Research Paper ■

Attitudes of First-year Medical Students Toward the Confidentiality of Computerized Patient Records

LUKE DAVIS, JENNIFER A. DOMM, MICHAEL R. KONIKOFF, RANDOLPH A. MILLER, MD

Abstract **Objectives:** To investigate the attitudes of students entering medical school toward the confidentiality of computerized medical records.

Design: First-year medical students at the Vanderbilt University School of Medicine responded to a series of questions about a hypothetic breach of patient's privacy through a computerized patient record system.

Measurements: The individual authors independently grouped the blinded responses according to whether they were consistent with then-current institutional policy. These preliminary groupings were discussed, and final categorizations were made by consensus.

Results: While most students had a sense of what was right and wrong in absolute terms, half the class suggested at least one course of action that was deemed to be inconsistent with institutional policies.

Conclusions: The authors believe that medical schools should directly address ethical and legal issues related to the use of computers in clinical practice as an integral part of medical school curricula. Several teaching approaches can facilitate a greater awareness of the issues surrounding technology and medicine.

■ **JAMIA.** 1999;6:53–60.

> 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 one spread abroad, I will keep to myself holding such things shameful to be spoken about.
>
> — Hippocrates, *The Physician's Creed*[1]

Understanding and influencing the attitudes of future physicians toward the confidentiality of electronic patient records are essential to ensure the integrity of emerging health care delivery systems. While the tradition of preserving confidentiality and privacy in the doctor–patient relationship has become well established over several millennia,[1–3] many new technology-related confidentiality issues present ethical dilemmas for today's clinicians, legislators, and educators.[4,5] Although these dilemmas are frequently addressed in a general fashion, few studies have examined how physicians-in-training view these issues.

This paper examines opinions of first-year medical students regarding the confidentiality of computer-based electronic medical records, to provide insight into prevalent attitudes and thereby recognize opportunities for improved education. During the biomedical informatics component of the required first-year Introduction to Biomedical Research course at the Vanderbilt University School of Medicine, all students completed an open-book, open-computer, take-home informatics competency exercise with ten individual questions. One multipart question involved a hypo-

Affiliation of the authors: Vanderbilt University, Nashville, Tennessee.

Correspondence and reprints: Luke Davis, Vanderbilt University School of Medicine, Eskind Biomedical Library, The Informatics Center, Room 436, 2209 Garland Avenue, Nashville, TN 37232-8340. e-mail: ⟨luke.davis@mcmail.vanderbilt.edu⟩.

Received for publication: 7/20/98; accepted for publication: 9/18/98.

thetic breach of patient confidentiality in Vanderbilt's computerized medical record system. The students' responses to the question indicate that some areas of ethics education need greater emphasis in the training of future physicians. Examining their attitudes is important not merely because insiders pose the most immediate danger of disclosure of patient data[6] but also because they will determine how successfully future health care information systems function.

Background

Although the words ''privacy'' and ''confidentiality'' are often used interchangeably, their meanings are distinct. Privacy is the state of being free from intrusion, and in the context of health care it concerns the responsibility of a care provider to protect a patient from any disclosure (i.e., discovery by others), even unintentional, of personal health data, by providing security to the patient and the patient's records. Confidentiality, in contrast, is the limiting of information to only those for whom it is appropriate. In a health care context, confidentiality relates to the obligation, described by Hippocrates, of a health care professional never intentionally to disclose anything revealed in personal communication with a patient. Stated another way, ''If someone follows you and spies on you entering an AIDS clinic, your privacy is violated''; if someone who works in the clinic faxes your health care records to a newspaper reporter without your permission or knowledge, your records' confidentiality is violated.[7]

