;'

# Observed Practices for Improving the Security and Confidentiality of Electronic Health Information

## Interim Report

Committee on Maintaining Privacy and Security
in Health Care Applications of the National Information Infrastructure

Computer Science and Telecommunications Board

Commission on Physical Sciences, Mathematics, and Applications

National Research Council

National Academy Press

Washington, D.C., 1996

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This report has been reviewed by a group other than the authors according to procedures approved by a Report Review Committee consisting of members of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine.

The National Academy of Sciences is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce Alberts is president of the National Academy of Sciences.

The National Academy of Engineering was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulfis interim president of the National Academy of Engineering.

The Institute of Medicine was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Kenneth 1. Shine is president of the Institute of Medicine.

The National Research Council was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Bruce Alberts and Dr. William A. Wulfare chairman and interim vice chairman, respectively, ofthe National Research Council.

Support for this project was provided by the National Library of Medicine, the U.S. Department of Health and Human Services, the U.S. Department of Veterans Affairs, and the Massachusetts Health Data Consortium. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the sponsors.

Additional copies of this report are available from:

Computer Science and Telecommunications Board
National Research Council
2101 Constitution A venue, NW, HA 560
Washington, DC 20418
202/334-2605
202/334-2318

Copyright 1996 by the National Academy of Sciences. All rights reserved.

Printed in the United States of America

COMMITTEE ON MAINTAINING PRIVACY AND SECURITY IN
HEALTH CARE APPLICATIONS
OF THE NATIONAL INFORMATION INFRASTRUCTURE

PAUL D. CLAYTON, Columbia University, *Chair*
W. EARL BOEBERT, Sandia National Laboratories
GORDON H. DeFRIESE, University of North Carolina, Chapel Hill
SUSAN P. DOWELL, Medicus Systems Corporation
MARY L. FENNELL, Brown University
KA THLEEJI. A. FRAWLEY, American Health Information Management Association
JOHN GLASER, Partners Healthcare System
RICHARD A. KEMMERER, University of California, Santa Barbara
CARL E. LANDWEHR, U.S. Naval Research Laboratory
THOMAS C. RINDFLEISCH, Stanford University
SHEILA A. RYAN, University of Rochester
BRUCE J. SAMS, JR., Permanente Medical Group (retired)
PETER SZOLOVITS, Massachusetts Institute of Technology
ROBBIE G. TRUSSELL, Presbyterian Healthcare System
ELIZABETH WARD, Washington State Department of Health

*Special Advimr*

PAUL M. SCHWARTZ, University of Arkansas

*Staff*

JERRY R. SHEEHAN, Program Officer
HERBERT S. LIN, Senior Staff Officer
LESLIE M. WADE, Research Assistant

COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

DAVID D. CLARK, Massachusetts Institute of Technology, *Chair*
FRANCES E. ALLEN, IBM TJ. Watson Research Center
JEFF DOZIER, University of California at Santa Barbara
SUSAN L. GRAHAM, University of California at Berkeley
JAMES GRAY, Microsoft Corporation
BARBARA J. GROSZ, Harvard University
PAT HANRAHAN, Stanford University
JUDITH HEMPEL, Molecular Simulations Inc.
DEBORAH A. JOSEPH, University of Wisconsin
BUTLER W. LAMPSON, Microsoft Corporation
EDWARD D. LAZOWSKA, University of Washington
BARBARA H. LISKOV, Massachusetts Institute of Technology
JOHN MAJOR, Motorola
ROBERT L. MARTIN, AT&T Network Systems
DAVID G. MESSERSCHMITT, University of California at Berkeley
CHARLES L. SEITZ, Myricom Inc.
DONALD SIMBORG, KnowMed Systems Inc.
LESLIE L. V ADASZ, Intel Corporation

MARJORY S. BLUMENTHAL, Director
HERBERT S. LIN, Senior Staff Officer
PAUL D. SEMENZA, Staff Officer
JERRY R. SHEEHAN, Staff Officer
JEAN E. SMITH, Program Associate
JOHN M. GODFREY, Research Associate
LESLIE M. WADE, Research Assistant
GLORIA P. BEMAH, Administrative Assistant
GAIL E. PRITCHARD, Project Assistant

COMMISSION ON PHYSICAL SCIENCES,
MATHEMATICS, AND APPLICATIONS

ROBERT J. HERMANN, United Technologies Corporation, *Co-chair*
W. CARL LINEBERGER, University of Colorado, *Co-chair*
PETER M. BANKS, Environmental Research Institute of Michigan
LA WRENCE D. BROWN, University of Pennsylvania
RONALD G. DOUGLAS, Texas A&M University
JOHN E. ESTES, University of California, Santa Barbara
LOUIS HEGEDUS, Elf Atochem North America Inc.
JOHN E. HOPCROFT, Cornell University
RHONDA J. HUGHES, Bryn Mawr College
SHIRLEY A. JACKSON, U.S. Nuclear Regulatory Commission
KENNETH H. KELLER, Council on Foreign Relations
KENNETH L KELLERMANN, National Radio Astronomy Observatory
KEN KENNEDY, Rice University
MARGARET G. KIVELSON, University of California, Los Angeles
DANIEL KIJEPPNER, Massachusetts Institute of Technology JOHN
KREJCK, Sanders, a Lockheed Martin Company
MARSHA I. LESTER, University of Pennsylvania
THOMAS A. PRINCE, California Institute of Technology
NICHOLAS P. SAMIOS, Brookhaven National Laboratory
L.E. SCRIVEN, University of Minnesota
SHMUEL WINOGRAD, IBM TJ. Watson Research Center
CHARLES A. ZRAKET, MITRE Corporation (retired)

