Information in practice

Smart cards—the key to trustworthy health information systems

Roderick Neame

Health Information Consulting, Homestall House, Faversham, Kent ME13 8UT

Roderick Neame, *managing partner*

BMJ 1997;314:573–7

Summary

Some 20 years after they were first developed, "smart cards" are set to play a crucial part in healthcare systems. Last year about a billion were supplied, mainly for use in the financial sector, but their special features make them of particular strategic importance for the health sector, where they offer a ready made solution to some key problems of security and confidentiality. This article outlines what smart cards are and why they are so important in managing health information. I discuss some of the unique features of smart cards that are of special importance in the development of secure and trustworthy health information systems. Smart cards would enable individuals' identities to be authenticated and communications to be secured and would provide the mechanisms for implementing strong security, differential access to data, and definitive audit trails. Patient cards can also with complete security carry personal details, data on current health problems and medications, emergency care data, and pointers to where medical records for the patient can be found. Provider cards can in addition carry authorisations and information on computer set up.

Scenario for use of smart cards in health care

A doctor arrives at the consulting rooms she will use for this session. The computer on the desk invites her to enter her card: she inserts her smart card into the reader, enters her PIN (personal identification number) to enable it, and in a few seconds the screen is configured in the way she prefers it, with network connections established to her preferred resources and a copy of the most recent release of her preferred software loaded.

A patient arrives at reception and hands over his smart card at the desk: the bar code is scanned (or the magnetic stripe swiped), which serves immediately to locate any paper records and related documents (such as recent reports or results), to check the patient into the waiting room, and to append his name to the list of those waiting to see the doctor.

On entering the consulting room, the patient hands over his card and the doctor places it in a smart reader. He enters his PIN, thereby enabling records held locally to be retrieved and displayed on the screen. The doctor notes various entries on the patient's card relating to previous care encounters, tests, and reports. Some of these seem relevant to the present problem, and she asks the patient to authorise their retrieval. The patient re-enters his PIN, and, by simply clicking a button, the doctor can then retrieve notes, images, and physiological and audio traces held elsewhere, even from another country.

The doctor orders a blood test and prescribes some drugs. She also prepares a brief summary of the encounter. Both orders and the summary are de-identified and posted to a web server: pointers to those records are written on to the patient's card, together with a random password. A report of services provided is generated, verified by the presence of both the patient's and the doctor's cards, and is sent electronically to the contract management office for financial management.

The patient's card is removed and returned, and he goes to a pharmacy of his choice to retrieve the prescription and to a laboratory to have the test carried out. He can use his card at home or in various other locations to read and back up his records and update his personal details as well as to access various other resources, including a suite of high quality health information designed to support him in playing a greater role in his own health promotion and healthcare decisions.

At the end of her session the doctor removes her card, thereby returning the computer to a state of readiness to accept the card of the next user.

Introduction

Quite soon you may find yourself locking and unlocking the computer where you practise with a "smart card." This technology and the resources of the Internet will finally allow us to move away from the concept of the personal computer—owned and used by a single person and customised to his or her specific needs—to the personalisable computer—a generic and ubiquitous tool that can be quickly configured to match individual requirements. Software will be a network resource rather than a personal possession, and users will pay to use the software, just like the existing electricity and water utilities, rather than buying it outright and having to support, maintain, and replace it.

Your patients, too, will probably hold a card that carries personal and health information and acts as an access key to their data wherever they are held. None of this is new technology, and all of it is already working in one form or another. At present smart cards can be found in digital mobile phones, in satellite broadcast receivers, as "loyalty cards" for department stores and supermarkets, and as electronic "cash" (such as

Exeter Care Card pilot[3]

The Exeter Care Card trial was sponsored by the Department of Health and explored the potential of computerised medical records that were retained by patients. The trial ran from 1989 to 1992 and included 13 000 patients, two general medical practices, eight community pharmacists, one general dental practice, a community hospital, and a general hospital, all within one district.

