



Published in final edited form as:

J Law Med Ethics. 2010 ; 38(1): 7–13. doi:10.1111/j.1748-720X.2010.00460.x.

The Hippocratic Bargain and Health Information Technology

Mark A. Rothstein, J.D.

Herbert F. Boehl Chair of Law and Medicine and Director of the Institute for Bioethics, Health Policy and Law at the University of Louisville School of Medicine

Since the fourth century, B.C.E., the Oath of Hippocrates has been the starting point in analyzing the obligations of physicians to protect the privacy and confidentiality interests of their patients. The pertinent provision of the Oath reads as follows: “What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account must be spread abroad, I will keep to myself, holding such things shameful to be spoken about.”¹

This part of the Oath is subject to more than one interpretation,² but its commonly accepted meaning provides the ethical foundation for the physician’s duty of confidentiality. The Oath expressly declares that a physician’s obligation of confidentiality applies beyond matters of medical care. At a time when there were no hospitals or physician offices, patients received medical care in their homes or in public places. Physicians treating patients in their homes could be expected to see and hear a wide range of activities that might be considered embarrassing, immoral, or even illegal. These matters were not to be “spread abroad.” Thus, the Oath covered not only the medical condition of the patient, including history, symptoms, diagnoses, and prognoses, but social information as well. In addition, although not specifically a part of the Oath, the physician’s obligations were absolute in terms of duration, and continued beyond the death of the patient.³

Dr. Steven Miles cautions not to ignore the historical context of this passage of the Oath, because modern notions of privacy and confidentiality were not followed in ancient Greece.

Physicians took histories, examined patients, gave prognoses, and practiced surgery in public or in houses as relatives and strangers looked on. Male guardians or owners were entitled to medical information about women, children, and slaves, and they were empowered to dictate medical choices as well. The medical treatises published the names, addresses, and intimate details of many patients.⁴

In Miles’ view, this passage of the Oath is more of a general admonition for physicians not to dishonor patients in their communications to others.⁵ Regardless of the intended meaning of this part of the Oath, it is widely cited as the traditional basis of a physician’s duty of confidentiality.⁶ Thus, the generally accepted meaning ascribed to the passage is perhaps even more important than the words themselves.

The Oath of Hippocrates established the principles of privacy and confidentiality as fundamental aspects of medical care. Subsequent codes of ethics, including Thomas Percival’s code of medical ethics in 1803 and the American Medical Association’s first code of ethics in 1847, retained the professional commitment to confidentiality from the Hippocratic Oath.⁷

In effect, physicians and patients entered into a “Hippocratic bargain.” Physicians, explicitly or implicitly, said to their patients: “Allow me to examine you in ways that you would never permit any stranger, and tell me the most sensitive information about your body, mind, emotions, and lifestyle. These intrusions upon your privacy are essential in providing you

with sound medical care. If you provide me with this intimate access to your person, I promise to maintain your secrets for as long as I live and to disclose them only if directed by you or others you have authorized.” Patients agreeing to be treated under this bargain relinquished aspects of their privacy in exchange for their physicians’ assurances of confidentiality — that they would not re-disclose the patient’s health and other sensitive information to others.

The Hippocratic Bargain Today

The physician-patient relationship of today differs greatly from the relationship at the time of Hippocrates. A physician in the time of Hippocrates was a sole provider of health care. This model (as later modified by the development of the nursing profession) survived until the 20th century. Today, medical practice often is characterized by multiple physicians with multiple specialties, often in integrated delivery systems or coordinated in large institutions. Physicians also share health care responsibilities with nurses, dentists, pharmacists, psychologists, chiropractors, optometrists, social workers, physical therapists, respiratory therapists, audiologists, and other allied health professionals. Essential health care services also are provided by numerous technicians and staff members in the laboratory, pharmacy, imaging, and other departments. In teaching hospitals patient information is also shared with trainees.

Modern health care, especially in the United States, also has generated a vast financial structure, including personnel employed by health care providers, health insurers, health maintenance organizations, and other public and private payers. Patients usually do not pay for their health care services directly, and third-party payers require access to patient health records to verify the necessity of the care provided and the reasonableness of the charges. In addition, individual health records in various levels of identifiability are often reviewed by governmental and professional regulatory agencies with jurisdiction over health care providers, health care institutions, health plans, pharmaceutical products, medical devices, and other key elements of health care.