NORMAN METZGER, Executive Director

# Contents

INTRODUCTION
Site Visits: Basis for Information on Observed Practices, 1 Observed Practices for Improving the Security and Confidentiality of Electronic Health Information, 2
The Final Report, 2
Organization of This Interim Report, 3

TECHNICAL APPROACHES TO IMPROVING THE SECURITY AND CONFIDENTIALITY OF ELECTRONIC HEALTH INFORMATION 3
Physical Security, 3
Authentication, 4
Access Control, 4
Audit Trails,S
Control of External Communication Links and Access,S
Cryptography, 6
Software: Discipline, 6
Data Int(:grity, 6
System Backup and Recovery, 7
System Assessment and Technological Awareness, 7

INSTITUTIONAL APPROACHES TO IMPROVING THE SECURITY AND CONFIDENTIALITY OF ELECTRONIC HEAL TH INFORMATION 7
Communiication with Patients, 8
Internal Policy Statements, 8
Formal Structures for Implementation of Policies, 9
Employe(: Training, 10
Sanctions, 11

NOTES 11

# INTRODUCTION

At the request of the National Library of Medicine (NLM), the National Research Council's (NRC's) Computer Science and Telecommunications Board (CSTB) organized a diverse study committee to assess technical and institutional mechanisms for protecting electronic health information.! The request stemmed from NLM's recognition that (1) growing use of information technology in the health care industry has raised concerns about the confidentiality of health information stored, processed, and transmitted in electronic form[2] and (2) little information exists about practices used by the health care industry to improve security and confidentiality. This interim report of the Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure briefly describes current technical and institutional practices, observed during site visits by committee members, that site managers believe reduce the risk of unauthorized or inappropriate disclosure of electronic he:alth information. Whether any particular practice is essential or adequate for achieving an acceptable kvel of protection at a particular institution depends on many factors beyond the scope of this interim repoJ1. Here, the committee makes no attempt to evaluate, rank, or recommend these practices, nor does it discuss the relative costs of implementing the practices. These tasks are left to the final report. The purpose of this interim report is to inform managers and information systems professionals about mechanisms that individual organizations have implemented in an attempt to better protect electronic health information.[3] Although none of the sites visited makes use of every practice noted in this report, each of the described practices was observed in at least one site.

## Site Visits: Basis for Information on Observed Practices

To gather information regarding existing practices for improving the security and confidentiality of electronic health information, subgroups of the study committee traveled to six sites representing a wide range of health care organizations, including two integrated health care delivery systems;4 a large, urban hospital; a community health information network;5 a state health care system; and a large insurer. To encourage personnel at the various sites to share their experiences candidly, the committee decided to keep the sites' identities confidential in its interim and final reports. Sites were selected on the basis of their reputed leadership in the development of electronic health records, networked clinical systems, and security and t;onfidentiality policies. They varied considerably in the degree to which they had deployed information technology. Although no site had a fully integrated electronic medical record operational at the time of the committee's visit, all were actively developing one.[6] Most sites had some clinical information on-line.? Several sites had linked administrative, billing, and referral information among their various facilities through wide area networks or corporate "intranets." Some had implemented Internet connections for electronic mail applications.

Prior to each visit, the site visit team collected information from the site regarding its organizationall structure, information systems, security mechanisms, confidentiality policies, computer and data security policies, procedures for releasing health records, employee training and orientation programs, and disciplinary policies. During each one-and-a-half day site visit, committee members met with corporate executives; staff from the information systems, medical records, human resources, and legal departments; and doctors, nurses, and other system users. Where possible, they met with members of medical rel;ords committees and members of information security and confidentiality committees.

To supplement information gathered during the site visits, the committee also reviewed relevant policy and tedmical documents from a wide variety of public institutions, trade and advocacy groups, and industry representatives.[8] During four full committee meetings held between November 1995 and July 1996, th(: committee met with additional health care providers, insurers, pharmaceutical benefits

managers, vendors of health information systems, experts in computer security (from the health care, as well as banking and defense communities), privacy advocates, consumer advocates, federal agencies interested i11l health information systems, relevant industry associations, and other organizations that maintain health-related databases. Additional meetings were held with members of the Affiliated Health Information Networks of New England and representatives of European data commissions to understand the problems they face and the solutions they are implementing.

