UK
COMPUTING
RESEARCH
COMMITTEE

NHS IT Programme

Comments to the National Audit Office

1 Introduction

These questions have been prepared at the request of the National Audit Office to help them to review the NPfIT.

2 Specification Questions

2.1 Top-level objectives

- What are the top-level objectives that the new systems are designed to achieve and which, if not all met, would mean that the project had failed?
- Are there alternative solutions to the identified problems that would have a better ratio of benefits to costs than the proposed IT solutions?
- What lessons have been learnt from studying similar projects in other countries?
- What evidence exists that the proposed UK system would have the desired benefits, and at a level that justifies the costs of the system?

2.2 Scope of the proposed system

- How widely will the proposed systems have to be deployed and used before they can achieve their planned benefits at a level that justifies the costs? (% of NHS Trusts, % of doctors within a trust, % of staff in each other affected category).

2.3 Fundamental specification issues

- What is the mechanism for developing the specification?
- What mechanisms exist for identifying stakeholders, ensuring these are representative and consulting with them?
- Will the degree of correspondence between the output specification and the bidders' responses be validated with real users before contracts are placed? How?
- How will the acceptability of any compromises be established?
- How have you ensured that the stakeholders really understand how the new systems will affect their working processes?
- How have size estimates been made and how long are these applicable? (For example, the transmission of images or video by email could hugely increase the necessary size of mailboxes – currently assumed to be 14Mb, about enough for one high resolution X-ray or a few seconds of video)
- What contingency has been planned for on size and performance estimates?
- How will requirements change be managed once the contracts have been placed?
- What validation mechanisms will be put in place to ensure that the system meets the real needs of stakeholders?
- How long could access to data be permitted to take (mean, median and maximum) before the delays became unacceptable in the most time-critical of the required functions? How will you ensure that the delivered systems meet these criteria under maximum foreseeable load?

3 The Security And Integrity Of The Proposed System

Security and integrity are not absolute qualities, they need to be defined in the context of the functions that the system must perform and the data that it will hold, and they need to be expressed in terms of the properties that the system must display and the allowable rate of failure for the different failure modes.

The requirements specification must include a threat analysis related to the security and integrity of the system - what are the potential failures and security attacks that can occur, what are the probability, consequences and costs of these occurring.

3.1 System Availability

- For how many minutes per year is it acceptable for the system to be completely unavailable? [This could happen as the result of technical failure or following a 'denial of service' attack].
- What is the longest duration of any allowable loss of service for an individual function, or at an individual location?
- What will be the cost or consequence of system failures leading to longer periods unavailability than these limits?

3.2 Data Confidentiality

- How sensitive (private/secret) is the data? What level of compliance with the Common Criteria for security will the systems be required to meet? How do you know this is adequate?
- What is the maximum number of personal database records that could be leaked by the system each year (or in total) before it was deemed too insecure to remain in operation? (even setting this limit as low as 1000 [less than 0.002% of the population] would allow the theft of the personal details of the whole membership of the House of Commons and most Premier League football players each year!).
- How many people will need access to the system and what security clearance will each person and site require?
- What level of audit trail must the system maintain, for example to allow suspicious patterns of usage to be detected? (There are examples of sensitive databases that achieve a low level of unauthorised access and unauthorised modification—the Police National Computer appears to be an example where the only known leaks have resulted from bribing individuals who have authorised access, and where measures including detailed audit trails are in place to detect such leaks. We believe that the PNC is not attached to the Internet.)
- What mechanisms are required to allow the patient to have access to, or to modify, any or all of the data held about them?
- What will be the costs and consequences of a major breach of the system's confidentiality?

3.3 Data Integrity

- Do you have a written security policy? How will you ensure that supplied systems conform to this policy?
- What level of errors in the data is acceptable for the most demanding function for which the system would be required? How will the data integrity be established initially, and preserved?
- Who is responsible for cleaning the data that will go on to the system, and what budget has been allocated for this? (Data Cleansing – ensuring that the data is correct and complete – can take 25% of a project's budget. It can also take particular skills and considerable time).
- Will electronic signatures be used to control changes to data and to provide a cryptographically secure audit trail? Have you published a specification for such assurance and for the processes that surround it?
- Since the system will be connected to the Internet, how will the system be protected against hacking and other malicious corruption?
- What level of barrier is needed to deter deliberate corruption of the data? (Although defences can be identified for the known vulnerabilities, they are not likely to exist in current products and new types of attack are being identified every year.)
- What will be the costs, consequences and recovery mechanisms following a successful penetration of the system that leaves the integrity of the system in doubt?

4 Business Change

It is a commonplace of major IT system implementation that they involve considerable change to the previous way of working, and that many requirement issues emerge at this time. Introducing new systems in a very busy work environment can lead to substantial and lengthy degradation of service and to rejection of the new system.

- What estimates have been made of the cost and impact on NHS services of designing new workflows and processes, and training staff to use the new systems?
- How quickly is it estimated that NHS service levels will return to their pre-implementation levels (in terms of patient throughput, for example).
- What is the target level for improvement in these metrics once the new systems have been introduced? What is the minimum level of improvement that would justify the cost of the new systems?
- What will be the cost of ownership, annually, to local trusts, and how will this be funded?

5 Programme Management

- Have you adopted the OGC Gateway process for this procurement?
- What changes have you made to the Gateway process, and why?
- How will you manage the interfaces between the new systems and legacy systems that may be undergoing change, or other new systems that are outside the NPfIT programme?
- Do you have a risk register for the NPfIT? What are the top 10 risks affecting successful delivery? What are the top ten risks affecting successful implementation and use? What mitigation strategies have been established to manage these risks?

6 UKCRC's views

UKCRC believes that any sensitive database that is attached to the Internet (or otherwise available to a large and changing population of users) will almost inevitably be successfully attacked. If the system is built on commercially available products, we do not believe that it could be made secure against intelligent, resourceful and sustained assault. The systems engineering of the proposed national health system therefore needs to ensure that the inevitable failures will not be catastrophic or unacceptably costly.

UKCRC believes that:

- No existing system can meet the current, detailed operational requirements of the NHS, therefore it is essential that a complete and unambiguous specification of the system's requirements is drawn up, and that this specification is analysed rigorously to uncover any omissions or contradictions. We know this is technically feasible even for a system of this complexity; to fail to carry out this analysis before placing contracts would be unprofessional, and a serious waste of public funds.
- Any system that is implemented will be novel, complex, and will require the use of the best available software engineering incorporating good computer science. This requires a significant change to current procurement practices but, without such changes, the project will fail.

UKCRC would be happy to answer follow-up questions on any of these points.

Martyn Thomas
for UKCRC. September 19th 2004