Information technology in medical practice: safety and privacy lessons from the United Kingdom

Ross J. Anderson, MA, PhD, FRSA, CEng, CMath

University of Cambridge Computer Laboratory
Pembroke Street, Cambridge CB2 3QG, UK

1 Introduction

The previous UK government's strategy for managing information technology in healthcare caused serious safety and privacy problems, which led to a government review of healthcare computing that advocated some seemingly quite radical changes. Here I offer a personal view of what went wrong, as an engineer with a background in both safety critical systems and computer security, and who has been involved in advising the British Medical Association (BMA) on the safety and privacy of clinical information systems.

It is well known to engineers that one learns more from systems that fail, so let me first give some concrete examples of serious safety and privacy failures.

2 Safety failure – an example

One of the best known safety failures was the collapse of the London Ambulance Service on 26–27 October and 4 November 1992. The London Ambulance Service covers an area of 600 square miles and deals with 1500 emergency calls per day. The overload and collapse of a new computerised despatching system left London with partial or no ambulance cover for extended periods, and is believed to have led to the loss of about 20 lives.

The report of the official inquiry that followed [1] is a catalogue of management incompetence: poor planning, wishful thinking, unwillingness to heed warnings, reliance on 'cozy assurances' from suppliers, and a transition to an unstable system with no provision for reversion to manual working in the event of disaster. For example, the Service ignored an independent review in March 1992 which pointed out the need for a documented implementation strategy, proper change control and volume testing; but despite problems with several components of the system (including uncertainty about the effectiveness of automatic vehicle location, inadequacies of staff training and commitment, and problems with data transmission to and from mobile terminals) its chief executive claimed that *'there is no evidence to suggest that the full system software, when commissioned, will not prove reliable'*.

When the system went live, it could not cope with the volume of calls and broke under the strain. The transition to a back-up computer system had not been properly rehearsed and also failed. As often with management failures, there was a political angle: the Service was attempting to use the new system to change ambulance staff's working practices without consultation in a climate of poor industrial relations.

3 Privacy failure – an example

The Hampshire hospital system provides a good example of the failure to fully address privacy issues raised by information technology in the National Health Service (NHS). Because the then health minister held the constituency of Winchester (in Hampshire), new information technology systems were implemented more quickly there than elsewhere. These new systems had the feature that all laboratory tests ordered by general practitioners were entered into a hospital information system, which made them available to all staff on the wards and to consultants in the outpatient department. The stated goal was to cut down on duplicate testing; but the effect was that even highly sensitive matters such as HIV and pregnancy test results were no longer restricted to a handful of people (the general practitioner, practice secretary, the pathologist and the lab technician), but were widely available.

As with the London Ambulance Service, a timely warning of impending disaster was ignored, and the system duly went live on schedule. A nurse who had had a test done by her general practitioner complained to him after she found the result on the hospital system at Basingstoke where she worked; this caused outrage among local general practitioners and other medical staff, and may have contributed to the health minister's loss of his seat at the 1997 general election. The eventual outcome was that the relevant parts of the system were turned off at some hospitals.

4 Why do these failures happen?

It is my observation that many of the safety and privacy failures within the health system that have recently alarmed doctors and public in the UK can be traced to the civil service culture of the NHS's computing organisation, which tackles projects in a completely different way from private sector companies that develop safety critical systems for air traffic control, nuclear plant management and motor vehicle electronics. The private sector operates on the basis that successful system construction and operation requires a high degree of openness between users and developers. This is vital to communicate effectively about what precisely is required, what sort of failures have occurred or are likely to, and how the resulting risks can be managed. Systems must also support operational openness, so that there is constant feedback about what errors have occurred, and provide for mutual vigilance.

Perhaps the textbook example of safety culture is air traffic control, which is documented (for example) by Shapiro et al [2]. Here, controllers and chiefs work together in a highly cooperative way, sharing information resources and keeping an eye on each others' work (as well as the work of controllers and chiefs in neighbouring airspace sectors). The philosophy is that everyone makes mistakes, so it is vital that as many of these as possible should be caught by others, without egos getting in the way. A good controller is not just one who spots and points out others' mistakes but who, when he spots a mistake he himself has made, admits it at once and corrects it publicly. There is a continuous effort to maintain openness and honesty; the controllers who are failed are those who, having made a mistake, try to put it right quietly and incrementally.

By contrast, the UK civil service culture is one of secrecy and blame shifting. This is particularly evident in the NHS's attempts to deal with the 'Y2K' problem (the 'Year 2000' problem, or 'millenium bug') – the fact that many systems record the year in two digits only and will break down when first confronted with a date after the turn of the millenium. For example, many of the transfusion pumps used in the NHS will fail; they are set to become inactive if more than six months has passed since they were last serviced, and the date used to measure this is only two digits [3].