## Observed Practices for Improving the Security and Confidentiality of Electronic Health Information

The practices observed by committee members reflect attempts to improve the security and confidentiality of electronic health information within individual health care institutions. Health care practitioners, tend to define confidentiality as a state of controlled and deliberate information sharing that balances a patient's desire to limit disclosure of information with the practitioner's and payer's needs to access infonnation to deliver effective health care, facilitate payment, and prevent fraud. These practitioners typically view security as a set of technical measures for implementing confidentiality and for protecting data from intentional or unintentional deletion or alteration. The computer security community has a broader definition of security that includes availability in addition to confidentiality and data inte:grity. Availability entails assurances that computing and communications resources are accessible when needed. Because system availability is critical to successful application of information technology to health care, this report adopts the broader definition of security and describes practices for providing confidentiality, integrity, and availability.

The practices described in this interim report attempt to counter two classes of potential threats: an internal threat and an external threat.[9] The internal threat consists of authorized users who abuse their privileges by accessing information for inappropriate reasons or uses, whether to view records of friends, neighbors, or coworkers or to leak information to the press. The external threat consists of outsiders who are not authorized to use a system or to access its data, but nevertheless attempt to access or manipulate data or rendt:r the system dysfunctional.[lO] Health care organizations have considerable experience in addressing the internal threat based on their years of experience with paper records. They have less experience in protecting data from technical attacks by outsiders; currently, few health care installations are connected to publicly accessible networks.

The practices outlined in this interim report do not address *systemic* threats to the confidentiality of electronic health information that derive from the current and emerging structure of the health care industry. Patient information is increasingly valuable to a number of organizations not directly involved in the provision of patient care but concerned instead with containing costs and improving the quality of health care. These include such organizations as marketing firms, benefits managers, business units of managed care organizations, and self-insured employers. Current controls over these secondary uses of health infornlation are disjointed and are motivated more by business interests than by concerns about patient confidentiality. This threat is not addressed by the practices outlined in this interim report, but may be more amenable to public policy or industry initiatives. ıı This threat and possible solutions will be discussed at length in the final report.

## The Final Report

The committee expects to complete its final report in early 1997. It will expand on this interim report by evaluating technical and organizational practices currently used in health care organizations, by identifying practices from other industries that may be applicable to health care institutions, and by providing practical guidance to organizations seeking to better protect electronic health information. It

will discuss the systemic threat arising from changes in the health care industry and the growing use of health infonnation, suggest public policy solutions, and identify future research needs. The final report also will include the committee's conclusions and recommendations on ways of providing better protection for vulnerable electronic health information.

### Organization of This Interim Report

The remaining two sections of this interim report briefly describe observed practices for reducing risks to electronic health infonnation. These practices were used to varying extents at the six health care sites visited by committee members. Descriptions of technical practices appear first, followed by descriptions of practices related to institutional management and structure.

## TECHNICAL APPROACHES TO IMPROVING THE SECURITY AND CONFIDENTIALITY OF ELECTRONIC HEALTH INFORMATION

Technological security tools are essential components of modern distributed health care infonnation systems. At the highest level, they help ensure the availability of infonnation, the accountability of health care providers for its use, the definition of a boundary or security perimeter within which users can be trusted with access, and the granting of privileged access only within the scope of a user's job function. Technological security tools are useful for preserving infonnation confidentiality *within* provider institutions, but they do not address the problems of unrestricted use of infonnation (e.g., for data mining) after it has passed, with consent, *outside* the provider institution to secondary payers or to other stakeholders in the health infonnation service industry.

Security professionals assess technologies jointly in terms of their functional benefits and their costs: the cost of purchase and integration into the information system environment; the cost of ongoing management, operations, and maintenance; the cost of reduced ease of use; and the cost of user time spent navigating security mechanisms. Individual technologies vary widely in tenns of these characteristics, and system managers choose a set of technological interventions that provide effective protection against perceived threats to system security and impose acceptable costs. This choice requires ongoing evaluation and updating of threat models; ongoing technology assessments; integration and operation strategies; as well as education of managers, systems staff, and users.

This section describes technical practices for improving the security and confidentiality of electronic health infonnation that were observed by committee members during their site visits. Included are practices related to the following areas: physical security, authentication, access control, audit trails, control of external communication links and access, cryptography, software discipline, data integrity, system backup and recovery, and system assessment and technological awareness. The final report will evaluate a range of possible security tools that is far broader than those described below.

### Physical Security

Ensuring physical security entails having accurate knowledge of the inventory and configuration of communications and computing equipment within an organization and deploying appropriate controls to prevent an unauthorized person from tampering with or accessing information from this equipment. Committee members observed several practices-followed to varying extents at the six sites visited-for addressing physical security.

• *Computer terminal security.* Computer terminals are arranged in such a manner that unauthorized persons cannot observe confidential information on the computer screen by looking over an authorized user's shoulder. Workstations are programmed to clear the screen or log off automatically after a period of inactivity. Terminals that are used only intermittently (such as those located in an examination room or an interview room off a main lobby) are secured behind locked doors.

• *Knowledge of security perimeter/network layout.* Employees know and control the configuration, composition, and layout of network communication facilities within the enterprise. In particular, they understand what areas the network does and does not cover. They have detailed knowledge of and the ability to control effectively the kinds of lines involved in the physical network implementation (e.g., coaxial cable, fiber, twisted pair, wireless links) and their routings and interconnections (e.g., hubs, bridges, routers, gateways, point-to-point telephone links). They also understand the points of external access to the network, the ability of users to attach modems or other links to their computers, and the accessibility of the networking links intruders use to make unauthorized connections.

