Patient Confidentiality — At Risk from NHS Wide Networking

Dr Ross J. Anderson, C.Math., C.Eng.
Cambridge University Computer Laboratory
Pembroke Street, Cambridge CB2 3QG
Email: ross.anderson@cl.cam.ac.uk
Web: http://www.cl.cam.ac.uk/users/rja14

1 Introduction

The NHS is building a network to link up Britain's medical computer systems. The original motive was to transmit administrative data, but the system is now being promoted as a channel for clinical information as well. The claim is that this will enhance the quality of care afforded to patients, by improving communications in a number of ways:

- messages such as referrals and path lab reports will get to the addressee within minutes rather than days and will be less likely to get lost;
- videophones will enable remote consultation with specialists and thus save both patients' and consultants' travelling time;
- central collation of medical records will help clinical auditors and medical researchers evaluate the effectiveness of different treatments.

The available descriptions of the network are still somewhat confused[1], but we shall focus here on the NHS claim that that security worries about the Internet leave it no choice but to construct a private network[2], and the security documentation which has been made available to date.

2 Threats to Patient Confidentiality

Many organisations, in both the public and private sectors, have replaced dispersed manual record keeping systems with centralised or networked computer systems which give better access to data. Their experience is that the main new threat comes from abuse by insiders.

[1] these range from a pure X.400 EDI messaging system, through an Internet type service supporting TCP/IP and worldwide web, to a high-speed system supporting videoconferencing

[2] Dr G Winyard, letter to Dr EM Armstrong, 5th August 1995

For example, most of the big UK banks now let any teller access any customer's account. The effect, as widely reported in the UK press last year, is that private eyes get hold of account information by bribing tellers and sell this information onwards for £100 or so [1].

This could have been expected. The likelihood that information will be improperly disclosed depends on two things: its value, and the number of people who have access to it. Aggregating records into a large system increases both these risk factors at the same time.

In the days of paper records, a private detective who wanted access to your bank account had to suborn someone at your own bank branch — a large risk for a usually small reward. However, once a computer network links all the branches together, you may find that instead of fifty people having access to your account there are fifty thousand. If a private investigator can suborn any one of them, he can look at the finances of perhaps ten percent of the population. Computerisation made it both attractive and feasible to invade banking privacy.

Health systems are not likely to be different. At present, security depends on the fragmentation and scattering inherent in manual record systems; removing this without introducing effective compensating controls is highly irresponsible. We have already seen press reports of health records being available through private detectives for £200 [1], and abuse of both prescription systems [2] and research records [3]. Perhaps the most serious reported case is that of 'Dr Jackson', the Merseyside sex stalker, who wins the confidence of young women by discussing their family medical history over the telephone, urges them to examine themselves, and then tries to arrange meetings. In one case, a 15 year-old girl agreed to meet him, but bolted when he asked her to get into his car. Police believe that he is a health worker or a computer hacker [4].

Now the current networks are local — limited perhaps to a single FHSA or part of a region. Linking them into a national network will greatly increase the potential for mischief. This is confirmed by the experience of the USA, where networking has advanced somewhat more than in Britain.

- a banker on a state health commission had access to a list of all the patients in his state who had been diagnosed with cancer. He cross-referenced it with his client list and called in the patients' loans [5];
- a 1993 Harris poll on health information privacy showed that 80% of respondents were worried about medical record privacy, and a quarter had personal experience of abuse [6];

- Forty percent of insurers disclose medical information to lenders, employers or marketers without customer permission [7]; and over half of America's largest 500 companies admitted using medical records to make hiring and other personnel decisions [8];

- Eli Lilley has gained access to a database of prescriptions for 56 million people by purchasing PCS Health Systems for $4 billion. It now plans to trawl the database for patients whose prescriptions suggest that they might be suffering from depression manifested as several other minor illnesses, such as backaches and sleeplessness, and try to get their doctors to prescribe them Prozac [9].

The problem was studied by the US government's Office of Technology Assessment, which confirmed that the main threats come from insiders rather than outsiders, and that they are exacerbated by the data aggregation which networked computer systems encourage [10].