Patients were issued with a smart card that carried administrative, clinical, emergency, and prescription data that could be added to either automatically from a computerised medical records system or manually with a stand alone application. Access to the patients' data was regulated by the health professionals' card, which determined the level of access that was permitted to each user (based on a need to know analysis). The professionals' card also provided data to create an inerasable audit trail of transactions.

The evaluation showed that use of the card record system was associated with significant changes in the following areas: reduced cost of prescribing; reduced costs of investigations carried out; reduction in risk of iatrogenic illness, particularly in relation to dental care; reduced times taken for communicating data; and ready access to a useful patient medical record. Pharmacists thought that such a device was the only reliable and safe way of maintaining a pharmacy "medical" record. There were too few interactions of patients with the emergency services to evaluate the usefulness of the portable record in emergencies. Patients' acceptance of the devices and compliance in use of the system were extremely high.

Mondex[1]) or stored value (such as telephone) cards. They are about to become widely used in financial and credit cards of various types. About 90 million smart health cards were in use at the end of 1995,[2] constituting about 13% of all smart cards in use. The French are already issuing smart cards to healthcare providers, and in numerous locations, including Canada, Germany, and Britain, healthcare smart cards are in use in pilot or operational settings.

What is a smart card?

The term "smart" is used to distinguish such cards from the many "dumb" cards that we typically carry—for example, credit cards, which can be recognised by the magnetic stripe on one side. Magnetic stripe cards carry data (equivalent to about 200 characters) but those data are accessible to anyone with a reader such as can be found in almost every business or shop. Smart cards also carry data in an electronic memory, typically about 8000 characters (but larger capacity is available, as are routines for compressing the data to occupy less memory). However, the data stored on a smart card are secured against being read by anyone unless he or she has the enabling code (typically a PIN held by the card owner) and an authorised reader system. Even when the reader system is given the enabling code the card may be configured to reveal only some of the data it holds depending on the classification of the user (as identified by his or her personal smart card). Thus, it could be configured to reveal different data to a psychiatrist than it would reveal to a paramedic, general practitioner, or obstetrician. That is part of what makes it smart.

In fact a smart card is a miniature computer without a keyboard or screen. The reading system supplies power to the computer chip on the card, which can then communicate with the reader and process data according to its own software programs stored on the card. The card software is installed at the time of manufacture and cannot be altered thereafter. Most of the data on the card are added and updated after the card is issued. Data can be held with different levels of security, permitting differential access to different classes of authorised reader. Some data (such as passwords and "keys") are held in a secret area inaccessible to all users but accessible for use and for making comparisons (such as checking that the PIN is correct) by the card chip. The security is such that multipurpose smart cards could safely be produced, such as a combined credit card and health card, with complete separation of data contents: the credit data would be accessible only to authorised financial applications and the health data accessible only to healthcare systems. The opportunity to replace all those plastic cards in your wallet with a single smart card now exists, at the same time greatly increasing protection against loss or theft.

There is no reason why any card should be limited to just one form of data storage: as well as a smart chip, it could have a magnetic stripe, photograph, embossed name and address, signature, bar code, and even an "optical" memory surface (similar to a piece of a compact disc) for good measure.

Clearly, agreements on a card's physical aspects will have a large impact on speed of uptake of the technology. To a lesser extent, speed of uptake will also be affected by the adoption of one (or a small number of) communication protocol between host systems and cards and by agreements about the core health data that should be stored on the card and other issues about data and software.

What makes smart cards special?

Smart cards have two key attributes: they can carry a substantial quantity of data in a compact and computer readable form (as can many non-smart cards), and they

PANACEA

This is a European funded initiative to develop a universal interface for the exchange of medical records from different systems via several different communication methodologies. These include the use of patient held records on smart cards. Smart cards for healthcare professionals control the access to data on patients' cards and on local and remote medical record systems.

