Logging in and logging out: patient safety on ward rounds

Gordon Caldwell

ABSTRACT

In this commentary, Gordon Caldwell argues that tardy access to core clinical information systems may be close to paralysing clinical care processes for doctors, nurses and other health professionals to the detriment of safe high quality patient care. The number of logouts, logins and reboots required to use core clinical information systems must be reduced and simplified, if safe effective clinical care on ward rounds is to be delivered in a timely fashion. Undue emphasis on limiting ease of access to data, because of concerns about data confidentiality, may be endangering patient care. We need a new understanding of confidentiality within the clinical care teams, which will allow swifter access to essential clinical data.

Tardy access to core clinical information systems (CCIS) may be close to paralysing clinical care processes in many NHS hospitals. Urgent action is needed from senior leaders in the NHS to free the processes from the numerous delays that build up to significant amounts of wasted non-productive time spent just logging on and off CCIS. Such action would also release staff from the fear of breaching NHS policies and subsequent disciplinary action. This tardy access directly affects the pace of care in acute medicine. In acute care, the work of doctors and nurses must markedly outpace the progression of the illnesses of the cohort of patients under our care.

The work of acute hospital inpatient services is to take patients with acute major medical illnesses and swiftly return their health to a condition in which they can safely resume living outside hospital. For a small proportion of patients the work is to anticipate end of life and provide a calm comfortable death. Integral to the work is to train the current and future generation of healthcare professionals to be ever improving the service that is provided. All this must be done without adding harm to the patient. This can be summarised as:

- **Right diagnosis** and
- **Right treatment** at the
- **Right time** in the
- **Right place**, with the
- **Right to no avoidable harm** and
- **Better next time**.

The pace of the processes to make diagnoses, plan and deliver treatments must outpace the pace of progression of the acute illnesses of the patients under a team's care. If the pace of diagnosis and treatment is slowed the illness progresses untreated and the patient's condition will deteriorate.

The process of diagnosis is highly complex, and is crucial to decisions about the appropriate individualised treatments. All sources of information including computerisation should aid the timely flow of understandable information into doctors' brains to support the processes of diagnosis, planning and safe delivery of therapeutics.

Patients see computers around the wards and expect that doctors have instant access to critical results of investigations such as haematology and clinical chemistry results ('the bloods'), radiology investigations ('the X rays'), and microbiology results e.g. for MRSA screening, to support the processes of diagnosis and safe treatment. They would also expect that we had instant access to a listing of their current medications and drug idiosyncrasies. This is not the case in many NHS hospitals.

Access to CCIS is subject to the written and unwritten rules of hospital IT governance policies namely

Gordon Caldwell is a consultant physician, Worthing Hospital

Email: Gordon.Caldwell@wsht.nhs.uk

Submitted for peer review 02 September 2011; accepted for publication 21 October 2011

- Professional staff must only use their personal logon and never use a CCIS on another user's name and password. If the CCIS, e.g. the Picture Archiving and Communications System (PACS) is active on someone else's logon, they must logout of that CCIS and login with their own user name and password for that system
- Professional staff must log all the way out of a PC at the end of a session before leaving the PC, however brief the session, however urgent the need to leave the computer. If the PC is left logged on the next user must log all the way out and then all the way back in
- Group logons e.g. ward logons are not allowed
- For an individual every password for each CCIS must be different, and passwords must not be written down or stored electronically. It is of note that I have over 20 user name and password combinations just to do my ordinary NHS and clinical tutor work
- Non clinical staff e.g. secretaries and ward clerks may not have access to results of tests on CCIS, although they handle paper copies of these results and type letters containing the results all the time
- Breaches of NHS IT policies are very serious and may result in criminal charges because Data Law is criminal, not civil, law, disciplinary processes, sacking, and referral to professional bodies such as the General Medical Council (GMC) or Nurses and Midwives Council (NMC). Frontline staff constantly face a dilemma of either swiftly accessing an important result e.g. a chest X ray in a tension pneumothorax, or breaching NHS IT Governance policies. Of course the staff choose to access the result swiftly, and breach the policy
- If a policy, however long and unreadable, is sent out by email, professional staff are then personally accountable for any failures to adhere to the policies