Since the time of Hippocrates, the medical profession has required, as a condition of entry, an understanding of confidentiality. In the United States, the requirement has existed since the American Medical Association's first Code of Ethics was established in 1847.[2] Over time, the commitment to confidentiality has evolved from a responsibility to the medical guild into a responsibility to patients.[8] In the process, medical culture has come to acknowledge patient autonomy through moral and legal arguments supporting rights to privacy, confidentiality, and security.[9] Thus today confidentiality is accorded fundamental standing in the physician–patient relationship. Since at least 1977, the AMA has acknowledged this standing, by stating that ''the utmost effort and care'' is to be taken to protect these rights, even with respect to medical records that are computerized.[10]

Despite such philosophic changes, laws prohibiting the disclosure of health information have not provided fail-safe protection of privacy rights, nor do they promise to do so in this era of record automation.[11] As Donna Shalala, the Secretary of Health and Human Services, has noted,[12] significant violations of patient privacy and confidentiality persist, whether computerized or written patient records are involved. Seventy-five percent of Americans today reportedly express concern about the threats electronic medical records may pose to personal privacy.

Many knowledgeable persons point out that the increased amount of electronic data potentially accessible with each breach of security could make the damage to patient's privacy and confidentiality proportionally larger.[3] On the other hand, an Institute of Medicine special committee (the Committee on Improving the Patient Record in Response to Increasing Functional Requirements and Technological Advances) has argued that electronic records can offer greater confidentiality through security measures that limit the spectrum of information various users can see.[13] Either interpretation leads to the conclusion that technology should follow the dictates of policymakers,[14] including physicians, who have always provided the first protections of personal data.

For the new systems to uphold the tradition of doctor–patient confidentiality, they require user understanding from their conception to their implementation. Thus, examining medical-students' attitudes toward computerized medical records during their indoctrination into the medical profession is of primary importance.

Methods

As part of their Introduction to Biomedical Research course in the fall of 1996, all first-year Vanderbilt medical students were given six hours of introductory biomedical informatics lectures and two hours of hands-on instruction, in an effort to increase their awareness of the role of information technology in the research, practice, and independent learning of medicine. Two half-hour sessions covered general concerns related to patient confidentiality and computerized records and outlined specific policies in effect at Vanderbilt at that time (Appendix A).

Evaluation of students' mastery of the biomedical informatics material was carried out through a six-hour open-book, open-computer take-home essay exercise (Appendix B). Part of this exercise was a set of free-response questions regarding a hypothetic violation of a hypothetic patient's privacy. The first question asked students how they would respond if they heard that a fellow student had sold specific patient information to the media; the second question asked

whether they would respond differently if they heard that the student had instead sold a password to enter the system. The third question asked whether sensitive medical records or those of prominent persons should be given extra security measures. The actual questions to which the students responded are presented in Appendix B.

After the students completed the exercise, and prior to the initiation of the current study, one author (R.A.M., as the course segment director) prepared, in conjunction with the faculty of the Division of Biomedical Informatics, an ''answer key'' for the exercise. This was distributed to all participating students along with their corrected papers. For question 1, the answer key summarized then-current institutional policies regarding the hypothetic incident and appropriate responses to it. This answer key was used as a standard against which student responses could be judged during the analysis done in the present study. The medical school class was consulted after completion of the assignment, and unanimous consent was given for the authors to use and analyze the students' responses for the present study. The student authors (L.D., J.A.D., and M.R.K.) received blinded copies of the answers, which had been submitted by their classmates.

Independently of one another, the student authors categorized students' answers to the first question. They generated free-text descriptors that grouped student responses into similar categories. The initial categorizations were subsequently reviewed and combined (by R.A.M.) into a smaller number of more general groupings that covered all the initial categories.

Questions 2 and 3 required an initial response and an explanation of that response. Ideally, the initial response was to be ''yes'' or ''no,'' but the essay nature of the question allowed students to add free, subjective responses. For this reason, the student authors independently tallied the initial responses, and discrepancies were discussed and resolved.

