Ethical Dilemmas of the Practice of Medicine in the Information Technology Age

C J J Yeo

(This essay won the Singapore Medical Association Ethics Essay Award (Medical Undergraduate Category) in 2002 and has been minimally edited to reflect the original entry submitted by the author.)

Increasing reliance on computers and Information Technology (IT) has led to changes in the way we diagnose and treat patients. The development of new techniques of practising medicine presents novel challenges to our ethical and moral reasoning.

The ethical principles of non-maleficence, beneficence, autonomy, veracity, confidentiality, social responsibility and justice assist a physician in his relationships with patients, other physicians, healthcare systems and society[1]. Ethical dilemmas arise from conflicts between the guiding principles and other interests, or between the principles themselves.

With the popularity of the Internet in the IT age, a critical ethical dilemma involves protecting patient confidentiality and privacy while expanding access to information. The advent of e-commerce in the practice of medicine has drawn renewed attention to the conflict between economic interests and the principle of beneficence, which advocates the patient's welfare as the first consideration. While the computerisation of healthcare is productive and cost-effective, ethical dilemmas arise from friction between the goals of efficiency versus the principles of autonomy and confidentiality. Long distance or online consultations, as practised in telemedicine and cybermedicine, have created ambiguous patient-physician relationships that pose new ethical dilemmas. Finally, the contribution of artificial intelligence to diagnosis and treatment has originated ethical dilemmas over the extent of physician reliance on machine intelligence.

The electronic transmission of sensitive medical data in IT may cause the principles of autonomy and confidentiality to be inadvertently breached. Ethical dilemmas arising from conflicts between accessibility and efficiency versus patient privacy, confidentiality and informed consent are found in the use of computerised patient records, telemedicine and cybermedicine.

Although computerised patient records are widely accepted in hospitals because of cost savings through the efficient collection, aggregation and dissemination of personal information, privacy and confidentiality are often compromised when transmitting the records via the telecommunications network. This is because electronic communications through telephones, emails, fax machines and computers can be intercepted in transit and data can be read or altered. Hackers can potentially access computerised medical records on a network, and honest mistakes could result in confidential medical information being sent to a wrong address. In August 2000, it was made public that due to human error, the confidentiality of 858 members of the Kaiser Permanente Health Care System was breached[2]. In January 2001, the University of Washington Medical Centre affirmed that a hacker had gained access to administrative databases containing confidential records of at least 5,000 patients[3].

In addition, the highly sensitive medical information is routinely shared by third parties not involved in patient care. Privacy and confidentiality can hardly be upheld when social and welfare agencies, education institutions, civil and criminal justice systems, public health agencies, and medical and social workers have free access to classified information. Misuse of the computerised patient records may lead to personal humiliation, loss of reputation and risk to financial status.

Furthermore, since electronic collection and storage of personal health data cannot guarantee privacy, the patient has no real jurisdiction over who sees his medical history and may not understand the true implications of the disclosed information. Clearly, the criteria for informed consent, which includes the patient understanding the information provided, being competent enough to give consent and grant it voluntarily, are not met. Hence, not only is the patient's privacy and confidentiality lost, the key elements of informed consent are also absent. The conflict between the pursuit of efficiency and cost-effectiveness against the principles of autonomy and confidentiality constitutes the modern ethical dilemma in the use of computerised patient records.

The principle of justice and social responsibility, which states that physicians should work for the

Crystal Yeo Jing Jing
Medicine Year 1
NUS

Correspondence to:
Yeo Jing Jing Crystal
Email: crystaly@singnet.com.sg

greater good of the society and avoid discrimination on age, sex, religion, race, position or rank, embodies the basic tenet of telemedicine. By enabling health-care professionals to consult quickly with consultants or specialists without the need to travel or move patients, telemedicine eliminates geographical boundaries in remote places where there is no specialist treatment, and makes medical facilities and high quality healthcare available to all, rich and poor alike. Unfortunately, as knowledge is electronically shared between physicians via telecommunication devices such as "store-and-forward" images of X-rays and scans, remote monitoring, and interactive video conferencing, the same risks of data interception and alteration as that in computerised healthcare apply[4]. In addition, telemedicine undoubtedly requires medical record transmission via computers, increasing the potential for unauthorised exposure of classified medical information to third persons. Evidently, the ethical dilemma lies in the difficulty in maximising resources and access to medical knowledge and expertise, while preserving the confidentiality of transmitted patient data.

