Computerising the Chinese Army - Information Systems in the NHS

About the Conservative Technology Forum

Information economy and information society issues now play an increasingly important part in plans for the economic success of the United Kingdom and the future of the European Community. Led by Shadow Industry & Technology Minister Michael Fabricant MP and chaired by Malcolm Harbour, MEP, (European Information Society spokesman for the Conservatives), the Conservative Technology Forum is actively contributing to Westminster Front Bench thinking, on Information Society matters. In conjunction with the independent policy and research unit, Aediles, its objective is to enlist the creativity of those working with the new computing, communications and content industries in examining how society should be enabling constructive change while handling the consequences of rapid technology evolution. Its home page is www.conservative-technology.org .

1) Background

Twenty years ago the then Chief Executive of the National Health Services, (Sir Len Peach, previously personnel director of IBM UK) pointed out that the NHS was the third largest employer in the world, after the Chinese and Russian Armies and significantly larger than the fourth, the Indian State Railways. As such it was too large and complex to be centrally planned, directed and managed. His task should be to devolve authority to those in a position to know what they were doing. This was not a popular message and the Conservative Government had barely made a start before New Labour reversed the process.

The NHS is now the second largest employer in the world (the Russian Army has shrunk). The current National Plan is the largest civilian computer project in the world, ever. The UK public sector and many of its suppliers currently have a serious credibility problem with regard to the delivery of large programmes. The reasons are partly to do with the scale of outsourcing over the past decade or more (leading to a dearth of in-house skills), partly to do with neglect of the UK professional and technical ICT skills base over the same period (especially with regard to information systems engineering as opposed to "mere" technical skills) and partly to do with a cycle of public sector bad practice (top-down commitment to contract driven programmes in advance of any serious feasibility study or user consultation). There has been widespread neglect of the people disciplines necessary for success: beginning with clarity of objectives, priorities and responsibilities.

According to a series of articles in Computer Weekly the National Plan for IT in the Health Service fits that cycle: having begun as a top down exercise (supposedly after a seminar at Number 10, chaired by the Prime Minister), having bypassed the Gateway review of the business plan and with the Director General recruited after the event, with a massive budget to "reverse engineer" already published implementation commitments. There is little evidence of consultation with the users: who-over or however these might have been defined. The process has been described as "classic NHS management: name a principle of good practice and the politicians will mandate the opposite".

The private sector has moved away from large integrated projects to programmes of structured and phased evolutionary change, albeit some of them large and ambitious - such as the current roll-out of chip and pin cards across the banking system. None of the current lead suppliers to the NHS has experience of bringing in any comparable project to time and budget and a side effect of concentrating on a limited number of large, often US suppliers, has been to damage the UK market for smaller suppliers. Small and medium-sized enterprises have always provided for much of the peripheral ICT functions needed by NHS users and been the focal point for innovation in a newly developing area such as health information. Policy in other areas has been to encourage British Enterprise and the use of international standards. The NHS is doing neither.

Most General Practitioners use systems from a handful of suppliers who won their market dominance by reliably delivering what doctors wanted at prices they were willing to pay. As a result UK GP systems are more advanced than anywhere else in the world. Current problems such as:

- systems do not do not talk to each other, so when a patient moves from one practice to another all the electronic records are printed out, forwarded to the next practice, then typed in again
- they do not send prescriptions electronically to pharmacies which again forces retyping of the data

have been used to criticise the current systems. But the necessary facilities have been developed many times in the past. It has been inertia by the DoH that has prevented their introduction. Widely used, trusted, reliable systems appear about to be replaced with less functional new systems from new suppliers over which doctors do not feel they have been nearly as well consulted as by their previous suppliers.

This is a consequent risk to patient care because many GPs have built practice services around their IT. There will be significant disruption to these by the imposition of new and possibly less useful systems. There is also a risk that if the new systems are accepted as fit for purpose by NHS ICT staff with adequate input from the GPs who are to use them, suppliers may not be motivated to listen to their users and swiftly introduce any changes requested. If the users do not control the budgets, how will we ensure that suppliers have the necessary incentives to respond to their needs?