I run my consultant-led routine and new admission (post take wards rounds) to a set of quality standards to ensure thorough and reliable patient review, using the Caldwell Considerative Checklist (Herring, 2011b) and in Autumn 2010 felt the pace of my rounds was slowing, and a sense of irritation and distraction increasing, because of tardy access to CCIS. I started to split the rounds between myself with a junior and the SPR with another junior, just to get the patients seen before the start of the afternoon's work. On one occasion I split the round over two mornings. The final straw slowing the processes on my ward rounds was a new timed lockout of the PCs on the current user's name, if the PC had been idle for a few minutes. If a doctor, nurse or ward clerk found the PC in this state, the only way to reactivate the PC was either to login on the current user's password, in clear breach of NHS IT policy, or to shut the PC down and reboot back to the CCIS, which took up to 7 minutes. NHS IT rules suggested that the current user should log all the way out, which closes all the current CCIS, so that the new user 'only' has to log back in, load and log in to the various CCIS required for clinical care. This process of 'login and login' to the essential CCIS took over 3 minutes to complete.

I had data on the duration of ward rounds dating back to April 2009, and decided to model routine and post take ward rounds in which we putatively adhered to the written and unwritten rules of NHS IT and operational policies.

Background and methods

I have been a consultant physician with an interest in diabetes and endocrinology since 1993. During the study period I was 'on take' every Wednesday night in the acute medical unit and responsible for an additional 18 patients on a general medical ward, plus outlying patients during busier periods. The ward medical team consisted of myself, a specialist registrar, one or two core trainees and maybe one foundation doctor. On 'post take rounds' I reviewed the night admissions with the night team of a registrar, a core trainee and a foundation year one doctor. There are no computers at the bedside and the clinical information systems are accessed in the doctors' room.

In April 2009 our team developed and implemented the Caldwell Considerative Checklist Process (CCCP) to ensure a thorough review of each patient's case and to improve the reliability of the rounds (Herring et al, 2011a). The domains in the CCCP can be mapped to General Medical Council (GMC), National Institute for Clinical Excellence (NICE), National Patient Safety Agency (NPSA) and British Medical Association requirements for good medical practice (Herring et al, 2011b).

As part of this process, the ward rounds' data were collected onto a spreadsheet, including start and finish time and numbers of patients seen on each round. A stopwatch was used to measure the access times to the PCs during a routine round. The timings for login, logout and complete reboot were confirmed later by a member of the informatics team during another routine round.

The hypothetical calculations of ward rounds duration in compliance with hospital IT policies were based on the following model of a ward round, which is commonly practised by consultants in the medical unit. In the doctors' room, the consultant hears the verbal report on a case from the Junior doctor, looks at the written notes and discusses the case, while reviewing the 'bloods', and X-rays on the computer. Then the team go to the bedside and consults with the patient while reviewing the drug charts, vital signs, fluid balance charts, and makes the clinical management plans with the patient, and, if present, the nurse. The team then returns to the doctors room and discusses the next case. The modelling assumes that the computer will either have locked out and require a full reboot, login and the loading and logins of the various CCIS that are required, or that the last user has logged out in accordance with policy, which of itself takes 40 seconds, and 'only' a login and the loading and logins of the CCIS are required.

Modelling results

Login and reboot times

These were measured several times on two rounds using a stopwatch, once by Dr Caldwell and once by a member of the informatics service.

- Complete reboot of computer once locked out on current user who is no longer present; switch off, switch on, login, load results viewer and PACS takes 7 minutes
- Last user has logged out; new user logs in and loads results viewer and PACS takes 3 minutes 20 seconds.

Routine ward rounds

The working environment was unchanged between June and November 2010, and the team undertook 35 routine review rounds, seeing 637 cases to the standards set in the CCCP, taking a total of 6560 minutes, averaging 10 minutes 20 seconds per case review.

The average number of cases was 19, so the average duration of the routine round was 196 minutes (3 hours 16 minutes).

