Data Protection Among Junior Medical Staff: A Questionnaire Study

Andrew Gordon Titchener, MA, MRCS, Anil Ramoutar, Bsc, MBBS, MRCP,‡ Darryl N. Ramoutar, MA, MRCS,† and Almunir Yousef, FRCS (Tr+Orth)**

Objective: There have been numerous reports of loss of confidential information amongst UK public agencies. The aim of the study was to examine current standards of practice and knowledge of junior medical staff with respect to management of patient identifiable information.

Methods: An anonymous multiple choice questionnaire was completed by 50 junior medical staff in each of 2 separate district general hospitals in the UK.

Results: Sixty-two percent of physicians surveyed held patient identifiable information electronically, outside of normal NHS use. Thirty percent of physicians used portable memory sticks, of which, 68% were not password protected. Ninety percent of physicians used patient ward lists in paper format with 18% frequently using a domestic waste bin for disposal. Thirty-five percent of physicians were aware of the Caldicott principles, and 58% were aware of the Data Protection Act as applied to their duties.

Conclusions: Despite having statutory duties toward the management of patient identifiable information, many physicians are not aware of their responsibilities and obligations. This is unlikely to be an isolated local issue. More emphasis needs to be placed on data management in hospital induction procedures for new employees, and security measures, such as encryption software, should be made more widely available.

Key Words: education, medical, confidentiality/standards, questionnaires

(*J Patient Saf* 2013;9: 75–78)

The safekeeping and management of patient records and patient identifiable information is a statutory duty of junior medical staff in the NHS. It is also an obligation of all physicians registered with the GMC through the "duties of a physician."[1] There have been numerous reports of loss of information amongst UK public agencies, and the NHS is no exception. In 2007, HM Revenue and Customs lost 2 discs containing the details of 25 million child benefit claimants. Later in 2007, the Department of Health reported that 9 NHS trusts had dealt with breaches of their security rules; these involved the loss of a considerable number of patient's details and data.

Although many of the high profile cases have not involved junior medical staff, many juniors use and store patient data for audit and research purposes. They are therefore a group at high risk of losing or releasing sensitive data into the public domain. Guidance on information governance and handling of confidential data is usually included in hospital trust induction programs and is also available from many other sources,[2] including the GMC. Recent evidence is limited but does suggest that the standards of practice of some juniors are below acceptable levels.[3] We therefore aimed to analyze the current practice of junior physicians in 2 separate hospital trusts and to assess their awareness of the Data Protection Act and the Caldicott Principles.[4,5]

METHODS

The survey was carried out in 2 district general hospitals each in a separate region of the UK. These were situated in the East Midlands and Kent and were of similar size (525 and 409 inpatient beds, respectively). Multiple choice questionnaires (appendix A) were issued by the authors to 50 randomly selected junior physicians who attended the physician's mess (common room) on a single day. The 14 responses were required, including basic demographic details and analysis of information governance practice. The responses were anonymous and were collected by hand upon completion. The questions aimed to survey both the physicians' current practice as well as their awareness of the Data Protection Act and Caldicott principles with respect to storage and disposal of patient identifiable information.

RESULTS AND DISCUSSION

Of the 50 juniors who were allocated a questionnaire in each hospital, all 50 completed and returned them, giving a response rate of 100%. The junior physicians sampled consisted of a range of seniorities (Fig. 1) and specialties (Fig. 2). Across both hospitals, the majority were from physicians in Foundation Year One (FY1) who supplied 47% of responses and Senior House Officers (SHO) who included Foundation Year Two, Specialty Trainee Years One/Two and who supplied 36% of responses. Specialist Registrar and Specialty Trainee Years Three and above (SpR) supplied the remaining 17%. The questionnaire focused on 3 areas of practice: electronic data storage, data storage on paper other than regular medical records, and physician's awareness of their legal and professional obligations.

Electronic Data Storage

Patient identifiable information was stored electronically by 62% of physicians, with 95% (59/62) storing this on hospital computers, 48% (30/62) on memory sticks, and 8% (5/62) on personal computers. For those who used hospital computers, 62% (37/59) required a personal password, and 62% (37/59) required a generic password. One percent (1/59) required no password at all. Forty-six percent (14/30) of memory sticks used were not password-protected at all. Thirty percent of Trusts required the same password for Trust and personal logins.

From the *King's Mill Hospital, Mansfield; †Queen's Medical Centre, Nottingham; and ‡Respiratory Medicine, Basildon Hospital, Nethermayne, Basildon, Essex, UK.