The British trial is being conducted by the University of Exeter's Institute of General Practice and involves communications between general practice systems and a community information system. Full transfer of medical records using the interface is shortly to be tested between sites in Britain, Portugal, and Sweden. Smart cards containing plans for care are to be issued in selected situations to patients who make frequent use of services and need coordination of their care.

can carry it securely (a point of major difference from non-smart cards).[4] The second attribute is crucial to the role that smart cards will play in health care, in which security of data and confidentiality are generally recognised as being pillars of ethical practice.

Computing environments that have many users routinely experience problems in three areas: authenticating the identity of individual users, ensuring confidentiality of data in storage, and securing data against interception or alteration when in transit (communication).

Identifying and authenticating individual users

Establishing a person's identity is crucial as a foundation for any security system. Users of a computing system are granted privileges to read, write, and update the records it holds. In a health system authorised staff can, for example, issue requests, referrals, and orders for services, thereby committing funds and initiating processes that can profoundly affect the lives of their patients. Some systems may restrict certain transactions and functions to certain classes of user (for example, only registered medical practitioners may issue prescriptions). Clearly, there must be an indelible record to ensure that the responsibilities of those carrying out transactions are recognised and that they can be held accountable for their actions, both for the effects on patients and for the costs to purchasers. It must therefore be possible to authenticate definitively the identity of the author of every note comprising the electronic medical record for an individual patient.

Authenticating the identity of each patient is similarly important, particularly if the patient is not personally known to the doctor, since it is vital to ensure that records, results, orders, prescriptions, and other (electronic) documents do indeed relate to that person. It is here that the special properties of the smart card are invaluable, since the card can directly check that the PIN is correct (it is held in a secret area on the card) without reference to any central repository. Of course, it would still be possible for people to deliberately breach their own security by giving their card and PIN to someone else, but it is otherwise extremely difficult for a third party to breach a security system based on smart cards. Additional security against fraud could be implemented by storing a biometric key (such as a fingerprint) for the cardholder on the card that would be verified directly, ensuring that the card could be used only by its owner.[5]

Only when the identity of every individual can be authenticated does it become possible to implement strong security (control of access, audit trails) that can ensure accountability for transactions and to generate trustworthy electronic "signatures" for documents.

Ensuring confidentiality of stored data

Doctors and patients expect medical records to be kept confidential. Ideally, patients should be in a position to grant access to their data as they see fit, with the agreement of the author. The smart card can provide that capability: when patients provided their card and satisfied the authentication requirements they could enable access to their records wherever they may be stored. The holders of the stored data could therefore be sure that a patient had approved the access, and an electronic signature for the patient could be attached as evidence of that approval. Different users could have access to different data—for example, the data available to a first aid team could be different from those available to a specialist surgeon. Some data might be restricted to be accessible only to the person who made the entry.

Clearly, for this to happen the records must be held in a compatible format, and, fortuitously, such a format has recently emerged. The fundamental issue is that it is the user who must determine what information is required, not the holder of that information. The conventional paradigm for interchange of electronic data is based on the model of "pushing" — the holder of data pushes it to where he or she thinks that it is required. Inevitably, this is limited by the holder's present knowl-

Rimouski project and Quebec health card

The Rimouski pilot project tested the use of health smart cards during 1993-5 in the city of Rimouski, about 300 km from Quebec City. The software system has been designed to interact with any form of card, smart or optical, from any manufacturer, and is not dependent on the use of one specific type of card or technology. However, the pilot in Rimouski concentrated on the use of just one type of smart health card.

The pilot included 7250 patients and 300 health professionals (general practitioners, specialists, pharmacists, nurses, and ambulance staff). The card carried personal and health data, secured by a PIN, in five categories—identification, emergency, vaccinations, medications, and ongoing care (history, consultations, follow ups, etc). It was designed to enable patients to provide more complete information to their care provider to reduce redundancy of tests; to reduce the risk of drug interactions; and to improve the quality, continuity, and integrity of care. The evaluation judged the project a success in improving availability of clinical information while protecting personal privacy and encouraging better follow up, and it was especially useful in emergencies.

