawful purpose(s).
3. Processing data only in ways compatible with the purposes for which it was given initially.
4. Keeping data safe and secure.
5. Keeping information accurate and up-to-date.
6. Ensuring that data is adequate, relevant and not excessive.
7. Retaining data no longer than is necessary for the specified purpose or purposes.

* Address for correspondence: A. Hassab Errasoul, Galway/Roscommon Mental Health Services, Day Hospital, Ballinasloe, Co. Galway.
(Email: ahmedhassabu@yahoo.com)

Table 1. *Key terminologies used in the Data Protection Acts 1988 and 2003*

Terminology	Definition
Personal data	Data relating to a living identifiable individual.
Sensitive data	Personal data on physical or mental health, racial origin, political opinions, religious or other beliefs, sexual life, criminal convictions and alleged commission of offence and Trade Union membership.
Data processing	Performing any operation on the information, e.g., obtaining, recording, storing, retrieving and destroying the data.
Manual data	Data Structured by reference to individuals without the use of automatic equipments.
Automated data	Information that is processed by means of automatic equipments.
Data controller	A person – or legal person – who, either alone or with others, controls the contents and use of personal data
Data processor	A person who processes personal data on behalf of a data controller but does not include an employee of a data controller, e.g., tax advisers.

8. Allowing subjects access to their personal data on request.

In compliance with the DPA, the hospital where this audit was performed adopted a data protection policy that recognises, in addition to the Hospital Board, all employees who collect, control the contents and/or use personal data as responsible for compliance with the data protection legislation.

Aims

The purposes of this audit are (1) to assess compliance with the DPA by the Department of Psychiatry in the hospital (2) to implement measures that are likely to maximise compliance with the hospital data protection policy (3) to close the audit cycle by assessing the impact of such measures on departmental compliance with the DPA over 5-month period.

Methods

Setting

The department audited is situated in a portable, one storey building attached to the main building of the hospital. It contains seven small offices shared by various medical and nursing staff, social workers and psychologists. A front office is used as a reception and secretary office and also to store files of patients awaiting reviews in the outpatient clinics. All offices are supplied with computer units with access to the hospital intranet and a shared folder for the department. Filing cabinets are available in all offices but many do not have keys or have been locked for undefined periods of time. One office is used by a separate mental health team and was not included in this audit.

Twice a week, a 'common' registrar office is used for clinical meetings. It contains a whiteboard on which details on inpatients under regular follow-up are written to facilitate communication between team members. Department offices are regularly used for patient review appointments, psychotherapy sessions and family meetings. However, the bulk of outpatient activities are performed in the designated, main hospital outpatient department.

The department is guarded by a swipe card entry system and keys. The door is opened around 08:00 a.m. by security staff and locked in after 06:00 p.m. A small side door leading to outside lawns and car park is maintained open during this period as a fire exit. Each office has a key that is kept in a common place for all staff use.

Study instruments

A checklist on data protection policy was used to determine areas that needed to be audited and also to compile two separate data collection forms. This checklist was developed by the Office of the Data Protection Commissioner as part of their proposed data protection audit resources (Office of the Data Protection Commissioner 2009) and it summarises different elements of the DPA. Using this checklist, two data collection forms were developed:

1. An individual, anonymised staff questionnaire on data collection practices, procedure of disclosure of data to third parties (i.e. any person who is neither the data controller nor the data subject), previous training and readings on the DPA and awareness of the role of the Data Protection Officer in the hospital (Appendix 1).
   All department staff (medical, nursing, psychology, social work and visiting staff) were asked to fill this questionnaire.
2. An inspection checklist with slots for day, date and time of inspection. This checklist includes digital

https://doi.org/10.1017/ipm.2014.12 Published online by Cambridge University Press

and manual data security, data on screens and boards security and disposal of waste papers and printouts (Appendix 2).