If the computer had 'locked out' on the last user's login and had to be rebooted the ward round would be prolonged by 133 minutes (19 cases, 7 minutes extra per case). The model ward round would then last 329 minutes (5 hours 29 minutes).

If the last user had logged out properly and only a set of logins were required the ward round would be prolonged by 63 minutes (19 cases, 3 minutes 20 seconds extra per case). The model ward round would then last 259 minutes (4 hours 19 minutes).

Post take ward rounds

The working environment was unchanged in the acute unit from April 2009, during which period 79 post take ward rounds were completed, reviewing 960 cases in 15 242 minutes, averaging 15 minutes 54 seconds per case review. The average number of cases was 12, so the average duration of the post take ward round was 190 minutes (3 hours 10 minutes).

If the computer had 'locked out' on the last user's login and had to be rebooted the ward round would be prolonged by 84 minutes (12 cases, 7 minutes extra per case). The model ward round would then take 274 minutes (4 hours 34 minutes).

If the last user had logged out properly and only a set of logins were required the ward round would be prolonged by 40 minutes (12 cases, 3 minutes 20 seconds extra per case). The model ward round would then take 230 minutes (3 hours 50 minutes).

Implications for quality, improvement, productivity and prevention

Time spent logging in and out of computer software or rebooting a computer is non productive wasted time. Reducing the time taken for rebooting and logging in must improve productivity by cutting waste.

Our 'product' in acute care is a patient ready to safely resume living outside of hospital care. It is self-evident that reducing non-productive time must improve productivity, although of course there would be a cost involved in modifying software to reduce the need for logging in. For example, on one occasion in Autumn 2010 five doctors on one of my ward rounds stood for 7 minutes while a computer was rebooted, only to find that the CT scan had not yet been reported. This represented 35 minutes of wasted non productive expensive professional time. The many minutes a day that all clinical staff spend logging into clinical systems, will represent thousands of man hours a year across the NHS. It would be possible to model the costs of the wasted time, and potential savings, but the principle is more important; we must maximise the time that highly paid staff spend doing the work that only they can do, and minimise the non productive wasted time. In a small pilot study I have found that the amount of time wasted in outpatients because of multiple logins and poorly optimised software equates to at least one new patient appointment, or two review patient appointments per doctor per session. Money may not be saved by improving the systems, but productivity would certainly increase. Staff morale would also be improved, because most users find the multiple user names, passwords and need for repeated logins very irritating.

Other operational policies

Other NHS operational policies and targets impact on the potential duration of rounds. The team of juniors is in a constant state of flux, with unpredictable numbers and members of the team. New teams members are unfamiliar with the patients and the wards rounds routines.

The juniors on routine rounds cannot start work until 9 am, because of the EWTD and New Deal constraints. If they started at 8 am, they would have to leave at 4 pm. In theory, the ward rounds should all now finish by noon, when lunches are served. 'Protected meal times' notices on the wards indicate that patients must not be disturbed between noon and 1 pm.

We are told to write discharge prescriptions 'now' so that beds can be released to facilitate hitting the 4 hours targets in A&E. Patients are frequently moved overnight to meet the single sex bay requirements, and reviews on outlying wards may take twice as long, because we do not know the staff, and the ward layouts.

Lunchtime teaching sessions, essential for continuous professional development for consultants and for delivery of curricula for juniors run for an hour from 1 pm with clinics starting at 2 pm.

If we adhered to all of these requirements, the model ward rounds would run well into the afternoon and might not even finish before 5 pm. on some days.

The fact that the actual ward rounds finished before 1 pm. shows that the doctors on the rounds do not adhere strictly to IT governance policies, but adopt a pragmatic approach, accessing results if the software is 'open' without logging out and back in again. This results in their using systems on other user's logins, so that changes in clinical data will show on the logged in user's audit trail. Adopting this pragmatic approach implies that staff frequently disregard the IT governance policies, leaving themselves exposed to the risk of disciplinary measures, and even the possibility of sacking and or criminal charges. Frontline staff should not by put under additional pressure when they are already working hard and fast to try to outpace the illnesses of their acutely ill patients.