Quebec is to issue seven million health smart cards from 1998: initially, they will store administrative data to provide a check on eligibility for services and replace the existing insurance cards. The health data will be added later. The citizens of Rimouski are continuing to use their health smart cards.

Health cards in France

Smart cards in France go back to their original development by Roland Moreno in 1974. The Carte Sante (health card) was launched in 1990 at the instigation of the mutual insurance companies, with 250 000 cards issued and 1000 readers provided in medical practices in 1992. The system shows the trend towards convergence between medical and financial applications. The card is part administrative and part medical record. The administrative data include personal, social security, and health insurance contributions details as well as acting as a means for paying for health services. The medical record includes emergency data as well as some ongoing health records.

At the core of the system is a processing centre which manages the financial transactions, contributions from patients, and payments to providers as well as collecting some updated medical data. The current plan is to issue some 600 000 health professional cards and 50 million patient cards by the end of 1998 in the Sesam Vitale programme. The driver behind this initiative is primarily the electronic management of payments, although limited medical records will still be carried.

edge of the situation. A patient, however, may see various healthcare providers, any of whom might require access to relevant past information. Therefore, it is the users who need to be able to assemble relevant data by "pulling" it to their workstation: in some instances their needs may be predictable, but in many cases they will depend on the movements and health status of patients. The world wide web operates on exactly this paradigm,[6] storing large amounts of data that can be accessed and retrieved as required by millions of users across the world using readily available and cheap "web browser" technology.

A patient's smart card would "point to" the records belonging to the patient, enabling a doctor to retrieve them as required. The records themselves could be stored without any identifiers whatever, since the patient would hold the links between patient identity and stored records on his or her card. This transform overcomes the concerns about privacy and confidentiality of data stored in so public an environment.

The encounter, if non-trivial, might generate further orders or referrals and would normally give rise to a summary that should be accessible to other providers caring for the same patient. These notes, "de-identified" as outlined below, would be posted to a computer that was accessible to all users. Pointers to these new records would be added to the patient's card, together with a password, which would also be embedded in the new records. This would ensure that when a de-identified record was retrieved there was a simple way of checking that it did indeed belong to this patient, by checking that the passwords matched. The combination of both the health provider's and the patient's cards in the same place would verify that the encounter between the provider and patient had taken place. The paperwork related to the service and associated financial transactions could be substantially simplified by the use of this technology, thereby forging closer links between health and finance sectors.[7] The summary, orders, and claim could all be electronically "signed" by the doctor using a unique digital mark generated by the card (see below).

Securing data and communications

Electronic communications have two potential weaknesses: they can be intercepted in transit and their contents read or even changed, so raising concerns about their integrity; and it may be difficult to be certain of the origin and authorship of a message, so raising doubts about its authenticity. Encryption offers perhaps the best solution to these problems: encrypting a message is intended to render it meaningless to anyone without the necessary key, and if each person has his or her own unique key, a message can be transformed such that it can be read only by the person to whom it is addressed. At the same time, the sender can append his or her unique electronic signature to the message. Together, these two security measures mean that the receiver can be sure that the message came from the purported sender, could not have been changed en route, and cannot subsequently be denied by the sender. Important reassurance indeed.

The "keys" and routines (often called algorithms) for managing these essentially mathematical processes can be stored on smart cards and automatically retrieved whenever an encrypted message was sent or received. This relieves cardholders of any burden involved in remembering keys or passwords, other than the PIN required to enable their card to function.

It is necessary to have a chain of trust between the sender and receiver of a message, particularly when one may be unknown to the other. This would require setting up a network of "trusted third parties," each of which would vouch for the integrity of the people whom it authorised and to whom it issued "keys." The chain of trust is in the form of an inverted tree: at some point two people will share a common trusted third party and could therefore reasonably expect to be able to trust each other.

