NHS Wide Networking and Patient Confidentiality

Britain seems headed for a poor solution

The NHS is spending a nine figure sum on building a nationwide computer network, with the aim of making access to administrative and health records easier. For example, if a patient from another part of the country comes into the surgery complaining of abdominal pain, states that it is a recurrence of a chronic complaint but is unable to say what, then online access to his records would be convenient and might occasionally save life.

However, wider access brings with it a problem which the NHS has ignored — the threat of aggregation. At present, hospitals make do with relatively little security; after all, there are not many people who will walk into a ward and steal a file from the note trolley. But once the records are aggregated into a database covering tens of millions of patients, it will be a major target for data thieves, blackmailers and others with less than altruistic motives. Evidence for this comes from the military, the banking industry and the American health care system.

Firstly, soldiers know that if you gather a lot of information together, the collection may be much more sensitive that the individual items. Thus the Pentagon may occasionally release a satellite photograph to make a point, but they would never publish their whole collection as this would show its technical capabilities and the history of its intelligence priorities.

Secondly, the banking industry discovered the threat of aggregation the hard way. Thirty years ago bankers kept their records on paper, and customers' financial affairs remained private. But now that every teller can access every customer's account through a computer network the privacy is gone: when thousands of people have access to information some of them will always be prepared to sell it for cash. Last year, newspapers showed how banking records could be bought for a few hundred pounds [1]; even cabinet ministers and the head of MI5 were successfully targeted.

Thirdly, the USA has gone much further in building healthcare networks than the NHS, and the problems are starting to become apparent to doctors and patients there. For example, a banker who sat on a state health commission accessed a list of people who had been diagnosed as having cancer and promptly called in their loans. The records of sports and political personalities are regularly accessed by the curious, and a Harris poll in 1993 found that a quarter of all respondents had experienced improper disclosure of their medical information [4].

On the level of institutionalised abuse, prescription records are being used extensively for marketing purposes; 40% of US insurers now disclose medical records to third parties, such as employers; and fully half of the largest 500 companies admit to using medical records in hiring decisions, under the excuse of managing the costs of healthcare [4]. In fact, the largest medical information network under construction in the United States is being built by Equifax, a credit reference agency.

Wide and slippery slope

The NHS is rushing headlong down this wide and slippery slope. It proposes to grant network access to the 'extended NHS community' — officialese for social workers, insurance companies and the police. The proposed control is that they will sign a 'Code of Connection', a declaration that they will behave themselves; but this is backed neither by a credible security policy nor by the prospect of punishment for transgressors.

So we could shortly find ourselves sharing the Americans' problems. In fact, we could be even worse off, because of Britain's combination of a centralised health service, privatised data centres, and the fact that selling private records is not a criminal offence here (as it is in Germany).

It is not inevitable that computers will destroy privacy in medicine. While Germany tackled the problem with legislation, other states are using technical measures: Quebec has developed a record which patients carry around with them in a smartcard. This has five different zones — identity, emergency, vaccinations, drug treatment and the full medical history — and each health care profession can only access the zones it needs. This project has been judged a success and of special benefit to the elderly and the chronically ill [5]. Meanwhile, an EC project has developed encryption software which enables medical records to be transmitted safely over insecure networks[6]; and encryption software is now available for free [7].

The NHS has a long way to go to catch up. It has conceded that databases on patients with AIDS should not be connected to the network, but HIV status is not the only sensitive medical fact; contraceptive status is another, and the mere suggestion of a psychiatric problem may render a person uninsurable [8]. No easy way exists, however, to predict what is sensitive: adherents of some religions might consider even a blood transfusion to be profoundly shameful.

Once medical records become endowed with the power to cause great harm there will be strong incentives to alter them. Not only will patients try to gloss over unpleasant facts but we may even see companies offering to sanitise medical files — just as there are companies which "repair" credit ratings. The reliability of records will become suspect, with obvious consequences.

One way or another, the proposed network falls far short of reasonable standards; its security would not be acceptable in other government departments, or, for that matter, in industry. No doubt a carefully designed network could save costs and improve patients' care; but the profession should not be rushed into installing a poorly designed system with considerable potential to do harm instead.

ROSS ANDERSON
Senior Research Associate

Computer Security Group
Computer Laboratory
University of Cambridge
Cambridge CB2 3QG

References

[1] Luck N, Burns J. Your secrets for sale. *Daily Express* 1994 Feb 16:32–3.
[2] Rufford N, Leppard D, Chittenden M. How £200 can buy bank account details. *Sunday Times* 1992 Nov 29:1,3.
[3] Bartlett ED. RMS need to safeguard computerized patient records to protect hospitals. *Hospital Risk Management* 1993;15:129–33
[4] Who's Reading Your Medical Records?" *Consumer Reports* 1994 Oct:628–32.
[5] Quebec healthcard evaluation almost finished. Card World Independent 1995 May:4–5
[6] Bleumer G. Security for decentralized health information systems. *International Journal of Bio-Medical Computing* 1994:35(supp):139–45
[7] Schneier B. *E-Mail Security — How To Keep Your Electronic Messages Private.* New York: John Wiley and Sons, 1994.
[8] Bass A. Insurers spurn anyone in therapy. *Boston Globe* 1995 Apr 3:25.

BMJ volume 311 no 6996 1 July 1995 pp 5–6

This article was processed using the LaTeX macro package with LLNCS style