• *Network physical security.* Network links for local and wide area networks are physically secure. For example, cable junctions are not physically accessible without a special key to open a service closet.

• *Server physical security.* Information systems personnel take precautions to ensure that machines that provide centrally controlled services are well identified and are located in secure settings.

## Authentication

Authentication is any process of verifying the identity of an entity that is requesting or responding to a request for information in a computing environment. It is the linchpin for making decisions about appropriate granting of access to health information. Several alternative approaches implemented to varying extents were observed at the different sites.

• *Token-based authentication.* Employees use some sort of physical object or token (like a "smart" card or a magnetic swipe card) with a personal identification number (PIN) or password to validate their identity. Because an item of hardware cannot be easily duplicated, it is more difficult to share among individuals.

• *Log-on identification code and password* Employees type in an alphanumeric identification (ID) code and a unique, secret password to validate their identity.

• *Changes of passwords.* Computing environments require that users change their passwords or PINs on a regular basis so that these codes are harder to guess or steal.

• *Password discipline.* Employees are actively encouraged to protect their passwords. For example, management discourages employees from sharing passwords by holding them responsible for actions taken under their passwords, whether or not they did in fact undertake those actions.

• *Uniform user identification across enterprise ("single log-on").* Common identification and authentication techniques are used among all systems within an organization so that users do not waste time and become frustrated typing in their PINs several times for different information systems or face the requirement to remember multiple PINs.

## Access Control

Access controls restrict users' ability to retrieve and view or update information based on their identity and/or function in an organization. Access controls define and validate the scope of information access for a given individual, and may limit access to a certain set of patients, a given service, a given

physical domain, certain classes of information, and so on. Several types of practices were observed for controlling access at different sites.

• *Individual and group access controls.* Individuals or groups are granted or denied access to a particular application or data field within the records of a database based on their identities and the particular access rights they have been given (e.g., read, write, modify, delete, and so on).

• *Role-based access profiles.* User access is based on job descriptions. Specific roles are defined within the organization (e.g., primary care physician, attending physician, resident, nurse, clerk, and so on), associating each with a set of access privileges, and then assigning one or more roles to every worker within the enterprise.

• *Location-based access controL* Users are granted or denied access based on the location of a terminal; for example, terminals located in the accounting department are programmed to reject all requests for clinical data other than those required for billing.

## Audit Trails

Audit trails result from the practice of recording details about the accessing of information, including the identity of the requester, the date and time of the request, the source and destination of the request, and a descriptor of the information retrieved. Such records serve as a deterrent to potential abuse since audit logs can be reviewed to learn the particulars of inappropriate access. Committee members observed several practices-followed to varying extents at the six sites visited-for using audit trails.

• *Access logs.* Information systems personnel maintain audit trails of all instances of access (read, as well as write) to computerized records.

• *Employee self-audits.* Employees, such as hospital workers, who receive medical care from their employer can independently review instances of access to their own records and assess or question the appropriateness of such activity.

• *Patient-initiated audit reviews.* Organizations review audit logs in response to requests from individual patients.

• *Reminders of audit trails.* The network is configured to remind users that attempts to access particularly sensitive data or data associated with specific high-profile patients are recorded in an audit log.

## Control of External Communication Links and Access

Control of external communication links and access entails an accurate knowledge of the logical and physical configuration of communications services in an organization and the use of appropriate technological controls to prevent an unauthorized person from sending or receiving information over these links. During their site visits committee members observed several mechanisms for implementing such control. These mechanisms were implemented to varying degrees at the different sites.

• *Firewalls.* Firewalls are used to control communication to hosts on a protected network from a host on another external network. Firewalls include a set of policies, network configuration, routing hardware, and software that limit the services accessible to authenticated users outside an enterprise's network based on their authenticated identity.

• *Dial-in protection.* Users connecting from telephone dial-in lines are properly identified and authenticated for access to enterprise communications services. For example, remote users use a hardware token, type in additional passwords, or use "dial-back" modems to help ensure that the

enterprise's network can be used remotely only from selected telephone numbers (however, such a measure limits the mobility of users).

• *Control of IP addresses.* Network Internet Protocol (IP) addresses are assigned only to authorized machines. Export ofthese addresses through the Domain Name System is controlled (by firewall) to limit the knowledge an intruder can gain regarding intranetwork details.[12]

## Cryptography

Cryptography can support authentication and access control functions, protect (through encryption) stored information or on-line communications against eavesdropping, validate information content against unauthorized and undetected modification (integrity checking), validate the origin and content of transactions (like digital signatures on physician orders), and document the fact that such transactions took place (nonrepudiation). The committee observed the use of cryptography only in very limited settings, for protecting passwords during a few authentication procedures and for protecting specialized network links against eavesdropping.