It is interesting to compare the responses of the British and Dutch health services to this problem. The Dutch made a thorough study of one hospital, coming up with 9000 items that needed fixing; this information was then shared with other hospitals. In Britain, on the other hand, the NHS Executive has been sending out regular circulars since 1996 telling hospital trust chief executives that although there may be a problem, it is up to them to solve it without any help, or extra budget, from the centre. The government body with a statutory responsibility for the safety of things like transfusion pumps, the Medical Devices Agency, takes the following line: *'MDA believes that it would be irresponsible to set up any sort of general clearing house for information, since we could not verify information on numerous models and their possible variants, and it would be irresponsible to disseminate unverified claims that particular models are year 2000 compliant'* [4].

Vendors of computer-driven equipment are generally reticent about problems, despite the fact that Section 6 of Britain's Health and Safety at Work Act holds suppliers of equipment liable to warn customers of any potential hazards. In addition, most hospital managers refuse to let staff identify defective equipment to colleagues in other hospitals, for fear of legal action by suppliers should this warning prove incorrect. As a result there is a massive duplication of testing effort. Current unofficial estimates of the likely cost of failing to deal with the Y2K problem range from 600 to 1500 lives (lost through failures of medical equipment, radio systems used by ambulances, databases containing vital medical records) and up to GBP 600 million [5]. This assumes that there will be no significant failures of electricity distribution, transport systems and other critical infrastructure, the risk of which leaves us with an urgent need for coordinated contingency planning and supply chain management and little time in which to do it.

Of course, the London Ambulance Service and Y2K problems are only the most dramatic manifestations of an inappropriate culture leading to safety failure. There are many others, notably in hospital records and in the management of recall programs for cervical cancer screening [6,7].

5 Cultural problems with privacy

The NHS habit of conceiving systems without user consultation, using them to push through administrative changes sought on cost reduction grounds and, if need be, even dissembling about their goals and basic functionality, has led to privacy failures too. For example, the Hospital Episode System (HES) is a central government database used for planning purposes which records the nature and cost of every episode of hospital care, whether inpatient or outpatient, in the NHS. When the British Medical Association asked whether this would make personal health information available without consent to administrators, senior officials stated categorically that the data in HES would not only be non-identifiable but also non-linkable; that is, it would not be possible to link up successive hospital stays (or courses of outpatient treatment) for the same patient. This assurance was repeated on a number of occasions in public, including conferences and radio programs.

However, one of the statistics required in efficiency monitoring is a hospital's readmission rate: a hospital that discharges appendix patients after four days rather than a week will not save money if a quarter of them are back on the ward within a month. But how could readmission rates be computed if the data were not linkable? It transpired that records were only de-identified to the extent that the patient's name was replaced by their postcode plus their date of birth. This 'de-identification' scheme is ineffective for the 98% or so of British residents whom it identifies unambiguously and gives misleading results for the 2% where ambiguity arises – typically students, soldiers, prisoners and the homeless, who do not have fixed postcodes. These groups generate highly atypical healthcare statistics, and miscounting them can introduce serious errors into predictions based on statistical methods such as capture-recapture. It is thus objectionable from both privacy and safety points of view, and much inferior to the properly designed de-identification methods used by private sector healthcare informatics firms.

There are many other central systems under development which pose privacy problems, and it was these which spurred the medical profession into open revolt during 1995 and 1996. This not only involved acrimonious exchanges in the media, but also a medical boycott of a data network that the NHS wanted to introduce and which would have been used, inter alia, for centralised data collection of personal health information for management and other purposes. This revolt is merely dormant during the new Labour government's honeymoon period, and could break out again at any time.

6 The Caldicott Report

The previous government attempted to defuse the privacy row by setting up a committee under Dame Fiona Caldicott to consider the non-clinical uses of medical records. She identified dozens of systems, either fielded or under development, which share personal health information with administrators and others who are not involved in the patient's care. This committee did not include anyone with expertise in computer security.

Its main recommendation was that data should be de-identified by replacing the patient's name and address with an NHS number (the postcode and date of birth are also to be retained). As virtually everyone involved in patient administration will need to be able to link names with numbers, the NHS is building a tracing service which will enable names to be found from numbers and vice versa. So the privacy problems will become worse rather than better. The tracing service has had significant teething problems, with millions of pounds wasted on systems that do not work. If it eventually does work, it will provide a history of each patient's associations with healthcare providers. This appears to conflict with the Human Fertilisation and Embryology Act, which prohibits staff at fertility clinics from disclosing any information which might identify any person born as a result of in-vitro fertilisation; the fact of a woman's registration with such a clinic before the birth of a child will become widely visible throughout the NHS. There will be similar problems with mental health and sexually transmitted diseases. (The Caldicott committee should also have included a lawyer.)

7 The nub of the problem

One can describe the essence of the privacy problem brought about by the previous government's strategy as follows. The likelihood that unauthorised use will be made of information is a function of its value and the number of people who have access to it; and consolidating valuable private information, such as medical records, into large databases increases both of these risk factors simultaneously. We can live with the occasional disclosures that result from abuse of record access by general practice staff, but we could not accept a situation in which the staff of all 36,000 general practices had access to the records of all 56,000,000 patients in Britain. Yet it is precisely this broad access to huge databases that is being deliberately engineered in many NHS systems.