Results

The biomedical informatics exercise was distributed to 103 first-year medical students. A total of 97 essays were completed and returned (the course director exempted several students from the exercise for various reasons). Responses to question 1 (about students' actions after a fellow student reportedly sold confidential patient information) are shown in Table 1. Of the 97 respondents, 51 students (53 percent) indicated that they would notify a dean in the medical school; 18 (19 percent) would notify either the medical school or the graduate school honor committee; five (5 percent) would notify a faculty member, department, or other academic unit; 12 (12 percent) would notify the hospital; and one (1 percent) would notify the attending physician. The former responses were deemed to be consistent with institutional policy. However, 34 students (35 percent) would undertake at least one action independent of disciplinary authorities, and 16 (16 percent) gave vague responses or stated that no action should be taken.

Question 2 asked students whether their opinions would change if a password, and not confidential information, was sold. Thirty-eight (39 percent) believed that the student who had revealed the password should then be treated differently, 57 (59 percent) believed that the penalty to the student should be the same, and two (2 percent) were unsure.

Question 3 asked whether certain records should be given extra security measures, over and above routine measures. Sixty-six students (68 percent) were in favor of extra security measures, whereas 31 (32 percent) were opposed. Many of those opposed felt that all records deserve the best possible security.

Discussion

Reflections on Results of Study

At least three interesting observations follow directly from the study results. First, a majority of first-year students believed that they had a responsibility to report the potential breach of a patient's privacy. However, 53 of the 97 students who completed the exercise selected at least one course of action that could be viewed as unacceptable with respect to current institutional policies (Table 1). The answer key that was distributed following the exercise summarized the medical center guidelines in effect at that time (Appendix A) and explained several practical and philosophic justifications for those policies. Few medical students, if any, have the expertise or resources to investigate adequately and fairly either the legality or the technicalities of a supposed breach. Furthermore, students have an obligation to protect their classmate from the consequences of a possibly unfounded rumor. Each student response categorized in the results section as ''unacceptable'' is likely to be counterproductive, by delaying or interfering with the accused student's right to a confidential and unbiased investigation. The best course of action would be to report the incident, as it was related, directly to both the Dean of Students and appropriate hospital authorities, clearly emphasizing that the source of the information was an unconfirmed rumor. The Dean of Stu-

Table 1 ■

Responses of Students (N = 97) to Question about What Actions They Would Take in Response to an Alleged Breach of a Patient's Privacy by a Fellow Student

	Number	(%)
Responses consistent with institutional guidelines:		
Notify medical school deans	51	(53)
Notify medical/graduate school honor committee	18	(19)
Notify faculty, department, or other academic unit	5	(5)
Notify hospital	12	(12)
Notify attending physician	1	(1)
Responses not consistent with institutional guidelines:		
Investigate on my own	19	(20)
Confront student	15	(16)
Notify police or law enforcement	4	(4)
Do something too vague to interpret	15	(16)
Do nothing	1	(1)

NOTE: The wording of the question is given in full in Appendix B. The number of responses exceeds the number of students who completed the exercises because some students suggested courses of action involving more than one category.

dents oversees the conduct of medical students; hospital authorities take responsibility for the care and protection of patients. Both are capable of conducting a thorough, confidential investigation, which would protect the accused student if he or she were innocent and appropriately document the facts for punitive action if he or she were not. If the rumor were confirmed in this way, action could then be taken to prevent disclosure of confidential patient information and to contact police and other external authorities as soon as it was appropriate. In any case, each student has a duty to the patient, to the institution, and to the health care system in general to take action to help.

Second, the responses show that students believe that their responsibility for preserving patient privacy extends to the protection of computerized records. A majority said that even indirect disclosure of patient information (i.e., revealing a password to the system) would merit punishment as severe as that deserved for revealing the information directly.

Third, the issue of having different levels of security for "normal" patient data and for data that are considered more sensitive (either because a patient is a prominent person or because certain information, if revealed, is deemed likely to cause harm to a patient) prompted a variety of justifications on both sides of the issue. Many students argued against a double standard, insisting that any technology able to make records less accessible to unauthorized persons should be applied universally. Some worried that a higher level of security could compromise patient welfare if it prevented some care providers from accessing the protected records in an emergency. Others pointed out that it may be difficult to define objectively what information deserves extra protection. Finally, a few students wondered whether making selected computerized medical records harder to access than others would only make them more attractive targets for "hackers."