A new security paradigm

It is clear that security of information is near the top of the list of concerns about the electronic management of health information for both patients and professionals. Barrows and Clayton review some of the key issues.[8] If we are considering moving health data around the Internet, and it seems inevitable that this is the direction of the future, then it is clear that we must seriously consider issues of security given the essentially open nature of the Internet.

In fact, smart cards could resolve many of the confidentiality problems that bedevil existing electronic environments. Information is confidential only when it can be associated with an individual: remove all personal identifiers and the data no longer constitute a threat to personal privacy. However, this transformation can also make the data useless for providing care, unless there is some way to link stored records back to the patients concerned. If patients are able to identify their own records and documents this problem disappears: with a smart card this would be simple.

The medical record comprises dozens of notes, requests, reports, etc, often held in different places and often without anyone being aware of the full picture. The "medical record" in reality has no discrete physical existence but is a virtual entity comprising all the part records and notes held in all those different locations. Each entry, or group of entries, in the record comprises personal as well as clinical and administrative data. For each entry, the personal data could be removed, leaving de-identified records (which could be made generally accessible with a web server as outlined above) while the links or pointers to these de-identified records would be held on the card of the patient concerned. The capacity to assemble these fragments into an integrated whole is essential for continuity and integrity of patient care.[9] The de-identified notes held on a web server could be linked to the patient concerned only by the doctor who wrote them and by the patient, who would hold the index and the keys to access them on a smart card. Authors of care notes would, of course, always have access to their own records: in some circumstances they might be obliged to make parts of these data available to others (such as purchasers), which they would still be able to do.

In most jurisdictions legislation about the privacy of personal information prevents disclosure of personal information to third parties without the knowledge and consent of the person concerned other than in certain exceptional circumstances. The use of a smart card could give effect to this intention and put patients in control, if they so wished, over who else had access to which of their personal health records. Since none of these de-personalised records would be a security risk, they could be stored on computers accessible to the public on the Internet, even in readily readable form as is used for the world wide web (hypertext mark up language). This means that they could be accessed readily with cheap (currently free) browser software using cheap communications networks (the Internet): the potential to exchange medical records within and between service providers using the "pull" paradigm outlined above for improving continuity and integrity of care would be achievable at low cost. What is more, this could enable the goal of "patient empowerment" to be achieved at the same time: patients could control access to their own personalised records, as well as reading them when they chose to do so or when they wished to seek an independent audit or review of their care.

Lost or forgotten cards

What would happen if patients lost their card? Quite simply, they would be no worse off than at present, but none of the benefits of having a card would be available to them. Lost cards could not be read, and attempts to break into them would cause them to lock and render them useless. When a card was lost, none of the data it held would necessarily be lost since the card would hold only a secondary copy of primary data stored on practitioners' systems. Reassembly of that data would be possible (albeit at a cost) once the patient's identity had been satisfactorily authenticated by some other means. Patients would be encouraged to regularly back up their card on to paper, diskette, or their own computing facility to help recovery after loss.

When just the PIN was forgotten, or when a patient was unable to provide it (such as when unconscious), provision could be made for identified professionals to "break in." A break in would generate an audit trail, which could be made inerasable, and, since the professional breaking in would have to use his or her own smart card to do this, the identity of the person concerned and the reason for this course of action would be known to the system and could be communicated to the patient. The nature of the duty of care of a health professional to a patient is such that ethicists would most likely consider breaking into a personal health card as obligatory if there was any possibility that the data it held might be important in avoiding serious risk to the patient in terms of decisions about current care. This is one of the exceptional provisions for disclosure contained in most current legislation about privacy of information.

Other data on the card

I have emphasised the unique security features of smart cards, but we should not overlook the benefits conferred by the ability of the cards to act as portable stores of important information. This could include personal details (some of which could be updated by the cardholders themselves), data on emergency care, preferred computer configuration (for providers), etc.

