Inbox health check

Elizabeth Lomas elizabeth.lomas@northumbria.ac.uk
PhD student, School of Computing, Engineering and Information Sciences, Northumbria University

Email is now the main communication tool for all business sectors despite the fact that there are significant issues surrounding its management, confidentiality, security, legal compliance and long-term accessibility. Within the health sector, it has tended to be utilised as a tool for organisational communications separate from patient management. However, public expectations are changing and already the Royal College of General Practitioners (RCGP) has indicated that the provision of some level of patient email service is desirable.

Email is a key business tool, utilised globally by all business sectors. A recent survey by AIMM[1] concluded that it has become the main tool for business communications and, thus, has transformed the ways in which business is enacted. Email has replaced a large percentage of data that were previously transmitted by hardcopy letter, fax machine, internal memoranda, telephone and face-to-face conversation. It is a highly convenient tool enabling quick transmissions across the world in recordable and searchable formats, to multiple recipients, all at the touch of a button. It is easily copied and forwarded. It even has its own 'netiquette',[2] which includes NEVER TYPING IN CAPITALS UNLESS YOUR INTENTION IS TO CONVEY A SHOUTED MESSAGE!

The issues surrounding email management appear to be growing, rather than resolving themselves

However, no technology is without upside opportunities and downside risks. Email has presented organisations with new ways of working and also huge business and information management challenges. Although email was developed as long ago as 1971 and is now our most popular communication tool, the issues surrounding its management appear to be growing, rather than resolving themselves. Organisations face increased security and storage costs, information loss, staff management concerns and legal compliance issues surrounding its use and misuse. A recent Witness Seminar[3] was held at the University of Northumbria entitled *Examining the issues & challenges of email & e-communications* <http://northumbria.ac.uk/sd/academic/ceis/re/isrc/conf/wit07/>. The conference focused on the challenges of email from the perspectives of business, people, technology and future developments. Delegates discussed the information challenges facing all organisations and presented views on responses to these issues. Among the useful topics that were raised, Dr David Bowen highlighted the potential for applying plagiarism software technology with its highly sophisticated searching and word matching capabilities to email management. Dr Ishbel Duncan presented a corporate tale of Alice and her email management, which was recognisable to all and highlighted the requirement to train individuals in appropriate email behaviours and basic information management principles. The conference emphasised management's struggle to deal effectively with email as, despite its expansion into all business areas, it is rarely given the same level of attention as other dedicated information systems, e.g. an accounting or patient database.

The onus for email management is often transferred to individual users

The onus for email management is often transferred to individual users. Rarely do administrative personnel access and manage other users' email accounts. Thus, although email does have a number of indexing fields in the form of the date of email creation/receipt, an author address, recipients' email addresses and a subject field, together with the potential to classify the emails into hierarchical folders, the rules for utilising these fields and folders are rarely established. The result is that many individuals only manage their emails sporadically, often as and when they hit prescribed storage quotas at which time they are likely to focus on retaining what they need for personal usage rather than giving consideration to organisational requirements. Alternatively, PST files are often created, which are more difficult to search through centralised search engines. Thus, email becomes a tool for transient communications but not a longer term information and knowledge bank nor an intentional creator of legally auditable records. As there is a fairly frequent turnover in personnel within health trusts (in line with the national picture), this does have significant information implications. Email can only act as a low-level communication tool for short-term information exchange unless its management is significantly enhanced.

Email can only act as a low-level communication tool for short-term information exchange unless its management is significantly enhanced

Interestingly, most organisations recognise and resource strategies to minimise external security threats, but do not match the resources for internal email management. From an organisational perspective, the connection of any IT system to external networks presents additional threats that must be counteracted and mitigated. The types of malicious external security breaches diversify and expand daily, and range from hacking, malicious code, malware, non-repudiation, packet sniffing, phishing, spam, spoofing, spyware, Trojan horse, viruses, web-jacking and worm-viruses. However, recent information security reports have highlighted internal systems' failures as the main cause of security incidents. Many of these cases occur through employee action. Some internal security breaches may be malicious, such as cases of fraud, but many security incidents occur through genuine error often caused by lack of training.[4] Who has not accidentally sent an email to the wrong recipient?