The addition of all these individuals and entities into what was once a simple, two-party, physician-patient relationship has completely changed the original privacy “bargain” in the Oath of Hippocrates. Sharing medical secrets with one physician, known to and selected by the patient, is hardly the same thing as disclosing medical secrets to a physician or other health care provider with the reasonable expectation that the information will be disclosed to numerous unknown individuals and entities in the health care enterprise for a wide range of purposes.

Individual health information is also of great interest to entities outside of the health care setting, which often have legitimate economic, social, or legal reasons for learning about the current health status or likely future health of individuals. These entities usually have sufficient economic leverage so that individuals must sign an authorization for the disclosure of their health information as a condition of, for example, applying for a job or life insurance.⁸ It is not known precisely how many of these “compelled authorizations” are executed, but a conservative estimate is at least 25 million each year in the United States, including 10.2 million in connection with employment entrance medical examinations and 6.8 million as part of individual life insurance applications.⁹ Consequently, more health information is being disclosed to more entities for more non-medical reasons than ever before. Clearly, these disclosures are beyond the contemplation of the Hippocratic bargain.

Dr. Mark Siegler, in a much-discussed article in 1982, calculated that the health records of a typical patient at his teaching hospital were viewed by at least 75 health professionals and hospital personnel during an in-patient stay.¹⁰ Based on this widespread distribution of

health information, he concluded that confidentiality in medicine was a “decrepit” concept. It is difficult to say whether more health professionals have greater access to health records today. More individuals in an institution may have a need to know some elements of the record, but at least where electronic health records (EHRs) are used, role-based access, passwords, audit trails, and other measures may operate to limit the scope of access.

In 1982, Siegler concluded that “rather than perpetuate the myth of confidentiality and invest energy vainly to preserve it, the public and the profession would be better served if they devoted their attention to determining which aspects of confidentiality are worth retaining.”¹¹ The subsequent development of health information technology (HIT) demands a new conception of confidentiality and a new paradigm of physician-patient relations to protect confidentiality in health care settings and beyond.

The Effects of Health Information Technology

The uses and disclosures of health information for medical and non-medical purposes are being revolutionized by advances in HIT. The increased effectiveness, efficiencies, and integration of EHRs and networks are related to the following three attributes: EHRs and EHR networks are (1) longitudinal (containing records over an extended period of time, eventually including “cradle to grave” data); (2) comprehensive (containing virtually all clinical encounters with a wide range of health care providers); and (3) interoperable (accessible in standard electronic format via various EHR systems from any location). These same attributes combine to present the greatest challenge to health privacy. Longitudinal, comprehensive, interoperable records often include information about sensitive health conditions that may or may not be of any current clinical utility and that, in any event, are not needed by many of the diverse health care providers with unrestricted access to the record.¹² Furthermore, when individuals are required to sign an authorization for release of their EHRs for nonmedical purposes, unnecessarily detailed information is routinely revealed.

In the health care setting, if restrictions are not imposed, then too many providers increasingly will have access to too much information. For example, a dentist filling a cavity ordinarily does not need access to an individual’s genetic test results. Furthermore, the typical health care provider does not have time to scrutinize such detailed health information, especially if it is not organized in summary fashion. As a result, there is no clinical benefit from having access to the information; the only consequences of unrestricted access by all health care providers are patients’ anxiety, loss of privacy, and perhaps a reluctance to seek care at the outset.

If a health care provider receives expanded electronic health information, it is not clear that existing laws would require that they follow legislatively mandated security and privacy measures. For example, many thousands of health care providers are not covered by the HIPAA Privacy Rule because they do not submit claims for payment in electronic format.¹³ This fact underscores the need for comprehensive federal health privacy legislation.

In addition to excessive disclosures in health care, third parties (e.g., employers, life insurers) reviewing health records often have access to too much information. An employer who wants to know if an applicant has the physical ability to climb a telephone pole safely does not need to know about the individual’s reproductive health history. It is beyond the scope of this article to analyze such third-party disclosures, but it should be observed that the possibility of divulging private, personal health information *outside* of health care has important effects on what and how much information is disclosed *within* health care.