Incorporating discussion of institutional policies on privacy and confidentiality into courses addressing medical ethics, medical informatics, and introductory clinical practice could help entering medical students address these issues.

National Recommendations on Privacy, Confidentiality, and Security

Efforts to computerize all patient records[13] are fueling a number of ethical and policy debates in both the private and public sectors. These include discussions about technology's role in the privileged doctor–patient relationship, the advantages and disadvantages of improving scientific medicine through more efficient data gathering, and the increasing cost of health care.[15] While the U.S. government report on these issues, *Records, Computers, and the Rights of Citizens*,[16] was released in 1973, the legislative guidelines for protecting medical records have not kept pace with rapidly emerging information technologies. Thus, the issues of privacy, confidentiality, and security have been the focus of reform efforts by both Secretary Shalala and Congress. For example, the recent Kennedy–Kassebaum legislation, Section 264 of the Health Insurance Portability and Accountability Act of 1996, mandated that the Secretary propose and implement privacy and security rules for electronic medical records.[12] Professional organizations, such as the AMA, The American College of Physicians, AMIA, and the American Health Information Management Association, have also begun to address these topics through the individual research, working groups, and task forces of their members[7,14] and through their public policy committees.

Current Medical School Curricula in Health Care Ethics

Sir William Osler wrote of the dangerous tendency of "professional work . . . to narrow the mind, to limit

the point of view.''[17] The enduring importance of physician responsibility and institutional policy to patient privacy can be quickly forgotten as health care systems change. Instilling an awareness of these timeless values early in professional training can encourage future physicians to become leaders by example.

The authors' current survey found that, even after several hours of lecture-based instruction, almost half of first-year medical students possessed only a vague understanding of their responsibilities with regard to the institutional policies on the privacy and confidentiality of computerized medical records. Other evidence shows that even trained health care providers are not fully aware of their obligations toward patient confidentiality.[18] These data provide support for expanding medical education in this area. Currently, ethics instruction represents a small fraction of the curriculum of most medical schools: Two studies found that institutions in Britain[19] and Canada[20] devote an average of 12 and 23 hours, respectively, per medical degree to teaching health care ethics. A limited survey of Web sites of U.S. medical schools, conducted by the authors, suggests that low proportions probably apply in American medical schools as well.

How ought the demonstrated lack of awareness of the privacy and confidentiality issues surrounding computerized medical records be remedied? Some medical schools have successfully adapted the classic approach to teaching ethics by teaching students to apply skills of reasoning and valuation in the analysis of relevant clinical cases.[19,21–23] This allows students to address ethics and policy considerations simultaneously, as in the questions used in the current study. One group of prominent medical educators has argued that ''ethics is not readily separable from law and communication skills''[24]; they imply that physicians should become more directly involved in the philosophic issues that underlie health care policy considerations.

To teach professional ethics successfully, basic medical education should cover ethical aspects of computerized medical records in conjunction with legal issues, technology, and doctor–patient and doctor–institution communication. Yet the National Research Council has observed that ''one of the obstacles to improving privacy and security in health care organizations is a lack of knowledge about the types of technical and organizational practices that are effective in protecting health care information.''[25] This study itself illustrates that many students are unaware of how institutional policies can address the threats to the doctor–patient relationship that technology can make possible. Elsewhere, students note that even innovative approaches to integrating ethics into the curriculum overlook the crucial issue of organizational ethics, which are the values to which students are exposed during their clinical clerkships. As a student from another medical school remarked, ''you failed to address what is the most important aspect of confidentiality: the innumerable breaches in confidentiality which routinely occur throughout this hospital.''[24]

One approach would be to incorporate teaching on these topics into the mainstream instruction of physicians-in-training that occurs on the wards.[26,27] This is done currently at Vanderbilt through weekly clinical informatics conferences, during which faculty and staff from the Division of Biomedical Informatics discuss pragmatic, system-related issues with students, house staff, and faculty who are on clinical rotations (in informal noon sessions where free lunch is provided).