## Software Discipline

Software discipline is the attempt to control the dissemination, updating, and integrity of all software running on an enterprise's computers, including communications software, operating systems, database systems, user interface tools, and the full range of applications programs. Organizations visited by committee members used a variety of different practices for maintaining software discipline.

• *Use of antivirus technology.* Antivirus software is installed on servers or workstations to ensure that software imported from removable media or via network communications does not contain viruses, worms, or Trojan horses.[13] In addition, procedures and technology are in place to detect and remove such software defects if they are accidentally introduced into the enterprise's systems.

• *Control of user-installed software.* Procedural and technological mechanisms limit the ability of employees to install on user workstations, servers, or other machines software that is untested and incompatible with the enterprise's standards. For example, floppy or CD-ROM drives are disabled on user workstations to discourage users from loading unauthorized software or data.

• *Control over writable media.* Devices for writing or copying information are disabled on selected workstations. One method involves clipping the write heads of a floppy disk drive.

• *Network software census.* Programs stored and executable on the enterprise's computers are periodically catalogued, and administrators are alerted to the existence of unauthorized software.

## Data Integrity

The practices outlined above indirectly promote data integrity by limiting the ability of internal and external threats to access health information systems and the data contained in them. Committee members in their site visits observed additional mechanisms that attempt to ensure that data are entered into the record and altered only in a controlled manner.

• *Minimizing delay before signing orders.* Physicians are required to sign orders shortly after a record is created or data are entered. The permissible time delay balances the time physicians need for record keeping against the desire to enter data before it becomes stale.

• *Data tagging.* Users are required to type in their authentication code after entering, changing, or deleting data in a file. The system either tags each data element with the ID of the user who last modified it, or creates a new record keyed to the user ID.

### System Backup and Recovery

Policies, procedures, and technologies for system backup and recovery from disaster ensure that an organization can restore critical services and maintain system availability in the event of environmental or equipment damage or catastrophic failures. Committee members observed two types of practices for providing some degree of backup and recovery capability at sites visited.

• *Backups and the use of multiple storage sites.* Operational databases, information resources, and software are regularly copied. Copies are stored at appropriate, secure remote locations.

• *Operations recovery.* Policies, procedures, and technologies are in place for reinstating operations in the event of catastrophic system or environmental failures and are tested regularly to ensure that the policies and procedures are appropriate and that the technology works correctly. Operations recovery relies on system redundancy, temporary "outsourcing" of computation services, or provision of alternate sources of public utility services such as electric power.

### System Assessment and Technological Awareness

Maintaining information security in an enterprise requires policies, procedures, and technologies that help prospectively to identify system vulnerabilities to attack or failure and to correct defects when they are discovered. Organizations visited by committee members used a range of practices in an attempt to assess vulnerabilities and maintain awareness.

• *Use of intruders , tools.* Site personnel make use of the same software tools that intruders use (such tools are available from network sources) to scan for vulnerabilities in system software, guess passwords, and so on.

• *Vulnerability assessment.* Organizations conduct formal assessments of vulnerability to determine the adequacy of policy, procedural, and technical measures used to protect their systems.

• *Use of CERT alerts.* Employees take advantage of Internet community resources providing information on detected vulnerabilities, fixes, and alerts, such as those of the CERT Coordination Center.[14]

• *Avoidance of obsolete technologies.* Organizations upgrade communications, computing, and software technologies to avoid obsolete technology. Unneeded system services are deactivated so as not to expose obsolete software and interfaces to attack.

## INSTITUTIONAL APPROACHES TO IMPROVING THE SECURITY AND CONFIDENTIALITY OF ELECTRONIC HEALTH INFORMATION

Protection of electronic health information depends strongly on appropriate institutional policy and broad compliance with policy. While technical measures limit the types of data to which authorized users have access, they cannot prevent authorized users from snooping into the records of patients to which they have access, but which they have no medical need to review. Policies establish guidelines for proper behavior, outline appropriate uses and releases of information, create mechanisms for preventing and detecting violations of policy, and set rules for disciplining offenders. The goal of such policies is to

help all employees understand the need to protect health information and to follow requisite practices. IS Health care organizations attempt to develop policies that strike a proper balance between the patient's right to confidentiality and the provider's need to have access to relevant health information. Failure to achieve the correct balance can undermine the provision of health care by causing patients to lose confidence in the ability of an institution to protect their sensitive data or by preventing providers from gaining access to the information they need to treat a patient. Institutional practices are generally most effective in protecting against threats posed by insiders, but they can provide guidance for establishing mechanisms to protect against external threats, too.

The observed institutional practices outlined below fall into several categories: improved communication with patients, development of internal policy statements, establishment of formal structures for implementation of policies, employee training, and delineation and application of appropriate sanctions. Where possible, the committee has cast the practices in terms of concrete, tangible assets-such as the existence of a policy document or a training manual-that can indicate whether or not the practice is implemented. The final report will contain more examples and evaluation of these practices.