The unnecessary disclosure of sensitive health information is more than a matter of privacy: it is a matter of public health. Public policy strongly encourages individuals with sexually transmitted diseases, mental illness, substance abuse, or other stigmatizing conditions to seek treatment without delay. It is well known that many individuals will avoid doing so if they have concerns about their privacy. In an attempt to address one aspect of this problem, section 527 of the Public Health Service Act¹⁴ provides that a program receiving federal financial assistance for alcohol and drug abuse treatment generally may not disclose any information about an individual who is in the program.¹⁵ Without such protection, many individuals would be reluctant to undergo treatment, especially for addiction to illicit drugs, because they fear police access to the records and subsequent prosecution.

Limiting the Amount of Information Disclosed to Health Care Providers

Numerous consumer surveys have inquired about whether individuals have concerns about health records moving from paper to electronic formats. In general, based on stories about lost laptops and other security breaches, the public is apprehensive about having their health records stored electronically.¹⁶ These concerns, however, are more accurately described as relating to security, rather than privacy. At least conceptually, security issues are easier to address than privacy issues. At the risk of oversimplification, security involves permitting access to authorized individuals and denying access to others.¹⁷ Because there is generally agreement as to which individuals are authorized, the goals of security are clear, even though achieving them may be difficult. By contrast, measures to protect privacy are controversial at both the conceptual and implementation stages.

Protecting privacy in the electronic age requires a reformulation of the Hippocratic bargain. Today, because of diffuse treatment responsibilities, patient records are widely shared with various physicians and other health care providers. Therefore, to protect a patient's privacy, patients should have some control of the amount of information in the record accessible to any particular physician or other health care provider. There are many possible ways of disclosing health information only on a "need-to-know" basis. For example, limits could be based on the role of the health care provider (e.g., a physical therapist or podiatrist would have less access than a primary care physician); date of the prior encounters (e.g., only health information within a certain number of years of the current visit would be available); type of health care provided (e.g., psychiatric records would not be available without separate permission of the patient); diagnosis (e.g., disclosure would be limited to information relating to a specific condition); or procedure (e.g., disclosure would be limited to information related to a specific procedure, such as a laboratory test, imaging study, or medication). From the standpoint of HIT, these options present fascinating challenges beyond the scope of this article. This article focuses on the effect that such limitations would have on the physician-patient relationship.

Limiting the access of certain health care providers, especially physicians, to some types of patient health information represents a new version of the physician-patient relationship. Such a change from current practice also raises the following four contentious issues of professional responsibility. First, many physicians believe that the health records they currently use are substantially complete and accurate. In reality, the paper records still used by the overwhelming majority of physicians are often not complete, accurate, or timely.¹⁸ There are various reasons for this situation, including errors attributable to patients' use of multiple physicians without disclosure, clerical errors by health care personnel (e.g., laboratory or other reports filed in the wrong chart), and transcription or translation errors. Other errors stem from patients' faulty memories or deliberate omissions of matters they would prefer not to share with physicians, such as substance abuse or risky sexual activities. EHRs with some information made unavailable will not be less reliable than current paper

records. In fact, accurate, updated, comprehensive, and interoperable EHRs will be a significant improvement over current records even if the EHRs are not all-inclusive.

Second, many physicians believe they need access to complete health records, because only they have the expertise to determine what health information is relevant to a particular case. Nevertheless, medical training is unnecessary to know that some information has no current clinical utility. Two examples I have previously described involve a decades-old report of domestic violence at the hands of a former partner that did not result in serious physical harm, and a decades-old series of negative test results for various sexually transmitted diseases ordered after an ill-advised and not repeated sexual dalliance.¹⁹ No good and potentially much harm can come from having such information stored and available in EHRs indefinitely.

Third, many physicians believe they would be at risk of liability for medical malpractice if they based their health care decisions on incomplete information. Fear of malpractice liability is not a good reason for wanting access to complete health records. To the contrary, having access to detailed records could actually increase the likelihood of liability. In modern medical practice, physicians have a limited amount of time to see each patient. In virtually all cases, a physician does not have the luxury of carefully reviewing every medical encounter of a patient with numerous health care providers over many years. Yet, if a patient's complete records are easily accessible, it is possible that a court would conclude that there was a duty to discover some information buried in a patient's record that would have changed the course of the individual's treatment.