The UK market for hospital systems was, by comparison, fragmented and immature because most reputable suppliers had walked away after the failure of a series of over-ambitious projects and an overly bureaucratic, cumbersome procurement process. The result is a lack of practical experience in linking clinical and administrative systems. The attempt to move rapidly towards integrated national systems therefore involved high risk even before consultation processes were truncated in order to meet delivery deadlines.

One of the pre-conditions for success in any project (large or small) is continuity among the management team, on the user as well as the supplier side. The plan is about to have its second change of "senior responsible owner" inside 18 months and further major changes are expected on April 1st with a reshuffle of all the agencies involved. A national Audit Office investigation is under way and a number of lawsuits are now in process (believed to include some from existing suppliers to the NHS who have been excluded by the new lead suppliers, who may also give evidence to the new OFT investigation into public procurement processes).]

NPfIT has moved ahead without consultation of either the eventual users of the systems or of the people who have experience in health information systems. There is a huge body of experience and skill in and without the NHS. Very little of this has been used in building the NPfIT solutions. The imposition of a one-size-suits-all solution is also destroying those parts of the NHS which could claim to have "excellence" in their use of information.

Currently the model is to have a central National Data Spine. This would contain all the information collected by local services. With the exception of some (detailed) hospital admission data every system will have to send details of every patient encounter to the Spine. This will result in one central repository of patient data with all the risks of security and confidentiality that imposes. It is also technically very challenging and there is at present no evidence it can be constructed in a usable manner. The alternative of a "thin" Spine that just serves as a directory for local systems to communicate with each other when necessary has been dismissed. A "thin" Spine would leave the sensitive data on local systems under the control of the clinicians who entered it. This is much more acceptable to the professions and patients.

The task of the opposition should be to provide constructive and helpful comment and put forward a strategy for remedial action when a misconceived plan falls apart in lawsuits and acrimony.

2) Vision

The provision of optimal modern medical care is increasingly dependent on the rapid availability to health care professionals of accurate information on the treatments that a patient is (or has been) receiving from a variety of sources. That information is commonly fragmented over a variety of records, many using different (often incompatible) data types, file formats, coding conventions and coding structures, with different levels of accuracy and confidentiality, let alone different computer systems or technologies. The cost of delay and incompatibility, let alone inaccuracy, can be counted in unnecessary suffering and death, not just wasted time or money.

To achieve this goal the information has to be collected by healthcare professionals at the time of patient contact. There is much evidence that schemes to collect data after the event lead to errors and unusable information. However clinicians will not use computer systems if they are seen to interfere with patient care. Systems must be seen to **assist** in patient care. They must provide the clinician with some "added value" during patient contact that they could not achieve just using paper. Otherwise the evidence shows they will not use the systems. Systems designed just for data collection will fail.

The strategy most likely to succeed is to enlist the informed support of healthcare professionals and patients, as well as would be suppliers of systems and services, in setting realistic and trusted frameworks within which practical progress can be made. Once that consent has been gained the need is then to ensure step by step progress within those frameworks, avoiding both the pursuit of grandiose "national" projects of the type which have failed so expensively in the past and the concentration of scarce resources on prestige centres of excellence whose systems can neither be replicated nor joined up.

This is not easy because it requires the co-operation of a wide range of professionals in the application of programme and system development and application disciplines which they regard as a mundane distraction from their "real" job, patient care.

The position is complicated by the contractual arrangements already entered into with major suppliers who are convinced they know best. It is highly likely, however, that the suppliers will wish to see changes rather than take the blame, perhaps very expensively, for another set of high profile disasters.

The solution is probably to use the National Audit Office review to identify the changes necessary to ensure that the suppliers can and do consult and work direct with the various interest groups, nationally and locally, to improve the prospects of success. The key is probably to move away from an appearance of trying to impose centralised, standardised, one-size-fits-all, solutions and towards the adoption (at all levels) of common frameworks for sharing that information which is already available, and in contrast to build on these, step by step, over time.