Discussion and conclusions

The written and unwritten rules of NHS IT and operational policies, designed with the intention of protecting patients, may now be actively hindering the processes of timely diagnosis, therapeutics and patient review, at least in the processes of acute medical care. A 'work to rule' by doctors and nurses using 'login to rule' in the NHS could paralyse clinical care processes by significantly prolonging wards rounds. The written, and perhaps more importantly, unwritten rules of NHS IT and operational policy must urgently be reconsidered to provide almost instant access to CCIS for all members of the healthcare team who are busy providing diagnostics and therapeutics to acutely ill medical patients.

How did we get to this sorry state? The various logons, user names and passwords were developed, I think, to protect patient confidentiality and to provide an audit trail of the updating of information. Unfortunately there seems to have been little systems analysis prior to computerisation. Before computers, every member of the team had paper and pen, so the starting point for computerisation would have been to develop ways to provide every team member with a computer. With the advent of the tablet computers, this may soon be feasible. For as long as there are fewer input devices than team members, individual logons are inappropriate for the necessary patterns of team working. Any casual observer would soon note that one doctor might be writing in the notes, and be called away to answer a bleep, and another doctor pick up the notes and carry on writing. In this study such a simple handover of roles would take 4 minutes on a bedside PC or laptop—40 seconds to logoff and 3 minutes 20 seconds to log all the way back in.

We must recognise the difference between confidentiality in protecting one's online banking accounts, and confidentiality in acute clinical care. An individual may well be able to manage his bank accounts alone, and is interested of course in avoiding theft and identity fraud. When that same individual is acutely ill, he/she needs a co-ordinated team of healthcare professionals—from the consultant to the ward clerk and even the cleaner—to take concerted swift effective action to deliver safe treatments while providing for basic physical needs and emotional support. All of these workers must be well-briefed in this case, and sharing of information needs to be facilitated, not tangled up in a web of multiple software applications, many user names and passwords combinations, and unnecessary restricted access levels. In acute care confidentiality relates to what the owner of the information does with the information subsequently, not to limiting access to the data. Our rules and policies are actually making it slower and harder to work just to access the crucial information on which rapid risk-laden decisions have to be made. If team members use the confidential information within the hospital to aid the patients' treatment, recovery, and emotional wellbeing, then this should be entirely acceptable ethically and legally. It is only if the team member spreads, without the patient's explicit consent, that information outside of work to people with no right to the information, that confidentiality is breached. By coming to hospital the patient gives implicit consent to the sharing of his health information to all of those who will cooperate in his care. All staff members are bound by the code of confidentiality. This inevitably increases the risk of information seeping out of the organisation, but the risks to patient safety of delaying access to CCIS are far higher, and the patient's clinical treatment is meant to be the centre of care.

Other patients in a bay soon come to know the clinical information about the patient, by overhearing the bedside consultation, and this usually serves to benefit the patient. Each bay is a small community, and the members generally support each other, identifying as fellow human beings in need.

The Fort Knox-style security on hospitals' IT systems is amazing when compared with singular lack of security in relation to the paper records. Any data criminal or other person interested in obtaining clinical information about a patient, would find it extremely easy to access a patient's notes, drug charts, printed results of bloods, X-rays and microbiology tests. Any competent actor could obtain this information within minutes of entering an NHS hospital, by a number of simple ploys, which I had better not reveal. Why battle through all those logins and passwords, when the same information can be read by picking up the notes, or phoning in for information?

The rule that secretaries and ward clerks are not given permission to view results on a computer system also does not make sense. Secretaries and ward clerks are expert at scanning results and bringing important results to the consultant's attention. If the consultant has to look up the results, he/she then dictates a letter containing the results, which is typed by the secretary, who then knows the results! This is an excellent example of how limiting access to knowledge in healthcare is incorrect. It is what the secretary does with the knowledge that counts as confidentiality or not, rather than the knowing of the information.

In my experience the only people who have problems in accessing the notes and computer systems containing this confidential data, are the patients and their relatives. A patient reading his notes will soon be questioned by a nurse.