Conclusion

Smart cards enable people's identities to be authenticated and communications to be secured and provide mechanisms for implementing strong security, differential access to data, and definitive audit trails. They offer a mechanism for implementing trust in healthcare communications. They can also carry data, such as personal details, and can be used to configure any computer as a personal workstation, enabling the move away from personal computers to personalisable computers and towards information management as a public utility rather than a personal millstone.

Smart cards are set to play a pivotal part in the future development of computing in general, and particularly in health care. We need to come to grips with the issues now in order to control and direct their incorporation into systems and services that serve the needs of the profession and their patients. It will be exceedingly difficult to tack them on to systems based on information plans in which they do not feature, just as it is proving extremely difficult to tack adequate security on to systems based on information plans that lacked an appreciation of the security issues in health care.

1 Jones T. Mondex—the introduction of electronic cash. In: *Smart card technology international.* London: Global Projects Group, 1996: 144-9.

2 Datamonitor. Opportunities in global smartcard markets. *E-med News* 1996;30:2.

3 Hopkins R. *Exmouth Care Card evaluation report.* London: HMSO, 1990.

4 Pesonen L. The security of the smart card operating system. In: *Smart card technology international.* London: Global Projects Group, 1996: 112-20.

5 Carter B. Biometrics—is it the right time? In: *Smart card technology international.* London: Global Projects Group, 1996: 14-24.

6 Cimino JJ, Socratous SA, Clayton PD. Internet as clinical information system: application development using the world wide web. *JAMIA* 1995;2(5):273-84.

7 Monod E. Health care and finance: opportunities for convergence via the smart card. In: *Smart card technology international.* London: Global Projects Group, 1996: 186-92.

8 Barrows RC, Clayton PD. Privacy, confidentiality and electronic medical records. *JAMIA* 1996;3(2):139-48.

9 Engelbrecht R, Hildebrand C, Blecher M. Improving patient care by the use of smart cards. In: van der Lei J, Beckers WPA, eds. *Proceedings of AMICE 95 conference.* Amsterdam: VMBI, 1995: 227-33.

Netlines

Microbial genomes

- Sometime early in the next century, the human genome sequence will be completed (see **http://www.hgmp.mrc.ac.uk/Public/human-gen-db.html** for some human genome links). However, just now all the action seems to be in the field of microbial genomes. The genome of *Escherichia coli* has just been completed (see **http://mol.genes.nig.ac.jp/** and **http://www.genetics.wisc.edu**) and is the third bacterial genome to be published, following those of *Haemophilus influenzae* and *Mycoplasma genitalium* (**http://www.tigr.org/tdb/mdb/mdb.html**).
- As many as 100 microbial genomes are likely to be sequenced in the next few years. Terry Gaasterland's running list of genomes in progress (**http://www.mcs.anl.gov/home/gaasterl/genomes.html**) already lists 45 bacterial genome projects.
- One astonishing aspect of this subject is the rapidity and ease with which data on genome sequences are made available to the general public over the world wide web. In many cases you can do sequence similarity searches on genomes even before they are completed — examples include the genomes of *Mycobacterium tuberculosis* and *Plasmodium falciparum* at the Sanger Centre (**http://www.sanger.ac.uk/pathogens**) and that of *Neisseria gonorrhoeae* at the University of Oklahoma (**http://dna1.chem.uoknor.edu:80/gono.html**).
- Several other sites offer facilities that put genomic data into a functional context, including EcoCyc and HinCyC (**http://www.ai.sri.com/ecocyc/ecocyc.html**) and the NCBI (**http://www.ncbi.nlm.nih.gov/Complete_Genomes/**).