The conflict between the principles of beneficence versus that of confidentiality and autonomy comprises another ethical dilemma in telemedicine. While the patient's welfare remains the first consideration, elements of confidentiality, privacy and informed consent are sacrificed. This occurs because telemedicine consults are often done only between the physicians and without the knowledge or consent of the patient; for instance, when interactive video conferencing is used by a rural emergency room to consult with a trauma centre in a big hospital[5].

The intrinsic affiliation of cybermedicine with the Internet increases accessibility to medical expertise and information dramatically, but at the same time escalates the risks of privacy and confidentiality violations. As cybermedicine involves unknown physicians setting up web sites to diagnose unknown patients, email correspondence is the best, if not only, means of communication between physician and patient. Email messages from patient to cyberdoctor are confidential, as they may form part of the patient's medical record. Yet email is more easily intercepted than landline telephone communications and poses extra security and confidentiality concerns similar to other electronic communication devices. Unknown to the patient, email can be forwarded to other recipients. Also, records of email messages remain stored on a central server, even after they are deleted off the individual's hard drive[5].

In addition to email, online patients are often required to provide personal information and medical history to the websites. At Cyberdocs, Inc., a cybermedicine company established in October 1996, new patients fill out an online chart with their medical history, then enter their credit card number after describing their illness and reason for consulting the online doctor. Patient confidentiality is easily breached when the encryption for electronic transmission of data is broken, or when confidentiality protection fails at the level of the server.

Clearly, cybermedicine is vulnerable to violations of patient confidentiality and privacy because all its transactions are effected electronically, through the Internet. However, the anonymity of online consultations renders cybermedicine more accessible, as patients are more willing to approach cyberdoctors about embarrassing or sensitive problems. Hence, the clash between accessibility and confidentiality composes the inherent ethical dilemma in cybermedicine, and is similar to that in telemedicine.

Where there is tension between economic interests and patient welfare, the physician's competence, consideration and care may be suspect. The ethical principles of non-maleficence, beneficence, confidentiality, veracity as well as social responsibility and justice are in direct opposition with the emphasis on lucrative commerce, creating an ethical dilemma. Physicians employed as paid consultants to medical e-commerce sites, or who man their own online clinics may become caught up in this ethical dilemma. Many existing medical codes of conduct thus discourage dual obligations to financial interests and the well being of the patient, and insist on patient welfare first and foremost.

Despite the American Medical Association's perpetual reminder that "Physicians, as physicians, are not, and must never be, commercial entrepreneurs, gateclosers, or agents of fiscal policy that runs counter to our trust[6]", numerous surveys show an exponential increase in physician websites[7]. The promise of great potential wealth often tempts medical entrepreneurs into placing investor and shareholder interests above the welfare of patients. This practice runs counter to the principle of beneficence, which places the patient's welfare and benefit as the first consideration.