## Communication with Patients

Concern about protecting the confidentiality of health information points to the need for clear communication between providers and patients regarding the collection, use, and dissemination of such information. Although it is beyond the scope of this interim report to address the larger issue of patients' control over their health information, committee members observed during their site visits a number of practices that were used to varying extents to make individuals more aware of their rights regarding their health records, the consent they give for using and disseminating health records, and the existence of electronic medical records.[16]

• *Patient bill of rights.* A patient bill of rights outlines clearly the relationship between patient and provider, states the patient's rights to confidentiality, and outlines state and federal laws, regulations, and standards guaranteeing those rights. Additionally, names and telephone numbers of people to contact are included for patients who believe their rights have been violated. Employees coordinate patient bills of rights with forms authorizing disclosure of individually identifiable health information to ensure compatibility between the two sets of documents.

• *Patient access.* Patients are allowed to review the contents of their health record and submit amendments that correct information the patient believes is inaccurate.

• *Disclosure authorization forms.* Specific, separate forms are used to obtain permission from the patient to disclose individually identifiable health information. Authorization forms are made clearer, more accessible, and more comprehensible by removing detailed legal terminology and translating forms into foreign languages most often used by the site's patients. Authorization forms are prepared separately from other documents patients sign to authorize treatment, thereby making patients more aware of the separate authorizations they are granting.

• *Notification of the existence of an electronic health record.* Patients are informed of the existence of electronic health records and told of the health benefits of storing and processing information in an electronic form.

## Internal Policy Statements

Policy statements codify an organization's values, positions, expectations, and procedures concerning security and confidentiality. They address both paper and electronic records as long as the

two media are in use. Formal documentation of such policies in short pamphlets allows information to be distributed to employees, supervisors, physicians, and administrators to inform them of their responsibilities for protecting information. Supplemental information can be provided on-line or upon request. Such documentation can cover a wide range of topics. Committee members observed the use of policies to address several different types of concerns at different sites.

• *Physical access controls.* Such policies establish requirements for limiting physical access to data processing areas, equipment, and media, and for controlling access during the transportation of data processing media and other computing resources. Levels of control are related to the presumed levels of risk and level of exposure to loss within a particular organization or department.

• *Logical access controls.* Policies to control logical access limit user access to information contained in electronic form. Controls are often based on job descriptions or on individual user needs, as outlined in the section above titled "Access Control."

• *Data integrity.* Data integrity policies are intended to ensure the correctness of information contained in health records. Such policies typically require that data remain consistent with its source and that errors, duplications, omissions, and intentional alterations be identified and investigated.

• *Preventive measures, backup, and recovery procedures.* Policies to ensure ongoing operation outline procedures for disaster prevention, backup of computer facilities, and recovery procedures for the network, computer equipment, programs, data, and utility services. Such policies are intended to help ensure that an institution can continue to function in the event of an emergency or that it can limit its downtime. Managers require a schedule of regular testing to ensure the suitability of the policies.

• *Research uses of health records.* Policies regarding research uses of health information contain provisions for reviewing the intended use of health information by internal and external researchers and for establishing suitable procedures for "sanitizing" or removing identifying information from the records. Separate policies are prepared to govern releases of identifiable health data and aggregate (unidentified) health data. Site management uses such policies to encourage greater use of health information without identifying information.

• *Other (nonresearclt) approved releases of health information.* Such policies specify the types of recipients to whom an institution will release identifiable health information, the types of information that will be released to different recipients, the circumstances under which information will be released, personnel authorized to release information, and the specific procedures that are to be followed in making a release. The policies also delineate the boundaries of the organization to more clearly distinguish between internal transfers of information and external releases.

• *Periodic reminders.* Ubiquitous notices, memos, newsletter items, and updates are posted to remind users of health information of their responsibilities to protect patient information and to help instill an ethos of maintaining confidentiality throughout the institution. These notices are posted in elevators, public areas, and newsletters to remind employees not to discuss patient information openly.

## Formal Structures for Implementation of Policies

Organizations visited by committee members had established a variety of formal structures to develop, implement, and enforce policies. These structures took the form of policy-development committees, departments of information security or risk assessment, formally designated information security officers, and institutional review boards (IRBs) for reviewing external requests for researchrelated information. Each organization had established some combination of these structures.

• *Security and confidentiality committees.* Security and confidentiality committees are charged with systematically and proactively developing and maintaining security and confidentiality policies for paper and electronic health information. Though separate policies may be required for paper and electronic records, centralization can help to ensure consistency between the policies and allows greater

cross- fertilization of ideas for policy implementation.[17] These committees draw membership from departments with a strong stake in patient confidentiality and system security, such as the information systems, admitting, human resources, medical records, patient relations, risk management, nursing, physicians, and legal departments. They remain aware of a wide variety of programs or projects that might affect patient confidentiality or system security and can take necessary actions to ensure that security and confidentiality are upheld .

• *Department of security or risk assessment.* Departments of information security or of risk assessment conduct analyses of the threats to and vulnerabilities of electronic health information and make recommendations to the information security officer. They also conduct audits of access logs and develop practices for implementing policy .

. • *Information security officer.* Information security officers hold ultimate responsibility for developing, implementing, and maintaining a data security program and enforcing practices that fulfill . the policies established at the institutionalleveI. They often work in conjunction with upper management (such as a chief executive officer or chief information officer) and system users to establish practices that are both effective and unobtrusive.