Procedures

Regular inspections of the department offices were performed over a week period covering both ordinary working days and a weekend. Inspections were performed at four time bands thought to be mostly vulnerable: between 07:00 and 09:00 a.m., between 10:30 and 11:30 a.m. (coffee break time), between 01:00 and 02:00 p.m. (lunch break) and between 05:00 and 08:00 p.m. (after hours). A total of 14 inspections were performed over a period of 1 week. Staff members were not made aware of inspection times or areas audited. Twelve inspections were performed in ordinary week days and two inspections over a weekend day. Four inspections were performed before 09:00 a.m., four during lunch break and three episodes at each of coffee break time and after hours.

A scoring system was adopted counting the numbers of defaults to facilitate comparisons between different inspection times. Each office unit was counted as (one) default point on access to unattended manual files. If doors are locked but keys are readily available to 'potential intruders', default points were still counted. Each unattended and accessible (not logged off) computer unit was counted as (one) default point. Visible screen or whiteboard data through the windows was also counted as (one) default point. Accessibility to psychology or social work files by unauthorised staff was also counted.

Total number of default points for each inspection was calculated and recorded.

Intervention

Following the results of the baseline audit, areas of weakness were identified and suggestions on corrective interventions were made by multidisciplinary team. The intervention comprised a mixture of educational and practical measures:

(a) The audit findings were presented at the department's academic meeting. Staff members watched a 17 minutes' training video sourced from the Office of the Data Protection Commissioner for the purpose of training (*My Data – Your Business* 2005).New staff members joining the department were also asked to view the video. Members of the staff who were not present in the department meeting were briefed individually about the audit results and were supplied with the training video to view.

(b) We requested the Hospital Technical Services Division to cover the outer windows with a frosted coating, which allows light in but stops people outside from looking in.

(c) Old notes containing patients' data not in use (e.g. photocopies of previous assessments) were shredded.

(d) Keys were obtained for filing cabinets where possible and staff members were encouraged to use them.

(e) Reminders were displayed on the walls to ensure doors and cabinets are locked when not attended to.

(f) The IT Department was contacted to re-set a timeout for computers when not in use. Periodical change of passwords was also suggested.

(g) A swipe card access control to the offices where files are likely to be kept was suggested to the hospital administration but was not sanctioned at the time of re-audit due to cost considerations. Secretarial staff agreed to lock the main office when they go on lunch or coffee breaks.

Re-audit

Five months later, a re-audit took place using the same methods.

Results

Staff training and data handling practices

Twenty-four staff members filled the questionnaire. This represented 95% of staff. The results obtained from this questionnaire before and after the intervention are shown in Table 2.

Results for departmental inspections

The results obtained from departmental inspections before and after the intervention are shown in Table 3.

Time of the day and vulnerability

Figure 1 plots the four time bands and the mean default points both pre-intervention, post-intervention and for the total.

Discussion

This audit demonstrates (1) significant unawareness of the DPA at baseline among staff members of a psychiatry department in a general hospital (2) lack of staff training on the DPA 1988 and 2003 and (3) the fact that, significant improvement can be achieved with brief low-cost interventions. The data in Table 3 shows the magnitude of data storage problem, particularly that of manual data. As management of manual files appears to constitute the biggest problem in this audit, moving towards electronic patients' files may improve data security. Figure 1 shows the increased risk to stored

https://doi.org/10.1017/ipm.2014.12 Published online by Cambridge University Press

Table 2. *Staff responses to audit questionnaire before and after intervention*

Question	Baseline audit			Re-audit		
	Yes	No	Not applicable[a]	Yes	No	Not applicable[a]
At the time when you collect information about patients, are they routinely made aware of the uses for that information?	37.5%	50%	12.5%	61.9%	19%	19%
Are people routinely made aware of any disclosures of their data to third parties?	75%	25%	0%	95.2%	4.8%	0%
When you collect information about patients from a third party outside the hospital (e.g. from a husband about his wife), are patients routinely made aware of this?	79.2%	8.3%	12.5%	81%	4.8%	14.3%
Had you ever attended any form of training on the Data Protection Act?	12.5%	87.5%	0%	81%	19%	0%
Had you ever read about the Data Protection Act?	45.8%	54.2%	0%	85.7%	14.3%	0%
Are you aware of the role data protection coordinator and compliance persons in the Hospital?	33.3%	66.7%	0%	61.9%	38.1%	0%

[a] For staff members who are not involved in data collection (i.e. data processors).