We can live with a situation in which GPs' support staff have access to the clinical casenotes of that practice's patients; but one which gave staff access to the records of everyone in the country would be a disaster. Unless networked systems have better security, we can expect systematic erosion of privacy by commercial interests, as well as a number of quite unpleasant incidents like the Jackson case.

3 The NHS Security Proposals

The NHS has produced a number of documents on the security of the new NHS wide network. Unfortunately, they do not acknowledge the aggregation threat at all. Their document on threats and vulnerabilities [11] considers that the main additional risk is that user and network management failings may expose the network to outside 'hackers', and this misapprehension in turn drives an erroneous security policy [12] [13]. It is an adaptation of the 'multilevel' policy used by the military, and classifies medical information at four levels:

HIGHLY SENSITIVE
SENSITIVE
NONSENSITIVE
OPEN

Here, 'highly sensitive' means AIDS databases, 'sensitive' means other patient identified clinical records and 'nonsensitive' means accounting information. The main controls are placed between 'sensitive' and 'highly sensitive' (the latter systems will not be networked at all), and between 'nonsensitive' and 'open'.

The effect of adopting this policy model, with its horizontal security boundaries, is that all doctors would have to be cleared to view material classified as 'sensitive' and would thus have access to every patient record in the country.

This is at odds with the NHS' own draft guidelines on confidentiality, which include the 'need-to-know' principle [14]. This principle was elaborated by Dr David Bellamy, DoH principal medical officer, as

> It is a commonly held view ... that I as a doctor can discuss with another doctor anything about a patient because a doctor has a duty to maintain confidentiality by reason of his ethical obligations. It is just not true and it no longer holds water. Even if it helps professionals discussing individual patients with their colleagues, they must discuss only on the basis of the information the colleague needs to know [15].

There is another serious problem with the NHS proposals. They would isolate the NHS network from the Internet by means of a data pump — a firewall which will let data in but not out[3]. This would stop doctors replying to electronic mail from people who are not NHS employees, such as patients, research scientists and doctors overseas. It would also prevent doctors from using the world wide web's resources on a wide range of medical problems, from the spread of HIV and the Ebola virus through the latest research on a growing number of diseases [16]. This is not likely to be tolerated by the profession for long; it is comparable to insisting that doctors' telephones be prevented from initiating calls to non-NHS telephone subscribers.

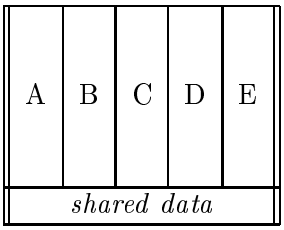
4 What is Needed

The real security requirement is to prevent information flows 'across' the system, rather than 'down' as in the military model. This is called 'compartmentation' and is widely used in the intelligence community; a controller

[3]Note of Meeting on NHS Network, held on Friday 4 August 1995, at the Department of Health

must not be able to see the records of another controller's agents, and similar rules are enforced on signals intelligence and satellite photographs.

A compartmented security architecture keeps most of the information within the department (or practice) in which it is generated, and lets only a closely defined subset be shared with other departments:



Only a compartmented architecture has a reasonable prospect of securing networked healthcare systems; but compartmentation is so tied up with the application detail that most of the control mechanisms need to be embedded in the end user system rather than in the network. The intelligence community has developed 'compartmented mode workstations' for this purpose; the healthcare informatics community will have to develop its own solutions. Data items need to be tagged so that the system can distinguish, for example, between a normal record which can only be sent to another clinician involved in the patient's care, a prescription which can be sent to a pharmacist, and an especially sensitive note which cannot be shared at all.

There are many details which need to be worked out, such as the controls needed when one practice requests a set of notes from another; the mechanisms to supply researchers and clinical auditors with anonymised records [17]; the restrictions on what may be given to administrators, social workers, policemen and insurers; the supporting physical security measures; rules for data backups held offsite; procedures for accrediting and auditing systems; and how archives can be kept in such a way that they can be relied on in evidence in court [18].

