Journal of International Information Management

Volume 3 | Issue 2 Article 2

1994

Information control and security policy in health care information systems

Binshan Lin
Louisiana State University

Lawrence Clark
Louisiana State University

Information control and security policy in health care information systems

Binshan Lin
Lawrence Clark
Louisiana State University, Shreveport

ABSTRACT

The reliance on information systems forces the health care organizations to consider two security management issues: information control and security policy. The objective of this article is to examine a direction to effectively support and enhance the health care delivery through information systems in hospitals. An integrated focus is provided through an information control framework for analyzing the three control elements: accessibility, confidentiality, and integrity. The security policy involves three aspects: prevention of unauthorized access into the system, controlling the input and output of the system, and monitoring the health care information systems. The framework has implications for research beyond the case of health care information systems. Specifically, we suggest that any information control and security policy founded on the system context approach will not be adequate unless organizational context is also considered. Hospital managers should see themselves as the key actors in monitoring the dynamic information systems environment, assessing organizational risk, coordinating with functional areas in hospitals, and disseminating appropriate information.

INTRODUCTION

Hospital managers have become aware that information and information systems are critical organizational resources in the health care environment (Lin, 1991). Medical information has been documented as being more sensitive than some other types of information (Harris, 1990). Several characteristics of computer technology and its use in health care organizations are important in understanding and managing the information systems security. Three salient features characterize the growing literature on health care information systems (HCIS). These are the nature of computerized information systems, the growing importance of end-user computing in health care organizations, and the development of networking technologies.

First, the high concentration of electronically stored information contributes to the efficiency of computerized HCIS. Second, a potentially serious implication for the incidence of

system security is the increase in many hospitals of end-user computing. End users of HCIS may program, enter data, operate, and have responsibility for entire information systems. Third, today's HCIS management must oversee their systems that run on multiple platforms, ranging from PCs to local area network to midrange systems to mainframes. As more hospitals adopt right-sizing strategies; distribution of information and processing to autonomous operation units; new design and deployment techniques such as client server architectures, the security and control specialists have new roles to work with.

Health care organizations need to understand the importance of HCIS security, how to reasonably implement security, and how to maintain an ongoing commitment to HCIS security. Three agents are assumed in the concern of HCIS security, each with different objectives - the hospital managers wish to maximize the value of its services net of the costs of providing them given its fixed capacity; the end users wish to maximize software quality given their access of HCIS; and the information systems department wishes to secure the use of HCIS.

Information technology raises concerns and makes traditional policy assumptions irrelevant (Diebold, 1984). Even though organizations continue to develop and implement more protective security policies, computer abuse may continue to be a problem in the 1990s (Straub & Nance, 1990). The leading issues raised by HCIS security include questions of privacy, integrity, ownership, and impact.

- *Privacy*: How is medical information collected, used, and protected? Privacy deals with the rights of the people and organizations to determine who, when, where, and how the information is to be used (Rob & Coronel, 1993). For many patients, the invasion of privacy constitutes their greatest fear about the misuse of information technology.
- *Integrity*: Who is responsible for maintaining the accuracy and completeness of information stores in HCIS? Who is responsible for mistakenly prescribing through a HCIS what could amount to an overdose of drugs?
- *Ownership*: Who owns the information and HCIS? How can that ownership be established when computerized information is so easily duplicated, distributed on network, or accessed from an information system?
- *Impact*: How do HCIS safety policies impact the health care process in a hospital?

There are three major challenges: (1) maintain a security infrastructure that is transparent to end users; (2) build a secure environment that is not overly complex to manage; and (3) determine how to interoperate in a distributed environment. These challenges force the health care organizations to consider two security management issues; information control and security policy. The objective of this article is to examine a direction to effectively support and enhance the health care delivery through information control and security policy in hospitals.

THE CONCEPTUAL FRAMEWORK

A conceptual framework is also needed. This framework shall provide a generic description of the control process. The conceptual framework assumes that the health care information system can be decomposed into a set of interlinked feedback data loops, each controlling a physical process.