Table 3. *Results obtained from departmental inspections before and after the intervention*

Criterion	Baseline audit		Re-audit	
	Yes	No	Yes	No
Is access to computers restricted to authorised staff only?	50%	50%	58.3%	41.7%
Is access to manual files restricted to authorised staff only?	14.3%	85.7%	8.3%	91.7%
Is access to the information restricted on a 'need-to-know' basis in accordance with a defined policy?	7.1%	92.9%	16.7%	83.3%
Is computer system password protected?	100%	0%	100%	0%
Is information on screens kept hidden from callers to offices?	14.3%	85.7%	41.7%	58.3%
Are all waste papers, printouts, etc. disposed of carefully?	0%	100%	91.7%	8.3%
Mean default points	8.36 (S.D. 3.67)		4.5 (S.D. 2.1)	

data during daytime breaks (lunch breaks and coffee breaks) comparing with out of office hours. This phenomenon continues to a lesser extent post-intervention.

The interventions used to improve compliance with the DPA included a mixture of educational and practical measures and targeted the areas of weaknesses noted in the baseline audit as they appear in Tables 2 and 3. As a result, staff awareness of the requirements of the Act rose, which in turn lead to better adherence to recommended practices in data handling and storage (Fig. 1).

The lack of compliance with the DPA seen at baseline in this audit is consistent with previous studies involving final year medical students in a university hospital in Dublin (Naughton *et al.* 2012) and surgical trainees in Northern Ireland (Mole *et al.* 2006). In their audit on final year medical students compliance with the DPA, Naughton *et al.* suggested that widespread breaches of the DPA among registered healthcare professionals exist and described the findings on medical students as the 'tip of an iceberg' (2012). This audit confirms this hypothesis. In contrast to earlier findings (Naughton *et al.* 2012), this study suggests some improvement in compliance with DPA as a result of a mixture of educational intervention and practical solutions.

An important strength of this audit is the use of objective inspections as well as self-reported questionnaires to assess staff compliance of the DPA and the evaluation of both staff state of knowledge about the DPA and everyday adherence to the DPA. Other strengths to this study are the inclusion of the whole multidisciplinary team and clerical staff in the assessment process, carrying out the inspections both during working days and over the weekends and inspecting the premises at staggering intervals during the day.

The most important limitation of this study lies in the fact that it does not show whether the improvement is noted in adherence to the DPA is sustainable on the

https://doi.org/10.1017/ipm.2014.12 Published online by Cambridge University Press

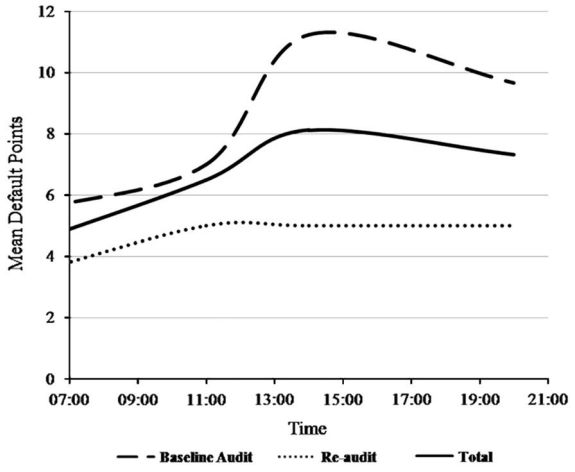

Fig. 1. Plot of the four time bands and the mean default points both pre-intervention, post-intervention and for the total

long term or not. It also does not include in detailed information on digital data handling through USB drivers or data transmission outside formal hospital email system. However, the hospital's digital data protection policy allows only encrypted external data drives on hospital computers. The use of external emails in data transfers is not monitored and remains an area for future audits.