People and chains of responsibility lie at the heart of security management

Within the health sector there is generally a high-level understanding amongst all personnel of the requirements for maintaining patient confidentiality; nevertheless, security incidents have still been reported <www.eveningleader.co.uk/news/Security-lapse-at-Wrexham-hospital.4299817.jp>. The Department of Health developed additional requirements for managing any information which contains data that identifies patients.[5] NHS trusts must appoint someone with the responsibility for information security for patient data, a Caldicott Guardian, in addition to the Data Protection Act's requirements that there is a nominated Data Controller for all personal information. This recognises the fact that people and chains of responsibility lie at the heart of security management.

Basic email training programmes often referred to as 'inbox health checks'

The critical component to the management of all information systems is training the user, yet most people do not effectively manage email. The growth of this digital data has in itself become a reported cause of work stress and distraction. Employees report failing to cope with the instant demands presented by the constant flow of arriving emails, all of which require review even if the sender has inappropriately copied the message to hundreds of colleagues <www.ehiprimarycare.com/comment_and_analysis/298/the_frustrations_of_gp_e-mail>. Some employees find that they cannot ever escape from the pressure of work and log in to email accounts from home or clutch a Blackberry whilst on leave. In addition, email users within all organisations tend to confuse personal and work boundaries when communicating within such a conversational format. Organisations are recognising the impact of distraction and stress upon their staffing resources <www.marketingservicestalk.com/news/meo/meo100.html> and some of these problems are being addressed through the development of basic email training programmes often referred to as 'inbox health checks' <www.timesonline.co.uk/tol/life_and_style/career_and_jobs/secretarial/article3153398.ece>.

Records and information managers grapple daily with the challenges of training users and managing digital data in order to ensure its accessibility over the short, medium and longer term. In the context of emails, some messages are not even captured in the first place (e.g. emails sent via Blackberries unsynchronised to servers or on personnel email accounts accessible through the internet such as Yahoo or Hotmail), the media on which they are stored deteriorates, or authorities fail to migrate records to new systems as technology changes, making the original email record inaccessible. Email also presents the problem of having numerous critical attachments in a wide array of formats.

The cost of email storage space

The financial and environmental cost of information storage is finally being recognised, if not the informational value of email communications. Computer-aided technologies have resulted in the creation of more records in one year than were previously generated in a decade and that increase magnifies daily. EMC[2] have calculated the costs of email storage and developed an information growth ticker which maps information generation to its actual power usage <www.emc.com/digital_universe>. The cost of email storage space is being minimised through new applications such as deduplification software which matches and deletes exact copies of emails stored across a system (e.g. global emails). Technologies exist to compress emails into systems referred to as 'vault' or 'archiving' solutions. These may help to reduce the cost of storing information although, in reality, the longer term access to emails and their attachments in multiple formats cannot be guaranteed beyond 2–5 years without migration strategies or where strategies fail IT recovery / forensic experts.

The risks and associated costs of not managing email will become unsustainable

Within the UK banking sector, new European legislation (*Markets in Financial Instruments Directive* [MiFID]) has required financial institutions to retain all emails to ensure auditability. New legislation may be enacted for other sectors as governments' desires to capture and monitor information grows. There is already a general legal requirement that, when a legal action is either brought or suspected, all related records must be retained, regardless of rules established within formal disposal schedules. This includes emails. Within the health sector, where there is a high level of litigation, the ramifications of legal discovery are significant. Without formalised and enforced email management systems, it is difficult to guarantee that all email data have been retained. As litigation and associated legal discovery requirements are likely to increase, the risks and associated costs of not managing email will become unsustainable.

The patient relationship adds a layer of complexity

Within the health sector, the same convenience and management pitfalls for using email exist as with other organisations, but the patient relationship adds a layer of complexity. For all of the above reasons, email has tended to be utilised as a tool for organisational communications separate from patient management. In the UK, patient relationships are still maintained largely through consultation and hardcopy letter. Sixty-two general practitioners within Dundee responded to a questionnaire and indicated that they regularly used email for communication within their practices and with outside agencies, but rarely with patients. Many perceived a need to provide an email service for clinical enquiries and repeat prescription requests, but felt constrained from doing so by a lack of an accepted system and workload concerns. In addition, there were concerns about confidentiality and social exclusion caused by literacy, language or technological barriers.[6]

> ... potential for applying plagiarism software technology with its highly sophisticated searching and word matching capabilities to email management.

