HealthManagement.org
Promoting Management and Leadership

Volume 11, Issue 1 / 2009 - E-Health

Patient Safety and E-Health

Since the publication in 1999 of arguably the most important call to action for patient safety, the Institute of Medicine's report 'To Err is Human', we have learnt a lot about how to reduce risk in healthcare and how to improve patient safety. Technology clearly has an important role to play but we know that it can also bring increased risks which every hospital board member should be aware of.

Research has shown that the context in which we work affects our behaviour and our chance of making mistakes. For example long hours and tiredness increases our chances of slips and lapses; insufficient staff or poorly designed equipment increases the likelihood of us taking short cuts and committing violations; a lack of communication and teamwork amongst colleagues and poor training increases the likelihood of knowledge based errors. Many of these latent, error producing conditions are organisational factors, often the result of management decisions taken to satisfy other priorities and needs, such as meeting externally imposed targets or balancing the finances.

Using Technology to Reduce Risks in Healthcare

Computerised decision support systems (CDSS) have grown in use in the last ten years, driven by clinicians suffering from information overload whilst being pressurised to make accurate, cost effective, evidence based clinical decisions. These systems provide access to a wealth of accessible information removing over reliance on memory; they use the power of the technology to analyse tests and compare the results to millions of stored images and evidence; and they accurately perform complex calculations taking into consideration multiple patient factors.

Once a clinical decision is made CDSS's can help with ongoing treatment. For example, electronic prescribing systems take the vagaries of the pen out of prescribing. They can ensure that blood tests are ordered when required for certain high risk drugs. Alerts are built in to laboratory systems highlighting abnormal values of test results. Reminders can pop up to prompt a review, for example a re-assessment of a patients risk factors for venous thrombo-embolism (VTE).

Electronic patient records enable fast access to important information at the point of clinical decisions being made, where ver the patient is.

Technology, People and Patient Safety

When considering e-health applications and patient safety it is important to recognise that we have mixed relationships with technology. Some of us feel at ease using the latest gadget, others haven't mastered the mobile phone and feel very uncomfortable anywhere near a computer. The way we see, feel, understand and

trust technology affects how we use it and this in turn affects patient safety.

The rapid development of technology makes it hard to keep up. The latest version always seems better than the one you bought last week and there are constant temptations to upgrade and improve. But this means multiple systems can be in use in one hospital, all of different ages and potentially not able to communicate with each other very easily. This increases the risk of staff not being familiar with the technology and not trained in its use. It also increases the risk of software related problems and the associated costs to sort them out. For managers it brings problems of not knowing who is most up to date and best able to advise the organisation on new technology.

Reporting and Learning About Adverse Events

It is vital in any organisation wishing to improve patient safety that staff report when things go wrong, or when there is a near miss. In any complex software there can be a hundred million lines of code and inevitably this will contain errors, making it difficult to find the source of a problem. Automatic error reporting systems are built in to some software, but not all, so other ways of capturing this information becomes essential.

Even if problems are reported, if it relates to the software it is often very difficult to repeat what happened and find the root cause. The vendors of e-health applications often can't find the root cause of a problem because they have assembled the system from components manufactured by different companies – so even they are uncertain about how the system works as a whole .

Design of the Processes to Use E-health Applications

In improving patient safety it is important to recognise that human behaviour is a function of the system in which people work. For example emailing pathology test results to doctors may appear on the surface to be very efficient but if they are too busy to look at their emails more than once a day then this new system will guarantee that a patient's abnormal test results will not be acted upon immediately. If there is only one computer on each ward and doctors are queuing up to use it, then computerised decision support systems will not be used. There are many techniques to help those implementing new technology to consider the processes and the potential risks that may arise. Failure modes and effects analysis is one such technique that is increasingly being used in healthcare. For example in one unit they had overlooked the need to ensure that the computer in the cardiac unit was always plugged into a socket powered by the hospital's generator in case of a power failure. If the computer screen showing where the probe was inside the patient's artery had gone blank in the middle of a procedure the outcome doesn't bear thinking about.

It is often faults in the design of the processes that create the conditions for staff to violate the rules and take short cuts. Leaving a computer logged in on a ward for all to use because it takes too long to keep logging off and on, sets up security problems and the possibility of one doctor reading records for the wrong patient. In one unit the staff took to carrying high risk drugs around in their pockets because of problems with the computerised pharmacy system. This highlights the importance of carefully designing and thinking through the process for using technology in healthcare, not only during installation but on a regular basis thereafter as other parts of the system change and develop.

Design of the Technology

With the increasing movement of professionals between hospitals and between countries the issue of familiarity with the technology in use in healthcare becomes important.

Hardware

We know that not being familiar with the technology can cause errors yet we still do not have standardisation of even the basic equipment. In one study by the National Patient Safety Agency in the UK over 60 different types of infusion device were found to be in use in one hospital. Starting in the top left, some of the keypads counted down from '9', others counted up from '0' with the potential for patients to be given massive overdoses. In a truly safe hospital system, all technology would have a common user interface allowing staff to walk in to any ward or clinic and be able to safely use any device or technology.

Software

Even if the technology is well designed, the software can let the operator down. For example drop-down boxes in electronic prescribing systems having drugs in alphabetic order putting highly toxic drugs with similar names next to the most commonly prescribed antibiotics, with inevitable consequences. Electronic prescribing systems have alerts built in to them to notify a doctor of a potentially toxic drug or combination of drugs but these systems often have ways of turning the alerts off or ignoring them by quickly pressing the return button. If alerts regularly appear they can become irritating and over time their impact lessens to the point where they are completely ignored.