If the objective is seen to be the improvement of patient care, including by making better use of the budgets and resources available, with open and accountable ways for reconciling conflicting priorities, then it should be possible to begin the process of moving from confrontation to co-operation. Talk of using ICT to enable the introduction of choice and of market forces should also be in the context of GPs or hospital clinicians being able to help patients to make informed choices, as well as nurses, who commonly spend more time with patients with chronic conditions and who use proportionately more resources, being motivated and able to keep them informed about progress: another dimension to "putting the patient at the centre". Key to this process are credible and reliable frameworks and processes, not just technologies, for data sharing.

3) The Benefits and Risks of Data Sharing within the Duties of Clinical Care and Protection of Privacy

Studies over the past twenty years as well as enquiries into many tragedies indicate the cost in personal suffering and/or death that can occur when accurate information is not available at the point of treatment. Most avoidable tragedies occur because the information is simply not available. Less often they occur because it is wrong or misinterpreted - including by staff transferred from another hospital using a different coding convention.

Meanwhile an increasingly common patient complaint is the need to give the same information at each stage of their treatment, leaving aside those who discover that essential information has not been passed on. Even if a patient is admitted to a hospital that has treated them before it is all too rare for the accident and emergency department to have early access to their records while GPs rarely have good access to hospital information on their patients and vice versa. Meanwhile vast amounts of treatment, prescription and reaction reporting information, routinely logged over nearly twenty year by GP and Hospital systems in still not available for use in epidemiological research.

Much is said on the need to protect patient data from abuse but little actual data on patient views is advanced beyond anecdotal evidence of abuse and lack of trust. Two years ago the NHSIA commissioned MORI to collect views and the results showed widespread support for the open sharing of information between health care professionals (98% happy for their GP to see their record and over 80% for Hospital Staff) concerned with their treatment, significantly less support for information being made available for medical research (about the same as for it being available to those managing the health service) and 43% against their medical information being available to practice administrative staff and 36% against access by social workers. Given the amount of information that is routinely passed to administrative staff to enter or which they are asked to look up and pass to the Health Care professional this means that multiple levels of confidentiality regarding the content of medical records are essential for expectations are to be met.

Many of the systems commonly used by GPs and specialist clinics have long had facilities for "sealed envelope" information available to named practitioners only for when patients may not wish some parts of their medical records to be available to their GP (e.g. young girl on the pill, who does not want her family doctor to share this with her parents or an individual with a sexually transmitted disease who may be sensitive about any other than their contact in a specialist clinics being aware). There are also some well recognized conditions (for example psychiatric or with diminishing frequency oncological) or combinations of conditions and individual patient requirements in which it may not be recommended by clinicians or desired by patients or relatives that they have access to all components of their clinical record.

The best protection of privacy is that health care professionals are responsible for their own conduct. They have confidentiality built into their professional codes of conduct and patients trust them. Some data protection professionals argue that that this should be backed up by logs of all accesses to a patient record so that staff know that any abuse would be detected. Not only could the system overheads from such an approach be substantial but such logs might be even more susceptible to abuse. The more important task is to ensure that the routine and secure use of patient information systems by those entering or accessing data that they need in order to help the treatment of the patient is easy and that *non-routine* accesses are properly authorised and recorded. A particular need is for practical facilities, routines and guidance for non-medical staff who have may have access to subsets of information for whatever purpose or are asked to provide assistance to clinical staff.

4) The Problems of Data Accuracy and Compatibility

Recent exercises to check the accuracy of data entered by clerical staff into public sector systems where accuracy is supposedly important (from health care to police and criminal records) have commonly shown errors rates from 10 - 30%. Experience from the private sector has long been that only data entered at the time and place of transaction by those with a direct interest in its accuracy is likely to be reliable. One of the biggest problems in the health service is to move towards direct data entry by health care professionals without increasing their net workload. Another, equally important, is to move towards standard and compatible terminologies from a situation where not merely many different terms be used but the same term may mean different things to different people in different systems. Finally the coding structures used in secondary care are often different between hospital practices - this can be a particular (and occasionally catastrophic) problem for those who may be called on to work long hours shortly after changing hospital or department (such as junior doctors). This issue has been an ongoing and significant problem for many years.