Correspondence: Anil Ramoutar, BSc MRCP, Respiratory Medicine, Basildon Hospital, Nethermayne, Basildon, Essex, SS16 5NL, UK (e-mail: anilram@doctors.net.uk).

The authors disclose no conflict of interest.

Funding: No funding was received.

A.G.T. designed and lead the study, analyzed and interpreted data, and wrote the paper. A.R. collected data and assisted with review of the final manuscript. D.N.R. analyzed and interpreted data and cowrote the initial manuscript. A.Y. is the consultant involved in the conception of the study and review of the final manuscript.

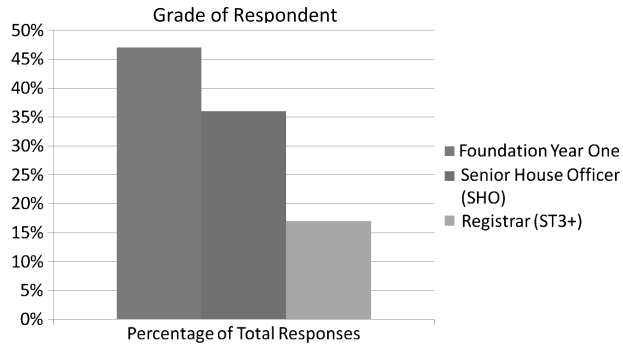

FIGURE 1. Grade of respondent.

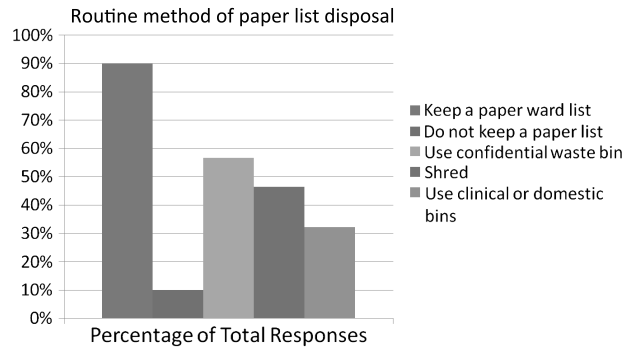

FIGURE 3. Routine method of paper list disposal.

It is a requirement across all public sector organizations set by the cabinet secretary that personal data kept on removable media must be encrypted, and it is the duty of employees to conform to this. Nevertheless, the authors have encountered a range of policies in different NHS Trusts toward this requirement. Some Trusts issue memory stick which are preloaded with encryption software, which ensures that the encryption is of the required strength and that there is no temptation to use a nonencrypted device. Other Trusts allow employees to use their own media and place the onus on them to ensure its correct and safe use.

Paper Records Used in Addition to Standard Medical Records

Ninety percent of juniors kept a paper ward list, with 56% (51/90) routinely disposing in the confidential waste bin, 46% (47/90) shredding it, but 11% used the clinical and 18% the domestic waste bins (Fig. 3). It is difficult to see an easy alternative to paper ward lists as they are simple to construct and use. However, the risks are high; it is easy to inadvertently take them off hospital premises and easy to lose them in public areas. Furthermore, they are used extensively by other groups of staff such as nurses and allied professions. It can also be debated how far it is practicable to respect patient confidentiality in some circumstances. The use of paper lists is a good example; is the benefit of better coordinated and expeditious care worth the risk of having ones details in the pockets of multiple health professionals? Gudena et al. found that most patients do not object to having their name displayed in hospital either above their bed or on a board at the nurses' station.[6] However, opinion may vary regarding the inclusion of test results and diagnoses on paper lists.

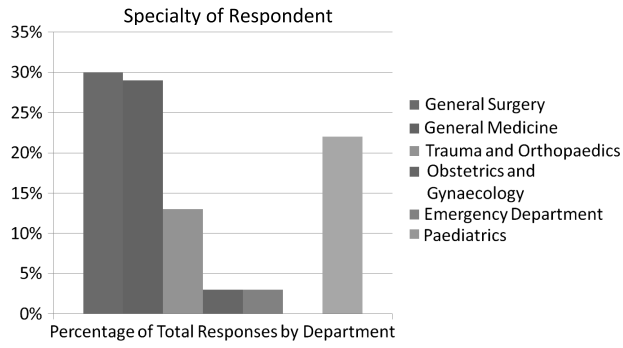

FIGURE 2. Specialty of respondent.

