UK COMPUTING RESEARCH COMMITTEE

The Electronic Patient Record and its Use

Executive Summary

1. UKCRC has the expertise to respond to two of the Committee's questions: whether patient confidentiality can be adequately protected; and why delivery of the new systems is up to 2 years behind schedule.
2. We believe that protecting patient confidentiality will present very substantial technical challenges and that the systems associated with the EPR need to be designed, built and analysed using state-of-the-art methods. We are unable to tell whether this will be done and, even if it is, we believe that there will almost certainly be security breaches.
3. We believe that there are many reasons why there can be very little confidence in any current schedule for the delivery of the EPR and its associated systems. In particular, it appears that the specifications are not yet complete and stable. Delivery schedules are almost never overestimated, so it is unsurprising that current forecasts are optimistic.
4. We believe that there are important aspects of the NPfIT EPR systems that should be openly reviewed by specialists.

Detailed Evidence

5. The UK Computing Research Committee (UKCRC), an Expert Panel of the British Computer Society, the Institution of Engineering and Technology and the Council of Professors and Heads of Computing, was formed in November 2000 as a policy committee for computing research in the UK. Its members are leading computing researchers from UK academia and industry.
6. UKCRC has the expertise to address the second and part of the fifth questions identified by the committee:
   - Whether patient confidentiality can be adequately protected;
   - Why delivery of the new systems is up to 2 years behind schedule.
7. Our expertise is in computer-based systems, not in clinical practice, although some of us have carried out research into computer systems in medical practice and into the ways in which clinical and administrative staff work with these systems and the work-arounds that they employ when the systems are seen to have deficiencies.
8. The Electronic Patient Record (EPR) is part of the National Programme for IT in the NHS (NPfIT). NPfIT is a very large socio-technical system, by which we mean that the computer systems have to interact with and support the work processes carried out by NHS staff. These work processes are very diverse, and many of them are carried out under stressful conditions. Professional, legal and human considerations all mean that the short-term interests of the patient will be given a very high priority by NHS staff, even if this means disregarding the documented operating procedures for computer systems.
9. We have not managed to find a clear business case for the EPR, that analyses whether the total benefits will exceed the total costs, and whether the equally valuable benefits could be obtained more cost-effectively in some other way. We hope that such an analysis exists, as otherwise the project may be a certain failure in cost-benefit terms even if it succeeds technically.

Whether patient confidentiality can be adequately protected

10. Whether the confidentiality of data contained in the EPR can be adequately protected depends on several factors:
    - whether the design of the EPR and related systems restricts access sufficiently to ensure confidentiality;
    - whether the procedural safeguards that restrict access are practical, fit in with the working practices and values of staff, and are perceived as usable by those staff so that they are followed consistently in practice;
    - whether the software implementation of the EPR has been designed with adequate technical security measures;

- whether the technical design has been implemented correctly;
- whether there is adequate control over data archiving, database maintenance, and software and hardware updating to ensure that the confidentiality cannot be compromised, deliberately or by accident.

11. All these factors are difficult to achieve, and the archives of the Forum on Risks to the Public in Computers and Related Systems, moderated by Professor Peter Neumann, contain many examples of the loss of confidential data from important systems in recent years.
12. As a general principle, a single system accessible by all NHS employees from all trusts maximises rather than minimises the risk of a security breach. It increases the number of patients affected by the worst case breach and increases the opportunity for access to any one patient's data from some point on the extended system. In short, it provides both a bigger target and a larger number of points of attack than a series of smaller systems. No system can be totally secure, and networked systems are particularly vulnerable; it is important that a formal analysis is carried out to identify risks and show that they have been reduced as low as reasonably practicable.