5) The issues of Consent and Data Protection

There is a fair degree of confusion as to what is required under current Data Protection Act legislation with regard to patient consent to data transfer. This is compounded by various items of legislation requiring the sharing of information with regard to, for example, law enforcement and child protection. The Act does not of itself require the consent of patients to the processing of data for medical purposes. However, because there is a general requirement that all processing of personal data is lawful and because in many cases the general law (including medical confidentiality) requires that patient consent is obtained for the processing of personal data, then consent becomes an implied requirement of the Act. There is a requirement for “data controllers” who will advise patients of the identity of the data controller, the purpose or purposes for which the data is intended to be processed and any further information which is necessary, having regard to the specific circumstances in which the data are to be processed, to enable processing in respect of the patient to be fair.

Any data-matching exercise would need to be lawful, which would require not only compliance with the Common Law duty of confidence but also compliance with other Statute Law determining the functions and powers of organisations intended to be part of the data-matching exercise. The patient must be given information as to whether the proposed uses or disclosures of data would be mandatory or optional. Failure to provide this information might result in personal data being unfairly collected. In deciding whether to offer an opt-out, data controllers should attempt to distinguish between those uses and disclosures of data which are essential in order to treat patients within the health service and those which are not. By the term “essential” is meant those uses and disclosures without which treatment could not be given and those uses or disclosures which the law makes mandatory. In effect, such uses and disclosures are necessary elements of the medical purposes for which it is proposed that patients’ data are processed. Since it is unlikely to make good administrative sense to offer patients the opportunity to object to the processing of their data for any “essential” elements, it would make little sense to provide an opt-out in this area.

However the means of ensuring meaningful patient consent must not be so onerous that medical care becomes too time consuming. This has happened in other countries. The mechanism must be capable of giving a patient some control, not necessarily routinely, and not so restrictive that important information is not available to treat that patient when required. Patients unilaterally declining consent for the reasonable and justifiable collection and holding of clinical data or simple administrative data must expect to experience degradation in the range, quality, promptness, accuracy and suitability of the medical care that they receive. There are circumstances in which such behaviour could additionally infringe the rights of other patients who would otherwise benefit from epidemiological research, and when such behaviour could be argued also to infringe the 'rights' claimed, often with misguided understanding or motivation, by those who demand accurate detailed information on the performance and experience of clinical services and individual professional healthcare staff.

6) Availability of Data

The split of roles between information officers who are expected to make information available and data protection officers who are expected to prevent abuse (with the consequent risk of adversarial approaches) is considered to be counter-productive. The priority in health care should be the accessibility of shared medical data when needed to the clinician. In order to ensure that information remains controlled, the current adversarial structure in which Caldicott Guardians' work to a set of principles focussed on protection should be replaced so that an Information Officer would have a Caldicott Guardian to deal with the clinical data, with accountability through an external monitor.

There is a risk of information overload in circumstances where an individual's medical history is very complex and it will be necessary for certain critical information to be brought to the forefront in presentation of the data so that the key facts of medical relevance are not hidden in a morass of less important data.

Traditional routines for handling of medical records on paper are regarded by many systems professionals as less secure than most electronic record systems. From the viewpoint of any individual there may be a trade-off between the current lack of security for paper records and the potential for improved security from casual or unauthorized enquiry that electronic systems ***can*** offer. The status quo does however offer different form of security by virtue of the difficulty that paper records pose for anyone wishing to collate all of "your" data. [i.e. that which would in principle be available across the many disparate databases that might be connected electronically.

By contrast, electronic records are potentially much more readily collated and more strongly protected. Once electronic security is compromised, commonly by human failure, the dangers of abuse are, however, very much greater. In large organisations, with multi-levels and circles of confidentiality and trust, the provision of effective security over electronic networks can become very complex. In order to address these concerns, any wide spread sharing of data across the Health Service needs to be accompanied by clear guidance as to who should have what access to which data under what circumstances, including how to check authorisation and resolve queries and conflicts when emergency access is supposedly required by someone previously unknown. The Department of Constitutional Affairs is looking at the provision of such guidance at a generic level but it is almost certain that many parts of the NHS will need specific guidance and protocols that can be followed routinely, not just statements of principle.

