The Royal College of Surgeons of England

AUDIT

Ann R Coll Surg Engl 2006; **88**: 550–553
doi 10.1308/003588406X117089

Electronic patient data confidentiality practices among surgical trainees: questionnaire study

DAMIAN J MOLE[1], COLIN FOX[2], GIULIO NAPOLITANO[2]

[1]Department of Surgery, and [2]Northern Ireland Cancer Registry, Department of Epidemiology and Public Health, Queen's University Belfast, Belfast, UK

ABSTRACT

INTRODUCTION The objective of this work was to evaluate the safeguards implemented by surgical trainees to protect the confidentiality of electronic patient data through a structured questionnaire sent to Northern Ireland surgical trainees.

PARTICIPANTS AND METHODS A group of 32 basic and higher surgical trainees attending a meeting of the Northern Ireland Association of Surgeons-in-Training were invited to complete a questionnaire regarding their computer use, UK Data Protection Act, 1988 registration and electronic data confidentiality practices.

RESULTS Of these 32 trainees, 29 returned completed questionnaires of whom 26 trainees regularly stored sensitive patient data for audit or research purposes on a computer. Only one person was registered under the *Data Protection Act, 1988*. Of the computers used to store and analyse sensitive data, only 3 of 14 desktops, 8 of 19 laptops and 3 of 14 hand-held computers forced a password logon. Of the 29 trainees, 16 used the same password for all machines, and 25 of 27 passwords were less than 8 characters long. Two respondents declined to reveal details of their secure passwords. Half of all trainees had never adjusted their internet security settings, despite all 14 desktops, 16 of 19 laptops and 5 of 14 hand-helds being routinely connected to the internet. Of the 29 trainees, 28 never encrypted their sensitive data files. Ten trainees had sent unencrypted sensitive patient data over the internet, using a non-secure server.

CONCLUSIONS Electronic data confidentiality practices amongst Northern Ireland surgical trainees are unsafe. Simple practical measures to safeguard confidentiality are recommended.

KEYWORDS

Electronic data – Confidentiality – Surgical trainees – Questionnaire

CORRESPONDENCE TO

Mr Damian J Mole, Research Fellow, Department of Surgery, Queen's University Belfast, Grosvenor Road, Belfast BT12 6BJ, UK
T: +44 (0)2890 632558; F: +44 (0)2890 321811; E: damianmole@doctors.org.uk

The NHS National Programme for Information Technology (IT) aims to develop, procure and implement modern integrated IT infrastructure and systems for all NHS organisations by 2010.[1] Protecting the confidentiality of the personal, non-anonymised data as part of this programme is of paramount importance. A breach in the confidentiality of any patient database would have wide-spread repercussions on public trust. In a survey commissioned by the National Programme for IT to gauge the views, expectations and concerns of the public about electronic patient records, one of the highest priorities for potential patients was information and re-assurance regarding data security and confidentiality.[1] In light of this, we explored the standards of IT security among surgical trainees, in particular the measures taken to safeguard patient confidentiality when handling electronic personal data.

Participants and Methods

The Office of Research Ethics Committees (Northern Ireland) advised that ethics committee approval was not required for this audit. DJM is registered with the Information Commissioner under the *Data Protection Act, 1988*.

Subjects and questionnaire

All basic and higher surgical trainees attending a Northern Ireland Association of Surgeons-in-Training meeting were invited to complete a structured questionnaire designed to evaluate the confidentiality protection measures taken when handling electronic patient data.

Data analysis

Chi-squared testing (Fisher's exact test when expected cell values < 5), and Mantel-Haenzsel common odds ratio analysis

Table 1 Registration under the Data Protection Act, 1988

	Yes	No	Unsure
Number of subjects regularly involved in audit or research	26	3	–
Number who store patient data on a computer or related device	26	0	–
Number registered with the *Data Protection Act, 1988*	1	28	–
Number of subjects whose supervisor is registered	1	–	–
Number who have a fellow researcher registered	1	–	–
Number where any member of the team is registered	2	1	26

were used to analyse confounding factors including differences related to grade and time elapsed since qualifying from medical school using the Statistical Package for Social Sciences (SPSS) v.12.0 for Windows.

Results

Thirty-two trainees were invited to participate, of whom 29 returned completed questionnaires (91% response rate). Two responders declined to answer questions relating to the characteristics of their secure passwords.