Centralising data also brings safety problems in its wake, both directly and indirectly. Large centralised systems may fail less often, but when they do break down the results can be much more serious. For example, it is proposed to use an NHS-wide network to book hospital appointments. If this were to be implemented, and the network were to fail, we could lose the whole machinery of hospital waiting lists.

8 What is to be done?

The British Medical Association's response to these problems, following wide professional consultation, was to develop the 'Blue Book', a security policy for clinical information systems (available for free both on the net and in paper form from the British Medical Association in London) [6]. The Blue Book sets out system design and administration principles which, if followed, ensure that personal health information is not shared without patient consent, except in the case of statutory exemptions. It is a conservative document, seeking to encapsulate accepted good paper records practice into systems language. Its recommendations have been implemented in a general practice, and in a hospital system now used at three sites (Hastings, Aintree and Exeter) [8].

This exercise showed that ethical computerisation of hospitals and medical practices was no problem, but what about the secondary uses of medical records, as in research, clinical audit, quality management and administration generally? In June 1996, the BMA reached an agreement with commercial providers of health data (such as the firms which buy data from hospitals and sell back performance statistics) would carefully ensure that no personal health information supplied by a provider (such as a hospital or general practice) would be identifiable to anyone outside that provider. (The first guidelines on this issue had already been issued by the RCGP and the BMA in 1988.) Industry has experienced no problem in abiding by these ethical guidelines. Since then, the private sector use of de-identified data has grown and tackled ever more complex challenges. In a recent project, a system has been built to collect prescription data from pharmacies for resale to drug companies (its principal use at present is in calculating drug sales staff commission payments). This was particularly difficult as the identity of doctors as well as patients had to be protected, to ensure that alert drug representatives could not identify doctors from the fall off in prescription volumes when they went on holiday [9].

The experience of the past three years have taught us that it is indeed possible to build clinical infromation systems that deal ethically with personal health information — and once the problems have been carefully analysed, and experience has been gathered from some prototypes, it is not even particularly difficult. Every reasonable non-clinical use of medical records that we have come across has been susceptible to a solution involving de-identified data. This is not solely a UK experience; similar systems are reported in Germany [10] and New Zealand [11]. Meanwhile, Switzerland has experienced a similar controversy over whether medical data held in central databases were properly de-identified, and following intervention by their Federal Data Protection Commissioner, systems are being redeveloped to much higher standards [12].

Building ethical systems is thus a matter of will rather than technology. This brings us to the last of the main lessons learned in the UK – an inappropriate systems culture, such as that of a civil service department, can fatally undermine the will to build systems properly. Safe clinical systems require a design team that can operate openly with a high level of user collaboration and consultation, just as in avionics or the nuclear industry. Above all, one must avoid organisational mistakes that allow clinical systems development to be hijacked by administrators; many of the NHS's problems arose from the fact that its computer department was controlled by the Department of Health in London whose principal goal was cost control. Administrative concerns thus naturally came to dominate the thinking of its management.

The problem now facing healthcare information technologists in the UK is how to climb out of the hole we find ourselves in. We need an environment in which doctors, nurses and other healthcare professionals can tell system engineers what they need, and the engineers can get on with the job of building it. But given all the interests vested in the old system, this is turning out to be easier said than done.

References

1. Report of the inquiry into the London Ambulance Service. London: South West Thames Regional Health Authority, 1993. `ftp://cs.ucl.ac.uk/acwf/info/lascase0.9.pdf`
2. Shapiro DZ, Hughes JA, Randall D, Harper R. Visual re-representation of database information: the flight data strip in air traffic control. In: Aspects of visual languages and visual interfaces. London: Elsevier, 1994: 249–376.
3. Vowler J. Patient care at risk from millenium bug. Computer Weekly 8 May 1997: 3.
4. Medical Devices Agency. Medical devices and the year 2000. In: Year 2000 and healthcare computing. Health Informatics J 1997 3(3/4): 173-175.
5. Collins T. NHS millenium fix goes on critical list. Computer Weekly 18 Dec 1997: 1.
6. Anderson RJ. Security in clinical information systems. London: BMA, 1996. `http://www.cl.cam.ac.uk/users/rja14/policy11/policy11.html`
7. Anderson RJ. Safety and Privacy in Clinical Information Systems. In: Lenaghan J, editor. Rethinking IT and Health. London: IPPR, 1998: 140-160.
8. Denley I, Weston-Smith S. Implementing access controls to protect the confidentiality of patient information in clinical information systems in the acute hospital. Health Informatics J 1998 4 (3/4) (to appear).
9. Matyas M. Protecting doctors' identity in drug prescription analysis. Health Informatics J 1998 4 (3/4) (to appear).
10. Blobel B. Clinical record systems in oncology. Experiences and developments on cancer registers in Eastern Germany. In: Anderson RJ, editor. Personal medical information – security, engineering and ethics. London: Springer-Verlag, 1997: 39–56.
11. Neame R. Managing health data privacy and security. In: Anderson RJ, editor. Personal medical information – security, engineering and ethics. London: Springer-Verlag, 1997: 225–232.
12. Schnyder M. Datenflüsse im Gesundheitswesen. In: 3. Symposium fuer Datenschutz und Informationssicherheit, ETH Zuerich, 29/10/98.