Awareness of Legal and Professional Obligations

Physicians have a duty to be aware of and conform with legislation regarding the use and management of patient identifiable information. There are many guidelines and statutes in this area, but the key ones for most physicians are the Data Protection Act (1998) and the Caldicott Principles contained within the Caldicott Report. The majority of physicians were not aware of the Caldicott Principles (65%) or the role of the Caldicott Guardian (86%), although 58% stated they were aware of the requirements of the Data Protection Act as applied to their duties (Table 1).

CONCLUSIONS

Junior physician's safe usage of patient identifiable information is of paramount importance, with most juniors using portable electronic data storage methods as well as paper ward lists. Often, however, the practice of many juniors falls short of required standards. We suspect that this is not just a local issue and that nationally improved education and vigilance are needed to improve care of data.

The education of junior physicians in this regard is a process, which must begin in medical school, as it is a large and difficult area to cover comprehensively in a Trust employee induction program. Indeed, medical students have the same responsibilities toward data, which they may hold for audits or research projects.

Confidentiality is an area, which is managed heterogeneously by individual NHS trusts.[7] More emphasis needs to be placed on data management in hospital induction procedures for new employees, and security measures, such as encryption software, should be made more widely available.

TABLE 1. Awareness of Legislation

		Percentage of Respondents (n = 100)
1. Are you aware of the Caldicott Principles?	Yes	35%
	No	65%
2. Are you aware of the role of the Caldicott Guardian for the Trust?	Yes	14%
	No	86%
3. Are you aware of the Data Protection Act as it applies to your duties?	Yes	58%
	No	17%
	Unsure	25%
4. Have you sent patient identifiable data over the internet, either to or from a nontrust/non-NHS e-mail address?	Yes	28%
	No	72%

REFERENCES

1. General Medical Council. *Maintaining Good Medical Practice*. London, UK: GMC; 2003.
2. Trivedi D, Joshi M, Hooke R. Information governance: a guide for the foundation year doctor. *Br J Hosp Med*. 2010;71:M130–M131.
3. Mole D, Fox C, Napolitano G. Electronic data protection: procedures need drastic improvement. *BMJ*. 2005;330;53.
4. Data Protection Act Stationery Office, London. 1998.
5. The Caldicott Report. The Department of Health, London. 1997.
6. Gudena R, Luwemba S, Williams A, et al. Data protection gone too far: questionnaire survey of patients' and visitors' views about having their names displayed in hospital. *BMJ*. 2004;329:1491.
7. Palmer R, Cragg R, Wall D. Do junior doctors practise to the UK General Medical Council standards? *Clin Teacher*. 2010;7:32–36.

Patient Identifiable Information Study

We are studying the application of trust policy, the Caldicott Principles and the Data Protection Act among the medical staff. Your assistance is very much appreciated. Please answer the questions as they apply to your current job, unless otherwise stated. This survey is completely anonymous, and honesty is essential. Many thanks.

1. What level doctor are you? (Please circle)
   a. FY1 b. FY2/ST1/ST2 c. ST3+/SPR d. Consultant

2. Which specialty do you work in? (Please circle)
   a. Gen Surgery b. Gen Medicine c. T+O d. O+G e. A+E f. Pediatrics g. Other

○ Do you regularly store names or other patient identifiable information electronically either at work or at home? (other than in regular hospital programs and applications)
   a. Yes b. No

3. If so, where do you store this? (Please circle all that apply)
   a. Hospital computer
   b. Personal memory stick/other portable storage.
   c. Personal computer /laptop that is removed from trust site
   d. Handheld computer
   e. CD/floppy discs

○ If using a hospital computer to store identifiable data, is the data file accessible from a generic (e.g., ward) login, or is your personal login required?
   a. Generic login b. Personal password c. No password required d. Unsure

4. If using a portable storage device, is this password protected?
   a. Yes b. No

○ Do you use the same password for all your logins within the trust and for your personal storage devices?
   a. Yes b. No

5. Do you keep a paper copy of your ward list?
   a. Yes b. No c. N/A

6. Does your ward list include details of patient diagnoses?
   a. Yes b. No

7. If yes to 8, how do you routinely dispose of this after use? (Please circle all that apply)
   a. Shredded
   b. Confidential waste bin (Green bag)
   c. Waste for incineration bin (Yellow bag)
   d. Usual waste bin (Black bag)

8. Are you aware of the Caldicott Principles?
   a. Yes b. No

9. Are you aware of the role of the Caldicott Guardian for the Trust?
   a. Yes b. No

10. Are you aware of the Data Protection Act as it applies to your duties?
    a. Yes b. No c. Unsure

○ Have you sent patient identifiable data over the internet, either to or from a nontrust/non-NHS e-mail address?
   a. Yes b. No

Many thanks indeed for completing this questionnaire.