Fourth, virtually all physicians believe they can preserve the confidentiality of health information merely by following legal requirements and good medical practices.

A physician's ability to preserve the confidentiality of information, however, is irrelevant to the issue of whether a physician can protect the patient's privacy. The routine disclosure of health information for treatment, payment, and health care operations, and the common use of compelled authorizations for the disclosure of health information for non-medical purposes make it impossible to protect an individual's privacy in a comprehensive, longitudinal EHR.

Underlying all of these concerns of physicians is the assumption that the primary value to be served by HIT policy is maximizing the amount of health information available to improve patient care and make it more cost-effective. Undoubtedly, quality health care depends on complete, accurate, and timely information. Yet, patients have other concerns that often override their interest in maximizing their physician's access to all possibly relevant information. An important societal value is encouraging individuals to seek timely treatment and to disclose information directly relevant to their current health concern. Public policy should promote trust between physicians and patients, but to do so, it must be clear that patients' interests are the primary concern of physicians. Public policy also should support preventing the non-medical harms associated with the excessive disclosure of health information, including embarrassment, strains on intimate relationships, stigmatization, and discrimination.

A New Physician-Patient Relationship

New organizational models of health care practice and advances in HIT demand a new version of the physician-patient relationship with respect to health information. Sensitive information about patients no longer can be protected by locking charts in filing cabinets. Providers and patients should embrace a new model of multi-tiered health records with access controlled by patients within clearly defined and widely understood boundaries.

Although the specifics of a system of sequestering sensitive information have yet to be determined, the National Committee on Vital and Health Statistics (NCVHS) has presented a useful framework for a national policy debate on the issue. Among its recommendations on the issue is the following:

The design of the [Nationwide Health Information Network] NHIN should permit individuals to sequester specific sections of their health record in one or more predefined categories. The list of potentially sensitive categories and their contents should be defined on a national basis so that it is uniform across the NHIN.²⁰

The illustrative categories for possible sequestration mentioned by the NCVHS were domestic violence, genetics, mental health, reproductive health, and substance abuse. The NCVHS also addressed the issues of notations to health care providers that some unspecified information has been sequestered, special access to sequestered information for certain patient-designated providers, a “break the glass” feature for emergencies, and other matters.²¹

Notwithstanding the nascent state of the nation’s EHR system, it is important to consider the inevitable changes HIT will cause in the relationships between health care providers and patients.

Physicians and Other Health Care Providers

Physicians and other health care providers will need to understand and accept that they might not have all of a patient’s health records when they are providing care. They will need to appreciate the challenges of making important decisions on the basis of possibly incomplete records. They will need to recognize that an EHR is not a substitute for a physician-obtained and continually updated patient history and physical examination, problem list, and progress notes. They will need to know the sequestration categories and criteria developed by public and private bodies. They will need to recognize when important information could be sequestered in health records, and they will need to know when and how to ask patients for additional permission to access certain information. They will need to know when possibly sequestered information may be so important that they need to tell patients it is impossible to treat them effectively without access to sequestered information. They will need to know how to utilize clinical decision support, which might also scan sequestered information for possible drug interactions and other complications.

Perhaps most importantly, physicians will need to recognize that sequestration does not indicate a lack of trust for physicians. The adoption of a system of sequestration would simply recognize that physicians no longer have sole responsibility for protecting patients from the possible consequences of disclosure of health information. That responsibility will rest primarily with the patient and, as the patient’s advocate and fiduciary, physicians should help their patients in efforts to control access to their private, personal health information.

Several other countries, including Canada, England, and the Netherlands, have begun to consider the important implications for health privacy and physician-patient relations of converting to EHRs and EHR networks with sequestration of part of the medical record.²² The architects of the United Kingdom’s new health information system have frankly declared that health professionals “need to . . . accept that unfettered access to personal health information is a thing of the past.”²³ Thus, at least for industrialized countries, the need to develop a new Hippocratic bargain is a global challenge.