Table 1 shows the extent of registration with the Data Protection Act amongst trainees actively involved in audit or research involving patients. Table 2 shows the use of different types of computer for research or audit involving patients. Table 3 shows awareness, knowledge and behaviour of trainees towards computerised patient data security. Figure 1 shows the distribution of password length amongst subjects.

Northern Ireland graduates were more likely than graduates of other medical schools to use more than one computer (chi-squared, 10.5; 3 d.f.; $P = 0.014$). Higher surgical trainees were less likely to use figures and numbers in their

Table 2 Internet connection and security by computer type

	Hand-held PC/Palm	Own laptop	Home desktop	Personal work desktop	Communal work desktop
Number of trainees regularly using this type of computer	14	19	26	2	15
Number of these machines connected to the internet	5	16	26	2	14
Number of machines where user has adjusted the firewall	5	8	14	1	7
Number of machines which force password logon at each use	3	8	8	1	9

Table 3 Measure to maintain patient data security taken by individual trainees

	Yes	No	
Do you have an array of passwords for different machines?	13	16	
Do they always contain letters and figures, *e.g.* boris69egg?	16	11	2 subjects declined to answer
Do you have any further security measures enabled?	1	28	1 subject enabled fingerprint ID scanning
Do you routinely encrypt your data files?	1	28	
Would you know how to encrypt your data files?	7	22	
Do you ever take digital photos of operations, wounds, X-rays, *etc.*?	20	9	
If so, do you routinely encrypt your photo files?	1	28	
Have you ever sent patient data over the internet?	10	19	

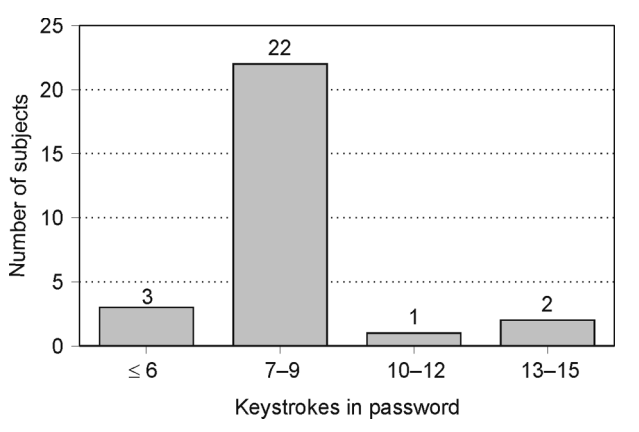

Figure 1 Distribution of password length.

secure passwords (Mantel-Haenzsel common odds ratio estimate, 0.1; 95% CI 0.0–1.0; $P = 0.048$). Higher surgical trainees recorded more work-related digital images than basic surgical trainees (Mantel-Haenzsel common odds ratio estimate 6.0; 95% CI 1.1–33.8; $P = 0.041$). Subspecialty interest within surgery had no statistically significant bearing on any dependent variable in the analysis.

Discussion

This study reveals serious deficiencies in electronic data safety practice in Northern Ireland which potentially have legal and practical implications.

Electronic patient data confidentiality and the law

We observed that nearly all surgical trainees stored non-anonymised personal data relating to patients on computers, but that only one was registered with the *Data Protection Act, 1988*. Under UK law, it is likely that any doctor or health-related practitioner who has input into the analysis, presentation and publication of a piece of research or audit, should be registered with the Information Commissioner.[2] Further details regarding notification or registration may be accessed at <www.informationcommissioner.gov.uk>. Under European Parliament and Council Directive 95/46/EC of November 1995 (*Protection of Personal Data*), data controllers must, by law, implement appropriate measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access.[3]

Four key areas of data protection were addressed by this study, namely user authentication, the securing of data by encryption, electronic data shredding and internet security.

User authentication

Of particular concern in this survey was the failure to implement simple password logon requirements. In our study, portable devices (hand-helds and laptops) were less well protected than desktops at home or work, yet these devices are most likely to be mislaid, stolen, or left unattended in the operating department changing room, or at a patient's bedside.[4] The requirement of communal desktops at work to force a password logon in 60% of cases is probably a reflection of a centralised IT administration policy. Even so, this proportion should be 100%. Where used routinely, passwords were too short, and frequently did not contain both letters and figures.

Biometric logon to enhance security

One solution is to adopt biometric logon technology such as a fingerprint. Fingerprint sensors can be embedded in the mouse or keyboard of the computers, and are available as USB plug-in devices. Biometric logon systems are not fail-safe, however, and we have experimented with techniques that can be used to fool fingerprint sensors. In the NICR, we were able to 'resuscitate' fingerprint images, left on the sensor's surface as fat deposits, by breathing on them. Wiping the sensor clean after every use is recommended.