The EPR and its Use: Evidence to the Health Committee

13. We do not know whether the EHR will be encrypted in the database and when transmitted between systems. This would provide some protection against data loss, if the encryption and key management were state-of-the-art. We recommend that the design of this part of the NPfIT is published in full, so that it can be scrutinised by experts.
14. We understand that access to the EHR will be controlled by the use of smartcards that identify individual staff and their roles, coupled with system policies designed to ensure that only staff with legitimate access to the data can see it. This form of access control suffers from several vulnerabilities; for example, smartcards may be shared or a user may leave a computer logged in or with sensitive data on screen where it can be read by others, smartcard security can be broken, authorised users of the system may access data illegitimately (possibly using colleagues' smartcards), or the data may be accessed by other means.
15. If the EHR is accessible on the internet, perhaps so that patients can check their own records as has been promised by Connecting for Health, it will be very difficult to prevent unauthorised access to these records, through password-cracking, phishing[1], or other standard attacks. Depending on the design of such web-based systems, it may be possible to break the server software and to gain access to large numbers of EHRs.
16. The Secondary Uses Service (SUS) provides access to patient data for research, billing and other purposes. It is very difficult to provide such data in a form that guarantees that the identity of the patient cannot be recovered, even when the data has been "anonymised", because many characteristic elements are necessarily preserved.
17. It is very difficult to design software systems that are really secure, especially where they include off-the-shelf software. It is impossible to establish that systems are secure by testing them because even several years of testing would leave most of the possible states of the system untested. Rigorous analysis can show that the system does not contain some of the possible security vulnerabilities, such as buffer overflows, but such analysis will only be possible if the systems have been designed with this analysis as a primary objective.
18. It is inevitable that the EPR will introduce some risks – of breaches of confidentiality, of loss of data, of corrupted or otherwise erroneous data, and of the EPR being temporarily inaccessible. These risks should be made public, just as the risks of any medical procedure are public.
19. For all the above reasons and more, we recommend that the NPfIT systems that handle the EHR, and all the procedures for maintaining the systems and the data, should be independently reviewed by experts in secure systems, and that the results of that review should be published. The history of IT system development consistently shows that a system's developers are often overconfident about its security and safety. Early third-party examination of the specifications and design will usually expose vulnerabilities that were not anticipated by the developers, leading to a more robust system.

Why delivery of the new systems is up to 2 years behind schedule

20. The introduction of new computer systems into an organisation almost always necessitates significant changes to the ways that staff work. Almost all successful projects recognise this explicitly; they are seen as business change projects, enabled by computer systems, rather than as IT projects. Business change takes time, resources, planning and commitment, and until the

[1] Phishing is the name given to luring internet users to fraudulent web-sites, usually by sending them fake emails, so that the unsuspecting user enters their account number and password and the fraudsters are then able to misuse the account.

plans are in place and the affected staff are committed to the success of the project, the technical requirements cannot be finalised. Self-evidently, until the technical requirements are finalised, the dates for delivering the computer systems cannot be forecast with confidence and the overall project timescales are at risk.

21. The alternative approach, of finalising the technical requirements and requiring staff to fit in with the decisions made by the package developers, runs the risk that the necessary adjustments to ways of working will prove impractical, or unacceptable to affected staff.
22. The NHS is a very complex organisation, so staff working practices may differ substantially from group to group. Until the full consequences of these differences have been understood and analysed, any implementation schedule is little more than a guess.
23. The scale of the NPfIT systems associated with the EPR is very great, and it is well established that the historic failure rate of large projects has been far higher than the failure rate of small projects. To maximise the chance of success, the EPR should be introduced as several small projects, shown to be successful, and grown incrementally into an interconnected national system.
24. We understand that the detailed content of the electronic patient record has not yet been finalised and that significant concerns have been raised by clinicians and patient groups about the uses to which the data will be put and the privacy implications. Until these issues have been resolved satisfactorily, it will not be possible to know whether the data in the patient record will be available, accurate, and up to date sufficiently often to support new working practices that depend on the EPR, nor to design working practices that can be shown to be practical and acceptable to staff and patients.

The EPR and its Use: Evidence to the Health Committee

25. It appears that many of the technologies are new and have not been tested. In particular, at the heart of the EPR are two standards - HL7 v3 and SNOMED-CT. We understand that neither has ever been implemented anywhere on a large scale on their own, let alone together. Both have been criticised as seriously flawed. It is imprudent to base the EPR, which will be part of the UK's national critical infrastructure, on a technology experiment.
26. It is essential that safety-related systems are as safe as reasonably practicable, and the NPfIT systems related to the EPR are, we assume, safety-related. Showing that these systems are adequately safe requires a safety-case: an analysis of the possible hazards and a logical argument, based on objective evidence, that the risk to patient and staff safety has been eliminated or reduced to a practical and acceptable minimum. For well-understood technical reasons, it is very difficult to produce an adequate safety case unless the software has been designed with this in mind; in particular, evidence from tests carried out on the system is rarely adequate on its own.
27. It is even more difficult to show that systems are adequately secure than that they are adequately safe, because of the need to consider all the ways in which the system can be deliberately subverted, in addition to the ways in which it may fail accidentally.
28. Whilst the techniques of safety analysis are well developed in the aviation and nuclear industries, and security analysis is well developed for military systems, the combined analysis for a very large socio-technical system such as NPfIT is beyond anything that we are aware has been done previously, and should be expected to take considerable time, effort and specialised expertise. We encourage the Health Committee to satisfy itself that adequate plans already exist for this work.
29. In summary, it seems from the information available to us that the EPR requirements focus on the technology rather than on the desired organisational changes, and that the technical specifications of the systems that implement and support the EPR are not yet complete. The implementation schedule for the EPR cannot therefore be well founded.

UKCRC would be pleased to provide additional evidence, orally or in writing, on any of the points mentioned above.

Submitted on behalf of UKCRC by Dr Martyn Thomas CBE.