Patients

In a system that permits sequestering of sensitive information in EHRs, patients will have greater responsibilities in maintaining control of their health information. They will need to understand the relationship between health information and health care. They will need to appreciate the possible tradeoffs between privacy and coordinated, safe, and effective health care. They will need to be familiar with the rules of sequestration and the contents of their sequestered files. Most importantly, they will need to recognize and accept the potential consequences when health care decisions are made on the basis of incomplete records.

Legal Rules

Sequestering sensitive health information in EHRs will change the legal landscape of the health professions. New rules will need to be established for developing the technical standards for sequestration as well as the categories and contents of sequestered information. In formulating these rules, policy makers should recognize that giving broad discretion to patients to sequester information might make EHRs less valuable to clinicians and increase the risk of medical error. It will be difficult to strike the proper balance. If patients were given “line item” control of their records, clinicians would be less likely to trust the accuracy and completeness of existing information, and they would be inclined to repeat tests and history taking, thereby undermining the efficiency gains of EHRs. On the other hand, if too little information were subject to sequestration, then patient privacy would be insufficiently protected, thereby risking adverse consequences to individual health, health care, and public health.

Sequestration will require important changes in the HIPAA Privacy and Security Rules, and perhaps require the enactment of new federal legislation or regulations. New regulations will have to define with much greater specificity what it means to disclose the “minimum necessary” amount of health information.²⁴ It is essential that these rules are understandable and accessible to health professionals and members of the public.

State professional licensing laws will need to be amended or their implementing regulations revised to take into account new rules for access to and uses of sensitive health information. For example, if certain health care providers access or disclose complete versions of a patient’s EHR without express permission, a previously acceptable practice, then they may be engaging in an unethical and perhaps illegal practice, which could lead to sanctions.

Finally, the relationship between a health care provider’s access to limited information and liability for medical malpractice needs to be considered. At present, it is unclear what, if any, duties physicians will have to query patients when potentially relevant information is not readily apparent in the patient’s EHR. It also is unclear whether a patient’s sequestration and nondisclosure of health information should operate as a bar to recovery or merely as a setoff against liability under comparative negligence principles.

Conclusion

The Oath of Hippocrates is over 2500 years old. Today, physicians no longer swear oaths to Apollo, and most do not take the Oath formally upon graduation from medical school. Yet, the Oath of Hippocrates remains influential because of its symbolic and inspirational value.²⁵ The Oath is an ancient declaration of the centrality of professionalism, integrity, beneficence, and human dignity in the practice of medicine. A physician’s duty of confidentiality, based on respect for patients, standards of professional decorum, and utilitarian concerns for the free flow of information, is one of the essential tenets of the Oath.

In the world of ancient Greece, the Hippocratic bargain bound patients with their solitary treating physicians. In today's complex health care environment, especially with the widespread adoption of EHRs, physicians and patients need a new Hippocratic bargain. Physicians and other health care professionals should be obliged to respect their patients' choices regarding information disclosure, to preserve the confidentiality of the information entrusted to them, and to disclose information only in accordance with the law and prior agreements with their patients.

Acknowledgments

The author is indebted to Robert J. Esterhay, M.D., David Orentlicher, M.D., J.D., and Kenneth N. Zegart, M.D., for helpful comments on an earlier draft of the article. Kristen Kohn, J.D. 2010, University of Maryland School of Law, provided valuable research assistance.

