JOHN D. CLOUGH, MD
Chairman, Division of Health Affairs, Cleveland Clinic; Editor-in-chief, *Cleveland Clinic Journal of Medicine*

DAVID W. ROWAN, JD
General counsel, Cleveland Clinic

DANIEL E. NICKELSON
Division of Government Affairs, Cleveland Clinic

Keeping our patients' secrets

ABSTRACT

Protecting the privacy of the patient's medical record is a central issue in current discussions about a patient bill of rights, and controversy over a proposed "unique health identifier" has raised the decibel level of these discussions. At the heart of the debate is how best to resolve the inherent conflict between the individual's right to privacy and the need for access to patients' health information for reasons of public health, research, and health care management.

DEBATE ABOUT A "UNIQUE HEALTH IDENTIFIER" has refocused public attention on the privacy, confidentiality, and security of medical records.[1]

A person with syphilis may regard that fact as *private*, but by law it must be reported, so it is not *confidential*

The unique health identifier is part of a national health care identification system required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Many believe it threatens the privacy, confidentiality, and security of medical records; others see it as necessary to optimal public health, epidemiologic research, and management of care.

Unfortunately, in the real world, patient privacy and confidentiality are broken regularly, even without any increased vulnerability to breach of confidence that a mandated unique health identifier might impose.[2,3] These breaches benefit no one, and physicians cannot condone them.[4] Our time-honored, loosely controlled medical record system frequently fails to protect the individual's right to privacy, ignores confidentiality, and offers little security.[5,6] In addition, the openness of the academic environment may conflict with patient confidentiality. Electronic data technology may facilitate these violations of confidentiality, but it is not the real villain.[7]

HOW DO PRIVACY, CONFIDENTIALITY, AND SECURITY DIFFER?

The definitions of privacy, confidentiality, and security used here are those commonly used in the professions concerned with these issues:

Privacy is the limitation of awareness of personal information to the patient and possibly a few others whom the patient selects. Privacy is governed by the patient alone. Private information may or may not be recorded in the medical record; if it is, then it is regarded as confidential.

Confidentiality is the limitation of awareness of private information to those who must have it in order to provide desired service to the patient. Confidentiality is governed by the "need-to-know" principle. Through disclosure and formal authorization to release information, the decision about who needs to know private information is controlled to some extent by the patient. Information in the medical record is presumed to be confidential.

Private does not always mean confidential, however. Although similar, the concepts of privacy and confidentiality are not necessarily congruent. Information considered private by the patient should usually be held confidential by those to whom it is entrusted, but not always. For example, a person with syphilis may regard that information as *private*, but by law it must be reported; therefore, it is not *confidential*.

Security refers to safeguards to the confidentiality and integrity of recorded information. In health care, such protections have traditionally been loose, ostensibly to promote ease of information sharing among those who need to know it.

Downloaded from www.ccjm.org on April 20, 2024. For personal use only. All other uses require permission.

MANAGED CARE NEEDS ACCESS TO CONFIDENTIAL INFORMATION

In the rush to control health care costs, attention has focused on managing delivery of care by using increasingly controversial tools collectively referred to as managed care.[8] Patients have become the consumers, doctors and hospitals are now the providers, and third-party payers, including the government, are the customers.

In this uneasy ménage à trois, providers find themselves caught between the often competing interests of patients and payers. This situation raises significant ethical issues. Patients want their privacy respected. Providers are, for the most part, responsibile for keeping such information confidential, thus protecting patient privacy. Yet payers and other interested parties such as researchers and public health workers[9] may want the information. Their purposes might include, for example, monitoring immunization, disease screening rates, or compliance with treatment protocols. Because of the increasing use of computers to store medical data, such information is much easier to assemble and disseminate than in the past. As access to patient data becomes technically easier, patients are becoming progressively uneasier.

Passage of the HIPAA intensified physician concern because of its severe legal penalties for unauthorized release of medical data. The potential passage of a patient bill of rights promises more of the same.