Securing of data by encryption

In our study, only one respondent routinely encrypted sensitive files, and the majority of trainees did not know how to. If unauthorised people by-pass the username, password and biometric logon to gain access to encrypted file, it can not be deciphered without first obtaining the primary user's private key. If a different user needs to access the data for business continuity, a recovery agent can decipher the file to make it readable by the new user, with appropriate authorisation.

Electronic data shredding

Electronic data shredding is crucial for the preservation of data confidentiality. Confidential data stored on a disk disappear only when the disk is physically destroyed or new information is written over the file. Overwritten files can still be read by specialised techniques, such as those used by data recovery agencies, companies and researchers. True electronic data shredding must be achieved by more complex overwriting procedures. In the NICR, we have designed and developed a simple piece of software that achieves that target, in accordance with guidelines developed by the University of Auckland, New Zealand.[5] The software specifies the number of deletion 'passes' they wish to perform to 'clean' a disk. Removable disks may be then reclassified as 'safe in the internal environment' or 'safe to be re-deployed'.

Internet security

Alarmingly, in this study, we observed that a substantial proportion of trainees sent sensitive, non-anonymised,

personal data over the internet, through non-secure servers. Nearly all machines storing sensitive data were connected to the internet for extended periods of time without activation of simple electronic defences. This highlights the erroneous perceptions of the public and the practitioner regarding security in medical IT and in the internet in general. The wide-spread belief that computerised records are more secure,[6] or at least as secure as paper records, results in overconfidence.[7] In a survey presented in *makingITwork*,[1] potential patients felt equally comfortable booking an out-patient appointment by e-mail (which is highly insecure), compared to using a secure internet site, similar to those implemented by online banking providers. Wireless networking, including BlueTooth™ technology poses even greater potential problems, as remote access of unencrypted confidential data is possible without physical proximity.

The inadequate IT security practised by this group is disturbing enough to warrant remedial action through education and training. We have already begun to implement medical IT security training through the postgraduate education programme, and will re-assess data protection practice after this training.

Conclusions

Electronic data confidentiality practices amongst Northern Ireland surgical trainees are unsafe. Existing password protection should be enhanced and consideration given to implementing biometric logon systems. Files containing sensitive data should be routinely encrypted. Magnetic and solid state computer storage devices (including hard disks, floppy disks, CD-ROMS, DVD-ROMS and memory sticks) should undergo routine physical or electronic data shredding after their final use. Educational programmes to improve IT security should be implemented.

Acknowledgements

Damian Mole had the original idea for the study, designed and distributed the questionnaire, analysed the data, co-wrote the paper and approved the final version of the manuscript. Colin Fox and Giulio Napolitano designed and implemented the changes in IT security at the NICR, co-wrote the paper and approved the final version of the manuscript.

No specific funding was sought or allocated for this work. All authors declare that they have no competing interests with the publication of this work.

This paper was given as an oral presentation at the Association of Surgeons of Great Britain and Ireland Annual Scientific Meeting, Best Practice, Glasgow, 2005.

We are grateful to Estelle Askew-Renaut, EU Legal Advisor, The AIRE Centre, for directing us to the relevant EU legal information sources and for advice regarding the manuscript. We thank Mr Mike Stevenson, medical statistician, Royal Hospitals NHS Trust, Belfast for his statistical advice and comments on the manuscript.

References

1. National Program for Information Technology. *MakingITwork*. 2004. <http://www.dh.gov.uk/assetRoot/04/07/71/57/04077157.pdf>.
2. The Information Commissioner's Office. 2005. *Do I need to notify?* <http://www.informationcommissioner.gov.uk/eventual.aspx?id=2662>.
3. European Parliament and Council Directive 95/46/EC <http://www.europa.eu.int/scadplus/leg/en/lvb/114012.htm>.
4. Al-Ubaydli M. Handheld computers. *BMJ* 2004; **328**: 1181–4.
5. Gutmann P. *Secure Deletion of Data from Magnetic and Solid-State Memory*. <http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html>.
6. Coombes R. GPs worried about having to change to new untested software systems. *BMJ* 2004; **328**: 1157-a-.
7. McAlearney AS, Schweikhart SB, Medow MA. Doctors' experience with handheld computers in clinical practice: qualitative study. *BMJ* 2004; **328**: 1162.