• *Designated custodians.* Designated custodians throughout an organization are given responsibility for protecting particular databases or for granting access privileges to system users. Employees who want to access particular databases or applications need to request access privileges from the relevant authority and demonstrate their need to know.

• *Institutional review boards.* Institutional review boards (IRBs) are composed of members from various departments within an organization. IRB members review and approve researchers' requests for information. They establish restrictions on the types of data individual researchers can access, ensure adequate protection of health information, and require suitable procedures for protection of researchers' data files.

## Employee Training

By helping employees understand and implement an institution's policies for protecting information, education and training programs support institutional data security and confidentiality initiatives and deter inappropriate behavior. Members ofthe committee observed practices for education and training that included the development of regular training schedules and curricula, retraining, and the use of employee confidentiality agreements. These practices were used to varying degrees at the six sites visited.

• *Regular training schedules and curriculum.* Regularly scheduled training classes help ensure that employees understand an organization's security and confidentiality policies. IS Courses are offered at both the institutional level and the department level so that they focus on the institution's general policies as well as on the particular responsibilities or concerns of an employee's department. On-line training incorporating interactive instruction and feedback is offered at sites to supplement book training and provide more hands-on experience. Training programs are directed at all employees and medical staff, including temporary and transferring personnel, contractors, vendors, students, admitting and referring physicians, and volunteers.[19]

• *Retraining at all levels.* Employees are retrained on a regular basis to help reinforce security and confidentiality policies and educate employees about modifications to policy. Some workers (e.g., physicians) require special training mechanisms because their schedules do not easily allow regular, formal training courses. Employees are required to view an organization's video presentation on confidentiality each year, and their participation is noted on the checklist portion of performance review forms.

• *Confidentiality agreements.* All new employees with access to patient information sign confidentiality agreements stating their understanding of and agreement to abide by the organization's

security and confidentiality policies?O These agreements typically provide an explanation of users' individual responsibilities for ensuring patient confidentiality and require a user's signature as proof of understanding. Such agreements are typically signed at the time a user receives access privileges and annually thereafter.

## Sanctions

Disciplinary actions or sanctions complement policies and procedures for maintaining security and confidentiality by establishing penalties for violating them. Without sanctions, the validity of the structure to protect security and confidentiality is nullified. If sanctions are applied irregularly, with great delay, or with little effect on violators, the structure is severely undermined and its legitimacy may become suspect. Several practices aimed at ensuring the effectiveness of policies and procedures were observed by committee members during their site visits. These practices were used to varying extents at each of the sites.

• *Clear and well-publicized standards for disciplinary actions.* Descriptions of sanctions are included in policy manuals outlining security and confidentiality policies. Sanctions range from mild to severe, depending on the seriousness of the transgression. Different sanctions are defined for willful violations of policy and for violations that result from carelessness or unintentional actions (such as leaving a computer terminal logged on). An oral or written warning is provided to employees for a first or minor offense; second or greater offenses result in suspension. Employees who commit major or repeated violations are immediately dismissed.

• *Policy of zero tolerance.* "Zero-tolerance" policies imply that all breaches will be punished, no matter by whom or for what reason the breach occurred.

• *Uniform application of disciplinary actions.* Policies are applied in a consistent and evenhanded manner. If evidence shows that a breach has occurred, punishment follows quickly and in accordance with signed agreements and/or other training statements. Penalties are applied to employees and members of the medical staff equally. The committee observed that if administrative workers and nurses are sanctioned more severely than doctors, friction among staff undermines security and confidentiality policies.

• *Publicize incidents/sanctions.* Management's responses to violations of confidentiality policies are publicized ("public hal1gings") to provide a strong example of management's willingness to enforce policy and as a strong deterrent to other employees. Carefully worded memos distributed to all employees outline the infraction, and the punishment serves to remind employees of stated policies. Organizations using such a practice attempt to publicize cases of wrongdoing without creating an atmosphere of mutual suspicion between workers and supervisors and do not violate employees' rights to confidentiality .

## NOTES

1 The complete charge of the committee is to observe and assess mechanisms (both technical and nontechnical) for protecting privacy and maintaining security, and to identify other methods of assuring data privacy and security that are suitable for research, development, and testing in the health care environment.

2 For a discussion of these concems, see Institute of Medicine. 1991. *The Computer-based Patient Record: An Essential Technology for Health Care,* Richard S. Dick and Elaine B. Steen (eds.), National Academy Press, Washington, D.C.; Institute of Medicine. 1994. *Health Data in the Information Age: Use, Disclosure, and*

*Privacy*, Molla S. Donaldson and Kathleen N. Lohr (eds.), National Academy Press, Washington, D.C. See also Don E. Detmer and Elaine B. Steen. 1996. "Shoring Up Protection of Personal Health Data," *Issues in Science and Technology*, Summer, pp. 73-78.

3 Additional reference material regarding some of these practices is identified in National Library of Medicine. 1996. "Confidentiality of Electronic Health Data: Methods for Protecting Personally Identifiable Information. January 1990 through March 1996: 448 Selected Citations," U.S. Government Printing Office, Washington, D.C. This document also may be viewed on-line at gopher.nlm.nih.gov.