THE PUBLIC NEEDS ACCESS TO CONFIDENTIAL INFORMATION

The need to protect the public against threats to health or safety conflicts with the need for confidentiality of health information.[5,10] It is a conflict between the needs of the many[11,12] and the rights of the individual[13]—an ethical issue that has concerned physicians since the time of Hippocrates.

The issue is particularly poignant in the case of deadly infectious diseases such as AIDS,[14] mental health issues potentially affecting public safety,[15] criminal investigations,[16] and certain disastrous genetic conditions whose transmission to the next generation could be prevented.[17]

OTHERS NEED ACCESS TO CONFIDENTIAL INFORMATION

Other examples where an individual or entity has or perceives a compelling need to obtain confidential medical information include:

- The "right" of family members to know genealogic information of interest, such as biological parentage[18]
- The "need" of an employer to know an injured employee's readiness to work[19]
- The "need" of a victim to have the assailant tested for transmissible disease
- The desire of insurance companies to know medical information for coverage and underwriting purposes.[20]

History suggests that the list of such examples will expand as medical understanding produces more uses for the information that can be found in personal medical records.

LEGISLATION AND THE UNIQUE HEALTH IDENTIFIER

Health Insurance Portability and Accountability Act of 1996 (HIPAA, PL 104-101)

The HIPAA mandates six requirements for patient data. The requirements include:

- Ability to transmit health information electronically
- Unique health identifiers for individuals, employers, health plans, and providers
- Code sets and classification systems for each data element in electronic health care transactions
- Security of health care information systems
- Procedures for electronic transmission and validation of signatures
- Data elements needed to coordinate benefits and process claims.[21]

In August 1998, the Health Care Financing Administration proposed rules for implementing these requirements, with a comment period that ended in October 1998. Interestingly, the deadlines for finalizing some of these rules had already passed when the draft rules were published. Final rules have not yet been promulgated.

Options for the unique health identifier

The unique health identifier was viewed as

Managed care puts providers in the middle of patients' and payers' competing interests

Downloaded from www.ccjm.org on April 20, 2024. For personal use only. All other uses require permission.

essential to administrative simplification, and was expected to result in better quality of care, lower administrative costs, and other benefits.

Options for the unique health identifier were subjected for public comment in July 1998.[1] It was an eye-opener. Those options included a numerical identifier based on the Social Security number, a totally new numerical identifier not based on the Social Security number, a biometric identifier based on physical attributes (eg, fingerprints, retinal pattern analysis, iris scan, voice pattern, DNA analysis), and a numerical identifier based on the Civil Registration System (eg, birth files, visas, "green cards"). Additional proposals recommended methods that would allow cross-linking of medical records across systems without a unique personal identifier.

Some of the more exotic options such as iris scan or DNA analysis smacked of a Big Brother and other predictions of paranoid futuristic fiction.

The unique health identifier would allow individuals to be tracked throughout their use of the health care system.[22] As in some other countries, it could permit the establishment of a state or national health database,[23–25] which would be useful not only for keeping track of utilization, but also for public health and research.[26]

Handle confidential information as you would want your own medical information handled

Government's good intentions greeted with skepticism

To say opinion on the unique health identifier is deeply divided[1] may be the understatement of the year. The tracking ability that such an identifier would give the government—or any organization with access to it—has Big Brother overtones. General confidence in the good intentions of government agencies interested in controlling costs would go a long way toward defusing public opposition, but such confidence does not appear to exist now. The public outcry resulted in suspension of the attempt to define a unique health identifier.

Research and the unique health identifier

People are also concerned about the use of identifiable data in research pertaining to epidemiologic,[27] genetic,[28] and public health,[29] and requirements for consent have been revisited and strengthened.[12,30,31] People have even raised doubts about the use of statistically analyzed, aggregated data stripped of personal identifiers.[32,33] There is little trust in the integrity of the whole clinical research apparatus, and the patient bill of rights and the HIPAA address these misgivings in proposals for providing guarantees about informed consent for the release of data. Other countries have been more sanguine about trading off some confidentiality for the perceived public good.[34]