Conclusions

A combination of educational and practical interventions including training of staff on the DPA resulted in overall improvement in compliance and reduction in default points. However, management of manual (physical) data proved to be more difficult and hence will need more input. Using electronic medical records may be a way forward to improve sensitive data security.

Recommendations

We recommend assigning a permanent member of the team to undertake the responsibilities of continuous monitoring of levels of compliance and assurance of training of new staff. Commonly known as the 'Caldicott guardian', such a provision has already been in place in United Kingdom for more than 2 decades following the publication of the Caldicott report on patient confidentiality issues in 1997 (Roch-Berry 2003). As recommended by the Office of Data Protection Commissioner, periodical audits are needed to ensure long-lasting compliance. Further audits are needed to investigate the extent of the use of unsecured common emails in data transfer. We also recommend the inclusion of training on data protection in staff educational sessions on regular intervals.

Acknowledgements

The authors would like to acknowledge the participation of all staff of the Department of Psychiatry, Beaumont Hospital; we also wish to thank Professor Kieran Murphy, RCSI and Beaumont Hospital for reviewing an earlier draft of this paper.

References

Bunreacht na hÉireann (Constitution of Ireland) (1937). Article 40.3.1° (on the personal rights of the citizen).

European Union (2000). Charter of Fundamental Rights of the European Union, Official Journal of the European Communities (2000/C 364/01).

Mole DJ, Fox C, Napolitano G (2006). Electronic patient data confidentiality practices among surgical trainees: questionnaire study. *Annals of the Royal College of Surgeons of England* **88**, 550–553.

My Data – Your Business? (2005). [DVD]. Without Director. Ireland: The Office of the Data Protection Commissioner.

Naughton M, Callanan I, Guerandel A, Malone K (2012). Medical students' knowledge of data protection legislation. *Clinical Governance: An International Journal* **17**, 28–38.

Office of the Data Protection Commissioner (2009). *Data Protection Audit Resource*, Office of the Data Protection Commissioner (http://www.dataprotection.ie/documents/enforcement/AuditResource.pdf). Accessed 27 November 2013.

Roch-Berry C (2003). What is a Caldicott guardian? *Postgraduate Medical Journal* **79**, 516–518.

The Data Protection (Amendment) Act (2003). (number 6 of 2003). Dublin: The Stationery Office.

The National Hospital's Office (NHO) (2007). *The National Healthcare Records Management Code of Practice* (http://www.hse.ie/eng/services/Publications/services/Hospitals/NHO_ Code_of_Practice_for_Healthcare_Records_Management_ Version_2_0.pdf). Accessed 27 November 2013.

https://doi.org/10.1017/ipm.2014.12 Published online by Cambridge University Press

Appendix 1. *An individual staff questionnaire on data collection practices*

Please tick as appropriate:

No	Criterion	Yes	No	Not Applicable	Comments
1	At the time when you collect information about patients, are they **routinely** made aware of the uses for that information?				
2	Are people **routinely** made aware of any disclosures of their data to third parties?				
3	If you collect information about patients from a third party outside the hospital (e.g. from a husband about his wife), are patients **routinely** made aware of this?				
4	Had you ever attended any form of training on the Data Protection Act?				
5	Had you ever read about the Data Protection Act?				
6	Are you aware of the role data protection coordinator and compliance persons in the Beaumont Hospital?				

Appendix 2. Department inspection checklist

Date: _____ Day: _____
Time _____ Total default points: _____

Criterion	Yes	No	Default Points	Comments
1. Is access to computers restricted to authorised staff only?				
2. Is access to manual files restricted to authorised staff only?				
3. Is access to the information restricted on a 'need-to-know' basis in accordance with a defined policy?				
4. Is computer system password protected?				
5. Is information on screens kept hidden from callers to offices?				
6. Are all waste papers, printouts, etc. disposed of carefully?				

https://doi.org/10.1017/ipm.2014.12 Published online by Cambridge University Press