4 Integrated health care delivery systems (IDSs) are emerging as the predominant organizational model in today's health care environment. According to *U.S. Hospitals and the Future of Health Care* (Deloitte and Touche LLP, Philadelphia, 1996),71 percent of U.S. hospitals either belong to an IDS or are participating in the development of one. An IDS usually includes some combination of hospitals, clinics, physician offices, nursing homes, pharmacies, and laboratories. It also may include other organizations offering such services as dental care, health care supplies, transcription, ambulance transportation, and home health care. An IDS may be structured as a tightly managed organization in which information systems infrastructure and policies are centrally controlled or it may be affiliated by contractual agreements among separately owned and managed organizations.

5 Community health information networks (CHINs) are entities set up to share information across corporate boundaries, among competitors, affiliates, researchers, government organizations, and other entities with an interest in health care information.

6 For a description of electronic medical records and their applications, see Institute of Medicine, *The Computer-based Patient Record, 1991*.

7 Clinical information typically includes diagnoses, laboratory results, discharge summaries, radiology findings, drug lists, and other test results. On-line physician order entry and decision-support tools were also observed. Decision support tools provide physicians with treatment options based on a diagnosis code entered elsewhere in the record.

5 These documents included Massachusetts Health Data Consortium, Waltham, Mass., *Confidentiality of Health Data-An Exploration of Principles, Policies, and Practices*, draft dated March 28, 1996.

9 As used in this report, a "threat" is an agent that seeks to exploit vulnerabilities in an information system and do harm. A "vulnerability" is defined as a flaw or side effect of a system and its associated procedures that enables someone to violate policy or otherwise initiate an adverse outcome.

10 The motivations of external intruders are unclear but may range from monetary gain (as in the case of selling information about a celebrity to a newspaper), malice (to embarrass a public official), or mischief (to see if it can be done).

11 The Privacy Act of 1974 is one attempt by the federal government to provide confidentiality for individuals, but it applies only to federal organizations. Several other (and more broadly applicable) legislative initiatives are under consideration currently to address these concerns. S.1360 ("Medical Records Confidentiality Act of 1995"), HR.435 ("Fair Health Information Practices Act of 1995"), and HR.3482 ("Medical Privacy in the Age of New Technologies Act of 1996") have all been proposed. The Health Insurance Portability and Accountability Act of 1996 (formerly HR.31 03), introduced by Senators Kennedy and Kassebaum, recently was signed into law by President Clinton.

12 The Domain Name System (DNS) is a decentralized system for cataloging host names and Internet addresses (and other host-related information). Under DNS, local organizations responsible for the operation of groups of hosts on the Internet create sections of the distributed DNS database relating to their own machines and make this information available to other hosts on the Internet so they can look up addresses and connect to services those organization provide.

13 A Trojan horse is a computer program that appears to provide normal functionality, but whose execution results in undesirable effects, generally unanticipated by the user.

14 The CERT Coordination Center is the organization that grew from the computer emergency response team formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988. Its charter is to work with the Internet community to facilitate incident prevention, incident response, and communication during system emergencies. It attempts to raise the Internet user community's awareness of computer security issues and

conducts research targeted at improving the security of existing systems. CERT is a service mark of Carnegie Mellon University. (Information on CERT is available on-line at www.cert.org.)

[15] "Employees" is used broadly here to include actual employees as well as medical staff, contractors, students, volunteers, and vendors who may have legitimate needs to access information but who may not be paid directly by the health care organization owning or providing the information system.

[16] In the short term, making patients more aware of data issues and their rights through use of these (and other) practices may create liabilities for an institution: better informed patients are more likely to hold institutions responsible for data protection. In the long term, however, institutions using these practices are likely to evolve cultures that value the protection of data and to avoid potential liabilities. By enhancing patient trust in the provider organization, such practices may lead to more open and candid interactions between patients and providers, increasing the likelihood that relevant data will be available for patient care.

[17] At present, the electronic medical record is an attempt to transfer paper records into an electronic form. Over time, the electronic medical record will incorporate content such as pictures, images, and sound that cannot be stored in paper form. Modem telecommunications may also provide the opportunity to capture, in digital form, content not previously considered part of the patient record, such as teleconferences and on-line consultations. Such changes will likely raise new questions regarding confidentiality that have few parallels in the paper record.

[18] The Computer-based Patient Record Institute (CPR!) has developed guidelines for information security education programs. See Computer-based Patient Record Institute. 1995. "Guidelines for Information Security Education Programs," CPR!, Schaumburg, III., June.

[19] Recognizing that various user groups may have significantly different access to electronic health records, some institutions revise the content of training classes to better address user needs. For example, a class for new nurses may be more comprehensive and detailed than a class introducing volunteers to the admitting department.

[20] The Computer-based Patient Record Institute (CPR!) has developed guidelines for confidentiality statements. See Computer-based Patient Record Institute. 1996. "Sample Confidentiality Statements and Agreements," CPR!, Schaumburg, Ill., May.