SECURITY ISSUES

Although a detailed discussion of the fine points of data security is beyond the scope of this paper, the topic is important ethically,[35] and medical record security is necessary to meet regulatory requirements.[36]

Security protects both the confidentiality and the integrity of data.[37] The growth of telemedicine complicates the issue of security.[38] Military-type security measures and standard database protection methods are inappropriate, however, because they prevent ready access to data, which is essential for efficient delivery of medical care.[39]

Currently available security methods include:

- User validation and access control, including secure electronic signatures[40]
- "Depersonalization" of data with a secure identifier control facility acting as a network file access table
- A "virtual record" instead of an integrated file, which would be reconstructed at the time of access[41]
- Encryption of data.[42,43]

In Europe, standards for health data security have been promulgated.[44] Grotan and Iverson[45] pointed out the inadequacies of present day safeguards on medical data. This was reemphasized in a 1997 report of the National Research Council of the National Academy of Sciences.[40] In the United States, no system has yet been widely recognized as ideal, although several are under investigation.[46,47]

Even though strong security procedures are in place to protect confidential medical information, individuals are regularly asked to waive confidentiality (eg, when applying for insurance), and few controls on dissemination exist once the waiver is signed.

Downloaded from www.ccjm.org on April 20, 2024. For personal use only. All other uses require permission.

WHAT IS THE MESSAGE FOR PHYSICIANS?

Careful attention to confidentiality and security of patient-related information, especially the medical record (whether paper or electronic), is an absolute must.

An adequate review mechanism is needed, possibly involving the physician, to ascertain that requests are legitimate before information is released.

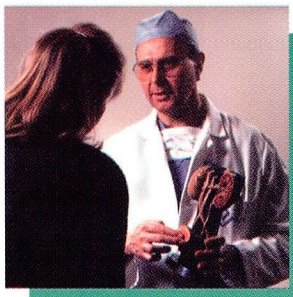
Totally aside from any threat to confidentiality posed by converting medical records to electronic form or using a unique health identifier, discussing sensitive information in public places such as elevators and cafeterias is all too common and must stop.[2] A simple standard is to handle confidential information the way you would want your own medical information handled. Accrediting agencies, such as the Joint Commission on Accreditation of Health Care Organizations,[48] have developed formal standards that should help office-based physicians devise specific, useful approaches.

Physicians and other health care providers will increasingly be held accountable for breaches of confidentiality, and the penalties, not to mention the loss of patients' trust, will be severe. Beyond that, we owe it to our patients to respect and protect their confidences. Only then can the trust that underlies the doctor-patient relationship survive.