The conceptual framework addresses utilitarian and respect for persons' viewpoints. Classical utilitarianism can be stated as an action is right if and only if it produces the greatest balance of pleasure over pain for everyone (Boatright, 1993). In general, the utilitarian is interested in the greatest total preference-satisfaction of all considered possible alternatives. The greatest good for the greatest number is a utilitarian notion. The most consistent form of utilitarianism is one which disregards the distribution of utility and simply tries to achieve the greatest total utility (Harris, 1986). In respect for persons, the ethicist is mainly subscribing to the belief that those actions are right that treat human beings, whether you or another person, as an end and not simply as a means.

It seems clear that concerns about abuse of patient privacy in HCIS must be addressed. Privacy exists when individuals can make autonomous decisions without outside interference, can limit their accessibility to others and/or can control the release and subsequent circulation of personal information (Bennett, 1992; Stone & Stone, 1990). Invasions of privacy occur when patients perceive they have a reduced sense of autonomy or control, or when autonomy is lost because a patient's actions are unknowingly manipulated by others. From the utilitarian viewpoint, the question of privacy in HCIS must be decided as a compromise between full privacy and no privacy. The use of HCIS requires trade-offs with respect to confidentiality of medical information. There are many benefits that can be accrued from information disclosure, such as instant access to medical databases with patient histories in cases of emergencies. Legitimate users can more conveniently access computer-based records in well-designed HCIS. Without sufficient information control, however, unauthorized users may threaten the confidentiality and integrity of HCIS.

Brown (1990) describes the concept of social roles as pivotal to our understanding of information privacy and proposes the following moral principle to guide our dealings with confidentiality and integrity: Access to particular information about persons ought to be systematically related in the appropriate way to the network of social relationships in which they stand to others by virtue of their places in the role structure. An invasion of privacy may then be described as a divorce of the flow of information from the social role structure. Privacy issues arise as a result of the subsequent use of information gathered about a particular health care transaction rather than the intrinsic attributes of the health care service itself.

One way for health care organizations to address potential privacy concerns raised by the reuse of medical information is to observe fair information practices in dealing with patients. Fair information practices define procedural guarantees that allow individuals to balance their privacy interests with an organization's need for personal information. Fair information practices are similar to fair trade and labor practices, and to the due process principles embodied in the Fifth and Fourteenth Amendments to the Constitution (Bennett, 1992).

Two major principles are addressed as follows. The first principle is the control independence. The principle of control independence advocates that control function should be as objective as possible, i.e., independent in order to fairly and accurately monitor organizational outcomes, including deviation of performance from standards and goals (Straub, 1987). The person charged with designing, implementing, and operating a control should not be the same

person who is to be controlled thereby. This idea is used in business and is referred to as "separation of duties." For example, peer review or security committee may be used to control the HCIS in hospitals.

The second principle is the least privilege. This principle implies that access to HCIS, the ability to execute certain programs, and other system privileges should be restricted to those who can demonstrate for a business- or medical-related need. It has been stated in terms of executing processes (Saltzer & Schroeder, 1975), i.e., a process should have exactly those privileges needed to accomplish its assigned task, and none extra.

INFORMATION CONTROL IN HOSPITALS

Information is control (Pettigrew, 1972). Information systems security is distinguished from conventional computer security in that it involves more than the logical security that controls access to centralized programs and data and physical security. Information control in HCIS refers to the protection of the information that a system processes, transmits, and stores. To put it more positively, information control is employed to make sure any sharing of information resources is on a controlled basis.

HCIS can be treated as an administrative resource having both allocative and authoritative aspects, and as capable of significantly influencing the manner and form of control employed in hospitals (Lin, 1993). An integrated focus is provided through an information control framework for analyzing the three control elements: accessibility, confidentiality, and integrity.

Accessibility

Accessibility means end users can extract the data they need, when they need it. Accessibility starts at the point the data are collected, and includes the way HCIS process the data and the way errors are corrected. The principle of least privilege translates into a requirement for accessibility. There are two major aspects of accessibility: access privileges, and access restriction.

Access privileges are precise statements of which systems and data an individual can access and under what circumstances (Alter, 1992). There are four levels of access privileges: absolutely no access, access following authorization, access to statistical data only, full working access (Gritzalis, et al., 1991). For example, the fact that someone can log onto a HCIS does not mean he/she would be permitted hospital-wide access. Many HCIS use file access lists that grant individual users or groups of users different levels of access to specific files. Privileges for defining certain alarm states can be limited to a specific group of end users.