The privacy and confidentiality of computerized medical records are a fundamental issue that should form the basis for teaching innovations related to both informatics and ethics. The authors believe that the current study documents a need for focused medical education covering both ethical and legal aspects of computer usage in clinical care and research. The authors believe that this should be done in a clinical setting, in conjunction with instruction on using computer-based biomedical informatics tools as adjuncts to lifelong professional development.

The authors thank the Vanderbilt Medical School Class of 2000 for releasing their responses to the Introduction to Biomedical Ethics exercise for this research; Ms. Joyce Green, of the Division of Biomedical Informatics at the Vanderbilt University Medical Center, for her support and assistance throughout the project; Dr. George Reed, of the Department of Preventative Medicine at VUMC, for his advice regarding statistical treatment of the data gathered in this research project; Dr. Stuart Finder, of the Center for Clinical and Research Ethics at VUMC, for his comments and suggestions about the paper; Dr. Dario Giuse, Associate Professor of Biomedical Informatics and leader of the MARS (Medical Archival System) project at VUMC, for providing information about the system access and confidentiality agreements protecting patient records at Vanderbilt; and Ms. Dawn Miller, of the Eskind Biomedical Library at VUMC, for her guidance in searching computerized bibliographic databases and the Internet.

References ■

1. Etziony MB. The Oath of Hippocrates. The Physician's Creed: An Anthology of Medical Prayers, Oaths, and Codes of Ethics Written and Recited by Medical Practitioners through the Ages. Springfield, Ill.: Charles C. Thomas, 1973.
2. Proceedings of the National Medical Conventions Held in New York, May, 1846, and in Philadelphia, May, 1847. Philadelphia, PA: Collins, 1847.