Although the principle of non-maleficence exhorts physicians to "first do no harm" and guard the sanctity of life, there have been reports of medical web pages misleading patients. For example, the hugely popular health information website, DrKoop.com, has been criticised for frequently blurring the line between objective information and its advertising or promotional content[8]. When the quality of information on medical and healthcare websites is not stringently regulated, patients may

experience difficulty in separating the wheat from the chaff and end up making decisions deleterious to their welfare. In addition, when business ties, partnerships or conflicts of interest are not disclosed, the principle of veracity, which emphasises truth telling and the physician's obligation to full and honest disclosure, is violated. Indeed, when he was still chairman of DrKoop.com, the former United States Surgeon General Dr. C. Everett Koop was roundly criticised by medical ethicists, consumer advocates and others for not properly disclosing his business ties and financial arrangements with the website[8]. Keeping undisclosed information is hardly a consistent, accountable and transparent practice consistent with the principle of social responsibility and justice. Obviously, the patient-first consideration of the principle of beneficence is also disregarded, especially when blatant conflicts of interest lead to officers profiting from insider stock trading. Furthermore, with cookies on the websites surreptitiously tracing unsuspecting visitors, the patient's online surfing habits and interests are stored and may be sold to advertisers. The principle of confidentiality is transgressed, as the patient's privacy and confidentiality are not respected[9].

Thus, a distinct ethical dilemma exists where medicine and e-commerce merge and economic interests take precedence over patient welfare. As ethical principles of non-maleficence, beneficence, confidentiality, veracity as well as social responsibility and justice are breached, the trust between physician and patient becomes strained.

Ambiguous patient-physician relationships are clearly a product of the practice of medicine in the IT age. The unconventional long-distance or online consultations practised in telemedicine and cybermedicine render it difficult to define the patient-physician relationship. In fact, even case law has not determined at which point the physician-patient relationship commences, in cases without direct contact. Whether the patient-physician relationship exists at all under certain circumstances becomes an ethical dilemma in itself, because it will directly affect the physician in his relationships with patients, other physicians, healthcare systems and society. Without knowing the ethical obligation of the physician to the patient, it is impossible to determine whether the physician has treated the patient to the best of his ability, and thus decide whether professional values in ethics, such as integrity and competence, have been strictly adhered to.

Whether a patient has to be seen and examined to have a relationship with his physician is the most pertinent and unanswered question. Without a comprehensive ethical framework to define the duty of the physician, a remote physician interpreting data of a patient whom he has never met, examined or communicated with could claim that no physician-patient relationship was ever established. The physician-patient relationship becomes more ambiguous if the consulting doctor only spoke to the other physician and never to the patient. Essential questions, which further define the physician's responsibility to the patient, like whether a physician consultant to a website has any ethical obligation to visitors and whether an online relationship requires an off-line one, remain largely unanswered.

Hence, in both cybermedicine and telemedicine, a fundamental ethical dilemma arises from the undefined physician-patient relationship, where the professional ethical obligation of the physician to the patient is indeterminate. The inability to establish if the physician has been fully responsible and ethical in carrying out his duty contributes to the dilemma.

Finally, ethical dilemmas also emerge from conflicts between cost cutting and efficiency in the application of artificial intelligence versus the responsibility of the physician to make decisions with proper reverence for the sanctity of life. Artificial intelligence is widely used in hospital-based basic computer technology, like automatic sphygmomanometers and Peak Flow meters, for the rendering of diagnosis. It reduces costs, optimises clinical outcomes and improves care. However, the physician may be required to take calculated risks by trusting machine diagnosis, and this may sometimes contradict the principle of non-maleficence, which exhorts physicians to respect the sanctity of life, as harm may be inadvertently brought about by computer-generated clinical systems errors.

As we become increasingly dependent on computers and hand-held devices for clinical practice, a key ethical dilemma would be deciding when and how computers should be used clinically. Virtual reality simulations, with excellent graphics and ability to change anatomy, pathology and operative problems, can be used for preoperative simulations. In cases where the simulation decides that a patient is unsuitable for operation, the surgeon faces an ethical dilemma, which is whether to believe the simulation and abandon the operation, or try anyway in a computer-diagnosed hopeless case. In addition, while training administrators and managed care gatekeepers to diagnose and treat patients using computer systems may be cost-effective, the sanctity of life is still the physician's ultimate responsibility. However, since nurses already watch and interpret computer-generated

data, for instance in the Intensive Care Unit[10], the question of who may use the decision-support systems to aid in diagnosing and treating remains an ethical dilemma.