On the other hand, access restriction is a prerequisite for accessibility. It is the procedures designed to limit entry to a physical area, or to limit use of an information system to authorized users. Access restriction takes three forms: physical, logical, or inherent. In order to determine access restriction we classify the end users into four groups: medical personnel (physicians),

paramedical personnel (nurses and laboratory personnel), administrative personnel, and the public. Variable access to the system then can be controlled for individual users or for groups of users. Some operations may be restricted to particular terminals. For example, the ability to modify patient charges might be precluded for financial personnel working from terminals located in the accounting office.

Data transparency to the medical doctors is the promise of a HCIS. However, most operating systems and databases in the health care environment usually require their own security clearance. The two aspects are in conflict. There is a need to seek system-wide authorization that would simplify access control of HCIS without sacrificing security.

Confidentiality

The growing use of HCIS has resulted in a major threat to privacy and has introduced into health care management concerns about the information being collected on patients and the uses of this information. For instance, information provided by patients/doctors is done so with the expectation that the information will be maintained in confidence and used only in the best interests of the patient/doctor. Confidentiality refers to how protected is the health care information from access by others. This expectation of confidentiality is supported by legal, accrediting, and regulatory agency requirements. The published codes of ethics of the American Medical Association's "Principles of Medical Ethics" and The American Nurses' Association "Code for Nurses" recognize an obligation of confidentiality with certain limitations.

Even with the protection provided by such requirements, HCIS is available to a vast variety of interested parties (Patrikas & Liebler, 1987). Various people may be informed of the details of a patient's medical history, for instance, nurses, insurance agents, social workers, researchers, etc. (Coleman, 1984). Moreover, the confidentiality of the physician-patient relationship is the most troublesome aspect of the use of HCIS. In some situations, for the physician not to reveal confidential information about a patient may greatly endanger innocent third parties. For example, a medical case concerning a physician's patient who has tested positive for the HIV virus and who is engaged to be married (Winston & Landesman, 1987). When the physician advises his patient to inform his fiancee of the results of the test, the patient refuses on the ground that doing so would disrupt his plan for marriage. The "duty to protect" is now based on the "harm principle," which requires moral agents to refrain from acts and omissions which would foreseeably result in preventable wrongful harm to innocent others (Winston, 1991).

A specific "right of information privacy," which extends to the privacy of personal conduct to information stored about a person, has been advanced, namely that individuals have the right to exercise control over the collection, storage, use, dissemination, and accuracy of information stored about them (Freedman, 1982). The debate about confidentiality often concerns who has a right to know, though, as pointed out by McLean and Maher (1985), confidentiality and right to know are by no means identical concepts. Confidentiality is described as "duty," whereas the right to know is just a "right." Doctors have a professional duty to maintain the HCIS in confidentiality; patients have a right to expect that the information disclosed in confi-

dence is maintained in confidence. When the duty is breached the patient may bring a legal action to protect his/her right and/or recover damages resulting from the breach.

In the realm of confidentiality least privilege is often called "need-to-know." Given that patients are not able to control access to the use of their medical records, it is the responsibility of hospital administrators to establish, and where necessary to enforce, public and institutional policies that ensure privacy protection safeguards for medical records (Hiller & Beyda, 1981).

Integrity

Security refers to the protection of information against unauthorized disclosure, alteration, or destruction; integrity refers to the accuracy or validity of information (Date, 1986). In other words, integrity concerns the overall assurance that the contents of the HCIS are accurate and consistent. Security and integrity have also been cited as the primary management concern in end user computing (Benson, 1983). Security cannot be added directly on to an information system; the information control mechanisms must be integral parts of the HCIS.

The basic foundation of integrity is the assurance that all updates are carried out by well-formed transactions. The concept of the well-formed transaction is that users should not be able to manipulate data arbitrarily, only in restricted ways that preserve the integrity of the information systems (Sandhu & Jajodia, 1993). In the integrity context the principle of least privilege is appropriately called "need-to-do."

Access controls are based on the premise that the end user has been correctly identified to the system by some authentication procedure. Authentication typically requires the user to supply his or her claimed identity (e.g., user name or identification number) along with a password or some other authentication token. Authentication may be performed by the operating systems, the data base management system, a special authentication server, or some combination.

Integrity is an issue that might be partially addressed with database technology, specifically the security functions of an integrated data dictionary. Data base access controls are often data dependent. For example, a doctor may be restricted to seeing medical records for other patients in his or her department. There are three information control mechanisms for implementing data-dependent access control in HCIS: view-based access control, query modification, and mandatory access control.