There seems to be little evidence that data criminals or other people even want to access private individuals' clinical records. Are we struggling to protect ourselves from a non-existent phantom enemy? The only times these data seem to leak out are when public figures enter hospitals and their clinical details seem to leak into the press, and this causes no surprise. Often a trust media spokesperson announces the clinical details–I hope that the doctors involved have not briefed the media spokesperson, without consent from the patient!

I do worry about organised cyber criminals gaining access to masses of clinical data, which would be of interest to health and life insurance companies and marketing organisations. The NHS spine may make this easier than in the past. Insurance companies could use the data to raise premiums or deny claims. Offshore marketing companies could target sales campaigns at likely target patients e.g. HbA1c monitors to patients with diabetes. The NHS spine seems to me to have the potential to increase this risk. I imagine it would be straightforward for a professional cyber criminal to find out the user name and passwords of systems analysts and programmers, who have access to the core databases. Some knowledge of object database connectivity protocols might then allow queries to extract data on episodes of care with patient name, NHS number, addresses and ICD codes for recent admissions. These are the sort of data that when encrypted leave the NHS to Dr Foster and CHKS, and then are returned to trusts still with the

NHS number attached. Data confidentiality might be better protected by isolating each Trust's data warehouses and only allowing transfer of individual patient data to another Trust using strict processes and a file transfer protocol on a patient by patient and need to know basis.

Other NHS operational policies are also impacting on clinical teams' ability to deliver care, especially when the restricted time available under EWTD and New Deal is eaten into by non-productive logging on and logging off. I have given the protected meal times as just one example. If we adhered to the meal time policy, our ward round would have to be suspended at noon, and resume at 2 pm after the lunchtime education session and simultaneous with the start of clinics.

As the number of software packages in our trust increase by the month, I now have over 20 user name and password combinations necessary for my day-to-day NHS and clinical tutor work. The number of user names and passwords for each member of NHS staff should be reduced to one. Software and hardware developers must strive to develop log on or audit processes that match the pattern and pace of clinical work. Unfortunately, the healthcare seems to have accepted that logon security processes designed for office work are acceptable for ward and clinic working. We owe it to our patients to develop systems that allow immediate access to core clinical information.

I wonder if the risk to patients' care would actually be reduced if we had hospital systems with no logons and no logoffs, where staff members in uniforms have free access to all CCIS, and results and information such as drugs lists are a fraction of a second away. I believe the risk to the systems would be negligible if all the internal security was removed, particularly for simply viewing results, and previous documents. The number of people out there wanting to come into a hospital and find confidential data, or maliciously damage systems is trivial. Security could be achieved in many other ways. For example visitors' access to wards could be tightened up, or computers could be set to switch off at 5 pm in more open ward areas. No other professionals do such complex work, struggling to maintain confidentiality and privacy, with members of the public passing through the workplace.

One of our new software packages has an interesting approach to data accountability. No password is needed to view the data, but a user code has to be entered whenever data is entered or updated. This mirrors what happens in paper clinical notes which can be read without a record of who read them, but when a new entry is made the notes are signed. Coupling this approach with near range radio frequency identification such as used in credit cards, ski and transport passes could do away with the need for keyboard based logins altogether while maintaining audit trails.

Trusts and the NHS IT Board must ensure that large data warehouses are secure from organised professional cyber criminals. Every day it is ordinary patient care that is being impeded by our adoption of security processes suitable for single user office-based financial systems and inappropriately applying them to the highly complex every changing and dangerous world of acute care.

We urgently need a review of the written and unwritten rules of NHS IT security and other operational processes that tie professional staff to the computer and not to the bedside with the patient who has entrusted his life to a coordinated multi-professional team committed to his clinical, physical and emotional care. Unless this is done the next additional user name and logon could paralyse the care in your hospital. BJHCM

Herring R, Caldwell G, Jackson S (2011b) Implementation of a considerative checklist to improve productivity and team working on medical ward rounds. *Clinical Governance An International Journal* **16**: 129–36

Herring R, Desai T, Caldwell G (2011a) Quality and safety at the point of care: how long should a ward round take? *Clin Med* 11(1): 20–2