A comprehensive legal and ethical framework is required to address and resolve ethical concerns. As former US President Bill Clinton notes, "Nothing is more private than someone's medical or psychiatric records. And, therefore, if we are to make freedom fully meaningful in the Information Age, when most of our stuff is on some computer somewhere, we have to protect the privacy of individual health records[11]." Therefore, the collection, processing, storage and communication of medical data have to be strictly regulated, and telecommunications systems must be secure to safeguard patient confidentiality. Measures to prevent unauthorised interception of information and to invalidate altered data can be implemented. Laws such as the Federal Privacy Act of 1994 have been passed to safeguard the privacy and confidentiality of computerised patient records. Public access to physician histories over the Internet can help patients assess the competency and integrity of the cyberdoctor. In 1999, California passed a new law allowing patients access to physician histories over the Internet, including disclosure of malpractice awards felony convictions, and serious hospital disciplinary actions. An extensive ethical framework is necessary to define the evolving physician-patient relationship in telemedicine and cybermedicine, such that the role of the physician is put into perspective and patients are assured of quality care. Finally, physicians must know more than the machines so they can recognise mistakes and inaccurate information in the computer systems, and ensure that decisions made are relative to treatment goals.

In conclusion, increasing reliance on computers and Information Technology in the IT age has expanded access to medical knowledge and expertise, cutting costs and increasing efficiency. However ethical dilemmas arise when there is conflict between productivity and protecting patient confidentiality, privacy and welfare, when unconventional consultations create ambiguous patient-physician relationships, and when physicians rely excessively on artificial intelligence. These ethical dilemmas can be resolved by establishing a comprehensive legal and ethical framework to guide the medical community.

REFERENCES

1. Beauchamp TL, Childress JF. Principles of Biomedical Ethics, 4th ed. New York: Oxford University Press; 1994.
2. Galewitz P. 858 Kaiser e-mails go to wrong patients. Contra Costa Times (Walnut Creek, CA) 2000 Aug 10; B01.
3. Chin T. Security breach: Hacker gets medical records. American Medical News 2001 Jan 29 [online]. Available at: www.ama-assn.org/sci-pubs/amnews/pick_01/tesa0129.htm. Accessed February 17, 2003.
4. Strode SW, Gustke S, Allen A. Technical and Clinical Progress in Telemedicine. JAMA 1999; 281:1066-8.
5. Harrington K. Legal implications of the practice of medicine over the Internet. In: Cyberlaw 1999 Nov 10 [online]. Available at: www.gase.com/cyberlaw/toppage11.htm. Accessed February 17, 2003.
6. Crawshaw R, Rogers DE, Pellegrino ED, Bulger RJ, Lundberg GD, Bristow LR, et al. Patient-physician covenant. JAMA 1995; 273:1553.
7. Nation s leading medical malpractice carriers and medical societies announce joint guidelines for physician-patient online communications. medem 2001 January [online]. Available at: http://www.medem.com/erisk. Accessed February 17, 2003.
8. Noble HB. E-MEDICINE - A special report; Hailed as a Surgeon General, Koop is faulted on Web ethics. The New York Times Sep 5, 1999.
9. Dyer KA. Ethical Challenges of medicine and health on the internet: A review. Journal of Medical Internet Research 2001;3(2):e23 [online]. Available at: http://www.jmir.org/2001/2/e23/index.htm. Accessed February 17, 2003.
10. Epshteyn E, Dyer KA. Oregon Health Sciences MINF 528 Course, advanced topics in medical informatics [online]. Available at: http://medir.ohsu.edu/~epshteyn/MINF528. Accessed February 17, 2003.
11. Department of Health and Human Services Washington, D.C. Remarks by the President on medical privacy. 2000 December [online]. Available at: http://www.hipaadvisory.com/news/NewsArchives/Stories/clinton1220.htm. Accessed February 17, 2003.