However, it is possible that public expectations may change the boundaries of health advice; indeed, within the RCGP's *Good Medical Practice for General Practitioners*, the use of email is clearly indicated as a desirable means of communication. The guidance states on page 11:[7] 'Patients value being able to talk to a doctor or nurse on the phone or consulting through email. This often avoids the need for a surgery consultation or visit. Your practice leaflet and website should make it clear whether you have arrangements for patients to talk to a doctor or nurse on the phone or accept emails from patients.'

The legal ramifications and workload implications of initiating patient advice through email communications are significant

The legal ramifications and workload implications of initiating patient advice through email communications are significant. Opening up an email dialogue can sometimes create the expectation of further rapid and continued communication. One could question whether emails are an improvement to telephone conversation, which could be offered as a legally recorded dialogue? In reality, speech is quicker than typing and email hides some potentially important social cues that can be addressed through direct communication. Hesitation or reluctance to articulate a problem can potentially be resolved through conversation. Email provides a complex recorded chain which may inevitably conclude with the requirement for a face-to-face consultation. However, a recent survey of patients with an email healthcare service in the USA concluded that most patients favoured email for communicating in preference to the telephone or letters. In contrast, doctors in the USA were more likely to prefer telephone communication and less likely to prefer e-mail communication.[8]

Studies related to specialist sites offering medical advice via email services have shown that these can provide a helpful source of information and, thus, mitigate the requirement for a consultation in person. However, these services have been clearly established for non-urgent cases where simple tips or advice sent within a few days time-span are deemed by the patient to suffice.

Conclusions

Emails are here for the foreseeable future. Web 2.0 technologies are creating many other communication tools, e.g. instant messaging, Twitter, Facebook, *etc*., but these hold the same and often additional management issues. As more users across society utilise virtual communication tools, it is likely that healthcare will need to embrace some form of online communication, albeit potentially customised. The pressure to embrace virtual communication is likely to intensify if patients' data are stored online nationally and are remotely accessible. The logical extension to this facility is electronic dialogue. In order to face current and future challenges, organisational and personal inbox health checks are ceasing to be a chronic complaint and rapidly becoming a case for critical action.

References

[All accessed 10 September 2008]

1. AIIM. *E-mail management: an oxymoron*? 2006; <www.aiimhost.com/AIIM_News/IndustryWatch_Email_AnOxymoron.pdf>.
2. Camden and Islington Mental Health and Social Care Trust. *Email etiquette (netiquette) guidance*. 2007; <www.healtharchives.org/docs/CANDI_Email_Etiquette_Guidance.pdf>. Additional email policies and guidance are available from the Health Archives and Records Group <www.healtharchives.org/>.
3. Childs S *et al*. Examining the issues & challenges of email & e-communications. *Exploring strategies with experts*. 2nd Northumbria International Witness Seminar Conference. Newcastle upon Tyne, 24–25 October 2007. Newcastle, Northumbria University.
4. Poynter K. *Review of information security at HM Revenue and Customs. Final report*. 2008; <www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf>.
5. Department of Health. *The Caldicott Committee. Report on the review of patient-identifiable information*. 1997; <http://confidential.oxfordradcliffe.net/caldicott/report/> and <http://static.oxfordradcliffe.net/confidential/gems/caldrep.pdf>.
6. Neville RG *et al*. A survey of GP attitudes to and experiences of email consultations. *Informatics in Primary Care* 2004; **12**(4): 201.
7. Royal College of General Practitioners. *Good Medical Practice for General Practitioners*. 2008; <www.rcgp.org.uk/PDF/GMP_web.pdf>.
8. Hassol A *et al*. Patient experiences and attitudes about access to a patient electronic health care record and linked web messaging. *J Am Med Informatics Assoc* 2004; **11**(6) 505–513 <www.ncbi.nlm.nih.gov/pubmed/15299001?ordinalpos=1&itool=EntrezSystem2.PEntrez.Pubmed.Pubmed_ResultsPanel.Pubmed_DiscoveryPanel.Pubmed_Discovery_RA&linkpos=2&log$=relatedarticles&logdbfrom=pubmed>.

Note: **Elizabeth Lomas** is currently conducting a records management co-operative action research project, *Continued Communication*, aiming to maximise information benefits for Information and Communication Technology Systems.