3. Miller RA, Schaffner KF, Meisel A. Ethical and legal issues related to the use of computer programs in clinical medicine. Ann Intern Med. 1985;102:529–36.
4. Shalala DE. Confidentiality of individually identifiable health information: recommendations of the Secretary of Health and Human Services, pursuant to section 264 of the Health Insurance Portability and Accountability Act of 1996. Office of the Assistant Secretary for Planning and Evaluation, Department of Health and Human Services Web Site. Available at: http://aspe.oe.hhs.gov/adminsimp/pvcrec1.htm#particular. Accessed Mar 16, 1998.
5. Benatar SR. Teaching medical ethics. Q J Med. 1994;87: 759–67.
6. Lewis PH. Threat to corporate computers is often the enemy within. Survey of the Computer Security Institute of the FBI International Computer Crime Squad. New York Times Web Site. Available at: http://www.nytimes.com/library/tech/98/03/biztech/articles/02hack.htr. Accessed Mar 2, 1998.
7. Goodman KW, Miller RA. Ethics and health informatics: user, standards, and outcomes. In: Shortliffe EH (ed). Medical Informatics: Computer Applications in Health Care. 2nd ed. Chapter 7. New York: Springer-Verlag, 1998.
8. Brannigan VM. Protecting the privacy of patient information in clinical networks: regulatory effectiveness analysis. Ann N Y Acad Sci. 1992;670:190–201.
9. Gostin LO, Turek-Brezina J, Powers M, Kozloff R. Privacy and security of health information in the emerging health care system. Health Matrix: J Law Med. 1995;1:1–36.
10. American Medical Association. Code of Medical Ethics: Current Opinions with Annotations. Chicago, Ill.: AMA, 1996:89.
11. Waller A. Legal aspects of computer-based patient records and record systems. In: Dick RS, Steen EB (eds): The Computer-based Patient Record: An Essential Technology for Health Care. Washington, D.C.: National Academy Press, 1991. Sponsored by the Institute of Medicine.
12. Shalala DE. Testimony before the U.S. Senate Committee on Labor and Human Resources. September 11, 1997. Office of the Assistant Secretary for Planning and Evaluation, Department of Health and Human Services Web Site. Available at: http://aspe.oe.hhs.gov/adminsimp/pvctest.htm. Accessed Nov 7, 1997.
13. The Computer-based Patient Record: An Essential Technology for Health Care. Dick RS, Steen EB (eds). Washington, D.C.: National Academy Press, 1991. Sponsored by the Institute of Medicine.
14. Barrows RC Jr, Clayton PD. Privacy, confidentiality, and electronic medical records. J Am Med Inform Assoc. 1996; 3:139–48.
15. Secretary's Advisory Committee on Automated Data Systems. Records, Computers and the Rights of Citizens. Washington, D.C.: Department of Health, Education and Welfare, 1973. Publication no. (OS)73–94.
16. Woodward B. The computer-based patient record and confidentiality. N Engl J Med. 1995;333:1419–22.
17. Osler W. In: Roland CG (ed). The Master-Word in Medicine: A Study in Rhetoric. Springfield, Ill.: Charles C. Thomas, 1972:27.
18. Shrier I, Green S, Solin J, et al. Knowledge of and attitude toward patient confidentiality within three family medicine teaching units. Acad Med. 1998;73:710–2.
19. Burling SJ, Lumley JS, McCarthy LS, et al. Review of the teaching of medical ethics in London medical schools. J Med Ethics. 1990;16:206–9.
20. Baylis F, Downie J. Ethics education for Canadian medical students. Acad Med. 1991;66:413–20.
21. Churchill LR. The medical ethics teaching program at UNC–Chapel Hill. N C Med J. 1993;54:405–7.
22. Seedhouse DF. Health care ethics teaching for medical students. Med Educ. 1991;25:230–7.
23. Randall T. Students challenged to make ethics part of their ''habit of thought.'' JAMA. 1992;268:2349–50.
24. Hope T, Fulford KWM. The Oxford Practice Skills Project: teaching ethics, law, and communication skills to clinical medical students. J Med Ethics. 1994;20:229, 232.
25. National Research Council, Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. For the Record: Protecting Electronic Health Information. Washington, D.C.: National Academy Press, 1997:5. Also available at: National Academy Press Web Site. http://www.nap.edu/readingroom/books/for/index.html. Accessed Mar 2, 1998.
26. Grundstein-Amado R. Values education: a new direction for medical education. J Med Ethics. 1995;21:174–8.
27. Hafferty FW, Franks R. The hidden curriculum, ethics teaching and the structure of medical education. Acad Med. 1994; 69:861–71.

APPENDIX A

Systems Access and Confidentiality Agreement, Vanderbilt University Medical Center (1996)

Due to the confidential nature of the data contained in all patient records, electronic, paper, or otherwise, measures must be taken to ensure that any such computerized patient record systems as are in use at the Vanderbilt University Medical Center (VUMC) and, where applicable, VUMC off-site subsidiaries and affiliates can only be accessed by authorized users. VUMC has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their health information.

Such computerized data systems include, but are not limited to, the integrated patient care system, the medical data retrieval system, the inpatient accounting system, the laboratory information system, the pharmacy information system, the radiology information system, and the physician billing system.

Your password and user ID are your unique identifiers for the system(s) you are authorized to use only pursuant to your VUMC or University employment or medical staff status and authorized activities only. You must not allow others to use your password. We require you to change your password every six months or it will be suspended (the system will give you ample warning).

I, [name], understand and agree to the following:

1. I understand that the confidentiality of patient records is required by law, and that there are statutes or policy reasons specifically mandating the confidentiality of, among other areas, mental health, HIV, and drug and alcohol-related treatment records.

2. I understand that the Department of Information Management conducts and maintains an audit trail of accesses to patient information that records the machine name, user, date, and patient identification of all accesses to patient medical record data that is electronically maintained.