The security features of an integrated data dictionary typically involve security of two levels:

- Table - A user may be permitted or denied access to a table.
- View - A user may be permitted or denied access to data within a view.

For example, a hospital has written a program which automatically logs off users if they do not choose "continue" on a menu after accessing patient files (Nash, 1992). In order to give a high degree of protection, authentication must go beyond simply requiring the end user to quote a password or use an encryption key (Wilkes, 1991). Query modification is another

mechanism for enforcing data-dependent access controls for retrieval. With this technique, a query submitted by a user is modified to include further restriction as determined by the user's authorization.

With mandatory access controls, the granting of access is constrained by the system security policy. These controls are based on security labels associated with each data item and each user. A label on a data item is called a security classification, and a label on a user is called a security clearance. Once assigned, the classifications and clearances cannot be changed, except by the security officer.

Too little control can lead to proliferation of equipment and software and subsequent integration and maintenance problems, while too much control can prevent end users from doing the job they alone are responsible for.

SECURITY POLICY IN HEALTH CARE INFORMATION SYSTEMS

The term "policy" is used in the management literature in two related but distinct ways. In general, policy refers to an organization's grand plan or strategy which defines its overall goals and objectives. More narrowly viewed, policy refers to specific statements that define desirable and unacceptable management practices and, as a result, limit managerial discretion at lower levels in the hierarchy (Camillus, 1986). This second definition most clearly conveys the level of concern in this study.

Security policy is a statement of top management's stance on the information security (Longley, 1989). It must be capable of expansion by middle and lower management, so that each member of staff has a clear, consistent, and unambiguous statement of their responsibilities toward the security of HCIS. Table 1 shows the four major aspects involved in the HCIS security policy.

Table 1. The Four Major Aspects Involved in the HCIS Security Policy

- Identify HCIS assets.
- Define who is responsible for classifying and valuing information assets.
- Describe the role of hospital employees in protecting the healthcare information.
- Construct an effective information infrastructure.

The HCIS security policy is a management issue. The techniques employed in developing enhanced security may be technically sophisticated but they will only be effective if they are implemented and deployed within an integrated framework. Too often, many hospitals are only interested in HCIS when a system virus attack or similar incident occurs. Health care managers need to understand both technical and organizational aspects in security policy.

HCIS security policy should take into account the information infrastructure of the hospital, the culture of the health care environment, and how resources will be allocated to cover the mixed precautions that will be employed. It should be clear what levels of protection are needed for which information and processing and when and where they should be applied as well as how to set up an appropriate computer security system, the components that are needed, and how they should be installed and work together.

HCIS security policy can be examined at several levels in the hospital, both from a vertical and a horizontal perspective. The *vertical* perspective has to do with management reporting level. Security administrators may report to top management, to middle-level managers, and finally to line managers. The *horizontal* perspective deals with the functional area of primary reporting responsibility. For example, HCIS security may report to accounting managers, to the Audit Committee of the Board of Directors, or to IS management.

Security policy depends on the type of application used. Loss of time-critical applications central to daily health care operations or serving customers could result in major financial loss or customer dissatisfaction. Security policy can be divided into three areas: (1) prevention of unauthorized access into the system, (2) controlling the input and output of the system, and (3) monitoring security and recovery of the HCIS.

First, information systems managers must be aware that end users may gain inappropriate access to sensitive information resources. Preventives screen access to the system to admit authorized users only. The preventive approach is advantageous, since it can face many problems before they occur, thus enabling the system administration either to prevent them or at least to minimize their undesirable consequences.

Mason (1986) suggests four ethical areas that should be protected by information policies: (1) an individual's right to keep data about himself/herself private; (2) an individual's right to assure that it is accurate; (3) an individual's right to maintain ownership of it; and (4) an individual's right to have access to it. Managers who address the ethical issues surrounding HCIS must be aware of the dilemmas posed by the various laws, regulations, and policies dealing with the information systems. Certain federal statutes prescribe legal penalties for unlawful accessing or disclosing information (e.g., Right to Financial Privacy Act), and require safeguarding of information (e.g., the Tax Reform Act of 1976 and the Computer Security Act of 1987). In addition, many states are expanding consumer privacy expectations and rights.