Many of these problems require better agreement on the format of the electronic patient record; even once we have this, the security issues are surprisingly complex [19], and it will take a lot of work to get a security policy on which the health professions, the equipment suppliers and NHS management can agree. There will then be a long process of educating system vendors to build the required features into their software; evaluating their product offerings; setting up the infrastructure to manage authentication; and developing training courses for users and auditors.

5 Conclusion

NHS wide networking has been attacked as a serious threat to patient confidentiality [20]. We have explained the nature of the problem, which has been brought about by the failure of the NHS Information Management Group to get its threat model and security policy right.

The situation can be rectified, but this will take both money and time, and the NHS Executive has made clear that in intends to press ahead regardless with its current proposals[4]. A charitable explanation would be that administrators are ill-advised, and sincerely believe that the problems are minor and can be fixed later.

However, the test 'cui bono?' (who benefits?) suggests another explanation. The main practical effect of the proposed security policy is to support a code of connection which will prohibit doctors from having any competing links to the outise world [12]. Given that the network will be provided by a commercial company and the costs recouped by user charges, this must be worth a lot of money. So one cannot help feeling that 'security' policy is motivated at least in part by a desire to justify, and to enforce, a monopoly over the provision of data networking services to the clinical professions.

References

[1] Luck N, J Burns, Your Secrets for Sale. The Daily Express 1994 Feb 16:32–33

[2] Anonymous, Nurse Jailed for Hacking into Computerised Prescription System. British Journal of Healthcare Computing and Information Management 1994;1:7

[3] Wilkins E, Consultant Accused of Inventing Details of Pioneering Operation. The Times 6 Jun 1995

[4] Thomas M, Sex Stalker Plays Doctor to Trick Victims. PA newswire no 1236, 1995:July 7

[5] Anonymous, RMs need to safeguard computerised patient records to protect hospitals. Hospital risk management 1993;9(Sep):129–140

[6] Gostin LO, J Turek-Brezina, M Powers et al., Privacy and Security of Personal Information in a New Health Care System. Journal of the American Medical Association 1993;20(24/11/93):2487–2493

[7] Anonymous, Who's reading your medical records?' Consumer Reports 1994 (Oct):628–632

[4] Winyard's letter cited above

[8] Levine Is your health history anyone's business? McCall's Magazine 1995 Apr:54. Reported by M Bruce on Usenet newsgroup comp.society.privacy, 22 Mar 1995

[9] Seecof M, Marketing use of medical DB. Usenet newsgroup comp.risks 1995;17.12

[10] Herdman RC, Protecting Privacy in Computerized Medical Information. Office of Technology Assessment, US Government, 1994

[11] Hayes S, NHS-Wide Networking Threats and Vulnerabilities. NHS document NWNS T1.22 version 1.0, 5/4/95

[12] Anonymous. NHS-Wide Networking: Data Security Policy. NHS document NWNS T3.3 (1994/5)

[13] Hilton J, S Hayes, J Stranger et al., Security Guide for IM&T Specialists. NHS document NWNS T5.11, 3/4/95

[14] Boyd N, Draft Guidance for the NHS on the Confidentiality, Use and Disclosure of Personal Health Information. NHS consultation document, 1994

[15] Griew A (ed), Proceedings of a Workshop — Confidentiality: Discussing Current Initiatives. Institute for Health Informatics, University of Wales, 1995

[16] Pallen M, A Guide to the Internet for Medical Practitioners. British Medical Journal. In press.

[17] Boe E, Pseudonymous Medical Registries. Norwegian Official Report 1993:22

[18] Anderson RJ, Liability and Computer Security: Nine Principles. Proceedings of Computer Security — ESORICS 94, Springer Lecture Notes in Computer Science v 875:231–245

[19] Griew A, R Currell, A Strategy for Security of the Electronic Patient Record. Institute for Health Informatics, University of Wales, Aberystwyth, 1995

[20] Anderson RJ, NHS-wide networking and patient confidentiality. British Medical Journal 1995;6996(1/7/1995):5–6