7) Recommendations

As part of a programme of "constructive criticism" to enlist the support of all parties in making NHS ICT work in practice, the opposition should call for:

- Non financial details of all NHS ICT contracts, including performance monitoring and change control processes, to be placed in the public domain. Lack of public confidence means that any case for confidentiality must be balanced against the need to avoid allegations that it serves to conceal incompetence, inefficiency and corruption. The Freedom of Information Act provides the necessary framework and guidance has already been drafted by the Office of the Information Commissioner.

- "Time and motion" studies to check that new systems really are quick and easy for clinicians and/or others to enter and/or confirm data at the point of treatment/decision/transaction. This is crucial to the acceptance of new systems since there is widespread concern over increasing the clinical workload to generate data that does not benefit patient care.

- NHS Information Officers to have responsibility both for ensuring that accurate information is passed, when needed, to those authorised to receive it AND for ensuring that any abuse results in corrective action - and also judged on their ability to manage the conflicting priorities that will arise.

- Central indices of permissions for data sharing to be collected from patients at a convenient time (e.g. registration) with facilities for refinement and updating as circumstances and views change. Thus someone reluctant to have their data used for unspecified "research" may be willing to take part in a specific clinical trial

- Those patients who wish (and/or are able) to check and/or manage the use of their patient records should be given opportunities to do so as part of their involvement in their own health improvement: within reasonable and practical limits. Amendments made by patients should be clearly marked as such and not be seen to disrupt the legality of the medical record. Except for specific category restrictions, patients should be able to see their data at little or no cost and to request a review with clinicians or administrators, at realistic cost, refundable if significant error or any malpractice were identified.

- All involved in medical records should be given clear guidance as to what information can and should be made available to whom, under what circumstances and what should not. "All" should include subcontractors et al (where-ever they are located). The provision of that guidance should have explicit inputs from the relevant clinical and other professional disciplines.

- The concept of the Data Spine should be reviewed. Consideration should be given to making the Data Spine a directory for communication with all NHS local systems plus a limited summary of patient information.

- The software produced by the Local Service and Application providers should have the ability for other software to interface with it. This means publishing the messaging standards and Application Programmer Interfaces (APIs): the means of allowing programmes to communicate effectively.

- Establish an Accreditation Process for all NHS computer systems, separately from NPfIT. This will ensure systems are monitored and controlled, both as regards functionality and adherence to standards for security, confidentiality and `data sharing

The delays in fulfilling the contracts are beginning to trigger non -compliance penalties on the part of the Service Providers. This gives an opportunity to renegotiate the contracts.

8) Action Plan:

- All NHS ICT contracts, including performance monitoring and change control processes, to be placed in the public domain.

- Announce series of high level round table workshops, involving ICT suppliers and clinicians as well as a cross section of Health Service Management, to discuss consultation and co-operation mechanisms with the National Audit Office.

- Extend National Audit Office terms of reference to include recommendations on how best to structure consultation processes with clinicians of all types (both hospital and general practice) and patient care groups to help ensure that systems also meet their needs

- Follow this by a proper analysis of the business processes in health care. This will ensure that the software solutions will solve the real problems not those deemed to be important by people who do not understand the environment.

- Announce timetable for production of practical guidance on information sharing with regard to health care information across the National Health Service and with those with whom external exchange may be required (including where it is not in patients benefit: benefit fraud, criminal offences etc.) This needs to include a review of Section 60 of the Health and Social Care Act 2001, which gives the Secretary of State authority to obtain data from medical records even if the patient has not consented, under penalty to the record holder of a fine of up to £5,000. There are concerns now about some of the orders made under this act.

- Explore using the non compliance with the current contracts to renegotiate with the Local Service Providers to produce contracts which can deliver an evolutionary development of NHS ICT.