3. My password/user ID is the equivalent of my signature. I am the only person authorized to use my password/user ID.

4. I will safeguard and will not disclose my password or any other authorization I have that allows me access to confidential information. I accept responsibility for all activities undertaken using my password.

5. I will use confidential information only as needed by me to perform my legitimate duties at VUMC employee. This means, among other things, that:
   a. I will not access confidential information which I have no legitimate need to know.
   b. I will not in any way divulge, copy, release, sell, loan, revise, alter, or destroy any confidential information except as properly authorized within the scope of my employment.
   c. I will not misuse or carelessly care for or fail to safeguard confidential information.

6. I understand that I have no right or ownership interest in any confidential information referred to in this agreement. VUMC may at any time revoke my password.

7. I will retrieve or attempt to retrieve from the computer system only medical data that is directly related to the treatment of patients for whom I have a clinical relationship, or those patients for whom I have been asked to provide a consultation, or for approved educational or research purposes. I agree to maintain the confidentiality of all such patients, and/or fiscal data. I will access fiscal data only as required by my employment or medical staff responsibilities.

8. It is my responsibility to log out of the system. I will not, under any circumstances, leave unattended a computer terminal to which I have logged on.

9. If I have reason to believe that the confidentiality of my password has been compromised, I will change my password. I will immediately report any known or suspected breach of the confidentiality of the system or records/data obtained from it to my immediate supervisor or the Department of Information Management, Security Administrator.

10. I understand that my user ID will be inactivated upon notification that I am no longer employed, or have no privileges at, a VUMC institution, or am not registered as a medical or nursing student or when my job duties do not require access to the computerized systems.

11. My signature below indicates my understanding of the above noted requirements for the use of any password/user ID I am assigned, pursuant to my employment, student or medical staff responsibilities with the Vanderbilt University Medical Center or Vanderbilt University.

12. It is my responsibility to be aware of the Vanderbilt University staff handbook General Policies Section ''Confidential Information'' and the Professional Conduct Section ''Misconduct That Warrants Immediate Discharge'' and/or other Faculty or Student handbooks that reference such activity. These documents further outline the policies for protection of information and the misconduct process.

13. I further understand that the VUMC has incorporated the requirements of such statutes into its policies and procedures for access to and treatment of

such specialized patient record information, and that it is my responsibility to be familiar with and adhere to such policies and procedures. Any fraudulent application, violation of confidentiality or any violation of the above provisions may result in disciplinary action, including termination of access to the system, appropriate medical staff or university disciplinary measures, up to and including termination of my employment or affiliation with the university or the VUMC, or appropriate medical or nursing school disciplinary measures, up to and including dismissal from the school.

14. I read and agree to all of the above as conditions of being granted a password.

15. This agreement will be on file in the Department of Information Management. I may review the agreement by contacting the Department of Information Management.

APPENDIX B

Essay Questions Regarding Hypothetic Breach of Patient's Privacy

Open-book Examination: You are on your honor not to consult with anyone else in answering these questions. You may use any written or electronic resources (excluding e-mail or similar communication programs that have human end users) to answer the questions. Do not spend more than six hours total in answering all the questions (taken as a whole). You may take far less time to do a good job if you are well organized.

QUESTION: [Hypothetic scenario.] In 1998, you learn from a friend that a third-year Vanderbilt medical student has accessed patient information about a well-known government official (stored in the VUMC hospital information system) and sold the information to a television station. Please answer the following questions with no more than three paragraphs each.

1. What related actions would you take, if any:

2. The student claims that he gave his password to a friend and that the friend was the person who gave the information to the media. Does this change your thinking about disciplinary actions? How could anyone prove what the truth was?

3. Should certain records (e.g., ''VIPs,'' patients with AIDS, psychiatric conditions, or sexually transmitted diseases) be given extra measures of protection over and above usual records? Explain your reasoning.