Technology and the Operator

Skills and knowledge can be acquired in using the technology but the human condition brings other factors into play that need considering in the context of patient safety.

Trusting the Technology

In two tragic cases in the UK patients were overdosed when receiving radiotherapy treatment. Despite the procedures for checking doses, the staff had begun to trust each other and the machine and their levels of vigilance had reduced. Lisanne Bainbridge (1987) set out some of the principle 'ironies of automation' and here we find one: the fact that vigilance and monitoring, checking the performance of a machine over long periods of time is notoriously difficult for humans to perform but we often rely on it.

Applying what we know from other systems

When the computer at home freezes, after we have made our usual attempts to sort out the problem, we press the re-boot button, never quite understanding why it froze in the first place. Applying this approach to e-health applications can have much more serious consequences, losing valuable patient data or at worst re-setting carefully calibrated patient monitoring systems.

Readily available and non-judgemental support for people using complex technology is costly but vital with all applications in the hospital. Here we find another of Lisanne Bainbridge's (1987) 'ironies of automation': we leave the operator to carry out the tasks that the designer couldn't find a way to automate – such as the operator being left to recover a system breakdown. If the new technology has been introduced with the requirement to save money then often there is a downgrading of the skills of the people operating the system and with fewer clinical staff operating e-health technologies, risks will inevitably increase.

Mental workload of the operator

Physician job satisfaction was measured in one study of telemedicine assessing in particular mental workload.

The research into the telemedicine system found that the mental workload scores were high for the doctors and commensurate with those of air traffic controllers. This area requires much more attention as the technology becomes more complex.

Security and Backup

The loss of identifiable data held on computers is not uncommon. In November 2007 the government lost 25 million records giving details of names, addresses and bank accounts for people claiming child benefit . Despite systems and procedures and policies to prevent such loss, the rules are violated to save time and to help doctors with patient care – in one hospital I worked in, a doctor regularly saved on a USB key the records of the patients he was due to see the next day in outpatients, reading them at home in the evening. I found out when a member of his son's computer hacking 'club' rang anonymously to say he had gained access to the records!

E-health applications are now being designed to allow remote access by healthcare staff and also by patients via the internet, making the systems increasingly at risk from viruses and illegal access . Good practice in IT dictates that hospitals have systems in place for regular security testing, reporting vulnerabilities; that vendors should take steps to 'harden' their systems when implemented, for example ensuring that applications that might increase vulnerability are switched off and services on the internet are disabled, pop-ups and cookies blocked for example, but even these can be violated, especially if it means time consuming log-on procedures or slow functionality.

What About the Patient?

Studies of patient satisfaction with telemedicine are revealing – some patients are concerned about telemedicine meaning reduced social interaction with the doctor, feeling 'distanced' from the hospital; some are unhappy about having photographs taken and transmitted electronically (just look at what appears on YouTube!). Yet other studies have found patients prefer to communicate over the internet, avoiding travel to hospital and avoiding face to face contact.

What we don't know is how all this affects patient safety – does the feeling of being distant from the doctor mean that patients are more or less likely to comply with their treatment? Are patients more or less likely to reveal personal details required for a diagnosis over a telemedicine link if they are not sure who is watching? What about cultural differences? What about language? More research is needed here.

What we do know is that patients and their families will interactwith health technology in hospitals and at home. For example they will turn off irritating alarms; change dosages; and interpret and act on warnings. Family members will be asked to help or may play with the machine to see how it works. Againthis is an unexplored area interms of patient safety.

Quality Assurance –is the Technology an Improvement?

How accurate are the decisions being taken using the CDSS? Are the prompts and reminders being acted upon? Are appropriate tests and drugs being ordered? If the CDSS relies on information from other systems within the hospital, such as the laboratories and pharmacy, what reliability checks are performed to ensure these systems always communicate? What systems are in place to ensure that over time the knowledge base is kept up to date and that any new knowledge is checked and verified and agrees with local and national guidelines? And of most importance, how is patient morbidity and mortality affected by the CDSS – has the change been an improvement for patient care?

Management, Governance and Accountability

In the book 'Management Mistakes in Healthcare' a case study is presented relating to the purchase and installation of a new computer system in Heartland Healthcare System. The study sets out the management failures that can occur with the introduction of new technology ranging from recruiting people without the requisite IT skills and knowledge; illdefined roles of IT contractors; an absence of goals and measures of success; the absence of accountability; non-adherence to purchasing protocols; and a failure to prevent the 'intrastaff' warfare that subsequently developed. Any one of the failures listed would cause problems with the introduction of new technology and could introduce the potential for systems not to be set up safely.

Patient safety needs to be writ large throughout the information technology strategy of any healthcare organisation and needs to be central to the running of all systems that interact with the technology and with patient care. For example in the human resource department issues arise such as staffing levels and skills mix required to use the new systems; policies about the use of temporary staff, who may not be suitably trained to use the applications; also the ongoing training and accreditation for both new and existing staff in the use of the technology. Many organisations have introduced new clauses in staff contracts concerning the misuse of IT for example.

E-health has the potential to enable significant improvements in patient safety, it also brings with it new risks. Hospital boards need to have an understanding of these risks, an understanding of the theory of human error and systems thinking and ensure they have the requisite management systems in place to deal with them.

Author:

Susan Burnett,

Programme Lead,

Organisation and Management Group

Centre for Patient Safety and Service Quality,

Imperial College, London, United Kingdom

Email: s.burnett@imperial.ac.uk

www.cpssq.org

Published on : Mon, 23 Feb 2009