REFERENCES

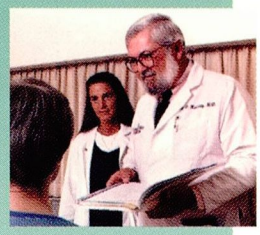
1. Unique health identifier for individuals. Available from URL: http://aspe.os.dhhs.gov/admnsimp/nprm/noiwp1.htm.
2. **Hasman A, Hansen NR, Lassen A, Rabol R, Holm S.** [What do people talk about in Danish hospital elevators?] Ugeskr Laeger 1997; 159:6819–6821.
3. **Rushton CH, Infante MC.** Keeping secrets: the ethical and legal challenges. Pediatr Nurs 1995; 21:479–482.
4. **Mlinek EJ, Pierce J.** Confidentiality and privacy breaches in a university hospital emergency department. Acad Emerg Med 1997; 4:1142–1146.
5. **Jordan TJ, Lindenthal JJ.** Methodological issues in the study of confidentiality: a reinterpretation of findings. Med Law 1991; 10:537–547.
6. **Fisher F, Madge B.** Data security and patient confidentiality: the manager's role. Int J Biomed Comput 1996; 43:115–119.
7. **Dodek DY, Dodek A.** From Hippocrates to facsimile. Protecting patient confidentiality is more difficult and more important than ever before. CMAJ 1997; 156:847–852.
8. **Boyle PJ, Callahan D.** Managed care in mental health: the ethical issues. Health Aff (Millwood) 1995; 14:7–22; discussion 23–33.
9. **Weissburg DJ.** Managed care organizations and confidential patient information: the need for a uniform standard. J Health Care Finance 1995; 21:42–46.
10. **Walzer RS.** The physician's physician: latent duties to protect third persons. Med Law 1992; 11:423–440.
11. **Cox LH.** Protecting confidentiality in small population health and environmental statistics. Stat Med 1996; 15:1895–1905.
12. **Grady C, Jacob J, Romano C.** Confidentiality: a survey in a research hospital. J Clin Ethics 1991; 2:25–30.
13. **Razis DV.** Medical confidentiality. Qual Assur Health Care 1990; 2:353–357.
14. **Jayawardena H.** AIDS and professional secrecy in the United States. Med Sci Law 1996; 36:37–42.
15. **Petrila JP, Sadoff RL.** Confidentiality and the family as caregiver. Hosp Community Psychiatry 1992; 43:136–139.
16. **de Gorgey A.** The advent of DNA databanks: implications for information privacy. Am J Law Med 1990; 16:381–398.
17. **Adams J.** Confidentiality and Huntington's chorea. J Med Ethics 1990; 16:196–199.
18. **Nachtigall RD.** Secrecy: an unresolved issue in the practice of donor insemination. Am J Obstet Gynecol 1993; 168:1846–1849.
19. **Rischitelli DG.** The confidentiality of medical information in the workplace. J Occup Environ Med 1995; 37:583–593.
20. **Charbonney R.** [Selection of seropositive persons for AIDS as practiced by group insurance agents (disease and professional caution) in Switzerland]. Schweiz Med Wochenschr 1991; 121:1212–1216.
21. **Security and electronic signature standards.** Federal Register 1998; 63:43241–43280.
22. **May DS, Kelly JJ, Mendlein JM, Garbe PL.** Surveillance of major causes of hospitalization among the elderly, 1988. MMWR CDC Surveill Summ 1991; 40:7–21.
23. **Bomba B, Cooper J, Miller M.** Working towards a national health information system in Australia. Medinfo 1995; 8 Pt 2:1633.
24. **Coward JH.** The BC health information standards council. Int J Med Inf 1998; 48:43–47.
25. **Dawson C, Perkins M, Draper E, Johnson A, Field D.** Are outcome data regarding the survivors of neonatal care available from routine sources? Arch Dis Child Fetal Neonatal Ed 1997; 77:F206–210.
26. **Pogach LM, Hawley G, Weinstock R, Sawin C, Schiebe H, Cutler F, Zieve F, Bates M, Repke D.** Diabetes prevalence and hospital and pharmacy use in the Veterans Health Administration (1994). Use of an ambulatory care pharmacy-derived database. Diabetes Care 1998; 21:368–373.
27. **Capron AM.** Protection of research subjects: do special rules apply in epidemiology? J Clin Epidemiol 1991; 44:81S–89S.
28. **Botkin JR, McMahon WM, Smith KR, Nash JE.** Privacy and confidentiality in the publication of pedigrees: a survey of investigators and biomedical journals. JAMA 1998; 279:1808–1812.
29. **Cox LH.** Protecting confidentiality in small population health and environmental statistics. Stat Med 1996; 15:1895–1905.

Downloaded from www.ccjm.org on April 20, 2024. For personal use only. All other uses require permission.



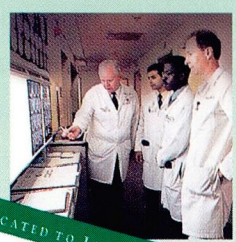
LET US HEAR FROM YOU

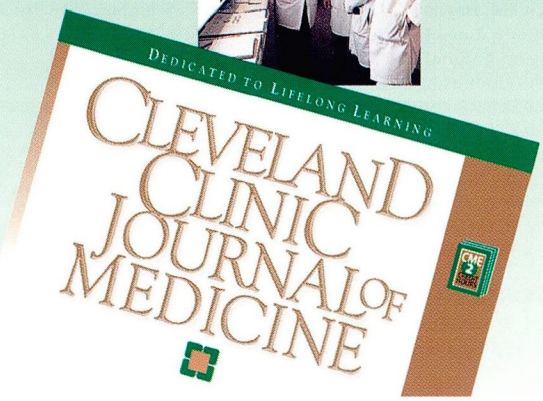
- Let us hear your opinions about the *Cleveland Clinic Journal of Medicine.*
- Do you like current articles and sections?
- What topics would you like to see covered and how can we make the Journal more useful to you?