Second, IS managers should see themselves as the key actors in monitoring the changing environment, assessing organizational risk, coordinating with functional areas in hospitals, and disseminating appropriate information. All exchanges of information regarding HCIS must be performed through medical personnel. Security must become a line item in each hospital employee's job description, and performance reviews include the protection of patient information. Password protection on all terminals and controlled physical access to some computers deters most data thieves and vandals.

However, hospitals must not grow complacent in protecting their information assets. There is a lot more potential for invasion of privacy as the health care environment becomes more

computerized. Very few people could have imagined that HCIS could be connected directly to collect and aggregate information from several files to build a dossier on a person. The result is that privacy laws operate at the record level rather than the data element level. Moreover, a closely related concern is the lack of security of mainframe data once downloaded to a portable floppy disk.

Third, security and disaster recovery in the health care environment were usually ignored by most IS managers, who delegated responsibility to subordinates with authority or direction. But the risks now force HCIS executives to comprehensively address the issue. Security and disaster recovery must be addressed together. A security policy reflects the mechanism and approaches used to protect HCIS from harm, and disaster recovery policy reflects the methods used to restore service following a disruption in the health care process. These two policies should be part of a continuum so that increasing prevention decreases the time spent figuring out how to restore health care service.

DEVELOPMENT AND RESEARCH GUIDELINES

This section attempts to distill out this research some guidelines for future development efforts in HCIS security and control. Similar to the discussion in the preceding sections, these guidelines are based on the conceptual framework previously introduced.

1. Set policy globally and act locally. First of all, IS managers have a primary responsibility to communicate to top management the need for establishing clear corporate security policies not only for HCIS functions, but also for end users as well. Second, IS managers need to assess the organization's general security requirements. Appropriate security requirements must be researched and defined, a task for a senior manager who must answer: How important are the HCIS? How secure are the HCIS? How would customers and patients be affected?

   These anwers can be provided by the senior managers who actually set the strategic corporate direction. Once the risks and implications are identified, managers must then implement the controls consistently database by database, system by system. Access to HCIS must be granted following well-predefined procedures. These procedures must be established collectively by committees in which representatives of all professional groups of the health sector participate.

2. Integrate security and recovery functions in the health care environment. Because of tradeoffs among functions, each should be aware of the other's plans. Security might prepare for a particular threat, while recovery prepares for the same threat through disaster recovery.

3. Information security techniques used in HCIS must not affect the quality and efficiency of the health care services rendered. A major problem in implementing security policies is that they reduce systems' ease of use and friendliness. HCIS managers need to determine what level of security is appropriate for their environment. This process includes determining how valuable the health care data is, then implementing security in accordance with that

value. It seems clear that the manager must maintain a difficult balance between the HCIS security and performance.

4. Education and training are needed. One challenge for information security managers in the health care environment will be to maximize their information security awareness efforts. Training end users to be savvy about information security is one of the most important tasks an IS manager can perform. Information protection policies must be beyond the technological internal security controls of access, flow, inference, and cryptography (Denning & Denning, 1979) to policy and training that encourage trust and honesty in employees (Straub & Collins, 1990).

In summary, the framework has implications for research beyond the case of health care information systems. Specifically, we suggest that any information control and security policy founded on the system context approach will not be adequate unless organizational context is also considered. IS managers should see themselves as the key actors in monitoring the changing environment, assessing organizational risk, coordinating with functional areas in hospitals, and disseminating appropriate information.

Researchers need to consider contextual dimensions, including the organization of care and care delivery, and the setting in which care occurs, as well as ethical and legal policies that affect information systems practice. As more health care information is done outside the IS department, our whole outlook must change if we are to maintain effective security. This change will lead to more effective solutions in the areas of end-user authentications, policy planning, and organization-wide security efforts.

Effective HCIS planning, policies and controls are more than a matter of sound business practice. If violated, the organization may lose the trust of the patient, perhaps the most important factor in the treatment and retention of patients. No health care organization can sustain a quality and reputation with the loss of patient trust. As such, HCIS should be a crucial concern to everyone within a health care organization.

REFERENCES

Alter, S. (1992). *Information systems: A management perspective.* Reading, MA: Addison-Wesley.

Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States.* Ithaca, NY: Cornell University Press.