References

1. Reich, WT., editor. *Encyclopedia of Bioethics*. Vol. 5. Simon & Schuster Macmillan; New York: 1995. Oath of Hippocrates; p. 2632reprinted inrev. ed.at Appendix
2. Miles, SH. *The Hippocratic Oath and the Ethics of Medicine*. Oxford University Press; Oxford: 2004. p. 149
3. American Medical Association. *Code of Medical Ethics of the American Medical Association 2008-2009 ed.* American Medical Association; Chicago: 2008. p. 165§ 5.051 – Confidentiality of Medical Information Postmortem
4. See Miles, *supra* note 2, at 150.
5. *Id.*, at 151.
6. Higgins G. The History of Confidentiality in Medicine: The Physician-Patient Relationship. *Canadian Family Physician* April;1989 35:921–926. [PubMed: 11650274] Moskop J. From Hippocrates to HIPAA: Privacy and Confidentiality in Emergency Medicine – Part I: Conceptual, Moral, and Legal Foundations. *Annals of Emergency Medicine* 2005;45(1):53–59. [PubMed: 15635311] Slowther, A.; Kleinman, I. Confidentiality. In: Singer, PA.; Viens, AM., editors. *The Cambridge Textbook of Bioethics*. Cambridge University Press; Cambridge: 2008. p. 45Winslade, WJ. Confidentiality. In: Reich, WT., editor. *Encyclopedia of Bioethics*. Vol. 1. Simon & Schuster McMillan; New York: 1995. p. 453rev. ed.
7. Gellman RM. Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy. *North Carolina Law Review* 1984;62(2):255–294. [PubMed: 16100795]
8. Rothstein MA, Talbott MK. Compelled Disclosure of Health Information: Protecting Against the Greatest Potential Threat to Privacy. *JAMA* 2006;295(24):2882–2885. [PubMed: 16804155]
9. Rothstein MA, Talbott MK. Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications. *American Journal of Bioethics* 2007;7(3):38–45. [PubMed: 17366232]
10. Siegler M. Confidentiality in Medicine – A Decrepit Concept. *New England Journal of Medicine* 1982;307(24):1518–1521. [PubMed: 7144818]
11. *Id.*, at 1520-1521.
12. Rothstein MA. Health Privacy in the Electronic Age. *Journal of Legal Medicine* 2007;28(4):487–501. [PubMed: 18066975]
13. National Committee on Vital and Health Statistics. Letter to Michael O. Leavitt, Secretary of Health of Human Services. Jun 21. 2007 available at <www.ncvhs.hhs.gov/070621lt2.pdf> (last visited December 11, 2009)
14. 42 U.S.C. § 290ee-3 (2008).
15. See 42 C.F.R. Part 2 (2008).
16. Harris Interactive. Many U.S. Adults Are Satisfied with Use of Their Personal Health Information: Substantial Minority Still Withhold Information from Health Providers Due to Worries About Security of Medical Data. Mar 27. 2007 available at <www.harrisinteractive.com/harris_poll/index.asp?PID=743> (last visited December 11, 2009)

17. Department of Health and Human Services. Health Insurance Reform: Security Standards. Federal Register February 20;2003 68:8334, 8335. [PubMed: 12596712] Hodge, JG., Jr., et al. Identifiable Health Information and the Public's Health: Practice, Research and Policy. In: Goodman, RA., et al., editors. Law in Public Health Practice. 2d ed.. Oxford University Press; Oxford: 2007. p. 238-261.p. 246
18. See, e.g., Barnum JF. The Misinformation Era: The Fall of the Medical Record. *Annals of Internal Medicine* 1989;110(6):482–484. [PubMed: 2919852] Beers MH, Munekata M, Storrie M. The Accuracy of Medication Histories in the Hospital Medical Records of Elderly Persons. *Journal of the American Geriatric Society* 1990;38(11):1183–1187. Romm FJ, Putnam SM. The Validity of the Medical Record. *Medical Care* 1981;19(3):310–315. [PubMed: 7218896]
19. See Rothstein, *supra* note 12, at 492-493.
20. National Committee on Vital and Health Statistics. Letter to Michael O. Leavitt, Secretary of Health and Human Services. Jun 20. 2008 available at <www.ncvhs.hhs.gov/080220lt.pdf> (last visited December 11, 2009)
21. *Id.*
22. Pritts, J.; Connor, K. The Implementaion of E-Consent Mechanisms in Three Countries: Canada, England, and the Netherlands (The Ability to Mask or Limit Access to Health Data). 2007. available at <<http://ihcrp.georgetown.edu/pdf/prittse-consent.pdf>> (last visited August 10, 2009)
23. Chalmers J, Muir R. Patient Privacy and Confidentiality. *British Medical Journal* 2003;326(7392): 725–726. 726. [PubMed: 12676824]
24. 45 C.F.R. § 164.502(b) (2008).
25. See Hasday L. The Hippocratic Oath as Literary Text: A Dialog between Law and Medicine. *Yale Journal of Health Policy and Ethics* 2002;2(2):299–323.