Human genetics on line

- Although only a small fraction of the human genome has been sequenced, powerful databases have been developed to provide information on human genetic disorders. The On-line Mendelian Inheritance in Man (OMIM) database (**http://www3.ncbi.nlm.nih.gov/Omim/**) is intended for use primarily by doctors and other professionals concerned with genetic disorders, by genetics researchers, and by advanced students in science and medicine. All the information you could want is there on over 8000 inherited disorders—including details of clinical and biochemical features, diagnosis, genetics, and animal models, together with pictures and hypertext references to Medline articles and sequence information in the Entrez database.
- Along the same lines as OMIM is Genline (**http://www.hslib.washington.edu/genline/**), although as yet it contains a much smaller set of entries.

Seek and ye shall find

- The semi-anarchic nature of the Internet means that there can never be an up to date, comprehensive index of what is available on line. However, searching for medical information is made easier by two indexing sites: in Britain OMNI (Organising Medical Networked Information) provides a searchable list of sites, with some commentary, on **http://www.omni.ac.uk**, while in the United States the medical matrix plays a similar role on **http://www.slackinc.com/matrix/**.
- If it's shareware that you are after, the Higher Education National Software Archive (**http://www.hensa.ac.uk**) provides a well indexed site full of shareware (although you have to be a British academic to access it).
- To find out what is being said on the network news groups, try DejaNews (**http://www.dejanews.com**), which stores all sorts of news group postings, or, to focus on biomedical news groups, visit the Biosci site (**http://www.bio.net/**).
- If you are looking for someone's email address try the Four11 site (**http://www.Four11.com/**).
- Finally, if you want to buy a book over the Internet, visit Amazon on **http://www.amazon.com.**

Post-traumatic stress disorder

- The US National Center for Post-Traumatic Stress Disorder (**http://www.dartmouth.edu/dms/ptsd**) has recently launched a web interface (**http://dciswww.dartmouth.edu/cgi-bin/dcis/wdi?&Alexandria.Dartmouth.EDU&51001&PILOTS%20Catalog&s**) to its bibliographic index of the worldwide literature on post-traumatic stress disorder. The site also features fact sheets on the condition and links to related material on the Internet.

Medicine and anti-medicine

- While within the medical profession we struggle to practise evidence based medicine, many outside are turning their backs on science and conventional medicine. Those wishing to reverse this trend would do well to visit Brian Wall's HealthWatch page on **http://user.itl.net/~brian/HWATCH.HTML**. HealthWatch is a British based charity which ensures that the alternative, the complementary, the unsubstantiated, and the plain silly are all put through the blast furnace of evidence based medicine.
- Sadly, one of the staunchest defenders of science against anti-science, Carl Sagan, died at the end of last year after a long struggle with myelodysplasia (**http://www.sciam.com/explorations/010697sagan/010697explorations.html**). Sagan was author of the best selling science book of all time, *Cosmos*, and, most recently, produced a defence of science in his *Demon-Haunted World: Science As a Candle in the Dark* (**http://www.amazon.com/exec/obidos/ISBN=1561006491/7154-8200924-333098**). For a review of Sagan's life and work, visit Michael Rapp's unofficial Carl Sagan web site on **http://wwwvms.utexas.edu/~mrapp/sagan/toc.html.**

Trauma Moulage

- Trauma Moulage is an interactive educational web site (**http://www.trauma.org/resus/moulage/moulage.html**) in which you are a casualty department doctor who must assess and treat an injured patient. It's not easy—I killed the patient several times over, so I had better stick to laboratory medicine. If, like me, you had never come across the word "moulage" before, you can look it up in the online Webster's dictionary on **http://gs213.sp.cs.cmu.edu/prog/webster?moulage.**

Compiled by Mark Pallen
email m.pallen@qmw.ac.uk
web page **http://www.qmw.ac.uk/~rhbm001/mpallen.html**

If you are not yet on line you can find help in getting connected in the *ABC of Medical Computing* (eds Nicholas Lee and Andrew Millman, BMJ Publishing), which has Mark Pallen's *Guide to the Internet* as a supplement.