Benson, D. H. (1983). A field study of end user computing: Findings and issues. *MIS Quarterly, 7*(4), 35-45.

Boatright, J. R. (1993). *Ethics and the conduct of business.* Englewood Cliffs, NJ: Prentice Hall

Brown, G. (1990). *The information game: Ethical issues in a microchip world.* New Jersey: Humanities Press International.

Camillus, J. C. (1986). *Stratetic planning and management control.* Lexington, MA: Lexington Books.

Coleman, V. (1984). Why patients should keep their own records? *Journal of Medical Ethics, 10*, 27-28.

Date, C. J. (1986). *An introduction to database systems.* Reading, MA: Addison-Wesley.

Denning, D. E. & Denning, P. J. (1979). Data security, *Computing Surveys, 11*(3), 227-249.

Diebold, J. (1984). *Making the future work.* New York, NY: Simon and Schuster.

Freedman, R. (1982). The right of privacy in the age of computer data and processing, *Texas Tech Law Review, 13,* 1361-1363.

Gritzalis, D., Katsikas, S., Keklikoglou, J., & Tomaras, A. (1991). Data security in medical information systems: Technical aspects of a proposed legislation. *Medical Informatics, 16*(4), 371-383.

Harris, C. E. (1986). *Applying moral theories*. Belmont: Wadsworth.

Louis Harris & Associates, Inc. (1990). *The Equifax report on consumers in the information age*. Atlanta, GA: Equifax.

Hiller, M. & Beyda, V. (1981, Fall). Computers, medical records, and the right to privacy. *Journal of Health Politics, Policy and Law*, 463-487.

Lin, B. (1991). Health care information systems: A management perspective. In *Management Impacts of Information Technology*. Szewczak, E., Snodgrass, C., & Khosrowpour, M. (Eds.), 370-387, Pennsylvania: Idea.

Lin, B. (1993). Health care information systems management: Structure and infrastructure. *Journal of International Information Management, 2*(1), 27-39.

Longley, D. (1989). Data security. In *Information Security for Managers.* Caelli, W., Longley, D. & Shain, M. (Eds.), New York, NY: Stockton Press.

Mason, R. O. (1986). Four ethical issues of the information age. *MIS Quarterly, 10*(1), 4-12.

McLean, S. A. M. & Maher, G. (1985). *Medicine, morals and the law.* Aldershot: Gower.

Nash, J. (1992, January-February). Rx for hospital data is better infosecurity. *Infosecurity News*, 9.

Patrikas, E. O. & Liebler, J. G. (1987). Clinical information services. In *Health Care Administration: Principles and Practices.* Wolper, L. F. & Pena, J. J. (Eds.), Rockville, Maryland: Aspen.

Pettigrew, A. M. (1972). Implementation control as a power resource. *Sociology, 6*(2), 187-204.

Rob, P. & Coronel, C. (1993). *Database systems: Design, implementation, and management.* Belmont, CA: Wadsworth.

Saltzer, J. H. & Schroeder, M. D. (1975). The protection of information in computer systems. *Proceedings of IEEE, 63*(9), 1278-1308.

Sandhu, R. S. & Jajodia, S. (1993). Limitations of relational data base access controls. *Information Systems Security, 2*(1), 57-71.

Stone, E. F. & Stone, D. L. (1990). Privacy in organizations: Theoretical issues, research findings, and protection mechanism. In *Research in Personnel & Human Resource Management*. Rowland, K. M. & Ferris, G. R. (Eds.), 8, 349-411, Greenwich, CT: JAI Press.

Straub, D. W. (1987). Positioning computer security in the organization. Working Paper MISRC-WP-88-01, Carlson Graduate School of Management, University of Minnesota.

Straub, D. W. & Collins, R. W. (1990). Key information liability issues facing managers: Software piracy, proprietary databases, and individual rights to privacy. *MIS Quarterly, 14*(2), 143-156.

Straub, D. W. & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-60.

Wilkes, M. V. (1991). Revisiting computer security in the business world. *Communications of the ACM, 34*(8), 19-21.

Winston, M. (1991). AIDS, confidentiality, and the right to know. In *Biomedical Ethics*. Mappes, T. A. & Zembaty, J. S. (Eds.), New York: McGraw-Hill.

Winston, M. & Landesman, S. H. (1987, February 17). AIDS and a duty to protect. *Hastings Center Report*, 22-23.