PHONE 216.444.2661
FAX 216.444.9385
E-MAIL ccjm@ccf.org
WWW http://www.ccjm.org

CLEVELAND CLINIC JOURNAL OF MEDICINE
The Cleveland Clinic Foundation
9500 Euclid Avenue, NA32
Cleveland, Ohio 44195





30. **Last JM.** Obligations and responsibilities of epidemiologists to research subjects. J Clin Epidemiol 1991; 44 Suppl 1:95S–101S.
31. **Earley CL, Strong LC.** Certificates of confidentiality: a valuable tool for protecting genetic data. Am J Hum Genet 1995; 57:727–731.
32. **Newcombe HB.** Cohorts and privacy. Cancer Causes Control 1994; 5:287–291.
33. **Mills ME.** Data privacy and confidentiality in the public arena. Proc AMIA Annu Fall Symp 1997; 42–45.
34. **Cooper JE.** Balancing the scales of public interest: medical research and privacy. Med J Aust 1991; 155:556–560.
35. **Feinleib M.** The epidemiologist's responsibilities to study participants. J Clin Epidemiol 1991; 44 Suppl 1:73S–79S.
36. **Brannigan VM.** A framework for "Need to Know" authorizations in medical computer systems: responding to the constitutional requirements. Proc Annu Symp Comput Appl Med Care 1994; 392–396.
37. **Waegemann CP.** IT security: developing a response to increasing risks. Int J Biomed Comput 1996; 43:5–8.
38. **Kvedar JC, Menn E, Loughlin KR.** Telemedicine. Present applications and future prospects. Urol Clin North Am 1998; 25:137–149.
39. **Orr GA, Brantley BA Jr.** Development of a model of information security requirements for enterprise-wide medical information systems. Proc Annu Symp Comput Appl Med Care 1992; 287–291.
40. **Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure.** For the Record: Protecting Electronic Health Information. Washington, National Research Council, 1997.
41. **Brannigan VM, Beier BR.** Patient privacy in the era of medical computer networks: a new paradigm for a new technology. Medinfo 1995; 8 [Pt 1]:640–643.
42. **Sardinas JL Jr, Muldoon JD.** Securing the transmission and storage of medical information. Comput Nurs 1998; 16:162–168.
43. **Michaelis J, Miller M, Pommerening K, Schmidtmann I.** A new concept to ensure data privacy and data security in cancer registries. Medinfo 1995; 8 Pt 1:661–665.
44. **Furnell SM, Sanders PW, Warren MJ.** Development of security guidelines for existing healthcare systems. Med Inf (Lond) 1995; 20:139–148.
45. **Grotan TO, Iversen KR.** An information security management strategy for healthcare institutions. Medinfo 1995; 8 Pt 1:652–656.
46. **Shea S, Sengupta S, Crosswell A, Clayton PD.** Network information security in a phase III Integrated Academic Information Management System (IAIMS). Proc Annu Symp Comput Appl Med Care 1992; pp 283–286.
47. **Halamka JD, Szolovits P, Rind D, Safran C.** A WWW implementation of national recommendations for protecting electronic health information. J Am Med Inform Assoc 1997; 4:458–64.
48. **Joint Commission on Accreditation of Hospitals and Healthcare Organizations.** Management of information, In 1998–1999 Comprehensive Accreditation Manual for Ambulatory Care. Chicago, 1998, pp 457–500.

ADDRESS: *John D. Clough, MD, Division of Health Affairs, H18, The Cleveland Clinic Foundation, 9500 Euclid Avenue, Cleveland, OH 44195.*

Downloaded from www.ccjm.org on April 20, 2024. For personal use only. All other uses require permission.